NERC CIP-003-09 – SECTION 6:

# Vendor Electronic Remote Access Security Controls



+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 CONTROLS

### 6.1. DOCUMENTATION SHOWING

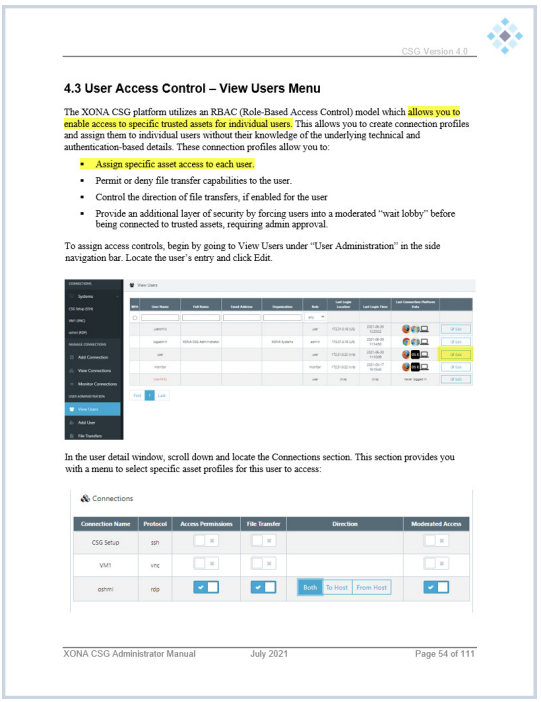
### 6.1.1. STEPS TO PREAUTHORIZE ACCESS.

---

**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.



CSG Version 4.0

### 4.3 User Access Control – View Users Menu

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 profiles 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.
- Permit or deny file transfer capabilities to 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.

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.

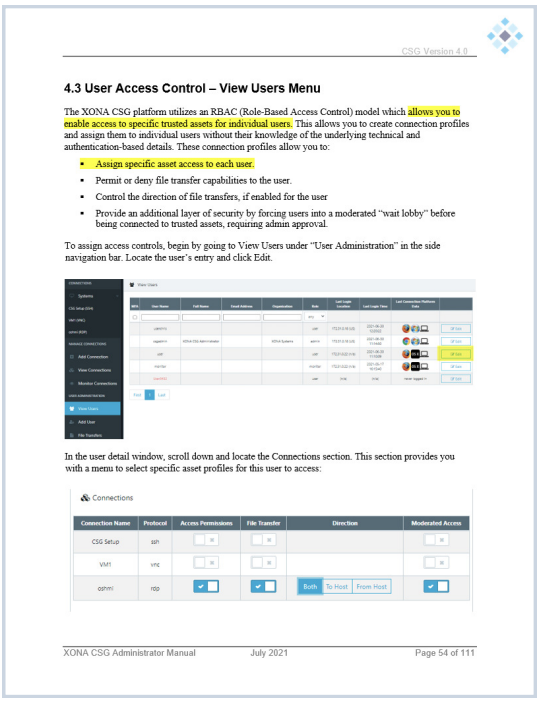


In the user detail window, scroll down and locate the Connections section. This section provides you with a menu to select specific asset profiles for this user to access:




XONA CSG Administrator Manual July 2021 Page 54 of 111

XONA CSG Administrator Manual v4.0 – Page 54



CSG Version 4.0

### 4.3 User Access Control – View Users Menu

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 profiles 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.
- Permit or deny file transfer capabilities to 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.

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.



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:

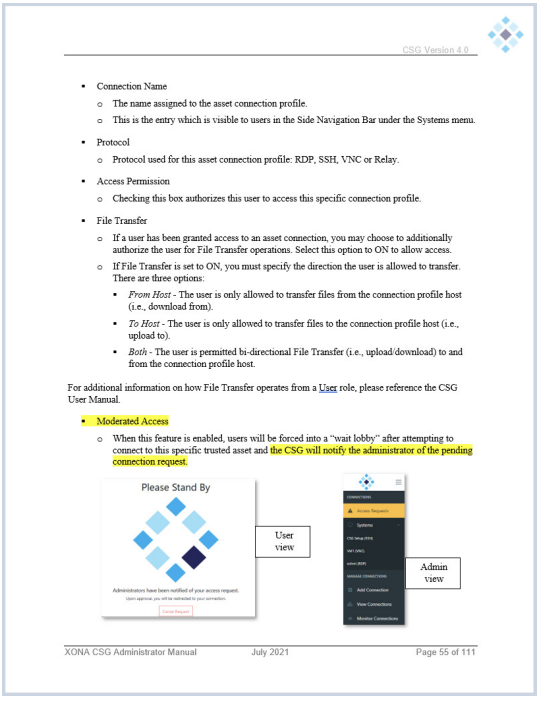



XONA CSG Administrator Manual July 2021 Page 54 of 111

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.



CSG Version 4.0

- Connection Name
  - The name assigned to the asset connection profile.
  - This is the entry which is visible to users in the Side Navigation Bar under the Systems menu.
- Protocol
  - Protocol used for this asset connection profile: RDP, SSH, VNC or Relay.
- Access Permission
  - Checking this box authorizes this user to access this specific connection profile.
- File Transfer
  - If a user has been granted access to an asset connection, you may choose to additionally authorize the user for File Transfer operations. Select this option to ON to allow access.
  - If File Transfer is set to ON, you must specify the direction the user is allowed to transfer. There are three options:
    - *From Host* - The user is only allowed to transfer files from the connection profile host (i.e., download from).
    - *To Host* - The user is only allowed to transfer files to the connection profile host (i.e., upload to).
    - *Both* - The user is permitted bi-directional File Transfer (i.e., upload/download) to and from the connection profile host.

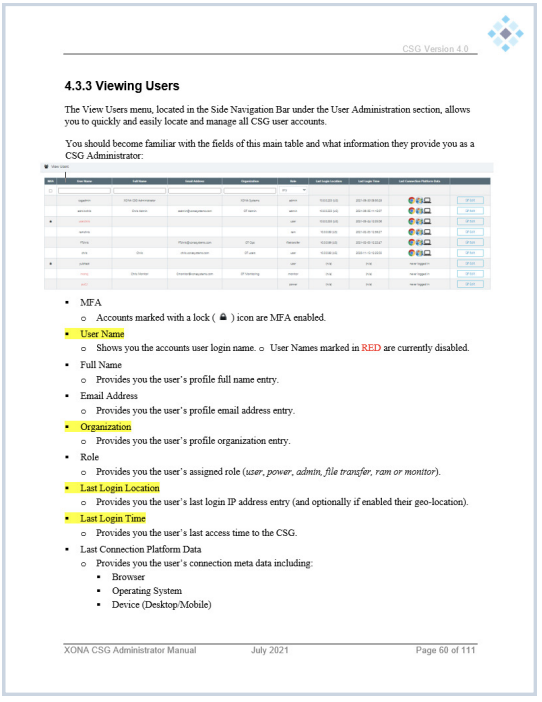
For additional information on how File Transfer operates from a User role, please reference the CSG User Manual.

- Moderated Access
  - When this feature is enabled, users will be forced into a "wait lobby" after attempting to connect to this specific trusted asset and the CSG will notify the administrator of the pending connection request.




XONA CSG Administrator Manual July 2021 Page 55 of 111

XONA CSG Administrator Manual v4.0 – Page 55



CSG Version 4.0

### 4.3.3 Viewing Users

The View Users menu, located in the Side Navigation Bar under the User Administration section, allows you to quickly and easily locate and manage all CSG user accounts.

You should become familiar with the fields of this main table and what information they provide you as a CSG Administrator:



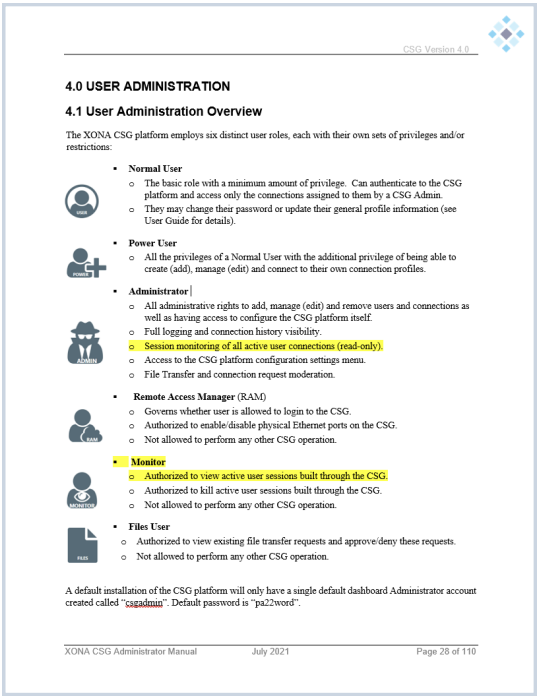
- MFA
  - Accounts marked with a lock ( 🔒 ) icon are MFA enabled.
- User Name
  - Shows you the accounts user login name. ○ User Names marked in RED are currently disabled.
- Full Name
  - Provides you the user's profile full name entry.
- Email Address
  - Provides you the user's profile email address entry.
- Organization
  - Provides you the user's profile organization entry.
- Role
  - Provides you the user's assigned role (*user, power, admin, file transfer, ram or monitor*).
- Last Login Location
  - Provides you the user's last login IP address entry (and optionally if enabled their geo-location).
- Last Login Time
  - Provides you the user's last access time to the CSG.
- Last Connection Platform Data
  - Provides you the user's connection meta data including:
    - Browser
    - Operating System
    - Device (Desktop/Mobile)

XONA CSG Administrator Manual July 2021 Page 60 of 111

XONA CSG Administrator Manual v4.0 – Page 60

## 6.1.3. SESSION MONITORING

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



CSG Version 4.0

**4.0 USER ADMINISTRATION**

**4.1 User Administration Overview**

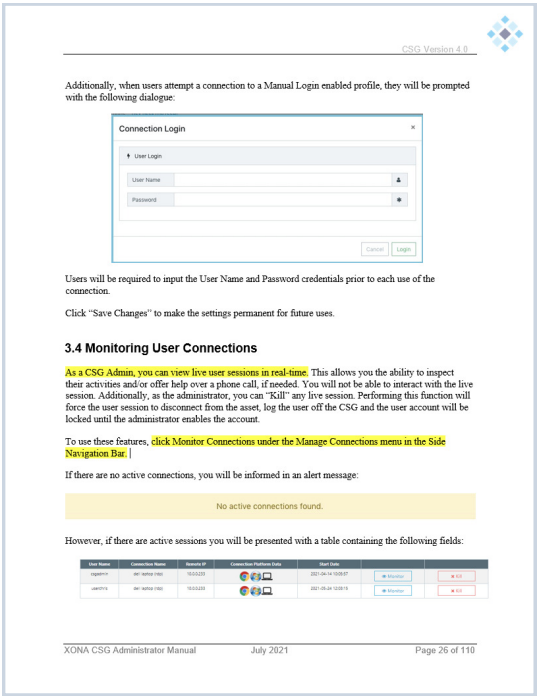
The XONA CSG platform employs six distinct user roles, each with their own sets of privileges and/or restrictions:

- **Normal User**
  - The basic role with a minimum amount of privilege. Can authenticate to the CSG platform and access only the connections assigned to them by a CSG Admin.
  - They may change their password or update their general profile information (see User Guide for details).
- **Power User**
  - All the privileges of a Normal User with the additional privilege of being able to create (add), manage (edit) and connect to their own connection profiles.
- **Administrator**
  - All administrative rights to add, manage (edit) and remove users and connections as well as having access to configure the CSG platform itself.
  - Full logging and connection history visibility.
  - Session monitoring of all active user connections (read-only).
  - Access to the CSG platform configuration settings menu.
  - File Transfer and connection request moderation.
- **Remote Access Manager** (RAM)
  - Governs whether user is allowed to login to the CSG.
  - Authorized to enable/disable physical Ethernet ports on the CSG.
  - Not allowed to perform any other CSG operation.
- **Monitor**
  - Authorized to view active user sessions built through the CSG.
  - Authorized to kill active user sessions built through the CSG.
  - Not allowed to perform any other CSG operation.
- **Files User**
  - Authorized to view existing file transfer requests and approve/deny these requests.
  - Not allowed to perform any other CSG operation.

A default installation of the CSG platform will only have a single default dashboard Administrator account created called "csgadmin". Default password is "pa22word".

XONA CSG Administrator Manual July 2021 Page 28 of 110

XONA CSG Administrator Manual v4.0 – Page 28



CSG Version 4.0

Additionally, when users attempt a connection to a Manual Login enabled profile, they will be prompted with the following dialogue:




Users will be required to input the User Name and Password credentials prior to each use of the connection.

Click "Save Changes" to make the settings permanent for future uses.

### 3.4 Monitoring User Connections

As a CSG Admin, you can view live user sessions in real-time. This allows you the ability to inspect their activities and/or offer help over a phone call, if needed. You will not be able to interact with the live session. Additionally, as the administrator, you can "Kill" any live session. Performing this function will force the user session to disconnect from the asset, log the user off the CSG and the user account will be locked until the administrator enables the account.

To use these features, click Monitor Connections under the Manage Connections menu in the Side Navigation Bar.

If there are no active connections, you will be informed in an alert message:

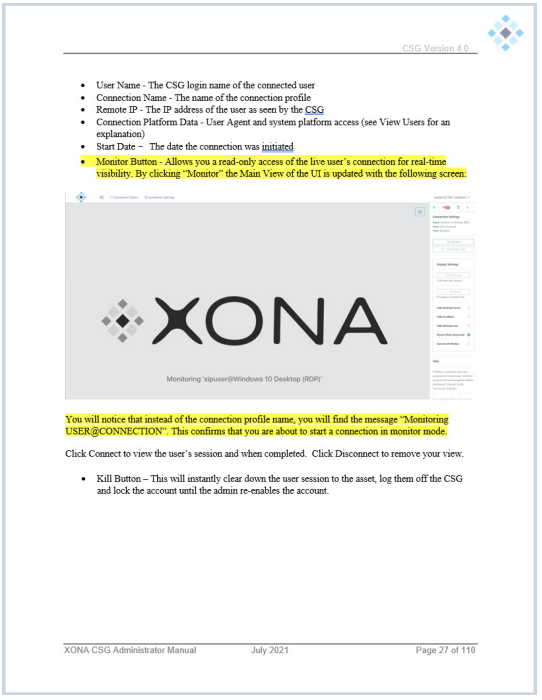
No active connections found.

However, if there are active sessions you will be presented with a table containing the following fields:



XONA CSG Administrator Manual July 2021 Page 26 of 110

XONA CSG Administrator Manual v4.0 – Page 26



CSG Version 4.0

- User Name - The CSG login name of the connected user
- Connection Name - The name of the connection profile
- Remote IP - The IP address of the user as seen by the CSG
- Connection Platform Data - User Agent and system platform access (see View Users for an explanation)
- Start Date – The date the connection was initiated
- Monitor Button - Allows you a read-only access of the live user's connection for real-time visibility. By clicking "Monitor" the Main View of the UI is updated with the following screen:




You will notice that instead of the connection profile name, you will find the message "Monitoring USER@CONNECTION". This confirms that you are about to start a connection in monitor mode.

Click Connect to view the user's session and when completed. Click Disconnect to remove your view.

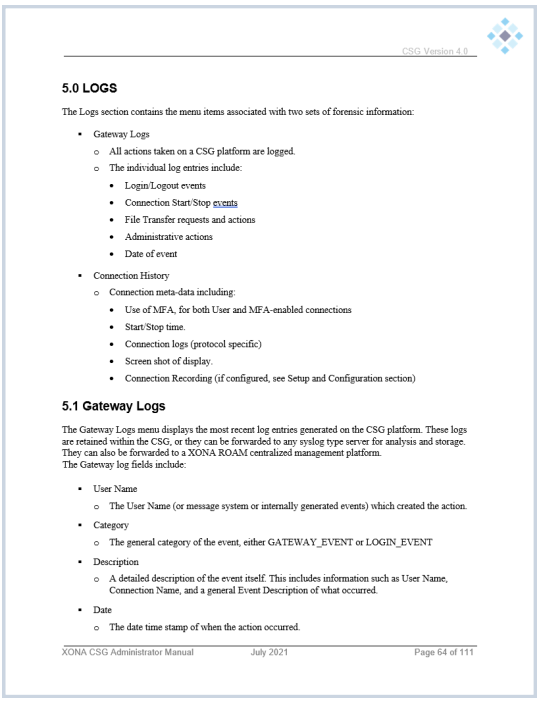
- Kill Button – This will instantly clear down the user session to the asset, log them off the CSG and lock the account until the admin re-enables the account.

XONA CSG Administrator Manual July 2021 Page 27 of 110

XONA CSG Administrator Manual v4.0 – Page 27

## 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.



CSG Version 4.0

**5.0 LOGS**

The Logs 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)

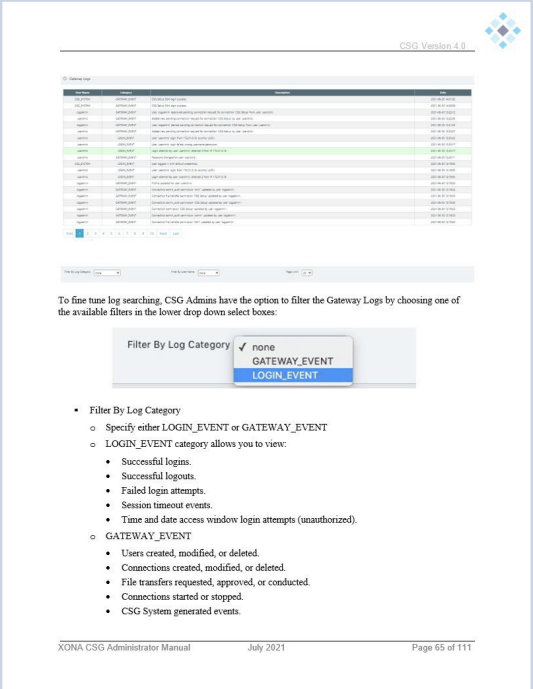
**5.1 Gateway Logs**

The Gateway Logs menu displays the most recent log entries generated on the CSG platform. These logs are retained within the CSG, or they can be forwarded to any syslog type server for analysis and storage. They can also be forwarded to a XONA ROAM centralized management platform.
The Gateway 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 July 2021 Page 64 of 111

XONA CSG Administrator Manual v4.0 – Page 64



CSG Version 4.0

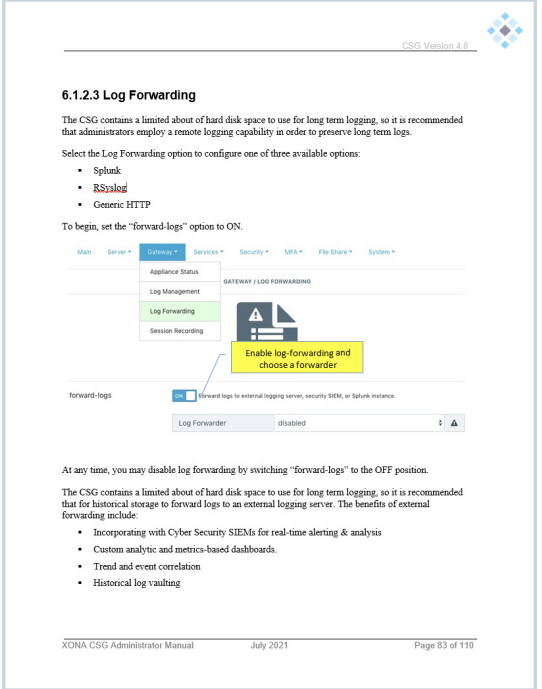
To fine tune log searching, CSG Admins have the option to filter the Gateway Logs by choosing one of the available filters in the lower drop down select boxes:




- Filter By Log Category
  - Specify either LOGIN_EVENT or GATEWAY_EVENT
  - LOGIN_EVENT category allows you to view:
    - Successful logins.
    - Successful logouts.
    - Failed login attempts.
    - Session timeout events.
    - Time and date access window login attempts (unauthorized).
  - GATEWAY_EVENT
    - Users created, modified, or deleted.
    - Connections created, modified, or deleted.
    - File transfers requested, approved, or conducted.
    - Connections started or stopped.
    - CSG System generated events.

XONA CSG Administrator Manual July 2021 Page 65 of 111

XONA CSG Administrator Manual v4.0 – Page 65



CSG Version 4.0

**6.1.2.3 Log Forwarding**

The CSG contains a limited about of hard disk space to use for long term logging, so it is recommended that administrators employ a remote logging capability in order to preserve long term logs.

Select the Log Forwarding option to configure one of three available options:

- Splunk
- RSyslog
- Generic HTTP

To begin, set the "forward-logs" option to ON.




At any time, you may disable log forwarding by switching "forward-logs" to the OFF position.

The CSG contains a limited about of hard disk space to use for long term logging, so it is recommended that for historical storage to forward logs to an external logging server. The benefits of external forwarding include:

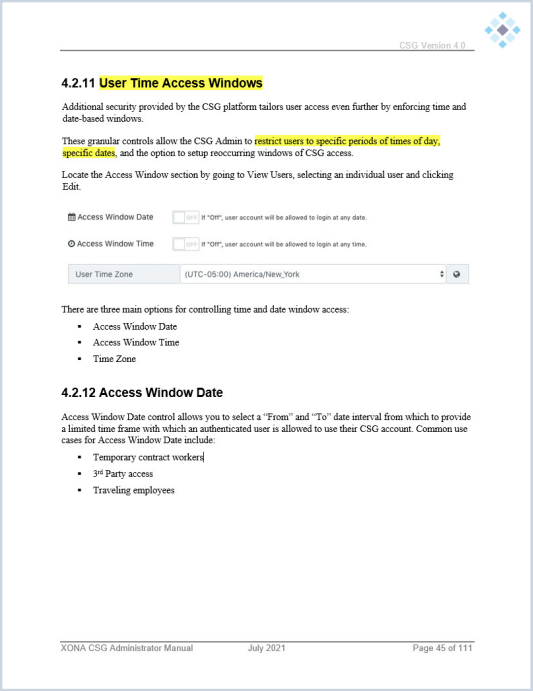
- Incorporating with Cyber Security SIEMs for real-time alerting & analysis
- Custom analytic and metrics-based dashboards.
- Trend and event correlation
- Historical log vaulting

XONA CSG Administrator Manual July 2021 Page 83 of 110

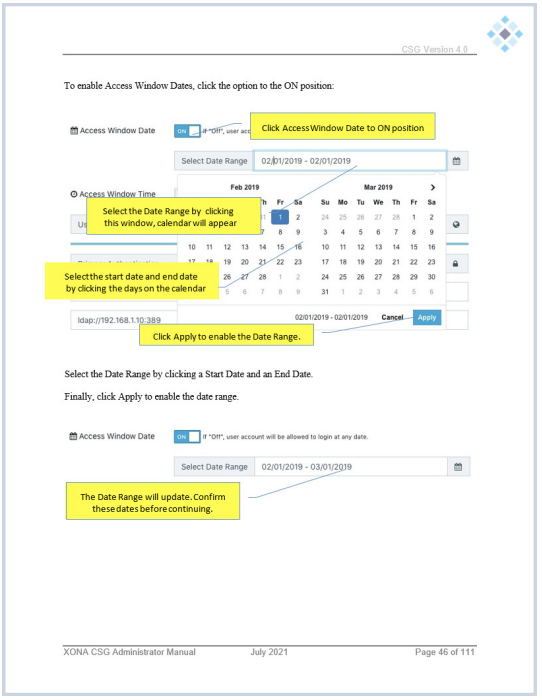
XONA CSG Administrator Manual v4.0 – Page 83

## 6.1.5. TIME OF NEED SESSION INITIATION

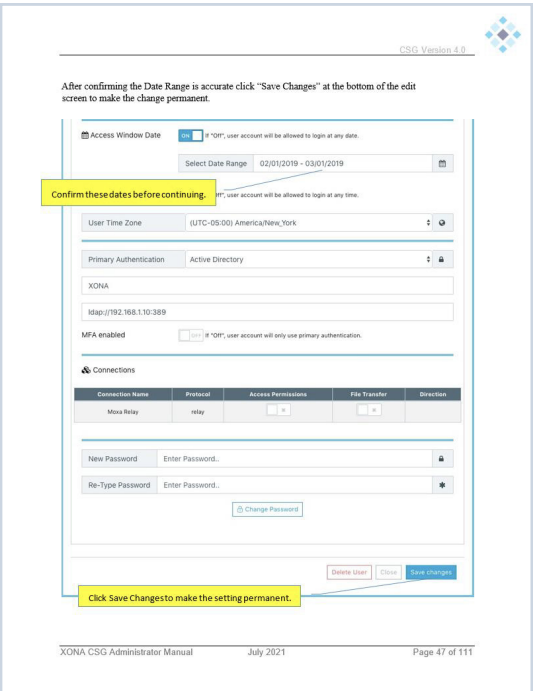
User access can be augmented with time and date controls – either specific times and dates, or ranges.



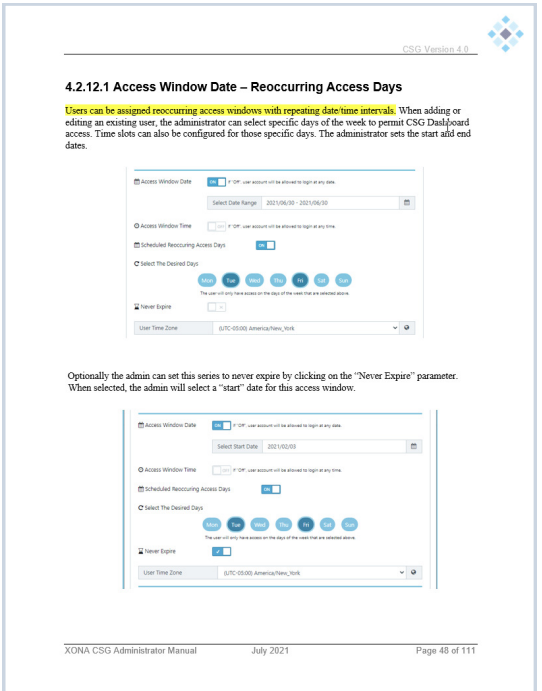

XONA CSG Administrator Manual v4.0 – Page 45



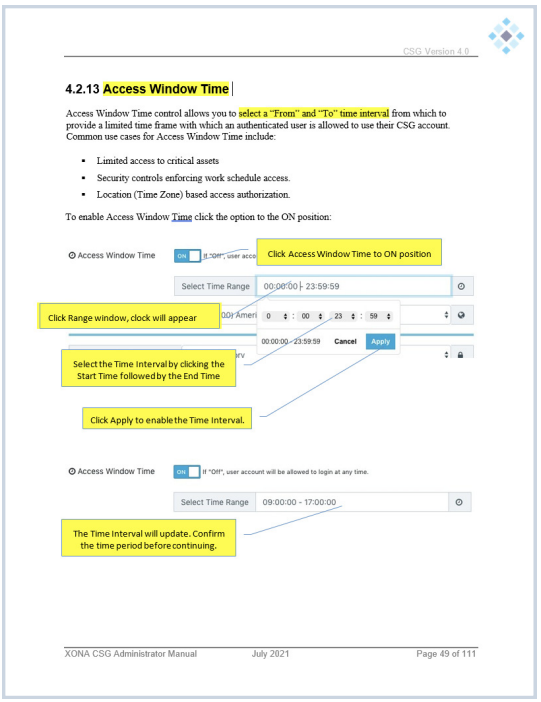

XONA CSG Administrator Manual v4.0 – Page 46



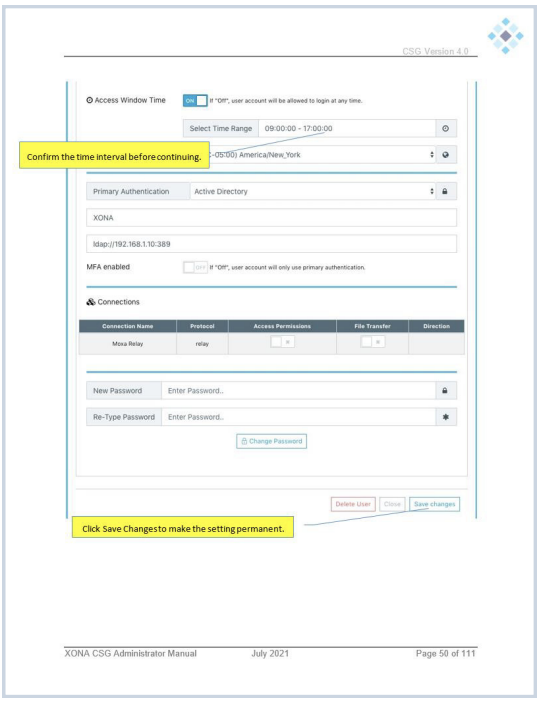

XONA CSG Administrator Manual v4.0 – Page 47




XONA CSG Administrator Manual v4.0 – Page 48



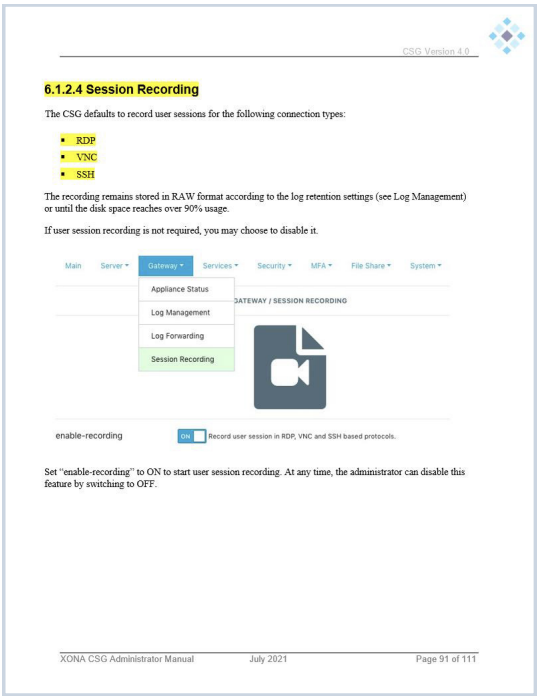

XONA CSG Administrator Manual v4.0 – Page 49




XONA CSG Administrator Manual v4.0 – Page 50

## 6.1.6. SESSION RECORDING

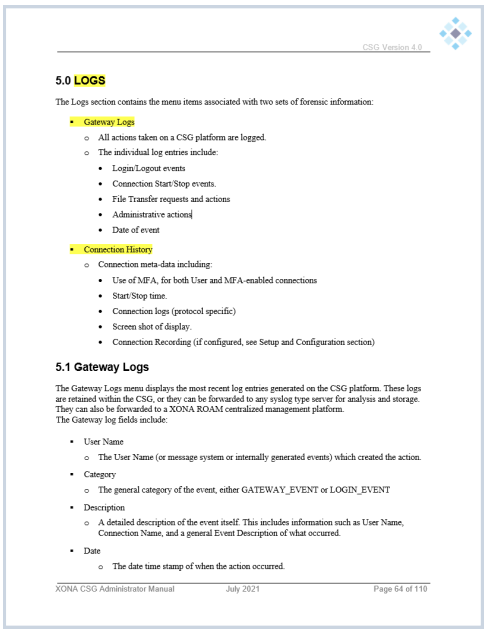
Sessions connecting to OT/ICS asset can be recorded if they use either the RDP, SSH, or VNC protocols.




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.



CSG Version 4.0

**5.0 LOGS**

The Logs 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)

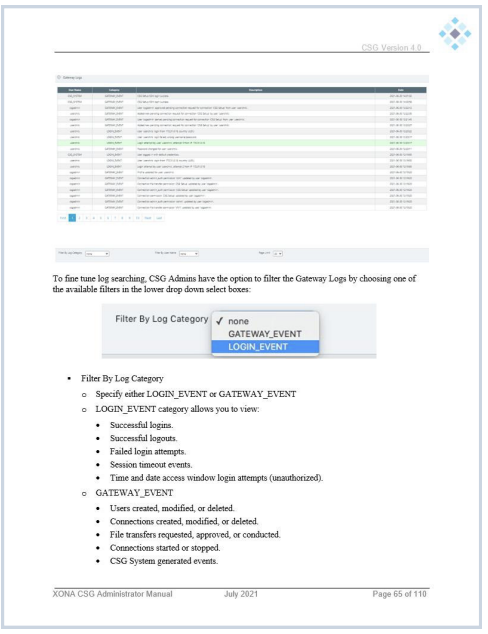
**5.1 Gateway Logs**

The Gateway Logs menu displays the most recent log entries generated on the CSG platform. These logs are retained within the CSG, or they can be forwarded to any syslog type server for analysis and storage. They can also be forwarded to a XONA ROAM centralized management platform.
The Gateway 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 July 2021 Page 64 of 110

XONA CSG Administrator Manual v4.0 – Page 64



CSG Version 4.0

To fine tune log searching, CSG Admins have the option to filter the Gateway Logs by choosing one of the available filters in the lower drop down select boxes:

Filter By Log Category ✓ none GATEWAY_EVENT LOGIN_EVENT

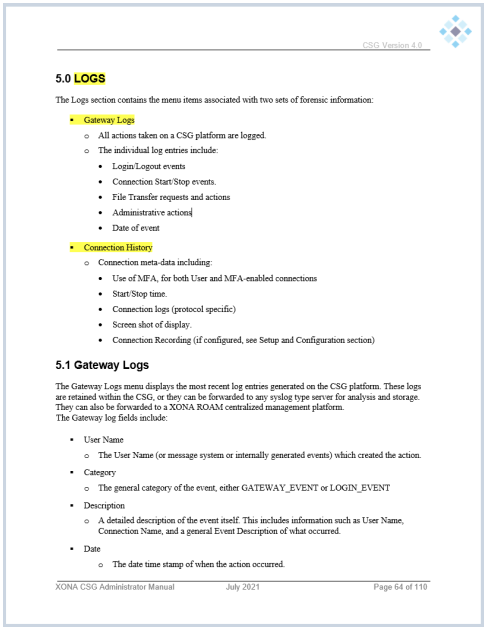
- Filter By Log Category
  - Specify either LOGIN_EVENT or GATEWAY_EVENT
  - LOGIN_EVENT category allows you to view:
    - Successful logins.
    - Successful logouts.
    - Failed login attempts.
    - Session timeout events.
    - Time and date access window login attempts (unauthorized).
  - GATEWAY_EVENT
    - Users created, modified, or deleted.
    - Connections created, modified, or deleted.
    - File transfers requested, approved, or conducted.
    - Connections started or stopped.
    - CSG System generated events.

XONA CSG Administrator Manual July 2021 Page 65 of 110

XONA CSG Administrator Manual v4.0 – Page 65

## 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 LOGS**

The Logs 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)

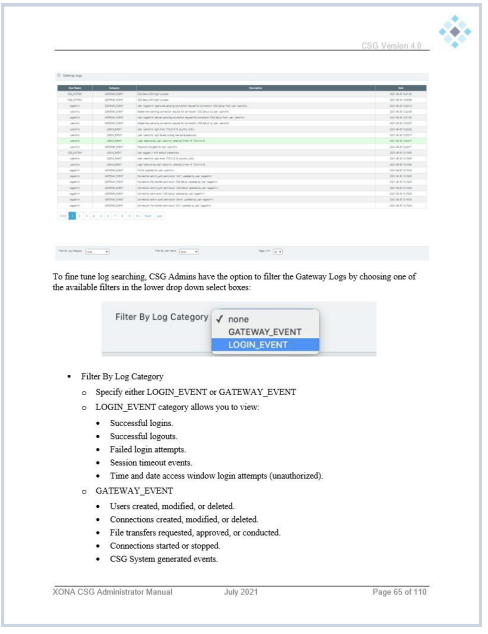
**5.1 Gateway Logs**

The Gateway Logs menu displays the most recent log entries generated on the CSG platform. These logs are retained within the CSG, or they can be forwarded to any syslog type server for analysis and storage. They can also be forwarded to a XONA ROAM centralized management platform.
The Gateway 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 July 2021 Page 64 of 110

XONA CSG Administrator Manual v4.0 – Page 64



CSG Version 4.0

To fine tune log searching, CSG Admins have the option to filter the Gateway Logs by choosing one of the available filters in the lower drop down select boxes:

Filter By Log Category ✓ none GATEWAY_EVENT LOGIN_EVENT

- Filter By Log Category
  - Specify either LOGIN_EVENT or GATEWAY_EVENT
  - LOGIN_EVENT category allows you to view:
    - Successful logins.
    - Successful logouts.
    - Failed login attempts.
    - Session timeout events.
    - Time and date access window login attempts (unauthorized).
  - GATEWAY_EVENT
    - Users created, modified, or deleted.
    - Connections created, modified, or deleted.
    - File transfers requested, approved, or conducted.
    - Connections started or stopped.
    - CSG System generated events.

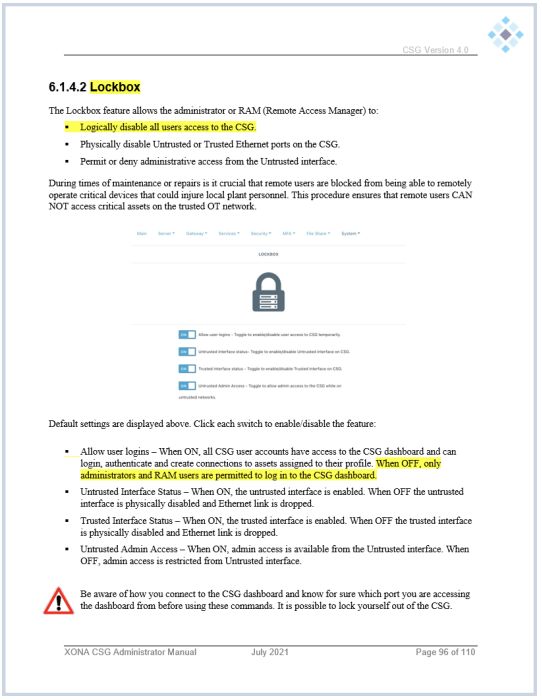
XONA CSG Administrator Manual July 2021 Page 65 of 110

XONA CSG Administrator Manual v4.0 – Page 65

## 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.



CSG Version 4.0

**6.1.4.2 Lockbox**

The Lockbox feature allows the administrator or RAM (Remote Access Manager) to:

- Logically disable all users access to the CSG.
- Physically disable Untrusted or Trusted Ethernet ports on the CSG.
- Permit or deny administrative access from the Untrusted interface.

During times of maintenance or repairs is it crucial that remote users are blocked from being able to remotely operate critical devices that could injure local plant personnel. This procedure ensures that remote users CAN NOT access critical assets on the trusted OT network.

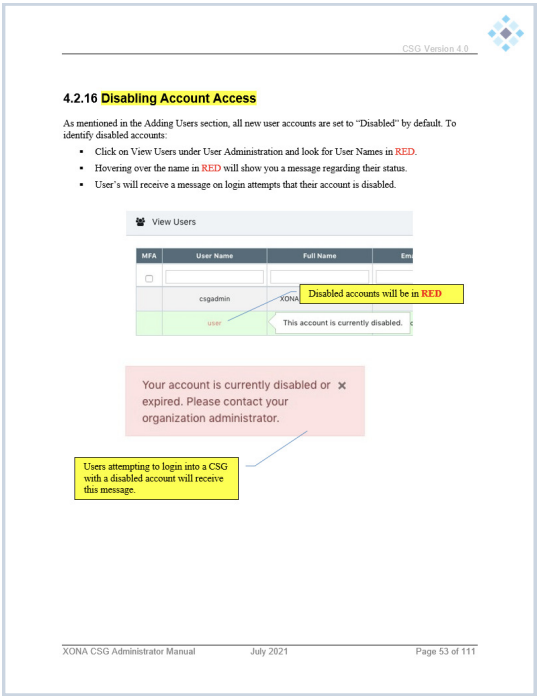
Default settings are displayed above. Click each switch to enable/disable the feature:

- Allow user logins – When ON, all CSG user accounts have access to the CSG dashboard and can login, authenticate and create connections to assets assigned to their profile. When OFF, only administrators and RAM users are permitted to log in to the CSG dashboard.
- Untrusted Interface Status – When ON, the untrusted interface is enabled. When OFF the untrusted interface is physically disabled and Ethernet link is dropped.
- Trusted Interface Status – When ON, the trusted interface is enabled. When OFF the trusted interface is physically disabled and Ethernet link is dropped.
- Untrusted Admin Access – When ON, admin access is available from the Untrusted interface. When OFF, admin access is restricted from Untrusted interface.

Be aware of how you connect to the CSG dashboard and know for sure which port you are accessing the dashboard from before using these commands. It is possible to lock yourself out of the CSG.

XONA CSG Administrator Manual July 2021 Page 96 of 110

XONA CSG Administrator Manual v4.0 – Page 2



CSG Version 4.0

**4.2.16 Disabling Account Access**

As mentioned in the Adding Users section, all new user accounts are set to "Disabled" by default. To identify disabled accounts:

- Click on View Users under User Administration and look for User Names in RED.
- Hovering over the name in RED will show you a message regarding their status.
- User's will receive a message on login attempts that their account is disabled.

View Users

MFA | User Name | Full Name | Em

csgadmin XONA

user

Disabled accounts will be in RED

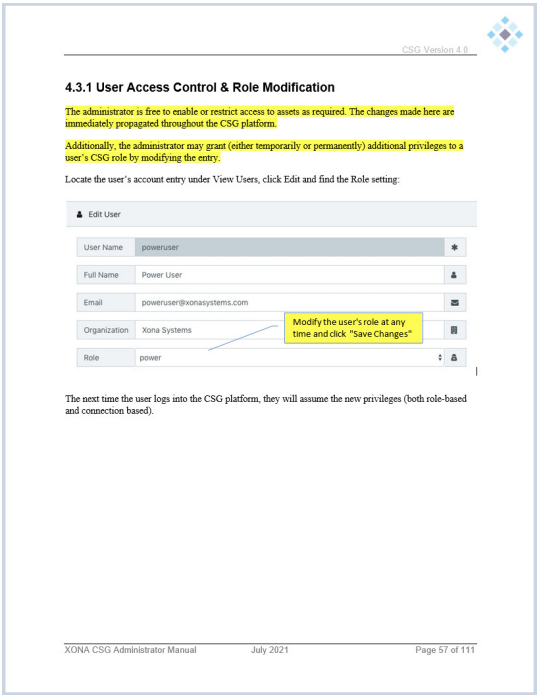
This account is currently disabled.

Your account is currently disabled or expired. Please contact your organization administrator.

Users attempting to login into a CSG with a disabled account will receive this message.

XONA CSG Administrator Manual July 2021 Page 53 of 111

XONA CSG Administrator Manual v4.0 – Page 2



CSG Version 4.0

**4.3.1 User Access Control & Role Modification**

The administrator is free to enable or restrict access to assets as required. The changes made here are immediately propagated throughout the CSG platform.

Additionally, the administrator may grant (either temporarily or permanently) additional privileges to a user's CSG role by modifying the entry.

Locate the user's account entry under View Users, click Edit and find the Role setting:

Edit User

User Name poweruser

Full Name Power User

Email poweruser@xonasystems.com

Organization Xona Systems

Role power

Modify the user's role at any time and click "Save Changes"

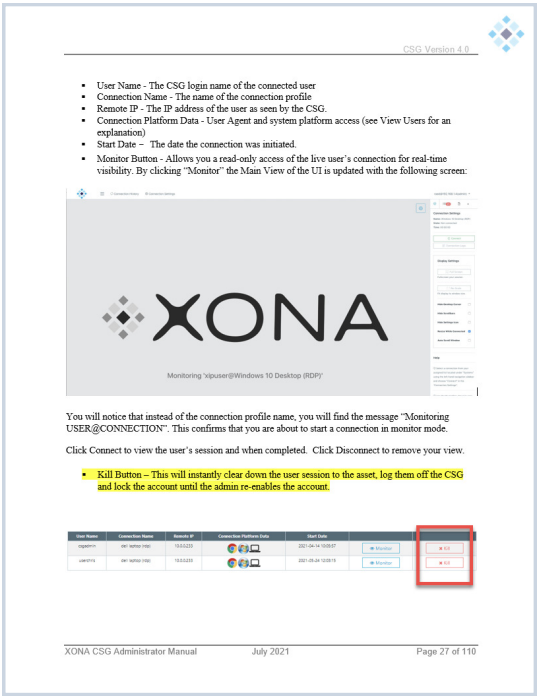
The next time the user logs into the CSG platform, they will assume the new privileges (both role-based and connection based).

XONA CSG Administrator Manual July 2021 Page 57 of 111

XONA CSG Administrator Manual v4.0 – Page 57

## 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 stand-alone appliance. User sessions can be immediately terminated using the 'Kill Button'. Inbound/outbound ports can be disabled using the 'Lockbox' function or admins.



CSG Version 4.0

- User Name - The CSG login name of the connected user
- Connection Name - The name of the connection profile
- Remote IP - The IP address of the user as seen by the CSG.
- Connection Platform Data - User Agent and system platform access (see View Users for an explanation)
- Start Date – The date the connection was initiated.
- Monitor Button - Allows you a read-only access of the live user's connection for real-time visibility. By clicking "Monitor" the Main View of the UI is updated with the following screen:




You will notice that instead of the connection profile name, you will find the message "Monitoring USER@CONNECTION". This confirms that you are about to start a connection in monitor mode.

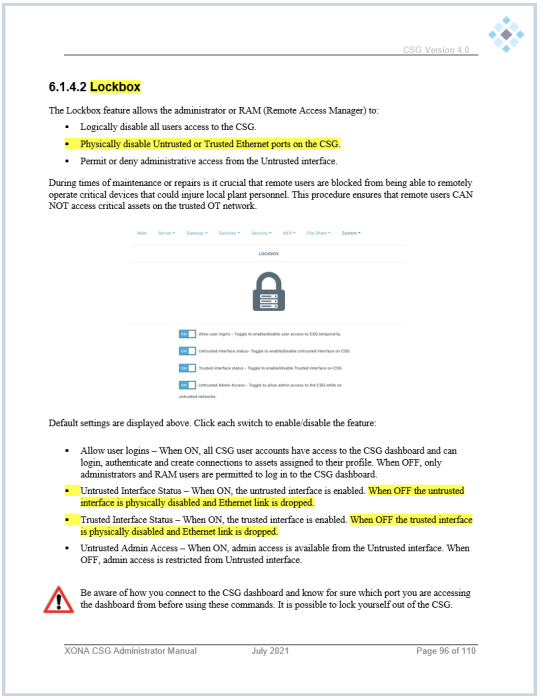
Click Connect to view the user's session and when completed. Click Disconnect to remove your view.

- Kill Button – This will instantly clear down the user session to the asset, log them off the CSG and lock the account until the admin re-enables the account.



XONA CSG Administrator Manual July 2021 Page 27 of 110

XONA CSG Administrator Manual v4.0 – Page 27



CSG Version 4.0

### 6.1.4.2 Lockbox

The Lockbox feature allows the administrator or RAM (Remote Access Manager) to:

- Logically disable all users access to the CSG.
- Physically disable Untrusted or Trusted Ethernet ports on the CSG.
- Permit or deny administrative access from the Untrusted interface.

During times of maintenance or repairs is it crucial that remote users are blocked from being able to remotely operate critical devices that could injure local plant personnel. This procedure ensures that remote users CAN NOT access critical assets on the trusted OT network.



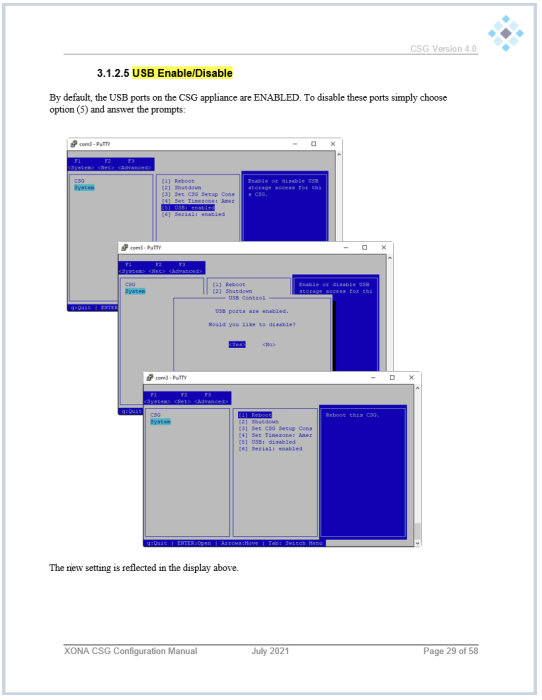
Default settings are displayed above. Click each switch to enable/disable the feature:

- Allow user logins – When ON, all CSG user accounts have access to the CSG dashboard and can login, authenticate and create connections to assets assigned to their profile. When OFF, only administrators and RAM users are permitted to log in to the CSG dashboard.
- Untrusted Interface Status – When ON, the untrusted interface is enabled. When OFF the untrusted interface is physically disabled and Ethernet link is dropped.
- Trusted Interface Status – When ON, the trusted interface is enabled. When OFF the trusted interface is physically disabled and Ethernet link is dropped.
- Untrusted Admin Access – When ON, admin access is available from the Untrusted interface. When OFF, admin access is restricted from Untrusted interface.

Be aware of how you connect to the CSG dashboard and know for sure which port you are accessing the dashboard from before using these commands. It is possible to lock yourself out of the CSG.

XONA CSG Administrator Manual July 2021 Page 96 of 110

XONA CSG Administrator Manual v4.0 – Page 96



CSG Version 4.0

### 3.1.2.5 USB Enable/Disable

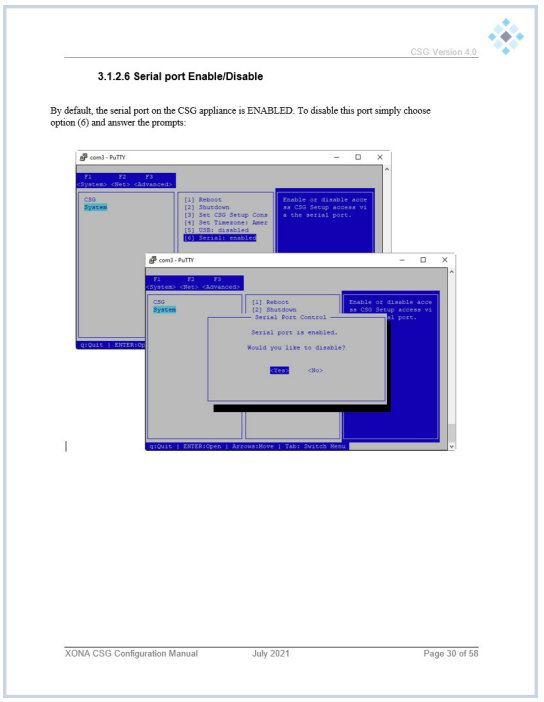
By default, the USB ports on the CSG appliance are ENABLED. To disable these ports simply choose option (5) and answer the prompts:



The new setting is reflected in the display above.

XONA CSG Configuration Manual July 2021 Page 29 of 58

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



CSG Version 4.0

**3.1.2.6 Serial port Enable/Disable**

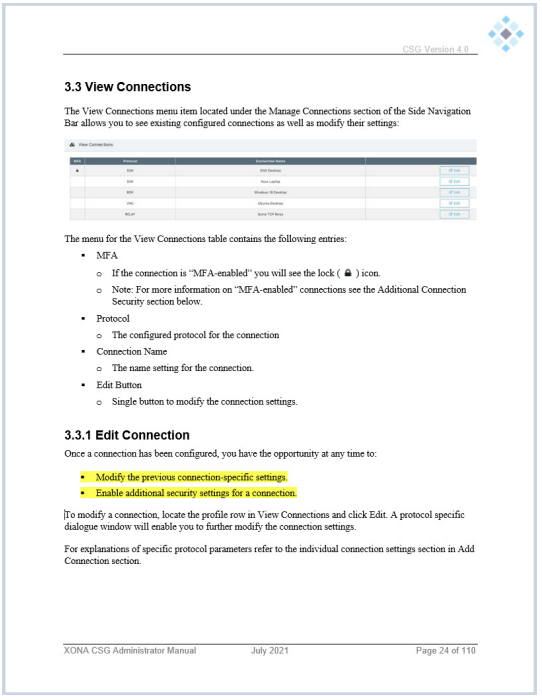
By default, the serial port on the CSG appliance is ENABLED. To disable this port simply choose option (6) and answer the prompts:

XONA CSG Configuration Manual July 2021 Page 30 of 58

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.



CSG Version 4.0

**3.3 View Connections**

The View Connections menu item located under the Manage Connections section of the Side Navigation Bar allows you to see existing configured connections as well as modify their settings:

The menu for the View Connections table contains the following entries:

- MFA
  - If the connection is "MFA-enabled" you will see the lock ( 🔒 ) icon.
  - Note: For more information on "MFA-enabled" connections see the Additional Connection Security section below.
- Protocol
  - The configured protocol for the connection
- Connection Name
  - The name setting for the connection.
- Edit Button
  - Single button to modify the connection settings.

**3.3.1 Edit Connection**

Once a connection has been configured, you have the opportunity at any time to:

- Modify the previous connection-specific settings.
- Enable additional security settings for a connection.

To modify a connection, locate the profile row in View Connections and click Edit. A protocol specific dialogue window will enable you to further modify the connection settings.

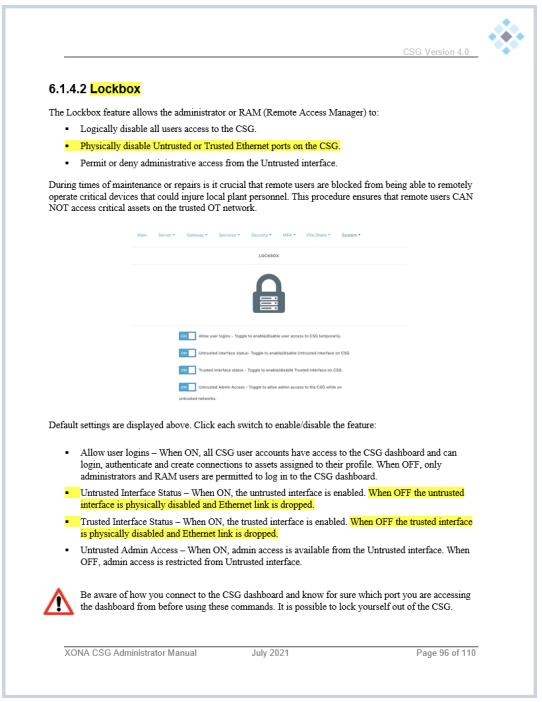
For explanations of specific protocol parameters refer to the individual connection settings section in Add Connection section.

XONA CSG Administrator Manual July 2021 Page 24 of 110

XONA CSG Administrator Manual v4.0 – Page 24

## 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.



CSG Version 4.0

**6.1.4.2 Lockbox**

The Lockbox feature allows the administrator or RAM (Remote Access Manager) to:

- Logically disable all users access to the CSG.
- Physically disable Untrusted or Trusted Ethernet ports on the CSG.
- Permit or deny administrative access from the Untrusted interface.

During times of maintenance or repairs is it crucial that remote users are blocked from being able to remotely operate critical devices that could injure local plant personnel. This procedure ensures that remote users CAN NOT access critical assets on the trusted OT network.

Default settings are displayed above. Click each switch to enable/disable the feature:

- Allow user logins – When ON, all CSG user accounts have access to the CSG dashboard and can login, authenticate and create connections to assets assigned to their profile. When OFF, only administrators and RAM users are permitted to log in to the CSG dashboard.
- Untrusted Interface Status – When ON, the untrusted interface is enabled. When OFF the untrusted interface is physically disabled and Ethernet link is dropped.
- Trusted Interface Status – When ON, the trusted interface is enabled. When OFF the trusted interface is physically disabled and Ethernet link is dropped.
- Untrusted Admin Access – When ON, admin access is available from the Untrusted interface. When OFF, admin access is restricted from Untrusted interface.

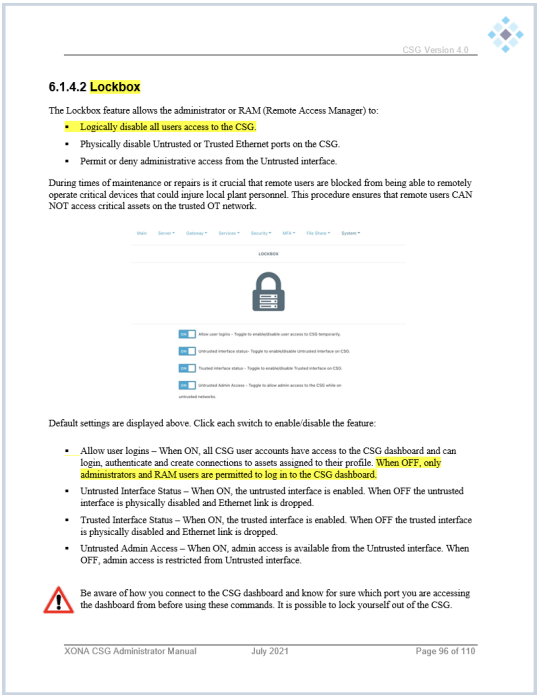
Be aware of how you connect to the CSG dashboard and know for sure which port you are accessing the dashboard from before using these commands. It is possible to lock yourself out of the CSG.

XONA CSG Administrator Manual July 2021 Page 96 of 110

XONA CSG Administrator Manual v4.0 – Page 96

## 6.2.5. ADMINISTRATIVE CONTROL DOCUMENTATION LISTING THE METHODS, STEPS, OR SYSTEMS USED TO DISABLE VENDOR ELECTRONIC 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.



CSG Version 4.0

**6.1.4.2 Lockbox**

The Lockbox feature allows the administrator or RAM (Remote Access Manager) to:

- Logically disable all users access to the CSG.
- Physically disable Untrusted or Trusted Ethernet ports on the CSG.
- Permit or deny administrative access from the Untrusted interface.

During times of maintenance or repairs is it crucial that remote users are blocked from being able to remotely operate critical devices that could injure local plant personnel. This procedure ensures that remote users CAN NOT access critical assets on the trusted OT network.

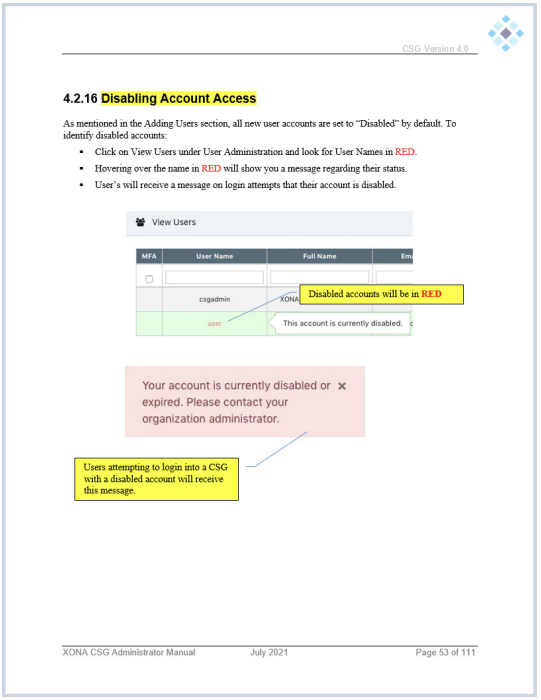
Default settings are displayed above. Click each switch to enable/disable the feature:

- Allow user logins – When ON, all CSG user accounts have access to the CSG dashboard and can login, authenticate and create connections to assets assigned to their profile. When OFF, only administrators and RAM users are permitted to log in to the CSG dashboard.
- Untrusted Interface Status – When ON, the untrusted interface is enabled. When OFF the untrusted interface is physically disabled and Ethernet link is dropped.
- Trusted Interface Status – When ON, the trusted interface is enabled. When OFF the trusted interface is physically disabled and Ethernet link is dropped.
- Untrusted Admin Access – When ON, admin access is available from the Untrusted interface. When OFF, admin access is restricted from Untrusted interface.

Be aware of how you connect to the CSG dashboard and know for sure which port you are accessing the dashboard from before using these commands. It is possible to lock yourself out of the CSG.

XONA CSG Administrator Manual July 2021 Page 96 of 110

XONA CSG Administrator Manual v4.0 – Page 2



CSG Version 4.0

### 4.2.16 Disabling Account Access

As mentioned in the Adding Users section, all new user accounts are set to "Disabled" by default. To identify disabled accounts:

- Click on View Users under User Administration and look for User Names in RED.
- Hovering over the name in RED will show you a message regarding their status.
- User's will receive a message on login attempts that their account is disabled.

View Users

MFA | User Name | Full Name

csgadmin | XONA

user

Disabled accounts will be in RED

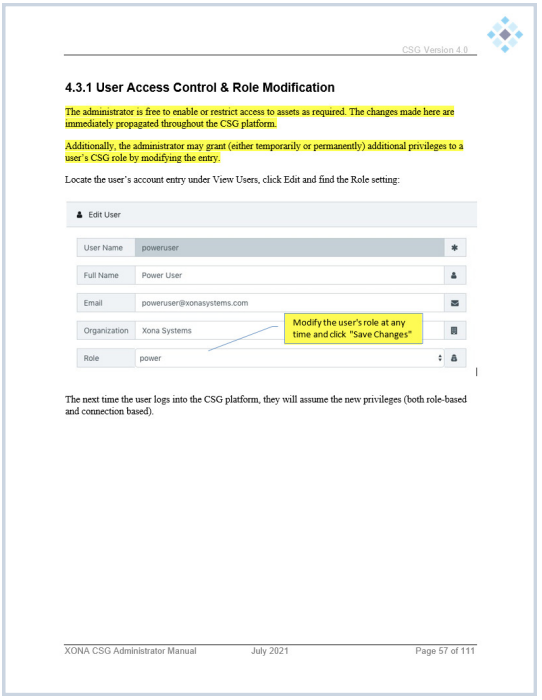
This account is currently disabled.

Your account is currently disabled or expired. Please contact your organization administrator.

Users attempting to login into a CSG with a disabled account will receive this message.

XONA CSG Administrator Manual July 2021 Page 53 of 111

XONA CSG Administrator Manual v4.0 – Page 2



CSG Version 4.0

### 4.3.1 User Access Control & Role Modification

The administrator is free to enable or restrict access to assets as required. The changes made here are immediately propagated throughout the CSG platform.

Additionally, the administrator may grant (either temporarily or permanently) additional privileges to a user's CSG role by modifying the entry.

Locate the user's account entry under View Users, click Edit and find the Role setting:

Edit User

User Name: poweruser

Full Name: Power User

Email: poweruser@xonasystems.com

Organization: Xona Systems

Role: power

Modify the user's role at any time and click "Save Changes"

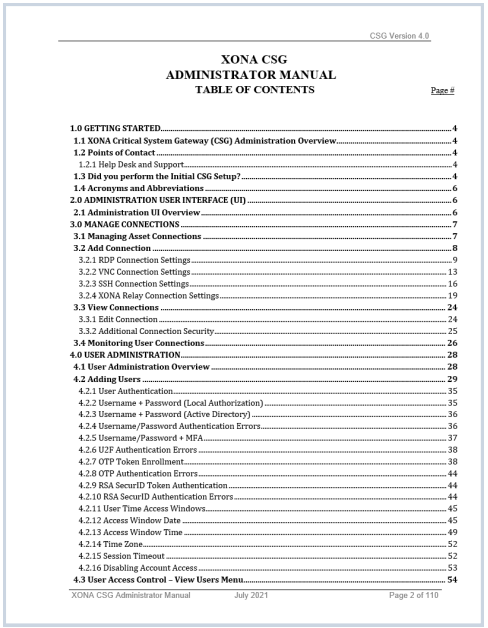
The next time the user logs into the CSG platform, they will assume the new privileges (both role-based and connection based).

XONA CSG Administrator Manual July 2021 Page 57 of 111

XONA CSG Administrator Manual v4.0 – Page 57

## 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.



CSG Version 4.0

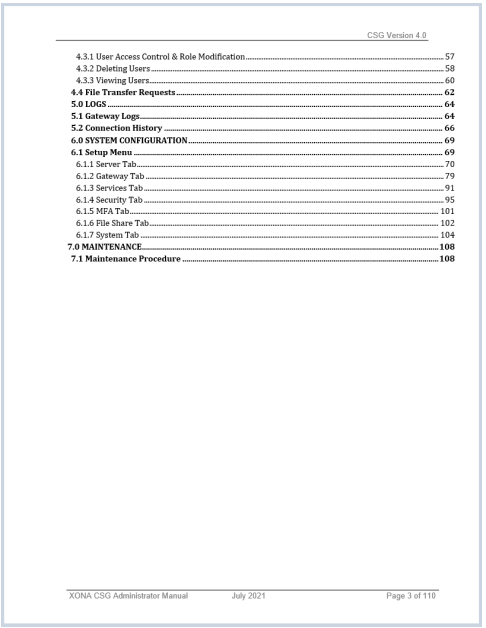
**XONA CSG**
**ADMINISTRATOR MANUAL**
**TABLE OF CONTENTS**

Page #

**1.0 GETTING STARTED** ... 4
**1.1 XONA Critical System Gateway (CSG) Administration Overview** ... 4
**1.2 Points of Contact** ... 4
1.2.1 Help Desk and Support ... 4
**1.3 Did you perform the Initial CSG Setup?** ... 4
**1.4 Acronyms and Abbreviations** ... 6
**2.0 ADMINISTRATION USER INTERFACE (UI)** ... 6
**2.1 Administration UI Overview** ... 6
**3.0 MANAGE CONNECTIONS** ... 7
**3.1 Managing Asset Connections** ... 7
**3.2 Add Connection** ... 8
3.2.1 RDP Connection Settings ... 9
3.2.2 VNC Connection Settings ... 13
3.2.3 SSH Connection Settings ... 16
3.2.4 XONA Relay Connection Settings ... 19
**3.3 View Connections** ... 24
3.3.1 Edit Connection ... 24
3.3.2 Additional Connection Security ... 25
**3.4 Monitoring User Connections** ... 26
**4.0 USER ADMINISTRATION** ... 28
**4.1 User Administration Overview** ... 28
**4.2 Adding Users** ... 29
4.2.1 User Authentication ... 35
4.2.2 Username + Password (Local Authorization) ... 35
4.2.3 Username + Password (Active Directory) ... 36
4.2.4 Username/Password Authentication Errors ... 36
4.2.5 Username/Password + MFA ... 37
4.2.6 U2F Authentication Errors ... 38
4.2.7 OTP Token Enrollment ... 38
4.2.8 OTP Authentication Errors ... 44
4.2.9 RSA SecurID Token Authentication ... 44
4.2.10 RSA SecurID Authentication Errors ... 44
4.2.11 User Time Access Windows ... 45
4.2.12 Access Window Date ... 45
4.2.13 Access Window Time ... 49
4.2.14 Time Zone ... 52
4.2.15 Session Timeout ... 52
4.2.16 Disabling Account Access ... 53
**4.3 User Access Control – View Users Menu** ... 54

XONA CSG Administrator Manual July 2021 Page 2 of 110

XONA CSG Administrator Manual v4.0 – Page 2



CSG Version 4.0

4.3.1 User Access Control & Role Modification ... 57
4.3.2 Deleting Users ... 58
4.3.3 Viewing Users ... 60
**4.4 File Transfer Requests** ... 62
**5.0 LOGS** ... 64
**5.1 Gateway Logs** ... 64
**5.2 Connection History** ... 66
**6.0 SYSTEM CONFIGURATION** ... 69
**6.1 Setup Menu** ... 69
6.1.1 Server Tab ... 70
6.1.2 Gateway Tab ... 79
6.1.3 Services Tab ... 91
6.1.4 Security Tab ... 95
6.1.5 MFA Tab ... 101
6.1.6 File Share Tab ... 102
6.1.7 System Tab ... 104
**7.0 MAINTENANCE** ... 108
**7.1 Maintenance Procedure** ... 108

XONA CSG Administrator Manual July 2021 Page 3 of 110

XONA CSG Administrator Manual v4.0 – Page 3

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

### 6.3.1. ANTI MALWARE TECHNOLOGIES

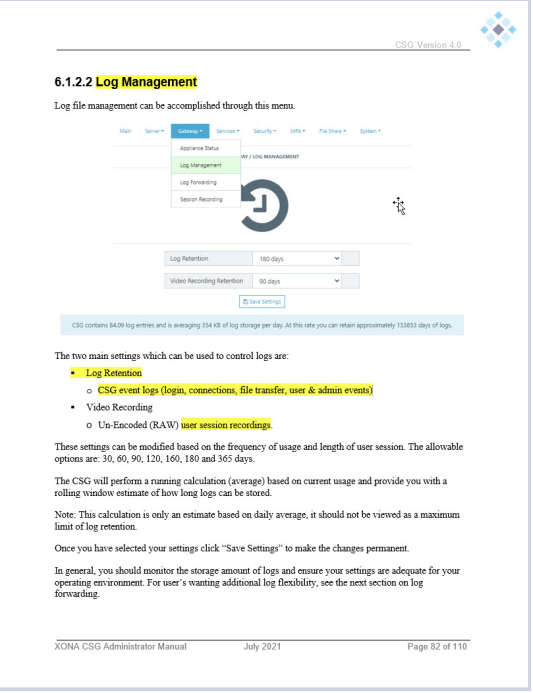
As a purpose-built appliance that protects the data stream between the user and the appliance and translates the OT protocols used between the appliance and the OT/ICS asset, there is no opportunity for malicious software to inject itself into the transaction between the user/OT operator and the OT environment. 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.



CSG Version 4.0

**6.1.2.2 Log Management**

Log file management can be accomplished through this menu.

Appliance Status
Log Management
Log Forwarding
Session Recording

Log Retention 180 days
Video Recording Retention 90 days
Save Settings

CSG contains 84.09 log entries and is averaging 354 KB of log storage per day. At this rate you can retain approximately 153853 days of logs.

The two main settings which can be used to control logs are:

- Log Retention
  - CSG event logs (login, connections, file transfer, user & admin events)
- Video Recording
  - Un-Encoded (RAW) user session recordings.

These settings can be modified based on the frequency of usage and length of user session. The allowable options are: 30, 60, 90, 120, 160, 180 and 365 days.

The CSG will perform a running calculation (average) based on current usage and provide you with a rolling window estimate of how long logs can be stored.

Note: This calculation is only an estimate based on daily average, it should not be viewed as a maximum limit of log retention.

Once you have selected your settings click "Save Settings" to make the changes permanent.

In general, you should monitor the storage amount of logs and ensure your settings are adequate for your operating environment. For user's wanting additional log flexibility, see the next section on log forwarding.

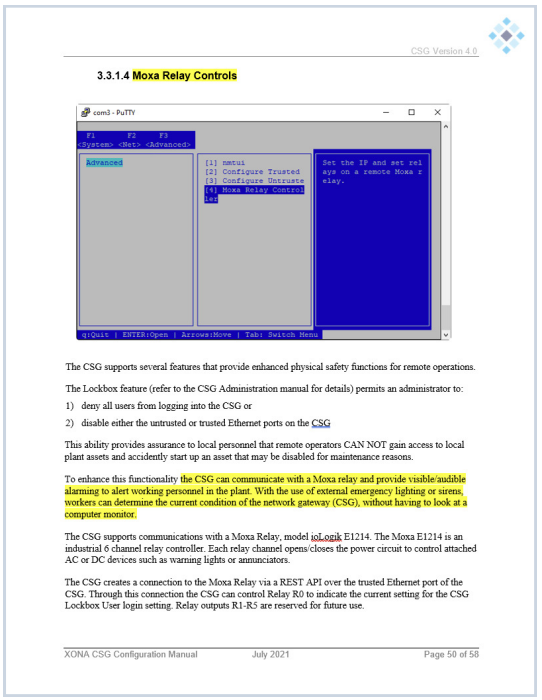
XONA CSG Administrator Manual July 2021 Page 82 of 110

XONA CSG Administrator Manual v4.0 – Page 24

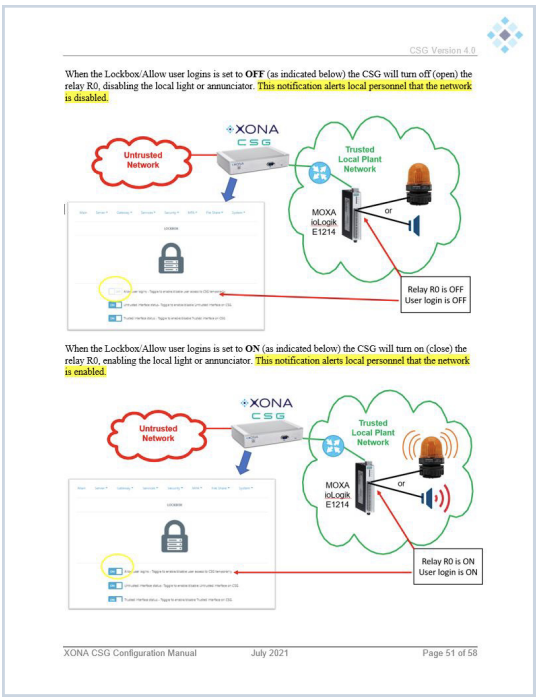
## 6.3.4. ALERTING

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.



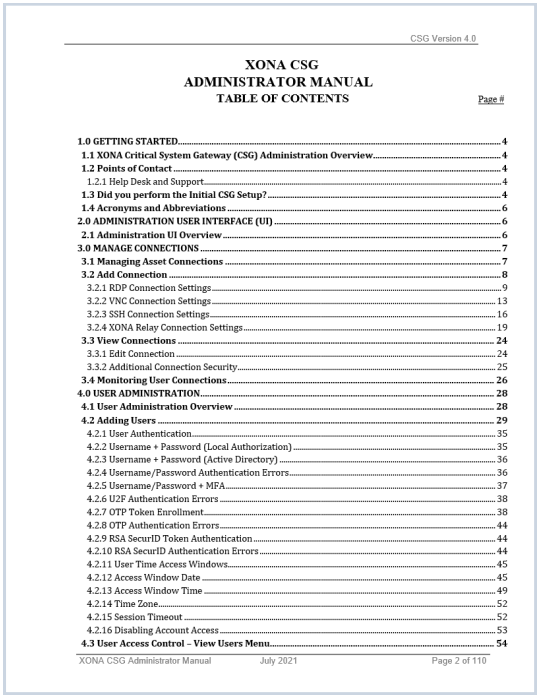

XONA CSG Configuration Manual – Software v4.0 – Page 50




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.



CSG Version 4.0

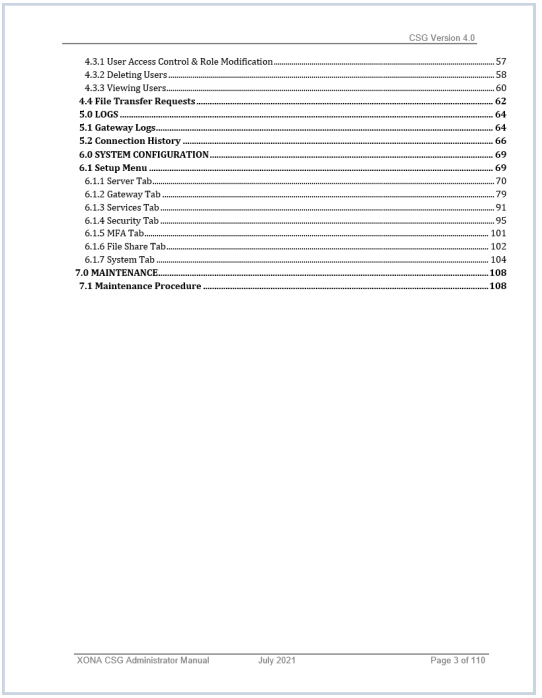
XONA CSG
ADMINISTRATOR MANUAL
TABLE OF CONTENTS

Page #

1.0 GETTING STARTED ..... 4
1.1 XONA Critical System Gateway (CSG) Administration Overview ..... 4
1.2 Points of Contact ..... 4
1.2.1 Help Desk and Support ..... 4
1.3 Did you perform the Initial CSG Setup? ..... 4
1.4 Acronyms and Abbreviations ..... 6
2.0 ADMINISTRATION USER INTERFACE (UI) ..... 6
2.1 Administration UI Overview ..... 6
3.0 MANAGE CONNECTIONS ..... 7
3.1 Managing Asset Connections ..... 7
3.2 Add Connection ..... 8
3.2.1 RDP Connection Settings ..... 9
3.2.2 VNC Connection Settings ..... 13
3.2.3 SSH Connection Settings ..... 16
3.2.4 XONA Relay Connection Settings ..... 19
3.3 View Connections ..... 24
3.3.1 Edit Connection ..... 24
3.3.2 Additional Connection Security ..... 25
3.4 Monitoring User Connections ..... 26
4.0 USER ADMINISTRATION ..... 28
4.1 User Administration Overview ..... 28
4.2 Adding Users ..... 29
4.2.1 User Authentication ..... 35
4.2.2 Username + Password (Local Authorization) ..... 35
4.2.3 Username + Password (Active Directory) ..... 36
4.2.4 Username/Password Authentication Errors ..... 36
4.2.5 Username/Password + MFA ..... 37
4.2.6 U2F Authentication Errors ..... 38
4.2.7 OTP Token Enrollment ..... 38
4.2.8 OTP Authentication Errors ..... 44
4.2.9 RSA SecurID Token Authentication ..... 44
4.2.10 RSA SecurID Authentication Errors ..... 44
4.2.11 User Time Access Windows ..... 45
4.2.12 Access Window Date ..... 45
4.2.13 Access Window Time ..... 49
4.2.14 Time Zone ..... 52
4.2.15 Session Timeout ..... 52
4.2.16 Disabling Account Access ..... 53
4.3 User Access Control - View Users Menu ..... 54

XONA CSG Administrator Manual July 2021 Page 2 of 110

XONA CSG Administrator Manual v4.0 – Page 2



CSG Version 4.0

4.3.1 User Access Control & Role Modification ..... 57
4.3.2 Deleting Users ..... 58
4.3.3 Viewing Users ..... 60
4.4 File Transfer Requests ..... 62
5.0 LOGS ..... 64
5.1 Gateway Logs ..... 64
5.2 Connection History ..... 66
6.0 SYSTEM CONFIGURATION ..... 69
6.1 Setup Menu ..... 69
6.1.1 Server Tab ..... 70
6.1.2 Gateway Tab ..... 79
6.1.3 Services Tab ..... 91
6.1.4 Security Tab ..... 95
6.1.5 MFA Tab ..... 101
6.1.6 File Share Tab ..... 102
6.1.7 System Tab ..... 104
7.0 MAINTENANCE ..... 108
7.1 Maintenance Procedure ..... 108

XONA CSG Administrator Manual July 2021 Page 3 of 110

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.



+1 866-849-6629 | info@xonasystems.com