



Volume

1

WebLEDS Administrators Guide

WebLEDS Administrators Guide

Table of Contents

CHAPTER 1 - INTRODUCTION..... 1

- OVERVIEW 1
- Administration Main Menu..... 2

CHAPTER 2 – ADMINISTRATION MENU..... 3

- 1. SYSTEM PARAMETERS 3
 - WebLEDS Server License Parameters 3
 - WebLEDS Mobile In-The-Car (MDT) License Parameters 4
 - WebLEDS DMV License Parameters 5
 - TCP/IP Communications Parameters To LEDS..... 6
 - Agency Identification Parameters 6
 - LEDS Transaction Headers and System ID 6
 - Authentication Methods (Desktop and Handheld)..... 7
 - Security / Password Parameters..... 7
 - User Preference Parameters 7
 - External SQL Logging Parameters 8
 - Auto Assignment of LEDS IDs/Mnemonics..... 8
 - Logging Retention Parameters 8
 - External Executable Program 8
 - Unsolicited APB Parameters..... 8
 - Signon Screen Text 9
 - Signon Screen Images 9
 - Signon Screen Footer Text..... 9
 - Help Button Text..... 9
- 2. MANAGE ADMINISTRATOR MENU AUTHORITIES 10
- 3. MANAGE ADMINISTRATOR ORI AUTHORITIES..... 10
- 4. MANAGE USER MAINTENANCE CAPABILITIES 10
- 5. APPLICATION AND TECHNICAL NOTES 11
- 6. DISPLAY SOFTWARE FIX LEVEL 11
- 7. SEND A MESSAGE TO ALL YOUR LEDS USERS..... 11

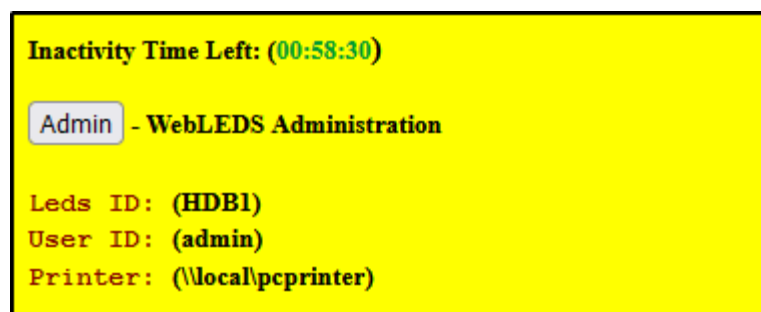
- 8. MANAGE LOCKED ACCOUNTS 11
- 9. MANAGE “LOCAL SYSTEMS” MENU ITEMS 12
- 10. MANAGE MASK SECURITY 13
- 11. MANAGE PRINTER TO DEVICE ASSOCIATIONS 13
- 12. EXPIRE USER PASSWORDS 14
- 13. USER MANAGEMENT 14
- 14. PRINTER MANAGEMENT 17
- 15. RESPONSE QUEUE MANAGEMENT..... 19
- 16. SPLIT MANAGEMENT 20
- 17. RESPONSE RE-ROUTING AND FORWARDING 22
- 18. VIEW SENT AND RECEIVED TRANSACTIONS LOGS... 22
- 19. VIEW TCP/IP COMMUNICATIONS AND ERROR LOGS 22
- 20. VIEW SUCCESSFUL AND FAILED LOGON LOGS 23
- 21. VIEW INDIVIDUAL USER LOGON HISTORY..... 23
- 22. VIEW INDIVIDUAL USER SECURITY QUESTIONS 23
- 23. MANAGE SYSTEM AND USER FAVORITES 24
- 24. VIEW ADMINISTRATION CHANGE LOGS..... 25
- 25. RESET A USER’S PASSWORD 26
- 26. STATISTICS AND REPORTS..... 26
- 27. MANAGE INCOMING API CONNECTION DEVICES 28
- 28. MANAGE OUTGOING API CONNECTION DEVICES ... 28
- 29. MANAGE REGIONAL QUERY TRANSACTIONS 29
- 30. MANAGE USER PRINTER CHANGING CAPABILITIES. 29
- 31. NETWORK CONNECTION TEST (PING) TO LEDS 30
- 32. DEPT OF CORRECTIONS – MANAGE PO CONTACT INFO 31
- 33. TWO FACTOR AUTHENTICATION – DISPLAY SETUP CODES..... 31
- 34. TWO FACTOR AUTHENTICATION – ENABLE BY IP ADDRESS 32
- 35. TWO FACTOR AUTHENTICATION – ENABLE BY IP USER 32

Chapter 1 - Introduction

This manual is the Administrator's Guide for the WebLEDS desktop application system. This manual covers all functions found under the "Administration" section within WebLEDS.

Overview

Within WebLEDS, the definition of an "Administrator" is any user who has been granted the "Administrator" privilege within their WebLEDS profile. Once granted, these users will see an "ADMIN" button located in the upper left corner of their WebLEDS screen.



Clicking on the "ADMIN" button will take the user to the **WebLEDS Administration** menu. All WebLEDS Administration functions are performed from this menu. Non-administrative users will not see the "ADMIN" button displayed.

Within the **WebLEDS Administration** menu, you can perform all administrative functions of your WebLEDS system, including such things as configuring your System Parameters, managing Users and Printers, resetting Passwords and Unlocking Accounts, managing System Security options, performing Auditing and Reviewing of logs, as well as numerous other system administration tasks. Below we discuss each option on the Administration menu.

ADMINISTRATION MAIN MENU

Clicking on the “ADMIN” button will display the **LEDS Administration** menu below. From this menu, simply click on the individual items to go to that section of WebLEDS Administration. Many items are limited by your ORI Authority, such that when clicked, you will only see data and users associated with the ORI(s) you have been given access to manage.

LEDS Administration

1. [Set System Parameters](#)
2. [Manage Administrator Menu Authorities](#)
3. [Manage Administrator ORI Authorities](#)
4. [Manage User Maintenance Capabilities](#)
5. [Application and Technical Notes](#)
6. [Display Software Fix Level](#)
7. [Send a Message to ALL Your LEDS Users - \(Limited by ORI Authority\)](#)
8. [Manage Locked Accounts - \(Limited by ORI Authority\)](#)
9. [Manage "Local Systems" Menu Items](#)
10. [Manage Mask Security](#)
11. [Manage Printer to Device Associations](#)
12. [Expire User Passwords - \(Limited by ORI Authority\)](#)
13. [User Management - \(Limited by ORI Authority\)](#)
14. [Printer Management](#)
15. [Response Queue Management - \(Limited by ORI Authority\)](#)
16. [Split Management - \(Limited by ORI Authority\)](#)
17. [Response Re-Routing and Forwarding - \(Limited by ORI Authority\)](#)
18. [View Sent and Received Transaction Logs - \(Limited by ORI Authority\)](#)
19. [View TCP/IP Communication and Error Logs](#)
20. [View Successful and Failed Logon Logs - \(Limited by ORI Authority\)](#)
21. [View Individual User Logon History - \(Limited by ORI Authority\)](#)
22. [View Individual User Security Questions - \(Limited by ORI Authority\)](#)
23. [Manage System and User Favorites - \(Limited by ORI Authority\)](#)
24. [View Administration Change Logs - \(Limited by ORI Authority\)](#)
25. [Reset A User's Password - \(Limited by ORI Authority\)](#)
26. [Statistics and Reports - \(Limited by ORI Authority\)](#)
27. [Manage Incoming API Connection Devices \(apitab\)](#)
28. [Manage Outgoing API Connection Devices \(hosttab\)](#)
29. [Manage Regional Query Transactions \(trantab\)](#)
30. [Manage User Printer Changing Capabilities - \(Limited by ORI Authority\)](#)
31. [Network Connection Test \(PING\) to LEDS](#)
32. [Dept of Corrections - Manage PO Contact Info](#)
33. [Two Factor Authentication - Display Setup Codes - \(Limited by ORI Authority\)](#)
34. [Two Factor Authentication - Enable by IP Address](#)
35. [Two Factor Authentication - Enable by User - \(Limited by ORI Authority\)](#)

Chapter 2 – Administration Menu

This section describes the individual options found on the WebLEDS Administration menu.

1. System Parameters

The System Parameters screen is where you will set global configuration parameters regarding your WebLEDS installation, such as your Software License Key, System Networking and Communications values, Security and Log-in Options, Log Retention parameters, Sign-On screen text and logos, and other settings that configure your system. Once accessed, to change a value simply change the parameter(s) you need and press the **UPDATE** button located at the top of the screen. Below is a description of each System parameter:

WEBLEDS SERVER LICENSE PARAMETERS

LICENSED USERS:

This is the number of users your WebLEDS system has been licensed for. This is the maximum number of **Active** or **Locked** Accounts that you can have in the system. **Disabled** accounts do not count towards this total. The system will not allow you to add more WebLEDS accounts than you are licensed for. This count does not include printers. This value must match the license key that you were provided.

LICENSE KEY 1:

This is the license key that has been generated by for your WebLEDS system. **THIS KEY IS GENERATED BASED ON THE TCP/IP ADDRESS OF YOUR SERVER.** If you ever change the TCP/IP address of your WebLEDS server, you will need to be supplied with a new license key. The TCP/IP address that this key is generated for is displayed in the following “Licensed IP” parameter.

LICENSE KEY 2:

This parameter provides for the capability to enter a second WebLEDS license key and is used only by those installations that have assigned a second TCP/IP address to their WebLEDS server. Instances where this might be utilized are in situations where an internal IP address is assigned to the WebLEDS server for internal access, and an external IP address is assigned to the server for external (Internet) access.

LICENSED IP:

This read-only field displays to you the TCP/IP address of your WebLEDS server. This is the IP address for which your License Key 1 has been generated.

CURRENT USERS:

This read only field displays to you the current number of individual user accounts which you have created so far within WebLEDS. Only **Active** and **Locked** accounts are counted, **Disabled** accounts are not counted. The system will not let you add more accounts than you are licensed for, and which are listed in the above “**Licensed Users**” parameter.

**WEBLEDS MOBILE IN-THE-CAR (MDT)
LICENSE PARAMETERS**

LICENSED USERS:

This is the number of users that have been licensed to use the optional WebLEDS Mobile (MDT) application. The MDT application is designed to be used in Police vehicles, and the system will limit usage of the application to the number of users licensed here. This value must match the license key that you were provided.

LICENSE KEY:

This is the license key that has been generated by WebLEDS support for your WebLEDS Mobile In-The-Car (MDT) use. **THIS KEY IS GENERATED BASED ON THE TCP/IP ADDRESS OF YOUR SERVER.** If you ever change the TCP/IP address of your WebLEDS server, you will need to be supplied with a new license key from WebLEDS support. The TCP/IP address that this key is generated for is displayed in the following “**Licensed IP**” parameter.

LICENSED IP:

This read-only field displays to you the TCP/IP address of your WebLEDS server. This is the IP address for which your License Key has been generated.

CURRENT USERS:

This read only field displays to you the current number of WebLEDS MDT workstations that have connected to the system so far.

Show Users Button:

This button will display the names of all PC workstations that have WebLEDS MDT installed, and which have connected to WebLEDS at some point in time. The total number of workstations saved here, and thus allowed to connect to WebLEDS, will be limited by your WebLEDS MDT License.

Clear Users Button:

This button will clear the list of workstations that have WebLEDS MDT installed, and which have connected to WebLEDS at some point in time. Clearing this list will allow new workstations running WebLEDS MDT to connect to WebLEDS. WebLEDS will then start collecting a new list of workstations, and allowing those stations to connect, up to the limit of WebLEDS MDT users your system is licensed for.

WEBLEDS DMV LICENSE PARAMETERS

LICENSED USERS:

This is the number of users that have been licensed to use the optional WebLEDS DMV application. The DMV application is a standalone PC program which allows users to look up DMV records only, and the system will limit usage of the application to the number of users licensed here. This value must match the license key that you were provided.

LICENSE KEY:

This is the license key that has been generated by WebLEDS support for your WebLEDS DMV use. **THIS KEY IS GENERATED BASED ON THE TCP/IP ADDRESS OF YOUR SERVER.** If you ever change the TCP/IP address of your WebLEDS server, you will need to be supplied with a new license key from WebLEDS support. The TCP/IP address that this key is generated for is displayed in the following "Licensed IP" parameter.

LICENSED IP:

This read-only field displays to you the TCP/IP address of your WebLEDS server. This is the IP address for which your License Key has been generated.

CURRENT USERS:

This read only field displays to you the current number of WebLEDS DMV workstations that have connected to the system.

Show Users Button:

This button will display the names of all PC workstations that have WebLEDS DMV installed, and which have connected to WebLEDS at some point in time. The total number of workstations saved here, and thus allowed to connect to WebLEDS, will be limited by your WebLEDS DMV License.

Clear Users Button:

This button will clear the list of workstations that have WebLEDS DMV installed, and which have connected to WebLEDS at some point in time. Clearing this list will allow new workstations running WebLEDS DMV to connect to WebLEDS. WebLEDS will then start collecting a new list of workstations, and allowing those stations to connect, up to the limit of WebLEDS DMV users your system is licensed for.

TCP/IP COMMUNICATIONS PARAMETERS TO LEDS

These parameters configure how to connect to LEDS:

- The TCP/IP address of the state's primary LEDS system
- The TCP/IP address of the state's backup (Disaster Recovery) LEDS system
- The TCP/IP Port to connect to LEDS on
- The DMPP security key provided by LEDS to authenticate to them with

AGENCY IDENTIFICATION PARAMETERS

These parameters configure your Agency Name and Server IP addresses:

- The textual name of your Agency
- Your WebLEDS IIS Server IP Address (IP assigned to the LEDS web in IIS)
- Your Server's IP address, which will be used as the source IP to connect to LEDS

LEDS TRANSACTION HEADERS AND SYSTEM ID

These parameters configure whether your system uses Standard (Short) or Extended (Long) Headers when communicating to LEDS. You also define your LEDS System ID. LEDS will provide you with both of these sets of information when they configure your system on their end. Typically, most agencies will use Short Headers.

AUTHENTICATION METHODS (DESKTOP AND HANDHELD)

These parameters configure how users will authenticate to both the WebLEDS Desktop and WebLEDS Handheld/Phone systems.

For Desktop authentication, options include using the standard WebLEDS Username/Passwords, or using your agency's Active Directory. WebLEDS support can provide you with more information on these particular authentication options.

For Handheld/Phone authentication, options include using the standard WebLEDS Username/Passwords, using Two-Factor authentication (Google Authenticator phone app, Microsoft Authenticator phone app, or WinAuth PC app), or using RSA SecureID Authentication.

SECURITY / PASSWORD PARAMETERS

These parameters allow you to define the criteria for passwords and logins:

- Whether to allow users to reset their own passwords from the Log-In screen, using the "Forgot Password / Unlock Account" button located at the bottom of the Log-In screen.
- The number of previous passwords that cannot be reused
- The number of days before passwords must be changed
- The number of invalid login attempts before an account is locked
- The inactivity timeout, in minutes, that logs users out after inactivity

USER PREFERENCE PARAMETERS

These parameters allow you to define user preferences:

- Whether users are allowed to change their printer to another printer
- Whether users can select to receive Unsolicited information sent is sent to your agency (BOLOs, APB's, State Broadcasts, etc.)
- The type of windows displayed when the "Show Transaction" button is clicked when filling out a transaction/mask screen. This simply shows the transaction in the "dot-delimited" format that will be sent to LEDS.
- Whether to disable RIGHT mouse clicking in the WebLEDS application.

EXTERNAL SQL LOGGING PARAMETERS

This function allows you to configure your WebLEDS server to log all sent transactions, and all received responses, to an external SQL database. Clicking the HELP link in the title will provide you with the information necessary to set up the appropriate SQL tables to log this information to. You'll also supply the username and password of the SQL user account to use to log this information.

AUTO ASSIGNMENT OF LEDS IDS/MNEMONICS

This option allows you to automate the assignment of LEDS IDs and MNEMONICS to new users, as you create new WebLEDS accounts. As users are created, the next available LEDS ID and Mnemonic is automatically filled in on the ADD A USER screen. As users are deleted, these ID's go back into the available pool for assignment. Please talk to WebLEDS support staff on how to set this function up, if it is desired to be used.

LOGGING RETENTION PARAMETERS

This option allows you to define how long responses are kept in each user's main response inbox, and how long responses are kept in their Deleted response inbox. This option also allows you to specify how many days to keep all system transaction logs on your system (sent logs, received logs, administration change logs, log-in history logs, etc.).

EXTERNAL EXECUTABLE PROGRAM

This option allows you to define a specific LEDS ID that, when an incoming response is received for, will have the received data passed to an external program. This allows for a customized external program to receive and process responses destined for a particular ID.

UNSOLICITED APB PARAMETERS

Historically, LEDS sent out "unsolicited" broadcast type messages to each agency server on a specific set of LEDS ID's, which was configured when the agency was first

set up and configured by LEDS on their end. Typically these LEDS ID's were set up as A1, A2, A3, A4 and A5., with various broadcast message types set to each ID by LEDS. This option allows you to define what ID's this unsolicited information will arrive on, and a description for each type of unsolicited ID (example: A1=All Oregon, A2=Weather, A3=Coastal Broadcasts, etc.). Within each user's WebLEDS profile, you can then specify which of these unsolicited broadcast categories (if any) that a user should receive.

SIGN-ON SCREEN TEXT

This option allows agencies to custom the text information that is displayed on the WebLEDS Sign-On screen.

SIGN-ON SCREEN IMAGES

This option allows agencies to customize the screen images that are displayed on the WebLEDS Sign-On screen.

SIGN-ON SCREEN FOOTER TEXT

This option allows agencies to custom the text information that is displayed at the bottom (footer) of the WebLEDS Sign-On screen.

HELP BUTTON TEXT

This option allows agencies to custom the text information that is displayed to users when the **HELP** button is clicked that is located on the bottom of the WebLEDS Sign-On screen.

2. Manage Administrator Menu Authorities

The “Manage Administrator Menu Authorities” option allows you to define exactly what items on the Administration menu each WebLEDS Administrator has access to. This menu item will display a list of all WebLEDS Administrators, along with checkboxes next to each name for each of the 35 Administration menu items. Simply check the boxes for each Administration menu item you wish each administrator to have access to.

By hovering your mouse over any of the numbered checkboxes, the system will display for you a popup text box explaining what Administration menu item that checkbox is for.

3. Manage Administrator ORI Authorities

The “Manage Administrator ORI Authorities” menu item allows you to specify for each WebLEDS Administrator exactly what ORI numbers they are authorized to work with and manage. Any items listed on the Administration menu that say “**Limited by ORI Authority**” will only show data and users associated with the ORI’s you have authorized each Administrator for.

If, for example, you grant an Administrator access to ORI’s “OR0100000” and “OR0200000”, they will only be able to Add, Change, Delete and List users with these specific ORI’s, or Reset Passwords, Unlock Accounts, or View Sent/Received logs for users with these ORI’s.

To allow an Administrator access to all ORI’s, simply check the “ALL” checkbox next to that Administrator’s name.

4. Manage User Maintenance Capabilities

The “Manage User Maintenance Capabilities” menu item allows you to specify for each WebLEDS Administrator, what user management functions (Add/Change/Delete) they can perform when managing users. This allows you, for example, to authorize an Administrator to be able to add new users, but not change or delete users. Or, as another example, it will allow you to remove all user management capabilities for an Administrator (by unchecking all boxes), so they can only View users, but nothing more.

5. Application and Technical Notes

The “Application and Technical Notes” section is an area where you can input free format notes and information regarding your WebLEDS system. You will be presented with an open input screen allowing you to record any information you feel pertinent to your installation. The system will come pre-loaded with contact information for support, as well as contact information for the State LEDS Operation Center.

Your usage of this informational screen is completely up to you to use to record anything that may be of value for you in the operation of the WebLEDS system.

6. Display Software Fix Level

This option will display to you your current WebLEDS fix level. In addition, it will list each fix level that has been installed on your system, and the date it was installed. You may need to reference this item if working with Technical Support folks. You will also need to refer to this area to verify that you have the prerequisite fixes installed before installing a new software fix update package. Each software fix update package requires and checks to verify that the previous fix package has already been installed.

7. Send a Message to All Your LEDS Users

This option will allow you to send a message to all your WebLEDS users. The message that you send will be placed as a response item in every user’s response inbox for them to view. This function does NOT send an interruptive message to your users. The message also does not leave your WebLEDS system, nor travel to LEDS.

8. Manage Locked Accounts

This Administration item allows you to “lock” any given WebLEDS account from being logged onto, as well as listing any WebLEDS accounts that are currently locked, allowing you to unlock them. Accounts may be locked by

using this function, or automatically by the system due to too many invalid login attempts by the user.

The number of invalid attempts allowed before the system automatically locks an account is controlled by the System Parameter “Number of Invalid Login Attempts Before Account is Locked”. Once an account has been locked, you must manually unlock it via this administration option. Locked accounts **WILL NOT** be automatically unlocked by simply waiting for some interval of time. Accounts will remain locked until unlocked by an Administrator. Also, you will only be able to unlock accounts which you have ORI authority to manage.

If any accounts are locked on your system, choosing this option will display a screen listing the locked-out accounts. Also included will be the date and time the account was locked, and the TCP/IP address that the account was locked out from.

This option will also show you “Invalid Locked Accounts”. These are account names that were used by a user in attempts to log in, but do not correspond to any valid WebLEDS user account.

9. Manage “Local Systems” Menu Items

WebLEDS contains a section called “Local Systems” that appears in the left side Navigation window for all WebLEDS users. Local Systems is an area that each agency can add links to that will be available to all of your WebLEDS users. These may be links to other installed Web applications at your installation, or other Internet Web links that you feel are valuable to make available to your users.

This option from the Administration menu will allow you to create these links, along with the Textual Description you wish to be displayed for each of these links. Once you are done editing, simply press the **Update** button located at the top of the screen. Users will see these updated links the next time they log into WebLEDS.

For the Description field, input the description of the link that you wish to be displayed on the Local Systems menu. For the link address, input the URL to the page/website you wish the link to point to.

10. Manage Mask Security

WebLEDS was designed with the concept of 9 levels of customizable security. As an Administrator, you can assign each transaction (mask) in the system to any of the 9 available security levels. By default, all masks are assigned to security level 1, except the LEDS Training Records masks (used by your agency's LEDS Rep), which by default are assigned to security level 9, and the SPLIT (Split) Transaction, which by default is assigned to security level 8. The split transaction will be covered in section #16 – Split Maintenance.

Once you have assigned your masks to the desired security keys (1 through 9), you will then authorize access to these keys to users inside their User Profile. The important thing to note is that security keys **are not** cumulative. In other words, granting a user access to security key 8 does not give them access to all the security keys below that (1-7). Security levels are independent, discrete assignments. An example is in order:

Examples:

Let's say you only want a small section of users to be able to use the Prisoner Transport transactions. Simply use this option to change the mask security level of these Prisoner Transport transactions to, say key 7. Now only users who have security key 7 checked in their user profile will be able to access those masks.

Another example may be to assign all of the LEDS inquiry transactions to key 1, and all of the LEDS update transactions to key 2. Now you can limit which users have update capability by the assignment of security key 2 to only users who should be able to access the update transactions.

11. Manage Printer to Device Associations

This option allows you to associate a workstation IP address with a particular WebLEDS printer. This provides the capability whereby any user who sits at and logs onto that particular workstation (IP Address) will have their default printer automatically changed to the specific printer you've associated with that workstation IP.

To make use of this functionality, a special printer in WebLEDS called "[\\local\devprinter](#)" is used. By assigning this as the default printer in a WebLEDS

user's profile, their printer will automatically be changed to the WebLEDS printer assigned to that workstation from this menu item, each time they log onto the system at that workstation. If they have this special printer defined as their default printer, but log onto the system at a workstation (IP address) that is not found in this option, their printer will automatically be set to the Local PC Printer "[\\local\pcprinter](#)".

If a user's default printer is not set to "[\\local\devprinter](#)", then logging in at a workstation that has had their IP setup in this option will have no effect on the user, and their default printer will not be automatically changed. The auto-changing of the printer will ONLY occur if the user's default printer is set to "[\\local\devprinter](#)".

12. Expire User Passwords

WebLEDS has the capability to automatically force your users to change their passwords after a certain interval of time. The default value is 60 days and is set in #1 Systems Parameter. If you wish to immediately force a user to change their password at their next sign on attempt, use this menu option.

Simply select the WebLEDS user account name whose password you wish to "expire", press the EXPIRE button, and they will be prompted to change their password at their next sign on. You may also use the "Expire ALL Passwords" button to expire ALL passwords on your system. After invoking this option, ALL users will be prompted to set new passwords at their next sign on.

13. User Management

This is where you will perform all of your User account Adds, Changes and Deletes, as well as being able to list all of the User accounts currently defined to your system.

From the User Maintenance menu, you may choose the following options:

List - Clicking this button will display a complete list of all users defined to your WebLEDS system. Once this list is displayed, you may click on any of the column headers to sort the list via that column (sort by Username or User Description or ORI, etc.). From this list, you may click on the highlighted Username, to go to the "Change A User" screen for that user. You may also click on the highlighted 4-character SYS/ID value for that user, which will display to you their response queue, and any responses located in it.

Add - Clicking this button will take you to the “Add A User” screen, enabling you to add a new user to WebLEDS. If you attempt to add a username that is already defined to the system, WebLEDS will inform you of this when you press the “ADD” button and will not re-add the user. To add a user, you will be required to supply the following information:

- **User Login Name** – This is the Username that the user will use to log into the system. The Username **is case sensitive**. There is no length restriction on this field, and any typographical characters may be used **EXCEPT THE COLON** character (:).
- **User Login Password** – This is the user’s password. The Password is **case sensitive**. Passwords are limited to 30 characters, and any typographical character may be used.
- **LEDS 2 Character System ID** – This is your System ID, as known and defined by LEDS. It will be prefilled in already, in the dropdown box. Simply use the value displayed. In VERY unique situations, an agency may be set up with multiple System ID’s, and if that is the case, simply select the appropriate System ID that corresponds with the following Terminal ID and Mnemonic you are going to use for this user.
- **LEDS 2 Character Terminal ID** – As part of establishing a connection to LEDS, you will be given by them a grouping of LEDS IDs (2-character) and LEDS Mnemonics (4 character). You will assign these ID/Mnemonic pairs to users. From WebLEDS perspective, each ID/Mnemonic becomes a response queue on the system. If more than one user is assigned to the same ID/Mnemonic, those users will share (i.e., view) the same response queue and responses on the system. Our recommendation is to define each user with their own unique ID/Mnemonic identifier.
- **LEDS 4 Character Mnemonic** – This is the 4-character Mnemonic associated with the 2-character Terminal ID entered above. Terminal IDs and Mnemonics are assigned together and must be associated together.
- **Default ORI Number** – This is the ORI number you wish to assign to this user, as their default ORI. ORI’s are created by LEDS for the agency the user works for. WebLEDS does not do any authority checking on ORI numbers (this is all done at the State LEDS system), but simply uses this number to pre-fill in the ORI field on any masks screens containing an ORI entry field.
- **Administrative Privileges** – This is the parameter which defines a user as an Administrator. If this field is set to yes, this user will have the “ADMIN” button

displayed to them on the left side of their WebLEDS screen, allowing them access to the WebLEDS Administration menu.

- **Default Printer** – This is the user’s default printer. The printers listed in this dropdown list are all printers defined to your WebLEDS system, which were added through the Administration menu #14 Printer Management.

Special Printers:

[\\local\pcprinter](#) - this will allow the user to print to any printer defined locally to their PC.

[\\loca\devprinter](#) - this will automatically change their printer to whatever printer is defined for the workstation they log into, which is setup via Administration menu #11 Manage Printer to Device Associations.

- **Users Full Name** – A free form field to document the user’s full name.
- **Description or Department** – A free form field to further describe the user.
- **Day/Evening/Other Phone Numbers** – Optional fields, to document a user’s phone numbers.
- **Alternate Name** – WebLEDS will automatically fill in a user’s name into any transaction screens that require the users name to be input. By default, the name filled in will be from the “Users Full Name” field. If an alternate name is desired to be used, fill it in here, and this Alternate Name will be filled in on transactions screens.

Example: A user’s name may be Susy Smith but enters “Judge Joe Jones” in the Alternate Name field, so that Judge Jones’ name will be filled in on any transaction screens that require an operator name, rather than Suzy’s name.

- **Security Keys** – The various security keys this user has access to. These key values relate to the various security keys your masks have been assigned to within the Administration menu #10 Manage Mask Security. These key values **are not** cumulative. Granting security key 3 does not grant access to security keys 2 or 1. Whatever keys they are assigned define the transactions/masks they will have access to, as setup in #10 Manage Mask Security.
- **Unsolicited Info This User Receives** – This defines whether this user will receive copies of any unsolicited information (APB’s, Statewide broadcasts, weather advisories, road advisories, training broadcasts, etc.) that your agency receives from LEDS.

Change - This button allows you to go directly to the “Change A User” screen for a particular user. You need to select the user profile name you wish to change from the dropdown box **before** pressing the Change button.

Delete - This button will allow you to delete a user profile. You need to select the user profile name you wish to delete from the dropdown box **before** pressing the Delete button. After pressing Delete, you will be presented with the User’s Profile, and will need to choose Delete again to delete the user.

14. Printer Management

This is where you will perform all of your WebLEDS Printer Adds, Changes and Deletes, as well as being able to list all of the printers currently defined to your system.

For printing, WebLEDS printing makes use of the Windows Printing subsystem. **Before** adding a printer into WebLEDS, you must first add the printer as a standard Windows Printer on your WebLEDS Server using the standard Windows “Add A Printer” dialog. You should also send a Windows test print to the printer to verify it is printing correctly from Windows **before** adding the printer to WebLEDS.

After adding the printer to Windows, you **must** then share the printer, and give it a share name. This UNC Share name for the printer ([\\servername\sharename](#)) is the name that you will use when adding the printer into WebLEDS. By using the robust printing facilities of Windows to create your printer, you have the capability to define printers across any of the supported protocols and platforms that the Windows Printing subsystem supports. It also centralizes all of your LEDS printing through a single Windows Print server (your WebLEDS server), giving you better print control and management.

From the Printer Management menu, you may choose the following options:

List - Clicking this button will display a complete list of all printers defined to your WebLEDS system. Once this list is displayed, you may click on any of the column headers to sort the list via that column (sort by Printer Name, or Location, or Description, etc.). From this list, you may click on the highlighted Printer Name, to go to the “Change A Printer” screen for that printer.

Add - Clicking this button will take you to the “Add A Printer” screen, enabling you to add a new printer to WebLEDS. If you attempt to add a printer name that is already defined to the system, WebLEDS will inform you of this when you press the “ADD” button and will not re-add the printer. To add a printer, you will be required to supply the following information:

- **LEDS 2 Character Terminal ID** – Printers can **optionally** be assigned a LEDS 2-character Terminal ID and 4-character Mnemonic that identifies them to the State LEDS System. This field (and the following Mnemonic field) are **optional** for printers. Only printers that you want directly addressable from the outside LEDS world should be assigned a Terminal ID and Mnemonic. If you assign a printer with a Terminal ID and Mnemonic, a user anywhere in the LEDS network can send messages directly to that printer by addressing the message to the 4-character Mnemonic name you have assigned to the printer.
- **LEDS 4 Character Mnemonic** – See the description above for the Terminal ID field. This is an **optional** parameter and is only necessary if the printer needs to be directly accessible from the LEDS network.
- **Printer Type** – This is the type of printer you are adding. For printers defined on your WebLEDS server, choose “Standard Server Print Queue”. If you are using our WebLEDS Encrypted Print Software to print to a printer in another network, choose “Encrypted Print Server”. Please consult with WebLEDS Support if you have a need to use Encrypted Printing to a remote network printer.
- **Printer Share Name** – This is the UNC Sharename of the printer as you created it on your WebLEDS server. Format is:

[\\servername\PrinterSharename](#)

Before adding a printer, you must first add it to Windows as a normal printer, and then Share that printer with a Sharename.

- **Printer Location** - A free form field to describe the location of the printer (ex: Records Department)
- **Printer Description/Type** - A free form field to further describe the printer, such as the printer make, model, and type (ex: HP Laser 5Si).
- **Unsolicited Info This Printer Receives** - This defines whether this printer will receive copies of any unsolicited information (APB’s, Statewide broadcasts, weather advisories, road advisories, training broadcasts, etc.) that your agency receives. Typically, you will enable this option for the main system printer in each agency/division.

Change - This button allows you to go directly to the “Change A Printer” screen for a particular printer. You need to select the printer name you wish to change from the dropdown box **before** pressing the Change button.

Delete - This button will allow you to delete a printer. You need to select the printer name you wish to delete from the dropdown box **before** pressing the Delete button. After pressing Delete, you will be presented with the Printer Profile, and will need to choose Delete again to delete the printer.

15. Response Queue Management

Response Queue Management is the facility which allows an Administrator to List, View and Clear other user’s Response Queues. Many times, it may be necessary for an Administrator to see a particular response that a user has a question about or is having a problem with. Using this facility, you can easily view their response(s).

From the Queue Management menu, you may choose the following options:

List - Clicking this button will display a complete list of all response queues (inboxes) defined on the system, and the User Profiles that are assigned to each. Clicking any of the column headers will sort the list by that column. From this screen, you can see how many responses are in each user’s Main response inbox, their Saved response inbox, and their Deleted response inbox.

Clicking on the number of responses displayed for any given response inbox will take you to that inbox and show you all of those responses. Clicking on the highlighted User Profile name will take you to the “Change A User” screen for that profile.

View - This button allows you to go directly to viewing a specific users Main response queue. You need to select the user profile name from the dropdown box and press the VIEW button to view that user’s responses.

Clear - This button will allow you to clear a user’s response queue of all responses. You need to select the user profile name from the dropdown box and press the CLEAR button to clear all of their responses. Be aware this will clear ALL responses, in all 3 of their inboxes (Main inbox, Saved inbox, Deleted inbox).

16. Split Management

Split Management is the concept whereby responses can be rerouted (split) to additional destinations other than just the original intended destination. As an example, responses sent to User A can also be routed to User B and to printer C.

Or responses routed to Printer X can also be routed to Printer Y. You can also configure, when the split is activated, whether the original recipient is to continue to receive their copy of the responses or not.

There may be two instances when splitting may be of value:

- The first instance may be in an audit or investigative mode. Supervisor Mary may wish to receive copies of everything employee Tom receives. By enabling a split on Tom, unbeknownst to Tom, Mary can receive copies of all Tom's responses.
- The second instance, which is more common, is where Dept A wishes Dept B to receive a copy of everything they receive at their main printer. This is common where a smaller division is only open during the daytime hours, say 8am – 5pm, and after hours they need copies of their responses to go to some other division's printer that is staffed 24 hours.

Once defined, a split can be turned on and off in one of 3 different ways:

- The first mechanism is to navigate to Administration menu #16 Split Management, choose "Change an Existing Split", and check ON the box that enables the split. This requires Administrative privileges and is a manual process to turn the split on and/or off.
- The second method is to make use of the built-in SPLIT transaction. This transaction can be entered into the Navigation "Go to Mask:" box by any user who has been granted authority to this transaction (by default security key 8 in their profile). This allows you to empower specific users to use this split facility, to turn splits on and off, without giving them access to the Administration menu.
- The third method is an automated way, via the Windows Task Scheduler on the WebLEDS Server. Using the Task Scheduler allows you to automate the enabling and disabling of splits that are repetitive in nature. A callable interface program has been provided that allows you to add this type of entry into the Scheduler.

To add an entry to the scheduler, you first must first define the split via the standard "Add A Split" process. Once the split is defined, simply create an entry in the Windows Task Scheduler, supplying the following commands:

Scheduler: Enabling and Disabling Splits

To Enable the Split:

```
C:\Strawberry\perl\bin\perl.exe c:\ledtables\splits.pl XX ON
```

To Disable the Split:

```
C:\Strawberry\perl\bin\perl.exe c:\ledtables\splits.pl XX OFF
```

Where “XX” is the 2-character LEDES ID of the split you created. Then simply set the dates and times that you need the split enabled and disabled.

From the Split Management menu, you may choose the following options:

List - Clicking this button will display a complete list of all splits defined to your WebLEDS system. From this list, you may click on the highlighted LEDES ID for a given split, to go to the “Change A Split” screen for that split.

Add - Clicking this button will take you to the “Add A Split” screen, enabling you to add a new split to WebLEDS. If you attempt to add a split that is already defined to the system, WebLEDS will inform you of this when you press the “ADD” button and will not re-add the split. To add a split, you simply select the LEDES ID/Username to split on, and then select up to 10 destination users/printers for the split copies to go to.

When adding a split, you will also select whether the original recipient (the ID/User you are splitting on), should continue to receive their copy of the message or not.

The “ENABLED” checkbox is what is used to turn the split ON or OFF.

Change - This button allows you to go directly to the “Change A Split” screen for a particular split. You need to select from the dropdown box the User or Printer of the split you wish to change, **before** pressing the Change button.

Delete - This button will allow you to delete a split. You need to select from the dropdown box the User or Printer of the split you wish to delete, **before** pressing the Delete button. After pressing Delete, you will be presented with the Split Profile, and will need to choose Delete again to delete the split.

17. Response Re-Routing and Forwarding

Response Re-Routing and Forwarding is the function that allows an Administrator to redirect and forward incoming responses for one User or Printer, to another User or Printer. It also allows the Administrator to configure whether the original user continues to receive their copies of responses or not, when the forwarding turned is on.

In addition to Administrator's setting up forwarding, individual users themselves can set up forwarding of their own responses, using the "Forward Responses" function listed on the left side of the WebLEDS screen. If any users have setup forwarding, this Administration menu item will display those forwarding's that users have setup.

18. View Sent and Received Transactions Logs

Every transaction sent, and every response received from LEDS is logged. For Sent logs, the Date, Time, User, ORI, IP Address, and Transaction is logged. For Received logs, the User and the received response data is logged.

Log files are listed by date, in descending order, with the newest date on top. Simply click on the View button next to the date of interest to view ALL data for that day.

When viewing these logs, you may choose to view the data in the browser screen itself (View in Browser) or choose to view the data in Windows Notepad (View in Text). Simply click on the VIEW button you desire.

19. View TCP/IP Communications and Error Logs

WebLEDS communicates to the state LEDS system via TCP/IP networking. Detailed communications logs are maintained of these communications. If networking issues occur, you may be asked by WebLEDS support personnel to use this option to display various communications and error logs to help diagnose any networking issues.

20. View Successful and Failed Logon Logs

WebLEDS maintains logs of every user log-in, logging whether it was successful or failed. This menu item will allow you to review those logs.

Logs are displayed by individual date and will show you the total Successful or Failed logons for every given date. Clicking on a specific date will show you the details of that date, including the date, time, user and IP the successful or failed logon occurred from.

21. View Individual User Logon History

WebLEDS maintains logon history files for every user of the system, allowing you to see whenever that user successfully logged into the system, or failed a logon into the system.

Simply select a user from the dropdown list and press the SHOW HISTORY button to see the complete logon history for that user. Information displayed will be the date, time, IP address, and Status (Successful or Failed) for every logon of that user.

22. View Individual User Security Questions

When a user logs into WebLEDS for the **second** time, they will be prompted to set a 4 digit pin and select 3 security questions/answers. The user may use these items to self-reset their password if they ever forget it, by using the “RESET PASSWORD / UNLOCK ACCOUNT” button located at the bottom of the logon screen.

Administrators may use this menu item to view a user’s 4-digit PIN and Security questions/answers, to allow them to confirm the identity of a user that might be contacting them on the phone. Administrators cannot change this information, but only view what a user has set. Users can change their Security information at any time, using the “**CHANGE PERSONAL SECURITY QUESTIONS**” link on the left side of their WebLEDS screen.

My WebLEDS:

- Logoff
- Change Password & Account Info
- Change Personal Security Questions ←
- Display & Search Sent/Received Logs

23. Manage System and User Favorites

WebLEDS allows each user to create a "Favorites" list, where their most commonly used masks can be listed for easy one-click access, and for one function key click via the F1 through F12 and Shift F1 through Shift F12 function keys.

Using this Administrative menu item, Administrator may List, Add, Change, and Delete all Favorites defined on the system.

This favorites list for users is located in the Navigation Window, which is the left-hand pane of their WebLEDS screen. Users may customize this list for themselves by clicking on the "**My Favorites: [...]**" title at the top of their Favorites list. Following the words "**My Favorites**" in the title, it will show whether the user is using the System Default Favorites or a personally setup Favorites list:

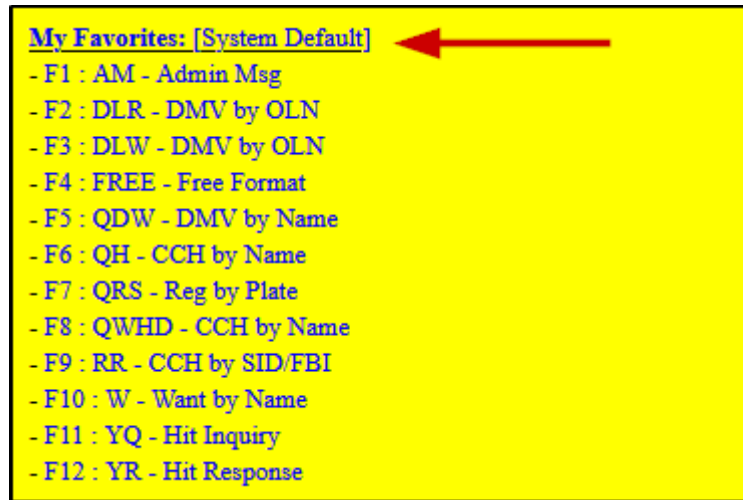
If using the System Default list it will display "System Default":

My Favorites: [System Default]

If using a personally customized list, it will display their name:

My Favorites: [Kevin]

Example Favorites screen using System Defaults:



The Administrative menu item "Manage System and User Favorites" option allows an administrator to update the system supplied Default Favorites list or create a Favorites list for an ORI. If an ORI favorites list is created, users will be assigned that Favorites list at logon if their default ORI matches that ORI, and if they have not already created a personal, customized Favorites list.

The order of precedence the system uses when determining which favorites list to assign a user is (the first item found is used):

1. Check for a personalized list that the user has created themselves, if found use that.
2. Check for an ORI favorites list that matches their ORI, if found use that.
3. If neither of the above has been set up, use the System Default Favorites list.

24. View Administration Change Logs

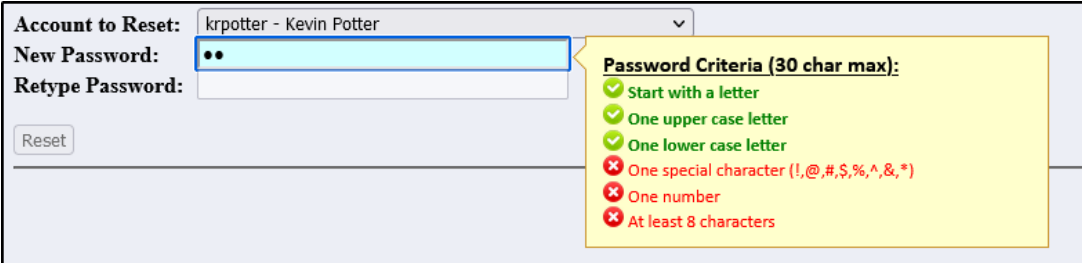
WebLEDS logs every Administrative change that is made to the system through the Administration menus. Administration items that do not result in a change to the system (i.e., Listing users, or Viewing Logs), are not logged.

The number of days these log files are saved is governed by the Logging parameter established in the #1 System Parameters screen.

A log will be created for each day (assuming change activity was generated on a given day), and each log entry will give the User, Time, and Administration Change Activity that occurred. The logs may be sorted by User or by Time, simply by clicking on the appropriate column header.

25. Reset A User's Password

WebLEDS allows an Administrator to easily reset a user's password. From this menu item, simply select the user from the dropdown list, and enter their new password. Passwords must meet system required complexity requirements, which will be shown to you as you enter the new password.



Account to Reset: krpotter - Kevin Potter

New Password: ••

Retype Password:

Reset

Password Criteria (30 char max):

- ✔ Start with a letter
- ✔ One upper case letter
- ✔ One lower case letter
- ✘ One special character (!,@,#,\$,%,&,*)
- ✘ One number
- ✘ At least 8 characters

As you type the password, each complexity requirement you meet will be checked off in green. You will not be able to click the “**RESET**” button to reset the password, until the password you typed meets all complexity requirements, and you have successfully re-typed the same password for validation in the second password box.

26. Statistics and Reports

WebLEDS contains a very robust and easy-to-use Statistics and Reporting feature that allows you to view all data sent and received to LEDS, by all users you are authorized to see (based on ORI authority).

When using this Administration menu, you will be prompted to select which data you wish to view, either “**Data for SENT Transactions**”, or “**Data for RECEIVED Responses**”. Depending on what you select, different reporting options are available.

If selecting **SENT** data, you can view your reports in either **TOTALS** format or **DETAILS** format. **TOTALS** format will produce a summary report with each individual user listed, allowing you to click on an individual user to see their complete SENT details. **DETAILS** format will show ALL users and all SENT details in one large report.

Formats you can select to report on **SENT** data include by:

- User
- ORI
- IP Address

- By Transaction Type
- By Searching for Specific Text

Formats you can select to report on **RECEIVED** data include:

- By User or Printer
- By ORI
- By Searching for Specific Text

To run a report, simply select the option to view **SENT** or **RECEIVED** data. On the next screen, select the Date(s) of interest to report on, and then select the report type you wish to run. The report will then be displayed to your screen.

Example report screen if selecting to report on **SENT** data:

The screenshot shows a web-based report selection interface. At the top, it is titled "Select Log File(s) to Process" in red. Below the title are two instructions: "<CTRL-Click> to select multiple individual dates" and "<SHIFT-Click> to select top & bottom files for selecting a date range". A scrollable list of log files is displayed, with "2023-03-16.txt" selected. The list includes dates from 2023-03-07 to 2023-03-16. Below the list is a "Select Report:" section with several radio button options: "Totals by User" (selected), "Details by User", "Totals by ORI", "Details by ORI", "Totals by IP Address", "Details by IP Address", "Totals by Transaction", and "Details by Transaction". There is also a "Search for Text:" label followed by an empty text input field. At the bottom left of the form is a "Run Report" button.

Once a report is displayed, you can click on the “**Transfer to Microsoft Excel**” or “**Transfer to Microsoft Word**” buttons, to transfer that report into Excel or Word.

27. Manage Incoming API Connection Devices

WebLEDS contains a programmatic feature (API = Application Programming Interface), that allows external, non-WebLEDS software systems (Dispatch 911 systems, RMS systems, E-Ticket systems, etc.), to easily send LEDS transactions to the state through WebLEDS.

With just a couple lines of computer code added to an external system, any external software application can easily be enhanced to be able to send LEDS inquiries and entries to the state, without having to write their own complete interface to the state.

External applications that connect to WebLEDS to use this feature must first be authorized by their IP address. This menu item allows you to enter the IP address of external systems that are allowed to connect to the WebLEDS API for sending LEDS requests. Systems that are not authorized here will be ignored by WebLEDS.

Please contact WebLEDS support first for a complete explanation of this feature.

28. Manage Outgoing API Connection Devices

WebLEDS contains a programmatic feature (API = Application Programming) that allows WebLEDS to return incoming responses to any external non-WebLEDS software system. This is typically used in conjunction with the above item #27 Manage Incoming API Connection Devices, to allow external software systems to send LEDS requests to the state through WebLEDS, and then have WebLEDS return the returning responses back to the external software system.

This item allows you to define the LEDS ID and MNEMONIC that WebLEDS will watch for in returning responses, and the DNS or URL that WebLEDS should forward those responses onto for handling. WebLEDS can forward the incoming responses to the external program using either HTTPS/POST (REST), or TCP/IP Sockets.

If the external name is listed using a URL:

<https://server.domain.com/cig/receiver.htm>

the response will be returned using HTTPS POST (REST)

If the external name is listed as a DNS name:

server.mydomain.com

the response will be returned using TCP/IP sockets, on TCP port 3335.

Please contact WebLEDS Support first for a complete explanation of this feature.

29. Manage Regional Query Transactions

WebLEDS contains a feature that allows it to handle queries sent to it by the state LEDS system. This is called a Regional Query. Agencies may work with LEDS to set up a customized state-wide available transaction code, that when submitted through the LEDS system by other agencies, will be routed to your WebLEDS server for handling and response.

This feature allows an agency to make available query capabilities into their own data applications that all other agencies statewide can use. You must first work with the state LEDS folks to define a unique LEDS transaction key that they will route to you, along with the specific fields that are required to be supplied for that particular transaction. Once done, any statewide agency that submits that transaction to LEDS will have that transaction routed to your server for handling and response.

Once your application receives the query and processes it, you must then format it into a proper query response and return the data back to LEDS, for return to the inquiring user.

This item allows you to define the LEDS Transaction ID that WebLEDS will watch for in incoming LEDS messages, and the DNS or URL that WebLEDS should forward the response onto in your network for handling. WebLEDS can forward the incoming message to the external program using either HTTPS/POST (REST), or TCP/IP Sockets.

If the external name is listed using a URL:

<https://server.domain.com/cig/receiver.htm>

the response will be forwarded on using HTTPS POST (REST)

If the external name is listed as a DNS name:

server.mydomain.com

the response will be forwarded on using TCP/IP sockets, on TCP Port 3335

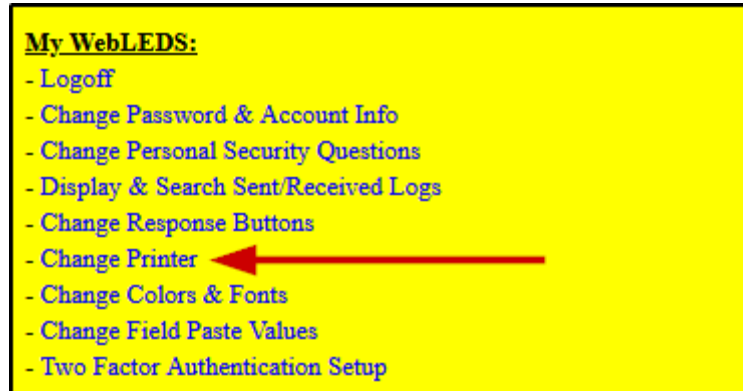
Please contact WebLEDS Support first for a complete explanation of this feature.

30. Manage User Printer Changing Capabilities

WebLEDS establishes a default printer for each user in their WebLEDS user profile. When users print a response, it will go to this printer. Upon printing, a popup message is displayed to the user stating the file has been successfully printed to that printer.

Users have the capability, if allowed, to change their printer at any time to any other printer defined on your WebLEDS server. This allows, for example, a Records clerk to print something to the Jail printer if needed. The user can change their printer, print the response, and then change their printer back to their normal printer.

Changing printers by a user is accomplished by the user clicking on the “**Change Printer**” link located in the Navigation Window on the left side of their WebLEDS screen:



Administrators, via this #30 Manage User Printer Changing Capabilities menu item, can restrict who can and can't change their printer. By default, all users are allowed to change their printer.

This item also allows you to specify if a user changes their printer, whether the change is temporary (just for this session, and resets back to their default printer when they log out and back in), or whether the change is permanent (their user profile is permanently updated with the selected printer as their new default printer).

31. Network Connection Test (PING) to LEDS

WebLEDS communicates to the state LEDS system, to send and receive all LEDS inquiries and responses. For networking diagnostic purposes, this item allows an administrator to send a network PING to the state LEDS system, to verify end-to-end communications is in place and working successfully between your WebLEDS server and the state.

If the PING test fails, networking is broken between your WebLEDS server and the state, and local technical diagnostics needs to be done to resolve the networking issue (usually an issue with the site-to-site VPN setup between an agency and LEDS).

32. Dept of Corrections – Manage PO Contact Info

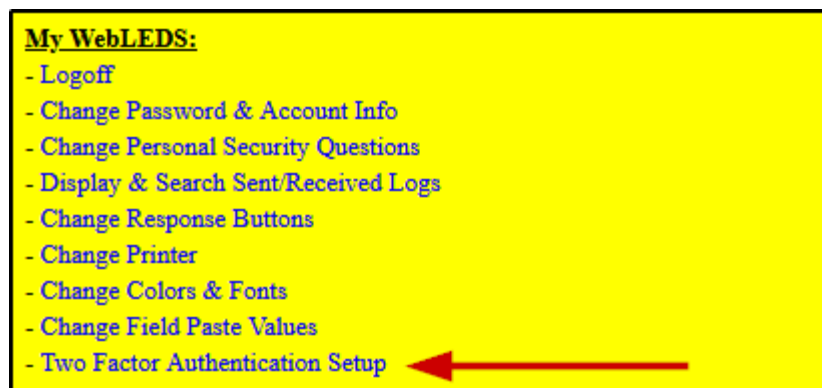
WebLEDS has a special feature used ONLY by the Oregon Dept of Corrections which allows them to determine what Parole Officer Name and Day/Evening/Other phone numbers are filled in on the EPR screen (Enter Person of Record) when the user is filling it out for submission to LEDS.

This Administrative screen will list all users on the system and allow the Administrator to select a user, and then enter a PO Name and Day/Evening/Other phone numbers, and then indicate which of these items should be inserted into the EPR screen when it is being filled out by the user.

33. Two Factor Authentication – Display Setup Codes

WebLEDS allows two-factor authentication to be enabled for user access into the system. Two-Factor authentication is setup by the user, using the “Two Factor Authentication Setup” link located in the Navigation window on the left side of the WebLEDS screen.

Clicking on this link by the user will provide them with complete instructions on setting up two-factor authentication.



This Administration menu item will allow an Administrator to see the unique secret key, for all users, that is required for each user to setup their two-factor authentication in their authenticating application (phone or Windows app). The user instructions included in the setup link above and displayed to the user also contain this key, but if users are away from their WebLEDS screen, or cannot get logged in to get this code, an administrator can provide this secret setup key to them using this menu item.

34. Two Factor Authentication – Enable by IP Address

WebLEDS allows two-factor authentication to be enabled for user access into the system. Users typically self-enable two-factor authentication, using the “Two Factor Authentication Setup” link provided to them on the left side of their WebLEDS screen (see instructions and screenshot provided in Administration menu #33 above).

Using this menu item, Administrators themselves can globally turn on two-factor authentication by individual IP address, or by a full class C subnet (x.x.x.0). This forces any user logging in from those IP address(es), to be prompted for a two-factor authentication code, whether the user themselves has enabled two-factor authentication or not.

Administrators can also input a special IP address (0.0.0.0), which will indicate that ALL users logging into the system, regardless of IP, will be prompted for a two-factor authentication code. In other words, this specifies the entire system will use two-factor authentication.

Before turning this on, be sure that ALL users on your system have already set up two-factor authentication on their authentication devices, or they will not be able to log in.

35. Two Factor Authentication – Enable by IP User

WebLEDS allows two-factor authentication to be enabled for user access into the system. Users typically self-enable two-factor authentication, using the “Two Factor Authentication Setup” link provided to them on the left side of their WebLEDS screen (see instructions and screenshot provided in Administration menu #33 above).

Using this menu item, Administrators themselves can turn on (or off) two-factor authentication for a specific user. If turning on, be sure the user has already logged in and followed the steps outlined in the “Two Factor Authentication Setup” link, to enable two-factor authentication on their device.

If a user is having problems logging in using two-factor authentication, this Administrative menu item can also be used to turn off (delete) two-factor authentication for the user, allowing them to log in, and re-follow the instructions in the “Two Factor Authentication Setup” steps to properly setup their device.

END
OF
DOCUMENT