

eSSL- eBioserverNew

--- eSSL eBioserverNew Help Manual

Version	:	eBioserverNew 1.2
Version Date	:	15 th November, 2024
No. of Pages	:	27

About This Manual: This document introduces the main functions, the user interface and operations of the eBioserverNew location wise

Table Contents

	Page
1) What is eSSL – eBioserverNew	
2) Master Setup	
1. Login Page	3
2. Dashboard	6
3. Employees	7
4. Devices	9
5. Device Commands	10
6. Access Group	12
7. Time Periods	13
8. Device Logs	14
9. Device Illegal logs	15
10. Utilities	
i. Import / Export Employees	16
ii. Import / Export Devices	17
iii. Parallel logs	18
11. System Users	22
12. API Settings	24
13. Database Settings	25
14. Change Password	26
15. License key	27

What is eSSL eBioserverNew?

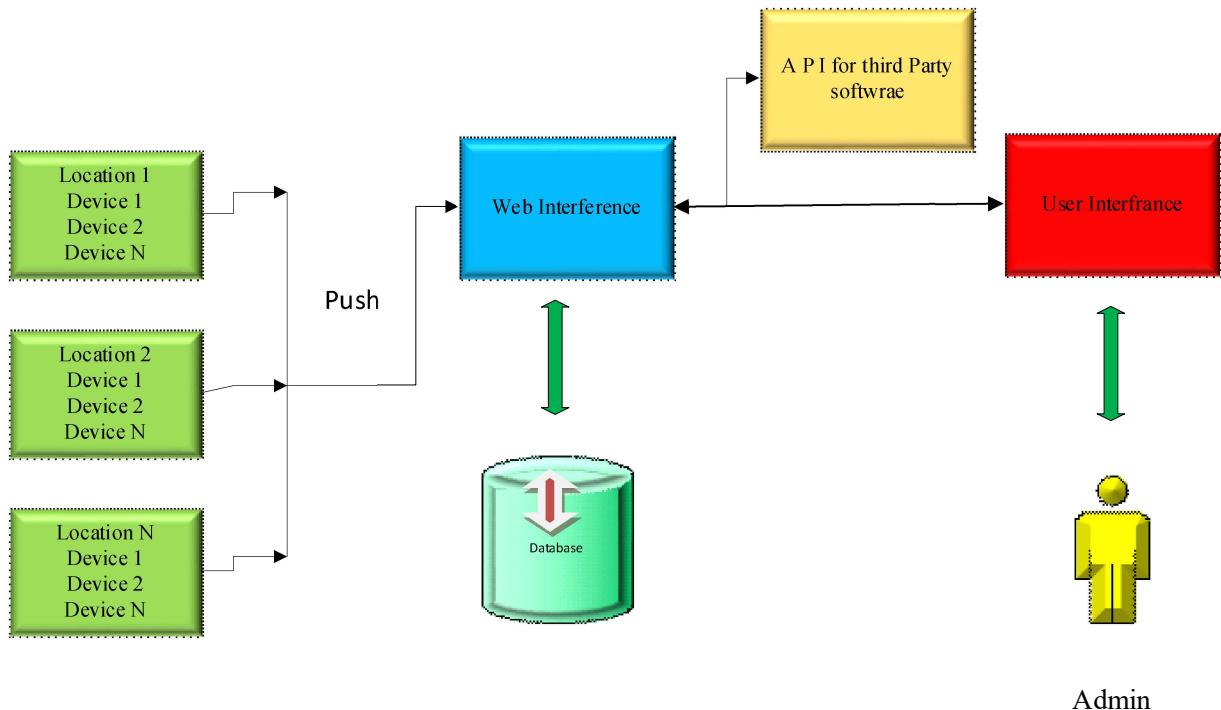
eSSL – eBIOServerNew is Web-based Biometric Data Management Solution which acts like a middleware between Biometric devices and Third party client Applications. As a middleware, eBioServer can be deployed on MS Windows Web server along with MS SQL databases for devices communication and transactions management.

Administrators can access eBioServer anywhere on a browser or third-party software by API to handle thousands of devices.

eSSL – eBioserverNew silent Features

- Dashboard – Present and Absent Employees and Device Online / Offline status
- Device Pushes data to Centralized server
- Auto Sync of the employees information like addition or deletion in location of respective devices
- Location wise Access of employees and Devices
- Device is mapped with single location
- Employee is mapped with multiple locations
- Bulk Import and export of employees and devices
- Through API , User addition and deletion from the location of respective devices
- Through API, Getting the Punch records of the users
- Parallel Logs, Pushing the data to third party database
- Single Location, System user access for employees and device operation
- Admin can access all the location of employees and the devices
- User friendly appearance requires less time to get you educated for the software

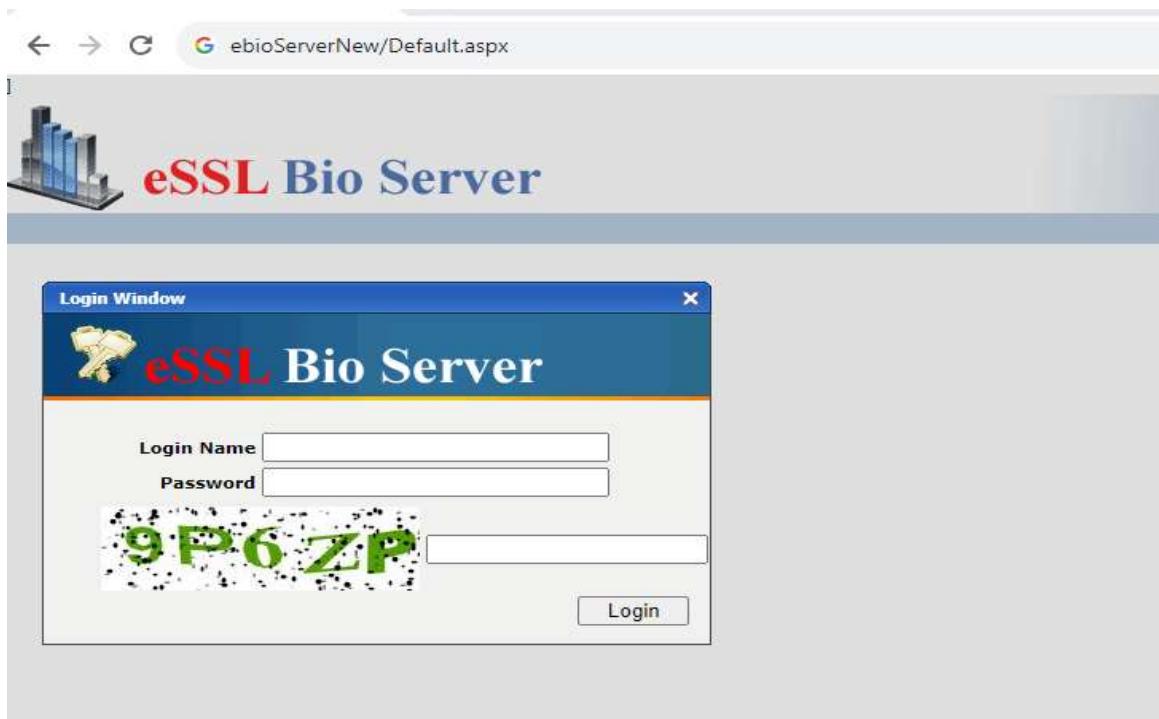
Centralized Server with Remote Device Communications



Go to browse & type Url of the application

User Name: essl

Password: essl



Welcome Page --- Dashboard

The screenshot shows the eSSL Bio Server dashboard. At the top, there are four colored boxes: green (Present Employees: 2), orange (Absent Employees: 2), blue (Online Devices: 4), and red (Offline Devices: 0). Below these are two tables. The first table, titled 'Present Employees List', shows two employees: Vijay (Employee Code 500) and Amitkumar (Employee Code 1123). Both were last punched on Sep 18, 2023, at 11:28:51 AM from Mumbai (MUM) and BLR respectively. The second table, titled 'Absent Employees List', shows no records.

Employee Code	Employee Name	Location	Last Punch	Last Punch Device	Last Punch Location	Last Punch Direction
500	Vijay	MUM	18 Sep 2023 11:28:51	Mumbai Dadar	MUM	OUT
1123	Amitkumar	BLR	18 Sep 2023 14:30:09	BLR JAYNAGAR	BLR	INOUT

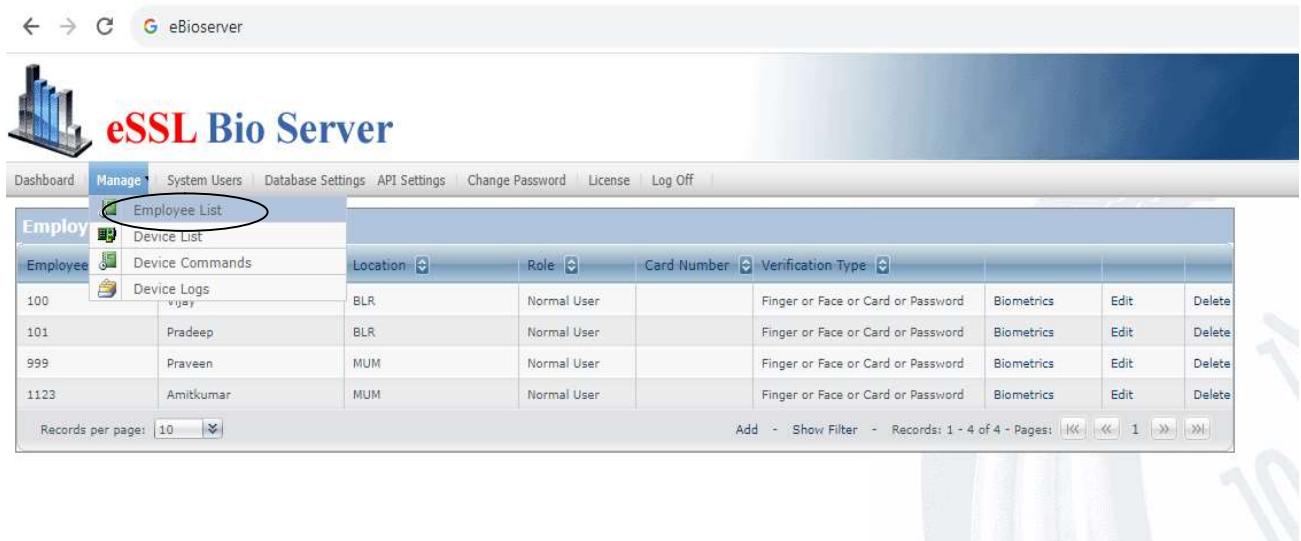
Records per page: 10 Show Filter - Records: 1 - 2 of 2 - Pages: << < > >>

Current Date employee present, absent, online devices and offline device count are displayed

If you click on the respective Title, Records list are displayed

Employees:

This form will display the list of all Employees, User can Add, Edit & Delete the Employees



Employee ID	Employee Name	Location	Role	Card Number	Verification Type	Biometrics	Edit	Delete
100	Pradeep	BLR	Normal User		Finger or Face or Card or Password	Biometrics	Edit	Delete
101	Praveen	BLR	Normal User		Finger or Face or Card or Password	Biometrics	Edit	Delete
999	Amitkumar	MUM	Normal User		Finger or Face or Card or Password	Biometrics	Edit	Delete
1123		MUM	Normal User		Finger or Face or Card or Password	Biometrics	Edit	Delete

Employee Code : Enter Employee Code

Employee Name : Enter Employee Name

Location : Enter employee location name

Card Number : Enter Employee RFID card number

Employee Password : Enter Employee device password

Device Role : Select the employee device role

Verification Type : Select the Verification type from the drop down

Expiry From : Enter Employee expiry date from

Expiry To : Enter Employee expiry to date

Note: - Employee should added or deleted in the application via software or API only

Click on Add, to enter Employee details

[←](#) [→](#) [↻](#) eBioserver

eSSL Bio Server

Dashboard | Manage | System Users | Database Settings | API Settings | Change Password | License | Log Off

Employee	Employee List	Device List	Location	Role	Card Number	Verification Type			
100	Pradeep	vjay	BLR	Normal User		Finger or Face or Card or Password	Biometrics	Edit	Delete
101	Pradeep		BLR	Normal User		Finger or Face or Card or Password	Biometrics	Edit	Delete
999	Praveen		MUM	Normal User		Finger or Face or Card or Password	Biometrics	Edit	Delete
1123	Amitkumar		MUM	Normal User		Finger or Face or Card or Password	Biometrics	Edit	Delete

Records per page: 10 | Add | Show Filter | Records: 1 - 4 of 4 - Pages: << << 1 >> >> >>>

[←](#) [→](#) [↻](#) www.ebioserver.com/Main.aspx

eSSL Bio Server

Dashboard | Manage | Utilities | System Users | Database Settings | API Settings | Change Password | License | Log Off

EmployeeCode	EmployeeName	Location	Role	Card Number	Verification Type			
1010	Pradeep	BLR	Normal User		Apply Group Mode	Biometrics	Edit	Delete

Records per page: 10 | Add | Show Filter | Records: 1 - 1 of 1 - Pages: << << 1 >> >> >>>

Employee Details

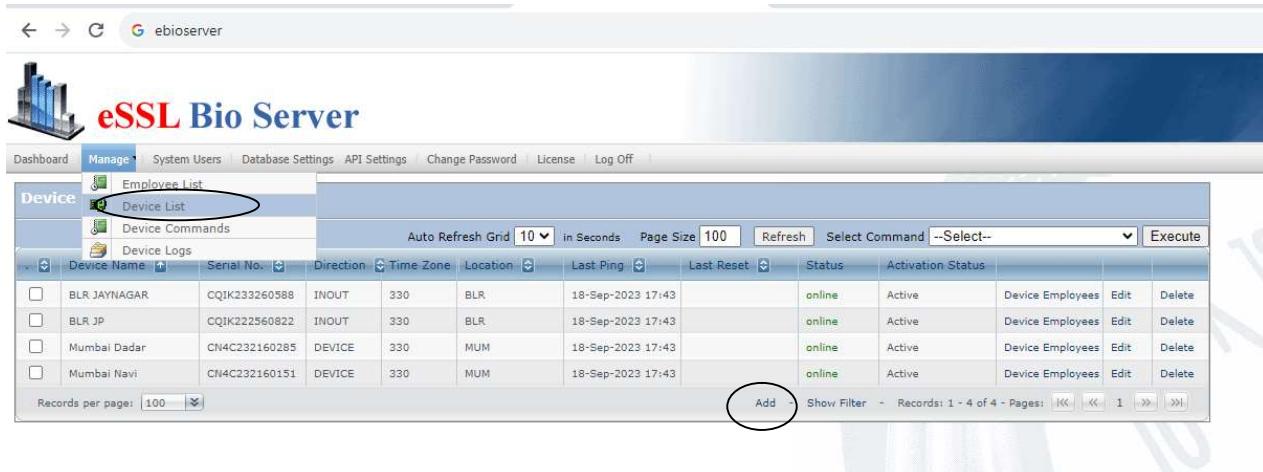
Employee Code	1123	Employee Name	Amitkumar
Location	BLR	Card Number	
Emp.Device Password	*****	Device Role	Normal User
Verification Type	Finger or Face or Card or	GroupId	1
Expiry From	2000-01-01 (yyyy-MM-dd)	Expiry To	3000-01-01 (yyyy-MM-dd)

Save **Close**

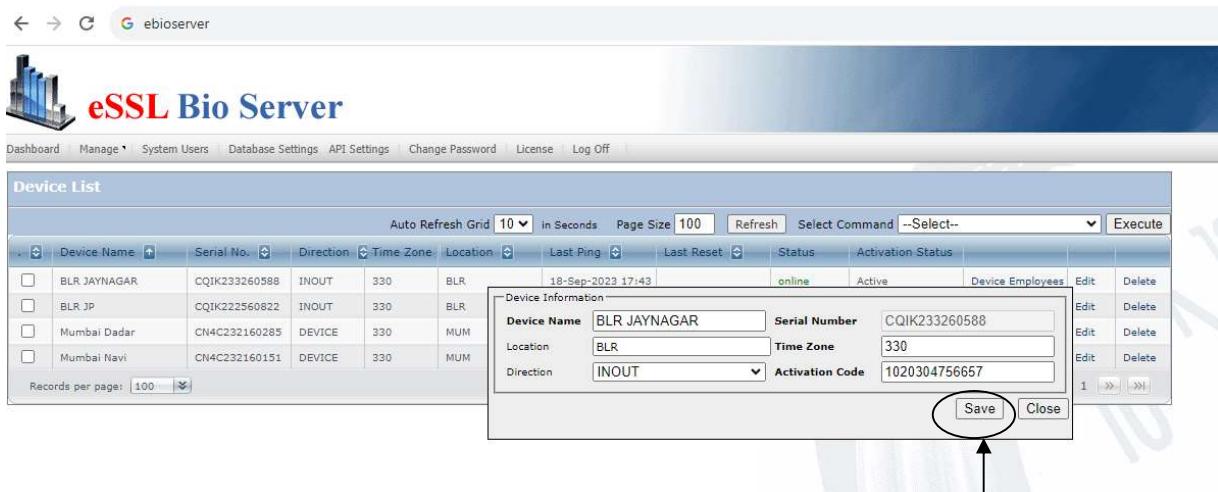
Click

Device Management:

User can Add, Edit & Delete devices



Device Name	Serial No.	Direction	Time Zone	Location	Last Ping	Last Reset	Status	Activation Status	Action
BLR JAYNAGAR	CQIK233260588	INOUT	330	BLR	18-Sep-2023 17:43		online	Active	Edit Delete
BLR JP	CQIK222560822	INOUT	330	BLR	18-Sep-2023 17:43		online	Active	Edit Delete
Mumbai Dadar	CN4C232160285	DEVICE	330	MUM	18-Sep-2023 17:43		online	Active	Edit Delete
Mumbai Navi	CN4C232160151	DEVICE	330	MUM	18-Sep-2023 17:43		online	Active	Edit Delete



Device Name	Serial No.	Direction	Time Zone	Location	Last Ping	Last Reset	Status	Activation Status	Action
BLR JAYNAGAR	CQIK233260588	INOUT	330	BLR	18-Sep-2023 17:43		online	Active	Edit Delete
BLR JP	CQIK222560822	INOUT	330	BLR			online	Active	Edit Delete
Mumbai Dadar	CN4C232160285	DEVICE	330	MUM			online	Active	Edit Delete
Mumbai Navi	CN4C232160151	DEVICE	330	MUM			online	Active	Edit Delete

Device Name

: Enter device name

Serial Number

: Enter device serial number

Device Direction

: Select device direction from drop down

Device Location

: Enter the device location name

Activation Code

: Enter the device activation code

Note: -

- Device activation code can be obtained from eTimetracklite portal
- Employee location and device location name should be same and its case sensitive

Device Commands:

This page will display the device commands list
 You can send commands to remote devices

The screenshot shows the 'Device List' page of the eSSL Bio Server. The page includes a header with navigation links like Dashboard, Manage, Utilities, System Users, Database Settings, API Settings, Change Password, License, and Log Off. Below the header is a table with columns: Device Name, Serial No., Direction, Time Zone, Location, Last Ping, Last Reset, Status, and Active. The table lists several devices: AI MUM, AI MUM2, MUM PAM NAVI, PAM, Silkbio, and X990. A context menu is open over the table, listing various commands such as Reset Transaction Stamp, Reset Operation Stamp, Get Device Logs By Date Time, Block User, UnBlock User, Enroll User Fingerprint, Enroll User Face, Clear Logs from Device, Change Webserver Address, Change Webserver Port, and Unlock Door. The 'Unlock Door' option is highlighted with a blue border.

Device Name	Serial No.	Direction	Time Zone	Location	Last Ping	Last Reset	Status	Active
AI MUM	CQIK233260588	DEVICE	330	MUM	10-Oct-2023 15:39		offline	Active
AI MUM2	CQIK222560822	DEVICE	330	MUM	17-Oct-2023 13:52	30-Sep-2023 14:30	offline	Active
MUM PAM NAVI	CN4C232160285	DEVICE	330	MUM	11-Jun-2024 14:10	11-Jun-2024 14:09	offline	Active
PAM	CN4C232160151	DEVICE	330	MUM	24-Jun-2024 15:04	11-Jun-2024 12:20	offline	Active
Silkbio	AEXY211060371	DEVICE	330	BLR	11-Jun-2024 12:43	11-Jun-2024 12:34	offline	Active
X990	BJ2C210961409	DEVICE	330	BLR	11-Jun-2024 12:42	11-Jun-2024 12:21	offline	Active

Steps to Add the device commands

- Go to device list page
- Select device commands from the list
- This command can sent to single device or multiple devices

Reset Transaction Stamp : Device will push all punch records from beginning to server

Reset Op-Stamp : Device will push all employees' data, Enrolled data to server

Get device Logs by date Time : This command will post punch records to server as set date time by user

Block user : This command will block the user access in device

Un Block user : This command will unblock the user access in device

Enroll user finger Print : This command will open FP window in device to enroll user finger Template

Enroll user Face : This command will open Face window in device to enroll user Face

Clear logs from device : This command will clear all the log records from device

Change Web Server Address : This command will set the URL or Web IP address in the device

Change Web Server Port : This command will set the Web Port number in the device

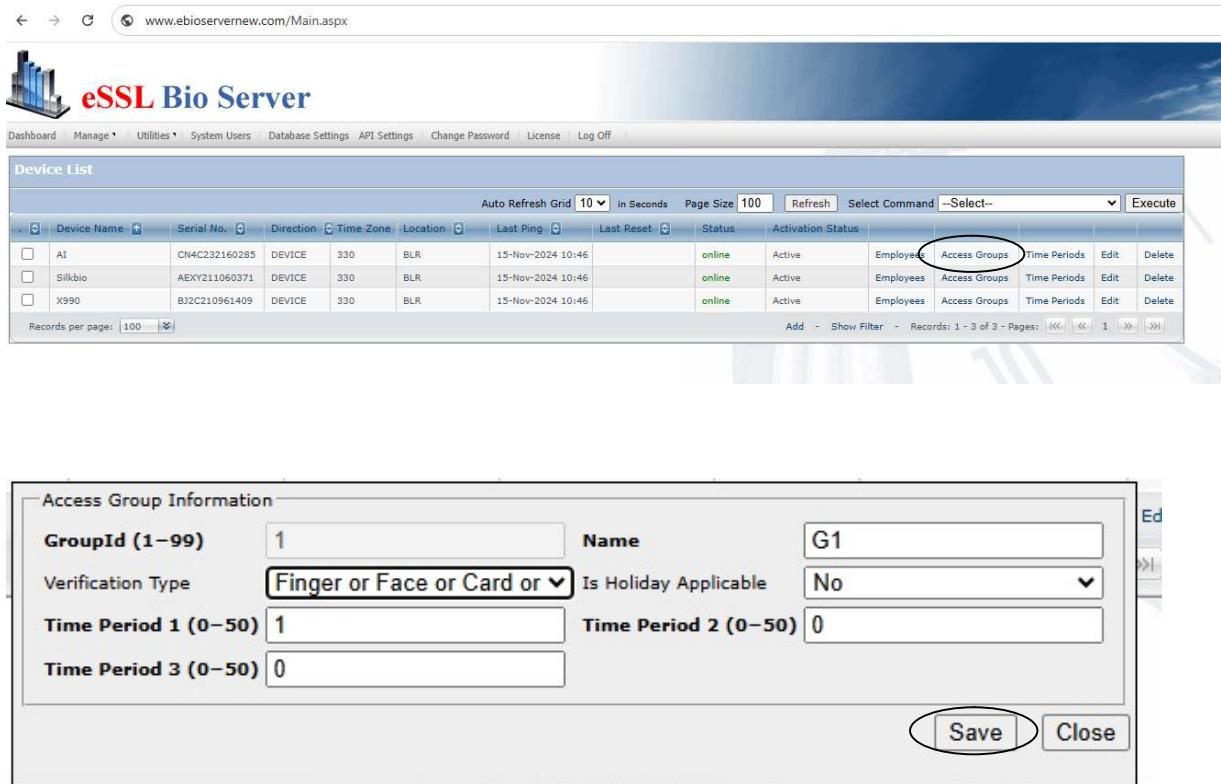
Un Lock Door : This command will Un lock the door

Note:

- a. Above commands can be sent to single device or multiple devices
- b. Device will send Employee code, Name, Password, Card Number & Finger Template
- c. Device will send Face template and Biophoto to server database

Access Groups

Users can add or update the Access Group Information from the GUI and this will reflect in remote devices



The screenshot shows the eBioserverNew web application interface. At the top, there is a navigation bar with links: Dashboard, Manage, Utilities, System Users, Database Settings, API Settings, Change Password, License, and Log Off. Below the navigation bar is a banner with the text "eSSL Bio Server". The main content area has a title "Device List" and a table with columns: Device Name, Serial No., Direction, Time Zone, Location, Last Ping, Last Reset, Status, Activation Status, Employee, Access Groups, Time Periods, Edit, and Delete. Three rows of data are listed: A1, Silkbio, and X990. The "Access Groups" column for all three entries contains a link that is circled in red. Below the table are buttons for Add, Show Filter, and pagination. In the center, there is a modal dialog titled "Access Group Information" with fields for GroupId (1-99), Name (G1), Verification Type (Finger or Face or Card or), Is Holiday Applicable (No), Time Period 1 (0-50) (1), Time Period 2 (0-50) (0), Time Period 3 (0-50) (0), Save, and Close.

Group Id : Enter group id between 1 to 99

Name : Enter group name

Verification Type : Select Verification type for the user from drop down

Is Holiday Applicable : Select Yes or No

Time Period 1 : Enter Time period value between 1 to 50

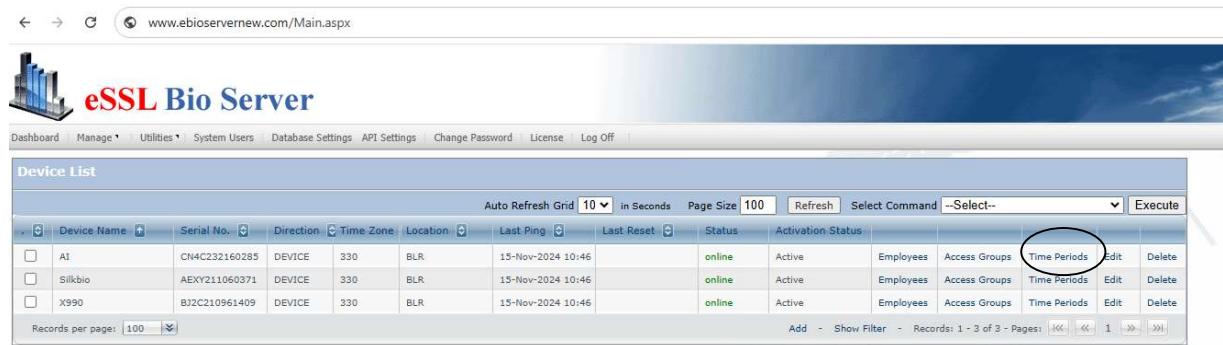
Time Period 2 : Enter Time period value between 1 to 50

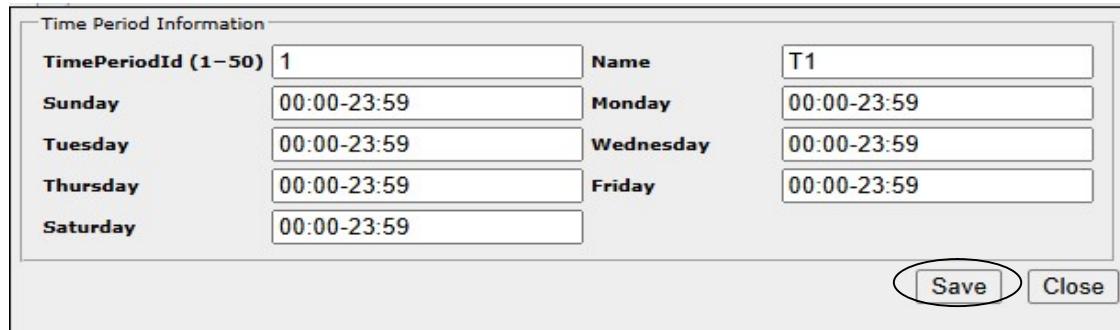
Time Period 3 : Enter Time period value between 1 to 50

Note: - You can set value “0” if you do not want to assign the time period

Time Periods

Users can add or update the Time Period information from the GUI and this will reflect in remote device





Time period Id : Enter group id between 1 to 50

Name : Enter time period name

Sunday to Saturday : Enter the time periods values for the weeks days

Note: - User should enter time values in 24 hrs format [Start Time (**hh:mm**) – End Time (**hh:mm**)]

Example: -

Sunday: - 00:01-23:59

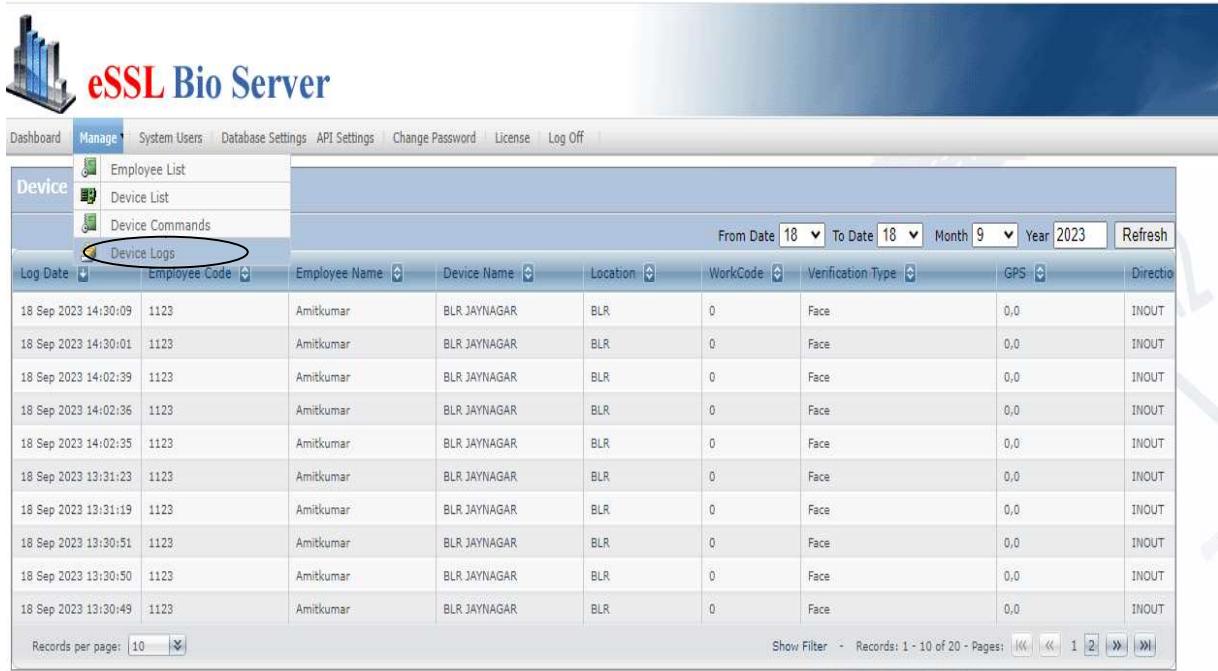
Start Time: - 00:01 and End Time: - 23:59

Monday: - 06:30-22:30

Start Time: - 06:30 and End Time: - 22:30

Device Logs:

This page will display the employee logs records downloaded from devices to the application database; User can filter log records by Employee code, name, location, date wise, device and verification type

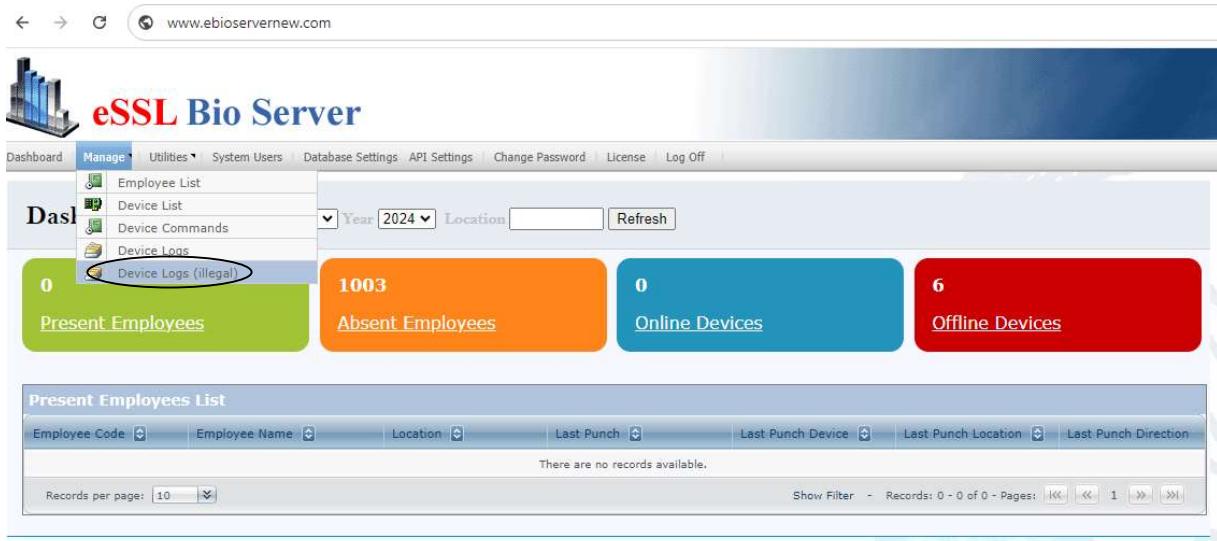


The screenshot shows the 'Device Logs' section of the eSSL Bio Server interface. The navigation bar includes links for Dashboard, Manage, System Users, Database Settings, API Settings, Change Password, License, and Log Off. The 'Device' menu is open, showing options like Employee List, Device List, Device Commands, and Device Logs, with 'Device Logs' highlighted and circled in yellow. The main content area displays a grid of log entries for an employee named Amitkumar. The columns include Log Date, Employee Code, Employee Name, Device Name, Location, WorkCode, Verification Type, GPS, and Direction. The data shows multiple entries for the same employee and device over a short period. At the bottom, there are pagination controls for 'Records per page' (set to 10), 'Show Filter', and 'Pages' (1-2).

Log Date	Employee Code	Employee Name	Device Name	Location	WorkCode	Verification Type	GPS	Direction
18 Sep 2023 14:30:09	1123	Amitkumar	BLR JAYNAGAR	BLR	0	Face	0,0	INOUT
18 Sep 2023 14:30:01	1123	Amitkumar	BLR JAYNAGAR	BLR	0	Face	0,0	INOUT
18 Sep 2023 14:02:39	1123	Amitkumar	BLR JAYNAGAR	BLR	0	Face	0,0	INOUT
18 Sep 2023 14:02:36	1123	Amitkumar	BLR JAYNAGAR	BLR	0	Face	0,0	INOUT
18 Sep 2023 14:02:35	1123	Amitkumar	BLR JAYNAGAR	BLR	0	Face	0,0	INOUT
18 Sep 2023 13:31:23	1123	Amitkumar	BLR JAYNAGAR	BLR	0	Face	0,0	INOUT
18 Sep 2023 13:31:19	1123	Amitkumar	BLR JAYNAGAR	BLR	0	Face	0,0	INOUT
18 Sep 2023 13:30:51	1123	Amitkumar	BLR JAYNAGAR	BLR	0	Face	0,0	INOUT
18 Sep 2023 13:30:50	1123	Amitkumar	BLR JAYNAGAR	BLR	0	Face	0,0	INOUT
18 Sep 2023 13:30:49	1123	Amitkumar	BLR JAYNAGAR	BLR	0	Face	0,0	INOUT

Device Logs Illegal:

This page will display the device Illegal logs records with photo pushed from devices to the server application
 User can filter log records by Date, Employee code, Employee Name, Device name and Device location name



The screenshot shows the eSSL Bio Server dashboard. In the top navigation bar, there is a 'Manage' dropdown menu. Below the navigation, there is a sidebar with links: Employee List, Device List, Device Commands, and Device Logs. The 'Device Logs (illegal)' link is circled in red. The main area displays four summary boxes: 'Present Employees' (0), 'Absent Employees' (1003), 'Online Devices' (0), and 'Offline Devices' (6). At the bottom, there is a 'Present Employees List' table with no records available.



The screenshot shows the 'Device Logs (illegal) List' page. The top navigation bar includes a 'Manage' dropdown. The main content area is titled 'Device Logs (illegal) List' and contains a table with columns: Log Date, Employee Code, Employee Name, Device Name, Location, and Photo. The table lists several log entries from May 29, 2024, to May 28, 2024, for various employees and devices. Each entry includes a 'View' link for the photo. At the bottom, there are pagination controls for records per page and a page number indicator.

Note: - Un registered user code will be “0”

Import Employees

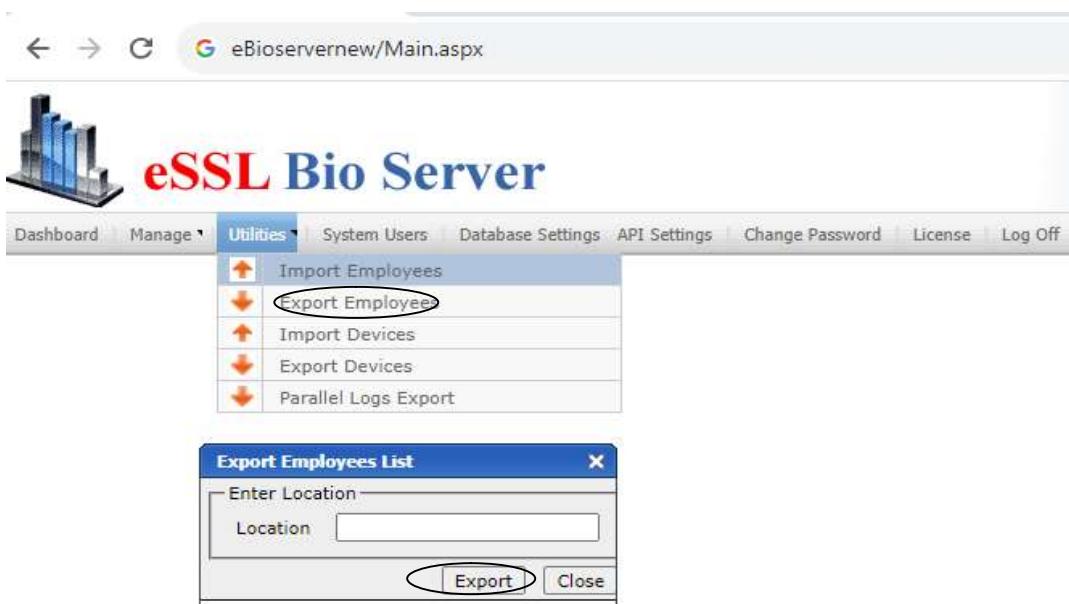
You can import employees through the csv file



The screenshot shows the eSSL Bio Server interface. The main menu bar includes Dashboard, Manage, Utilities, System Users, Database Settings, API Settings, Change Password, License, and Log Off. The Utilities menu is open, showing options: Import Employees (circled), Export Employees, Import Devices, Export Devices, and Parallel Logs Export. A sub-dialog titled "Import Employees List" is displayed, prompting the user to "Select the File" and providing a "Choose File" button (circled) and an "Import" button (circled).

Export employees

Location wise or all the location employees can be exported in the csv file



The screenshot shows the eSSL Bio Server interface. The main menu bar includes Dashboard, Manage, Utilities, System Users, Database Settings, API Settings, Change Password, License, and Log Off. The Utilities menu is open, showing options: Import Employees, Export Employees (circled), Import Devices, Export Devices, and Parallel Logs Export. A sub-dialog titled "Export Employees List" is displayed, prompting the user to "Enter Location" and providing a "Location" input field and an "Export" button (circled).

Import Devices

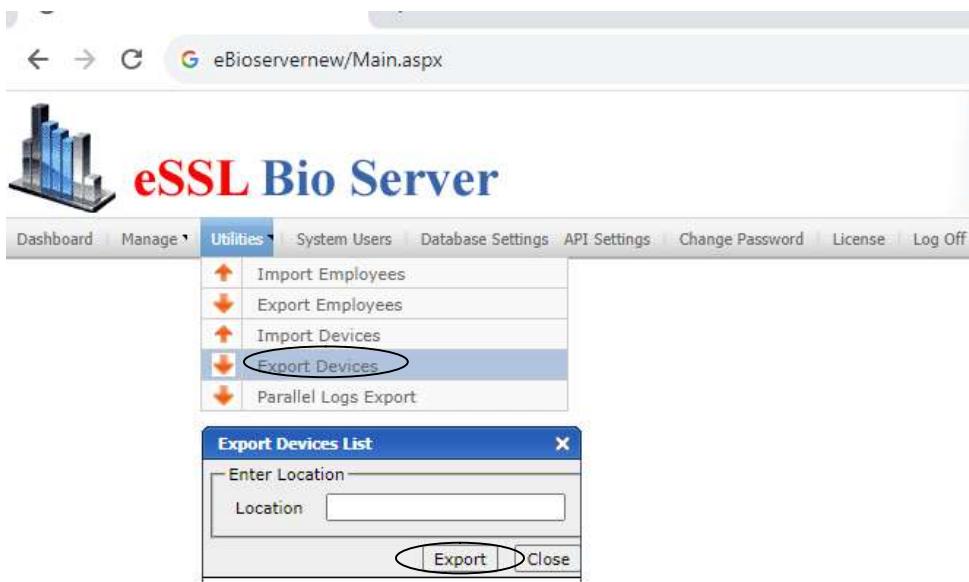
You can import devices through the csv file



The screenshot shows the eSSL Bio Server interface. In the top navigation bar, the Utilities menu is selected. Under Utilities, there is a dropdown menu with several options: Import Employees, Export Employees, Import Devices (which is highlighted with a blue oval), Export Devices, and Parallel Logs Export. A modal window titled "Import Devices List" is open. It contains a label "Select the File:" and a file input field with the placeholder "Import From" and a "Choose File" button. Below the file input is an "Import" button, which is also highlighted with a blue oval. To the right of the "Import" button is a "Close" button.

Export Devices

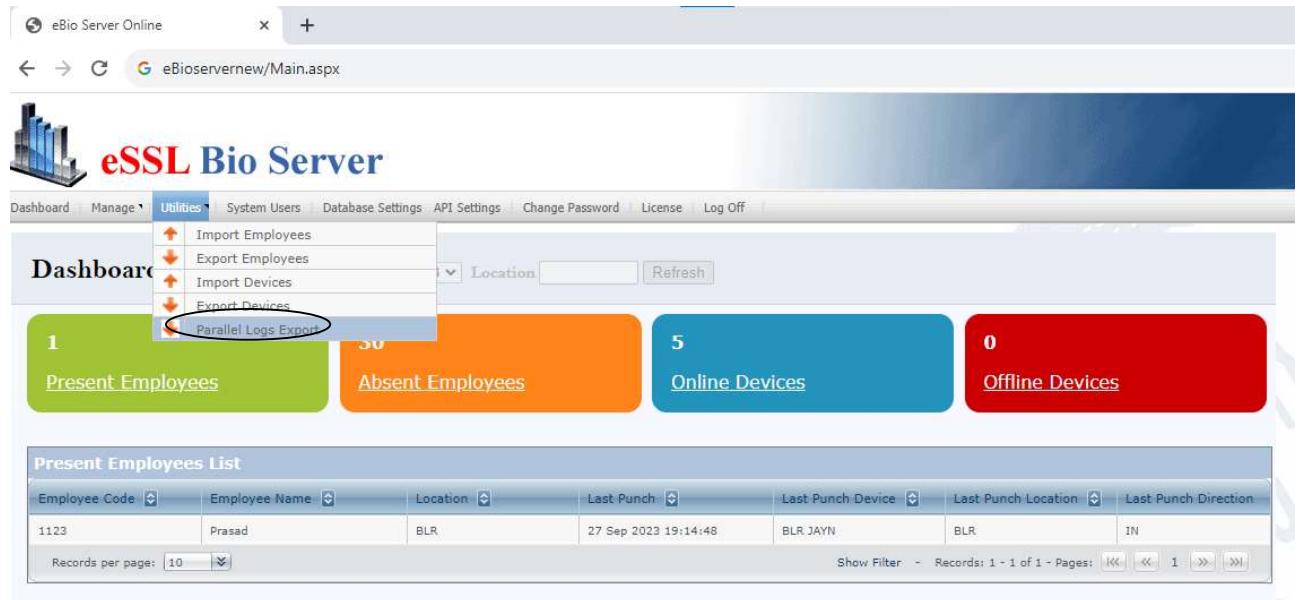
Location wise or all the location devices can be exported in the csv file



The screenshot shows the eSSL Bio Server interface. In the top navigation bar, the Utilities menu is selected. Under Utilities, there is a dropdown menu with several options: Import Employees, Export Employees, Import Devices, Export Devices (which is highlighted with a blue oval), and Parallel Logs Export. A modal window titled "Export Devices List" is open. It contains a label "Enter Location" and a text input field labeled "Location". Below the input field is an "Export" button, which is highlighted with a blue oval. To the right of the "Export" button is a "Close" button.

Parallel Logs Export :-

This will push the mapped field data to third party database



The screenshot shows the eSSL Bio Server dashboard. At the top, there's a navigation bar with links for Dashboard, Manage, Utilities (which is currently selected), System Users, Database Settings, API Settings, Change Password, License, and Log Off. Below the navigation bar, there's a sub-menu under Utilities titled "Parallel Logs Export". The main dashboard area displays four cards: "Present Employees" (1), "Absent Employees" (30), "Online Devices" (5), and "Offline Devices" (0). Below these cards is a section titled "Present Employees List" with a table showing one record:

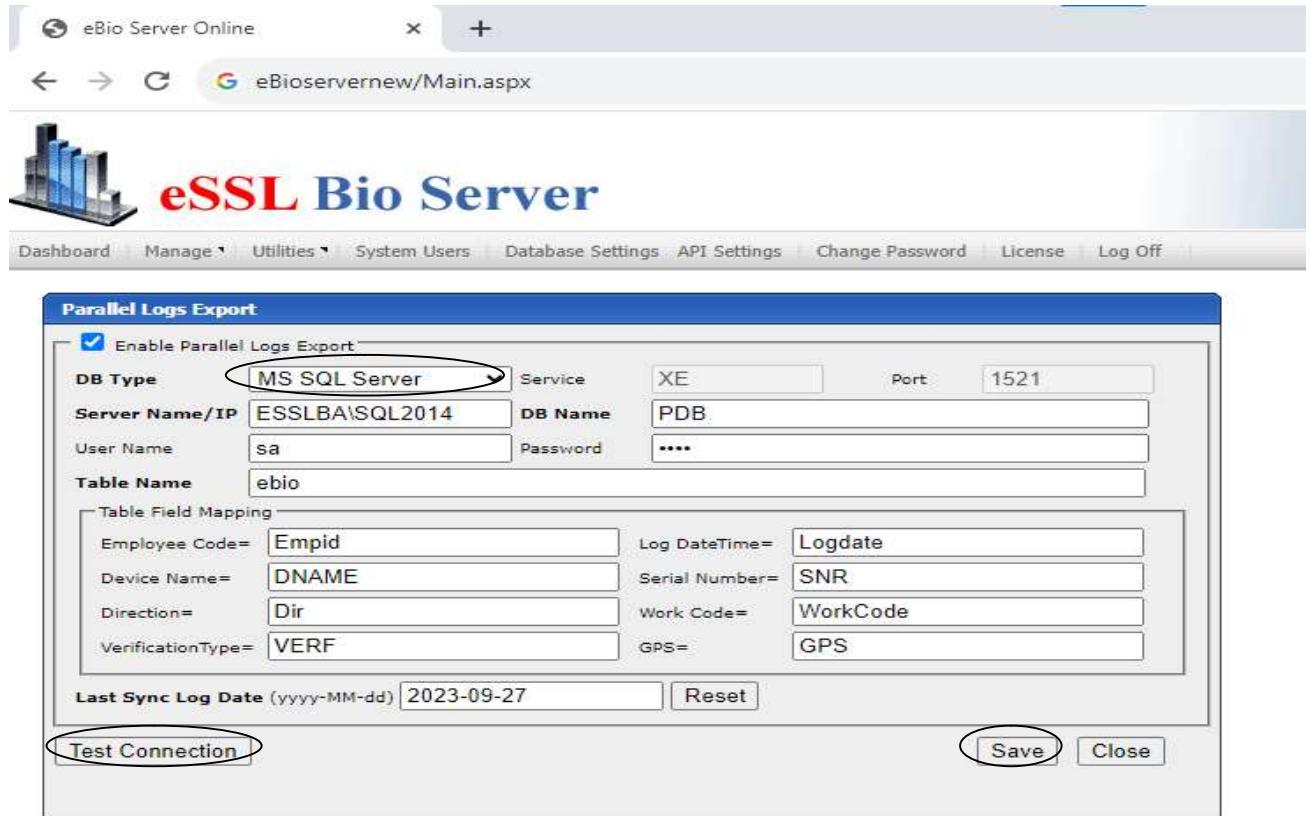
Employee Code	Employee Name	Location	Last Punch	Last Punch Device	Last Punch Location	Last Punch Direction
1123	Prasad	BLR	27 Sep 2023 19:14:48	BLR.JAYN	BLR	IN

At the bottom of the table, there are pagination controls: "Records per page: 10", "Show Filter", "Records: 1 - 1 of 1 - Pages: << << 1 >> >>>".

Supporting connections for third party database are following below

- 1) MS SQL Server
- 2) MY SQL
- 3) Oracle

1) Select Connection DB Type as MS SQL Server



The screenshot shows the 'Parallel Logs Export' configuration page. The 'DB Type' dropdown is set to 'MS SQL Server'. Other fields include 'Server Name/IP' (ESSLBA\SQL2014), 'DB Name' (PDB), 'User Name' (sa), 'Password' (****), and 'Table Name' (ebio). Under 'Table Field Mapping', fields are mapped as follows:

Employee Code=	Empid	Log Date/Time=	Logdate
Device Name=	DNAME	Serial Number=	SNR
Direction=	Dir	Work Code=	WorkCode
VerificationType=	VERF	GPS=	GPS

Below the mapping table, there is a 'Last Sync Log Date (yyyy-MM-dd)' field containing '2023-09-27' and a 'Reset' button. At the bottom left is a 'Test Connection' button, and at the bottom right are 'Save' and 'Close' buttons.

Server Name : Enter MS SQL Server Name or IP address

Login Name : Enter login name

Password : Enter the password

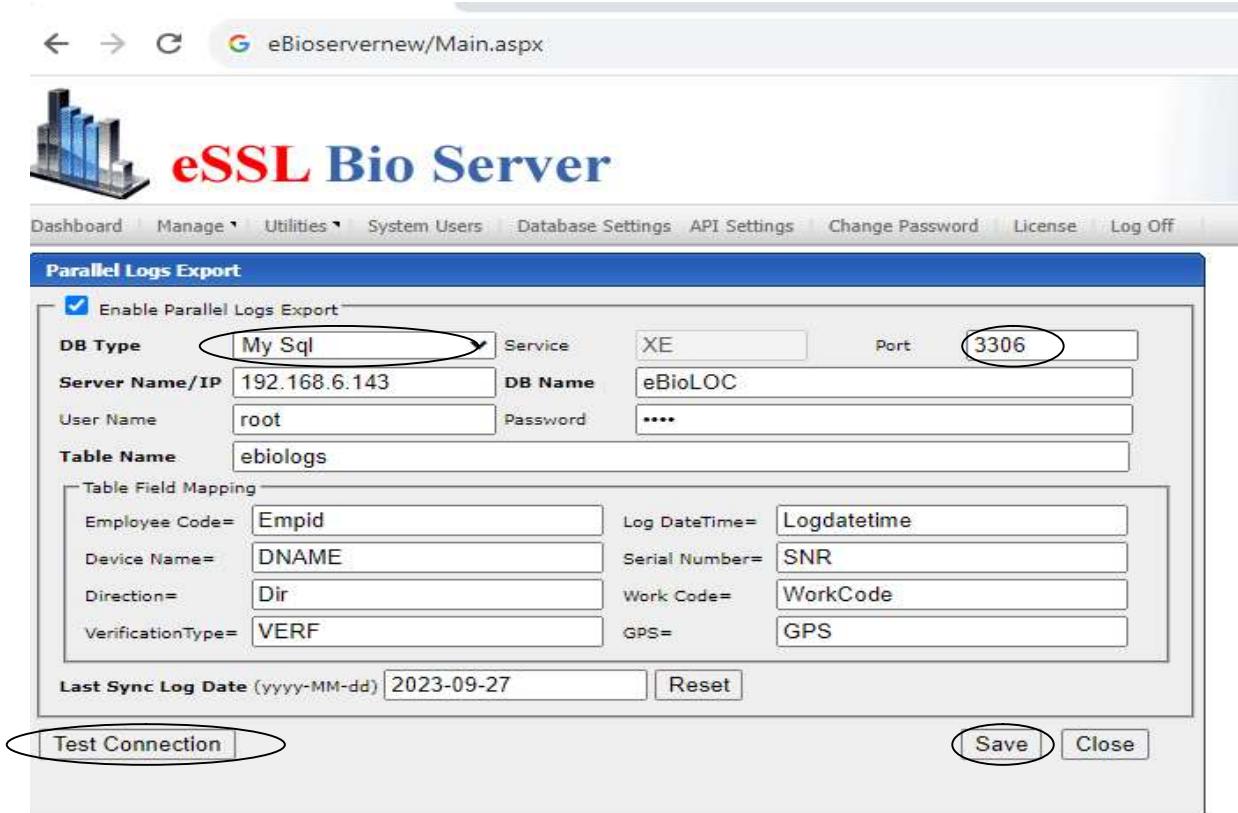
DB Name : Enter the DB name

Table Name : Enter the Table name

Map the required fields, Employee code and Log date time are mandatory fields, other fields are optional

Reset will dump the entire stored data from start date to current date time

2) Select Connection DB Type as MY SQL



The screenshot shows the 'Parallel Logs Export' configuration page. Key fields highlighted with ovals are:

- DB Type:** MySql
- Server Name/IP:** 192.168.6.143
- Port:** 3306
- User Name:** root
- Table Name:** ebiologs
- Table Field Mapping:**
 - Employee Code = Empid
 - Log DateTime = Logdatetime
 - Device Name = DNAME
 - Serial Number = SNR
 - Direction = Dir
 - Work Code = WorkCode
 - VerificationType = VERF
 - GPS = GPS
- Last Sync Log Date:** 2023-09-27
- Test Connection** button (circled)
- Save** and **Close** buttons

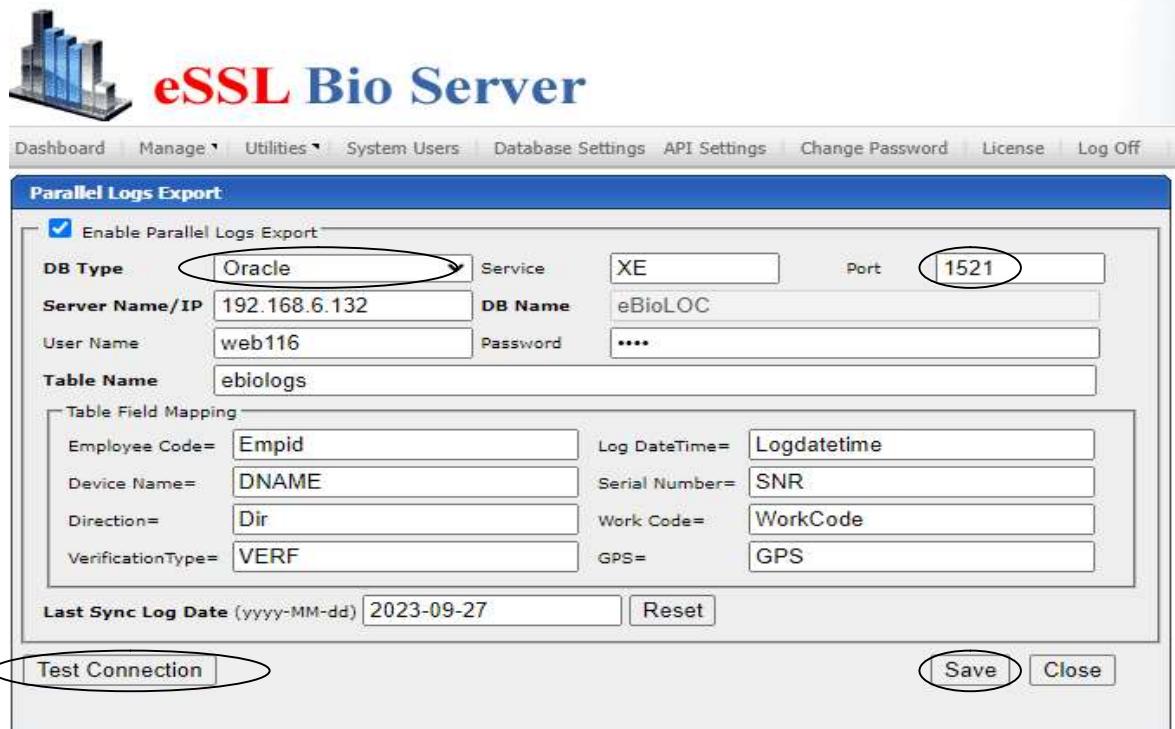
Server Name : Enter MY SQL Name or IP address
Login Name : Enter login name
Password : Enter the password
Port Number : Enter the port number
DB Name : Enter the DB name
Table Name : Enter the Table name

Map the required fields, Employee code and Log date time are mandatory fields, other fields are optional

Reset will dump the entire stored data from start date to current date time

3) Select Connection DB Type as Oracle

← → C eBioservernew/Main.aspx



The screenshot shows the 'Parallel Logs Export' configuration page. Key fields include:

- DB Type:** Oracle (circled)
- Server Name/IP:** 192.168.6.132
- Service:** XE
- Port:** 1521 (circled)
- User Name:** web116
- DB Name:** eBioLOC
- Password:** ****
- Table Name:** ebiologs
- Table Field Mapping:**

Employee Code=	Empid	Log DateTime=	Logdatetime
Device Name=	DNAME	Serial Number=	SNR
Direction=	Dir	Work Code=	WorkCode
VerificationType=	VERF	GPS=	GPS
- Last Sync Log Date (yyyy-MM-dd):** 2023-09-27
- Buttons:** Test Connection (circled), Save, Close

Server Name : Enter Oracle Name or IP address

Login Name : Enter login name

Password : Enter the password

Port Number : Enter the port number

Table Name : Enter the Table name

Map the required fields, Employee code and Log date time are mandatory fields, other fields are optional

Reset will dump the entire stored data from start date to current date time

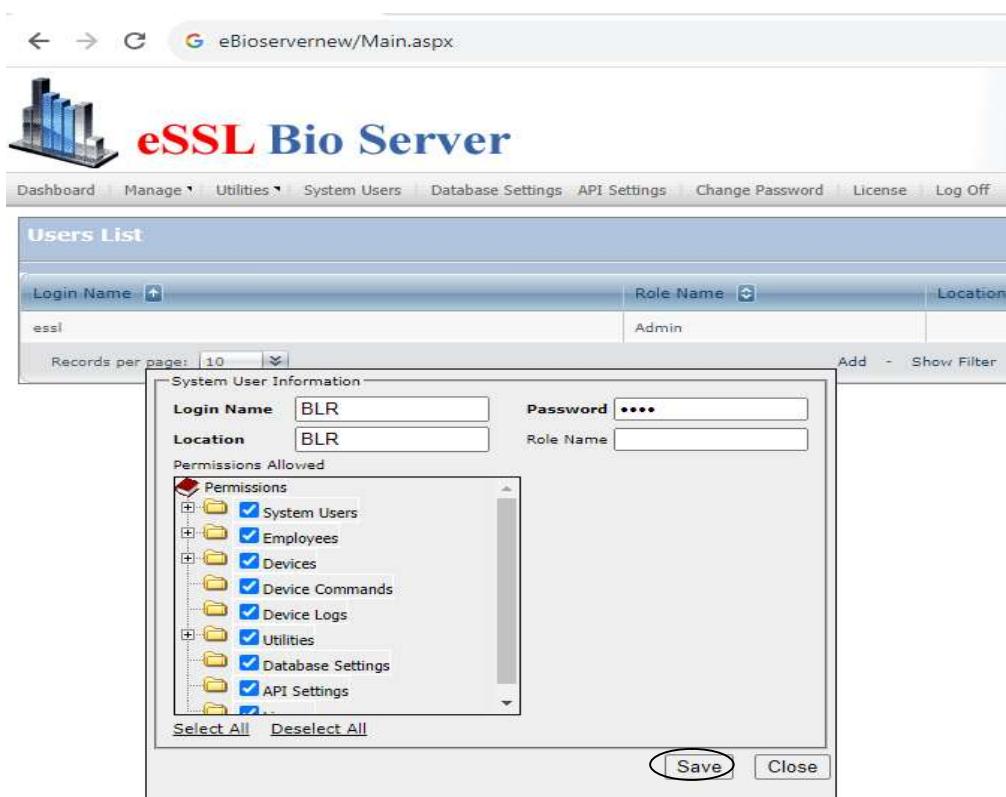
System Users

This form will display the System users list of the application; you can Add, Edit & Delete the users



Login Name	Role Name	Location	Edit	Delete
BLR		BLR	Edit	Delete
essl	Admin		Edit	Delete
mumbai		MUM	Edit	Delete

Click on Add users



System User Information

Records per page: 10

System User Information

Login Name: BLR Password: ****

Location: BLR Role Name: Admin

Permissions Allowed

- System Users
- Employees
- Devices
- Device Commands
- Device Logs
- Utilities
- Database Settings
- API Settings

Select All Deselect All

Save Close

Login Name : Enter the user login name

Password : Enter the user Password name

Location : Enter the user location name

Set the Permission like View, Add, Edit and Delete for

- System users
- Devices
- Employees

Note: - User can access only employees and devices of particular location and Admin access all location of the employees and devices

API Settings

Set the user name and password to access the API



URL name of the host server and followed by forward slash webservice.asmx

e.g. www.eBioserverNew/webservice.asmx

The screenshot shows a web browser window for 'www.eBioserverNew/WebService.asmx'. The address bar shows the URL. The main content area has a dark blue header bar with the text 'WebService'. Below the header, a message states: 'The following operations are supported. For a formal definition, please review the [Service Description](#)'. A bulleted list of supported operations follows:

- [DeleteEmployee](#)
- [GetDeviceIllegalLogs](#)
- [GetDeviceList](#)
- [GetDeviceLogs](#)
- [GetEmployeeCodes](#)
- [GetEmployeeDetails](#)
- [GetEmployeePunchLogs](#)
- [UpdateEmployee](#)
- [UpdateEmployeeEx](#)
- [UpdateEmployeePhoto](#)
- [UpdateEmployeewithExpiryDates](#)

Database Settings

You can save the database settings

localhost:92/Main.aspx

eSSL Bio Server

Dashboard Manage Utilities System Users **Database Settings** API Settings Change Password License Log Off

eBioServer Database Settings

MS SQL Server Database Settings-

Database Type	MS SQL Server
Database Server	localhost
Database Name	eBioServerNew
Authentication Type	Sql Server Authentication
User Name	sa
Password	*****

Test Connection **Save** **Close**

Server Name : Enter MS SQL Server Name or IP address

Login Name : Enter SQL login name

Password : Enter SQL Password

DB Name : Enter the DB name

Change Password



Old Password : Enter the old password

New password : Enter the new password

Confirm Password : Reenter the new password

License key

eBioserver license key can be obtained from eTimetracklite portal

