User Guide

BigLan Network Monitoring System

Content

Introduction

BigLan is a network management system designed primarily for medium to large internal networks. It aims to help system administrators and network engineers manage poorly or completely undocumented networks and devices. The system is used to map and monitor the network and keep the device inventory up to date.
BigLan is built from two main parts: a server (e.g. Ubuntu 24.04, Apache, MySQL) and client-side service applications. The client applications send data to the server, which creates a record and allows inferences to be made about the state of the endpoint devices and the network from the events.

Main features

Device Inventory: The software keeps track of computers, laptops, servers, network devices, and network printers.

IP Table: Automatic registration of IP addresses prevents network infrastructure errors and accurate registration improves efficiency.

Event Monitoring: Tracks events related to computers and network printers, such as errors, hardware changes, warnings, and status changes.

Data protection: The utility running on workstations monitors and immediately reports connections to P'n'P devices with storage capacity (Pendrive, Mobile Phone, External HDD) connected to the workstation, as well as applications enabling remote connections (AnyDesk, Teamviewer, RDP, VNC).

Interactive Topology: Creates an interactive network topology with minimal human intervention, showing the devices connected to the endpoints, their connections, and their status in real time.

Notifications: The software monitors specified events, such as SNMP status changes, port or IP address availability, server services, external sensors, and network outages by

continuously monitoring workstations. The system sends an immediate alert when the specified conditions occur.

Remote Execution: Through an encrypted connection, it is possible to run PowerShell scripts and cmd commands on Windows clients individually or in batches at a time. This allows for mass installation of software packages, performing various operating system modifications, or querying information without interrupting work on the workstation.

Documentation and supporting materials: It is possible to store documents and create blog-like supporting materials about professional experiences.

Intervention Log: Users are given the opportunity to create entries for each intervention they perform. These entries allow them to document the actions they take, add comments, and share their experiences with other users.

Dashboard: The main page always focuses on current events on the network, such as events related to endpoint devices, current statistics on individual device groups, and intervention recommendations to optimize and develop the IT infrastructure.

Platform-independent: The software has a utility that can be installed on Windows and a bash script version that can be installed on Linux, which run as a service.

Multilingual: Users can use the software in different languages.

Uploading data

Workstations: Workstations can be recorded manually or automatically.

- **Manually recording workstations:** A workstation can be created manually by clicking the *Workstations->New workstation* button.
  The following form fields must be filled in at least:
- **Name:** A freely selectable name that refers to the location or use of the device. For example: *Building B - 3rd floor - Office 12 - Accounting – Someone's machine*
- **Hostname:** The computer name registered in the operating system. For example: *DESKTOP3892*
- **Device type:** Desktop, laptop, server.

It is advisable to fill in for more accurate registration:

- **Serial number:** By entering the serial number, you can keep a more accurate device record. If the BigLan utility is later installed on the device, the utility will identify it based on the manually recorded serial number and automatically complete the data already entered.
- **IP addresses:** By recording IP addresses, BigLan automatically registers already occupied network identifiers.
- **Operating system:** Operating systems are automatically registered when you register them.
- **Processor, memory, disks:** For efficient work later, automated filters can be assigned to this data and necessary actions can be listed, for example, regarding the obsolescence of a hardware element.

Installing BigLanService: By installing the BigLanService utility, workstations will automatically submit the necessary data for registration to the server and start monitoring important events.

- **Windows computers:** BiglanService Installer works on Windows 7 Service Pack 1 with .NET Framework 4.8+ or later Windows systems.

When starting the Installer, you must provide the following information:

- Server availability (https://[SERVER IP ADDRESS or DOMAIN]/api/v2/)
- Installation type (alpha/beta)
- API Token
  API Token can be generated in Biglan->Personal Menu->API Tokens.

Registering network printers: Network printers can be registered by clicking the *Network Printers->New Network Printer* button. After registration, BigLan attempts an SNMP query on the device to obtain additional information about it. It is important that for this, the *SNMP read community* used must be specified *in Toolbox->Global Settings*, and SNMP query must be enabled on the device on port 161. The *SNMP read community is public* by default.

After connecting the network printer to the network and completing the network configuration, the following information is required:

- **Name:** A freely selectable name that refers to the location or use of the device. For example: *Building B - 3rd floor - Office 12 - A3*
- **IP address:** IP address set on the device.

Registering a network device: Network devices (switch, router) can be registered by clicking the *Network Devices->New network device* button.

When registering a network device, the following information is required:

- **Name:** A freely selectable name that refers to the location or use of the device. For example: *Building B - 3rd floor - Large switch*
- **Serial number:** The serial number found on the device or read from the device.
- **Number of ports** : The number of copper or optical ports on the device.

Specifying network connections: Network connections can be recorded by clicking the *Topology* menu item.
To connect two devices:

- right-click on the source device
- in the menu that appears, select the type of physical connection: UTP (copper), Optical single-mode, Optical multi-mode
- left-click on the device you want to connect to
- a line appears indicating the connection between the two devices

Dashboard

The Dashboard can be divided into 3 main areas

- Information blocks
- Event Log and Interventions
- Suggested interventions

Information blocks

- **Workstations**
  - Powered on: workstations that are currently running.
  - Locked: workstations that are up and running but not currently in use.
  - Unavailable: The workstation was powered on, but has not shown any signs of life for more than 121 seconds.
  - Off: workstations that are not currently turned on.
- **Security risks**
  - IP conflict: workstations with the same IP address.
  - MAC conflict: workstations with the same MAC address.
  - Teamviewer: You are currently connected to the workstation using TeamViewer.
  - AnyDesk: You are currently connected to the workstation using AnyDesk.
  - RDP: you are currently connected to the workstation via RDP.
  - VNC: you are currently connected to the workstation using a VNC program.

    - USB: A USB device with storage capacity is connected to the workstation.
- **Network printers**
    - Supplies Ordering: You can specify the availability of a website *in Global Settings*, which, when clicked, will open the website most often used to order supplies in a new window.
    - <=5%: The amount of ink or toner in the printer is less than or equal to 5%.
    - <=10%: The amount of ink or toner in the printer is less than or equal to 10%.
- **Notifications** (per user, freely selectable): By clicking on the *Add Block area, you can select* 5 supervisions recorded in the *Supervision Center , the status and value of which will be displayed in this block.*
- **Links** (per user, freely selectable): By clicking on the *Add Block* area, you can enter the names and links of 5 websites, which will open in a new window when clicked. This is essentially a bookmark function.

Event Log: This tab shows the events that occurred in the last 15 seconds on desktop, laptop, and server devices.

Interventions: Interventions (works) recorded by users in the last 30 days are listed here, grouped by day.

Recording a new intervention: By clicking on the *magnifying glass icon* in the lower right corner of the screen or by double-pressing the *CTRL key, a search window will appear. Here you can enter the name of the workstation on which the intervention took place. By right-clicking on the selected workstation, you must select the Record Intervention* menu item. In the new pop-up window, you can specify the intervention performed, select the users performing the intervention, specify the duration of the intervention, and whether it is an intervention performed in Standby. The *Save icon at the right end of the field can be used to save the intervention text, so that it appears as an automatic suggestion the next time you type. Automatic suggestions can be deleted with the x icon* at the end of the current line .

Suggested actions: The Workstations->Create Filter button allows you to perform various filters on the recorded workstations. These filters are saved and the number of workstations that match the filter is displayed on 1 card. The role of the cards is to allow users to see a list of workstations that match their various projects.

IP Table

The IP Table menu item displays a list of manually recorded subnets. Clicking on them will list the IP addresses belonging to each subnet.

By pressing the New Subnet button, a new subnet can be created. It is mandatory to enter its name, ID, mask and gateway.

For each IP address, you can use the edit icon to enter the name of the device that uses the IP address. The IP addresses of computers with BigLanService and fixed network printers are automatically filled in.

Notification Center

The Notification Center monitors the monitored devices and services every minute based on the specified criteria.

Types of supervision:

- **Ping:** At least 50% of packets must successfully reach the specified IP address. Otherwise, an alarm will be triggered.
- **Socket Polling:** The goal is to successfully access the port of the specified IP address. Otherwise, an alarm will be triggered.
- **Sensor Value:** The arithmetic expression or comparison specified in Parameters must be true. Otherwise, an alarm will be triggered.
- **BigLan command:** The arithmetic operation or comparison (expression) performed on the result of the specified Command (command) on the workstation with the identifier (wsid) specified in the Parameters must be true. Otherwise, an alarm will be triggered.
- **SNMP:** The arithmetic expression or comparison specified in Parameters must be true for the value of the OID code queried at the specified IP address. Otherwise, an alarm will be triggered.
- **HTTP Status Code:** The arithmetic expression or comparison specified in Parameters must be true. Otherwise, an alert will be raised.
- **Mass Heartbeat Loss:** The number of workstations that become unreachable in the same 2 minutes must be less than the number specified in Parameters. Otherwise, an alarm will be triggered.

Monitoring of the specified Notification can be turned on/off.
Alerts are sent to the Telegram channel specified in the Global Settings->telegram-bot-token parameter.

By clicking the Notification Event Log button, you can review what alarm and recovery events have occurred. If the Monitoring type is ping or socket polling, an automatic nmap command will also be run in the event of an alarm, helping to detect the error.

When managing many services and devices, the Dashboard view provides a more clear interface.

When a monitoring is deleted, an archive HTML file is created, which can be viewed under the Documents menu item.

Topology

IMPORTANT! To enable this feature, create at least one network device and add at least one workstation.

Topology is a visual representation of the logical structure of a local network. The topology is interactive, with the status of workstations updated in real time.

To establish or delete a connection between individual devices, right-click on the device and select the desired action from the context menu that appears.

Some of the Topology tools can be disabled for better visibility using the checkboxes at the top of the page.

The Topology can be exported in GEXF and SVG format for other uses using the dedicated buttons.

Command Center

BigLan has a feature that allows you to run Windows command line commands or Powershell scripts directly from the browser on the target workstation. See: Workstations->Console

Using this capability, workstations query the server when the device is turned on and every 30 minutes thereafter to see if there are any commands that need to be downloaded and executed.

After execution, the workstation sends the result back to the server for storage.

In the Command Center, only previously run and saved commands can be executed by workstations.

You can create a new command by pressing the New Command button.

You need to select the one to be executed from the predefined scripts, assign the workstations that you want to download and execute the script to, and set a date and time later than the current one.

After saving, the workstations automatically download and execute all scripts assigned to them in the next 30 minutes and send the results of the run back to the server.

The execution of commands can be stopped with the Emergency Stop button if its effect adversely affects the workstations or its further execution becomes unnecessary.

The results of running the scripts on each workstation can be viewed by clicking the Details button.

By clicking the Script Storage button, you can review the contents of each script, and by clicking the Delete button, you can remove them from the database.

KnowledgeBase

The essence of the Knowledge Base is to organize the experiences gathered during work and make them searchable later. The articles created here can be sorted into categories, which makes it easier to find descriptions and guides related to specific topics.

Articles created in the Knowledge Base can be modified later. The previous version will be saved and the latest version will always be available.

You can write comments for each article.

Documents

The purpose of Documents is to collect various user, developer documentation or other documents (e.g. delivery/acceptance receipt, etc.) in one place.
By entering keywords, documents become easier to search. Documents that become redundant or obsolete over time can be deleted, but they are not destroyed, they are just transferred to the Archive, where they remain accessible.
Archived workstations, network printers, network devices, and monitoring are also added to Documents in HTML format.

Workstations

Workstation: collective term. Any device that is suitable for running BigLanService (Server, PC, Laptop, etc.).

All devices that are created automatically or manually using BigLanService are listed under the Workstations menu item.

You can open each workstation by clicking on its name in the list, where detailed information about it is available.

- Workstation name: by clicking on edit, you can change the name of the workstation (e.g.: Building B - 1st floor - Office 3 - Workstation 12)
- WSID: the workstation's unique identifier according to BigLan (abbreviation of **W**ork**S**tation**ID**).
  A workstation's WSID remains until the end of the device's life cycle (disposal). In case of reinstallation, the server always identifies the workstation based on the identifiers sent by BigLanService. 4 pieces of data are used for identification:
    - Product serial number
    - Motherboard serial number
    - UUID
    - Primary MAC address (onboard eth/wifi/bluetooth)

At least 1 of the 4 pieces of data (25%) must be completely unique. If this condition is not met, the device cannot be automatically added to the database because it will be rejected by the server.
A device whose identifier appears in the database 0 times at least once is recorded as a new workstation.

- Inventory ID: For easier and faster inventory, the inventory ID of the workstations can be specified.
- Data sheet: This is where you can find the basic data for the workstation.
    - Identification data (Product serial number, Motherboard serial number, UUID, Primary MAC address)

    - Brand, Model
    - Device type: Desktop, Laptop, Server
    - Memory
    - Monitors (inventory numbers can be specified individually)
    - Disks (SSD, HDD, Other)
    - Tags: additional information important for categorization can be recorded regarding the workstation (e.g. “Virtual”/”Physical” in the case of a server, or “Device with warranty until 2028”, etc.)
    - Local user accounts
    - Processor (CPU BenchMark and processor release time must be manually entered when registering a new workstation. CPU Benchmark value is automatically updated on the 2nd of every month, ensuring device up-to-dateness.)
    - Operating system
    - Boot data
    - OS partition data
    - IP addresses and DNS addresses
    - Connected printers (fixed connection method, default setting, sharing status)
- Events: Here you can track events sent by BigLanService. Scroll down to see the older events section, which are continuously loaded. New events appear live, automatically.
- Interventions: Interventions can be recorded for workstations. These are jobs that are performed in relation to the workstation or its environment.
- Contacts: Virtual or physical contact information can be recorded for workstations
    - RealVNC: Workstation IP address and VNC port (If RealVNC viewer is installed, a connection to the workstation can be initiated by clicking the button)
    - AnyDesk: AnyDesk ID number
    - Teamviewer: Teamviewer ID number

    - Phone number: The closest landline or mobile number to the workstation. (In mobile view, the number can be dialed directly)
    - Email: Email address of the workstation users
    - Location: Physical address (e.g.: City, street, house number, floor, door)
    - URL: website address
- Console: This function allows you to send directly executable Windows cmd commands and PowerShell scripts to a computer running Windows operating system that is in the same subnet as the server (LAN), and the result is immediately received after execution. Its operation is similar to the command line, however, in the case of powershell scripts, it is also necessary to specify output (e.g.: " [*SCRIPT]* | *Format-Table -AutoSize* | *Out-String* "). This is necessary because BigLanservice executes the commands/scripts in windowless mode. Another difference when using scripts is that line breaks are not allowed, i.e. the end of a line must be closed with a semicolon ";" and the script must be continued in this way. Before running, the browser window always asks whether you really want to run the given script.

  IMPORTANT!

  Scripts can only be executed on workstations if a combination of 32 characters, letters and numbers, has been specified for the MASTER_KEY variable during installation or later in the BigLan configuration file (.ENV).

  This key ensures that the 256-bit key generated and sent by the workstations in the database when BigLanService is started is stored encrypted on the server. Without this, the server cannot communicate with the workstations directly.
- Network: You can specify which network device the workstation (as an endpoint device) is connected to within the transport network.
- Printouts: Daily statistics are generated from workstation prints.
- Actions: The workstation and its related data can be deleted from the database by clicking the Archive button. An HTML page is created from the deleted data, which can be retrieved if necessary under the Documents menu item.

Network printers

The Network Printers menu item lists the printers that have previously been manually registered and are capable of network communication.
To register a new printer, you must enter its name and IP address.
When registering a network printer, the server initiates SNMP queries and fills in additional available information about the printer. (e.g. Brand, Model, MAC address, toner level, etc.)
Statistics are generated on the toner levels and printed page counters of network printers, for which data is requested on a scheduled basis, every day at 10:00. Only data from printers that are in the same subnet as the server can be requested in this way.
If the latest data is needed, the “update data” button will immediately query the network printers.
IMPORTANT!
If the read community on the devices is not the default “public”, then the name of the read community to use must be specified in the Global Settings.
Clicking on the Network Printer will display its data sheet. This contains the most important data about the printer, where you can Archive the device, and under the statistics tab, you can view the typical toner consumption and the number of pages printed in the last 30 days.
Based on the toner consumption recorded over the past 30 days, the server estimates how long the toner/ink will last. This helps you plan your supplies orders more effectively.
If the network-printer-supply-order-link value is filled in the Global Settings, a supply order link will appear in the Dashboard->Network Printers section.

Network devices

Network devices form the basis of the local network in the Topology. Additional network devices and endpoint devices are connected to them.
To register a new network device, you must specify its name, brand, serial number, IP address and/or MAC address, type, and the number of available ports. As an optional parameter, you can also specify the speed of each port.
All information can be found on the data sheet of a network device, and operations can also be performed here.
In the case of Archiving, the network device and its related data are deleted from the database and an html file is created in Documents for later retrieval.
Deactivation and activation can be used to turn off the visibility of a network device in the Topology. When deactivated, its network connections are deleted and any additional network and endpoint devices assigned to it are placed outside the Topology (floating) until they are assigned to a new device.
Some parameters of network devices can be edited later by double-clicking on the corresponding cell in the list view. The changed information can be saved by pressing the Shift+Enter keys simultaneously. The editing can be exited without changing the information by pressing the Esc key.

Operating Systems

The Operating Systems listing page collects data from workstation information submitted by BiglanService and manually recorded.
In each row, you can view the number of workstations running the given operating system, summarized by type and version.
If you manually enter the operating system support date, operating systems with expired support will be highlighted.
The operating system collection is automatically updated every day or can be updated immediately using the Collect Data button.

Monitors

The Monitors menu item lists the display devices connected to each workstation. It allows you to view the type, age, and serial number of the devices.
This information can help you scrap or inventory your assets.

Local printers

The Local Printers menu item lists local or network printers installed on workstations.

My settings

In the My Settings menu, you can change the language and appearance of the page (dark/light).

Global Settings

Important settings that affect the entire site can be set in Global Settings.

- enable-notifications: This setting allows you to specify whether to send an alert for events recorded in the Monitoring Center. This setting turns all notifications on and off at once.
  When disabled, no notifications are sent, but enabled events are still logged.
- enable-registration: This setting controls whether or not registration is allowed on the BigLan server. Unless you expect new user registration, it is a good idea to keep this setting disabled.
- exclude-admin-username-list: If the main page is filtered for workstations with local administrator accounts, this setting allows you to specify which account names BigLan should not take into account. Each account name must be separated by a comma.
- network-printer-supply-order-link: If set, a “Supply Order” will appear in the Network Printers block on the Dashboard. The link will open in a new window.
- snmp-read-community: In case the network printers do not use the default “public” read community, the value to be used can be specified here.

- telegram-bot-token: To alert the Notification Center, a Telegram room must be created and its bot token must be inserted here so that BigLan can send alerts and recoveries about monitored events.

Downloads

In Downloads, you can upload files that may be needed for installation on individual workstations (e.g. printer drivers, Office, etc.). If file access is set to public, the files will be publicly visible via the BigLan URL and can be downloaded on the given workstation. Files that are not public can only be viewed and downloaded after logging in.
The files are stored in the /storage/downloads folder.

Updates

The page can be sent to workstations, listing BigLanService updates by channel and version number.

- a: Windows-based workstations, extensive update
- b: Windows-based workstations, limited update

Workstations check for updates every time they start up and every 30 minutes while they are on.
Updates are stored in the /storage/updates folder.

Updates must be activated after they are uploaded. Only then will they begin to be distributed. In case of an error, the update can be rolled back. If the update has not yet been downloaded by any workstation, it can be deleted. After the first download, an update cannot be deleted, only undone.
Workstations will only download updates with a version number higher than the current one.

API Tokens

In the API Tokens menu, tokens can be created to authenticate communication with Workstations or Sensors. This token must be provided to the technician during workstation installation or sensor configuration manually. All messages sent by the workstation or sensor must contain the token. Otherwise, the message will be rejected.

Tokens are stored encrypted in the database, encrypted with the unique key specified in the .env file (MASTER_KEY).

Tokens can be tied to a maximum number of uses or an expiration date, or can be manually revoked at any time for invalidation.

The Windows Agent asks for the token during installation. The token is stored encrypted using Windows DPAPI, tied to the specific hardware.

Users

Authorized users (e.g. the first user) can manage the access permissions of individual users.
You can also view the log of each user's system-related activities here.
When a user registers on the server, their user account is inactive and unchecked by default. The system administrator or an authorized user can approve and verify the user's account. Only then can a newly registered user log in to the system.