



INTEGRUM

**Security Systems
Management Software**

Installer manual

Version 3.1

integrum_i_en 11/24

SATEL sp. z o.o. • ul. Budowlanych 66 • 80-298 Gdańsk • POLAND
tel. +48 58 320 94 00
www.satel.pl

SATEL aims to continually improve the quality of its products, which may result in changes in their technical specifications and software.
Current information about the changes being introduced is available on our website.

Please visit us at:
<https://support.satel.pl>

The following symbols may be used in this manual:



- note,



- caution,



- operating system shell command,



- press Enter.

CONTENTS

1. Introduction.....	2
2. Software components.....	3
3. System architecture.....	4
4. Network requirements	5
5. Minimum hardware requirements	6
6. Installing the operating system	7
7. Installing the server environment.....	8
8. INTEGRUM system installation and update	11
9. Programming the settings.....	16
9.1 INTEGRUM-WEB application.....	16
9.2 INTEGRUM-APPSERVER application	17
10. Installing the Windows Server – Hyper-V platform	18
11. Useful commands.....	20
11.1 Verification of hardware requirements.....	20
11.2 Checking the container status	20
11.3 Collecting logs from system services and INTEGRUM components.....	21
11.4 Remote access to the Wildfly application server management console.....	21
11.5 Verifying configuration of connection to the Wildfly application server database	21
11.6 Offline backup and restoring database.....	22
11.7 Time server	22
12. Before you update the INTEGRA / INTEGRA Plus control panel firmware	23

1. Introduction

The purpose of the INTEGRUM system is to assist in the management and review of data on the premises equipped with SATEL devices. The INTEGRUM system is designed to be used on the premises where the following are installed:

- the INTEGRA-INTEGRA Plus alarm control panel (firmware version 1.16 or newer) with the ETHM-1 (firmware version 1.09 or newer) / ETHM-1 Plus (firmware version 2.04 or newer) communication module,
- the ACSP-402 addressable fire alarm control panel with the ACSP-ETH module,
- the ACCO NET access control system (firmware version 1.9).

This manual applies to the installation and configuration of the software. The system has been designed to manage up to a few thousand of distributed premises. Communication with the control panels is via Ethernet.



Knowledge of the Linux shell script commands is REQUIRED for installation.

2. Software components

For the INTEGRUM system to operate, the Linux operating system is required. This documentation has been prepared based on the Rocky Linux 9 distribution. Its installation is described later in this manual, but if you already have the system installed, you can skip this part of the manual.

The software is offered as a distribution package. It consists of:

- INTEGRUM Server – program that allows data exchange between the INTEGRA control panels and the INTEGRUM AppServer program,
- INTEGRUM DB – database in which all system data are recorded: configuration, statuses and events,
- INTEGRUM-WEB – application for management and remote control of the system,
- INTEGRUM-AppServer – central management component for data exchange between the database and the INTEGRUM Server and the INTEGRUM-WEB programs,
- SATEL MapEditor – installation file for the site plan creator.

Third-party software must be installed to create a server environment required for the system to function properly. That software is not developed by SATEL (for licenses of each program, go to the websites shown in parentheses):

- Apache (<http://www.apache.org/licenses/LICENSE-2.0.html>),
- PHP (http://php.net/license/3_01.txt),
- MySQL (<http://www.gnu.org/licenses/old-licenses/gpl-2.0.html>),
- Java (<https://adoptopenjdk.net/about.html>),
- Wildfly (<https://github.com/wildfly/wildfly/blob/main/LICENSE.txt>).



Please remember to legalize the server environment required by the system.

If you already have these programs installed, verify their versions and, if they meet the minimum requirements, you can skip their installation.

3. System architecture

The INTEGRUM system can be installed on one computer. You can also split it into several computer workstations and apply a distributed architecture to your system. The SATEL MapEditor application for site plan creation can be installed on several computers. To use the INTEGRUM-WEB application for remote system management, you just need a web browser on your computer, smartphone or tablet. An example of the INTEGRUM system is shown in Fig. 1.

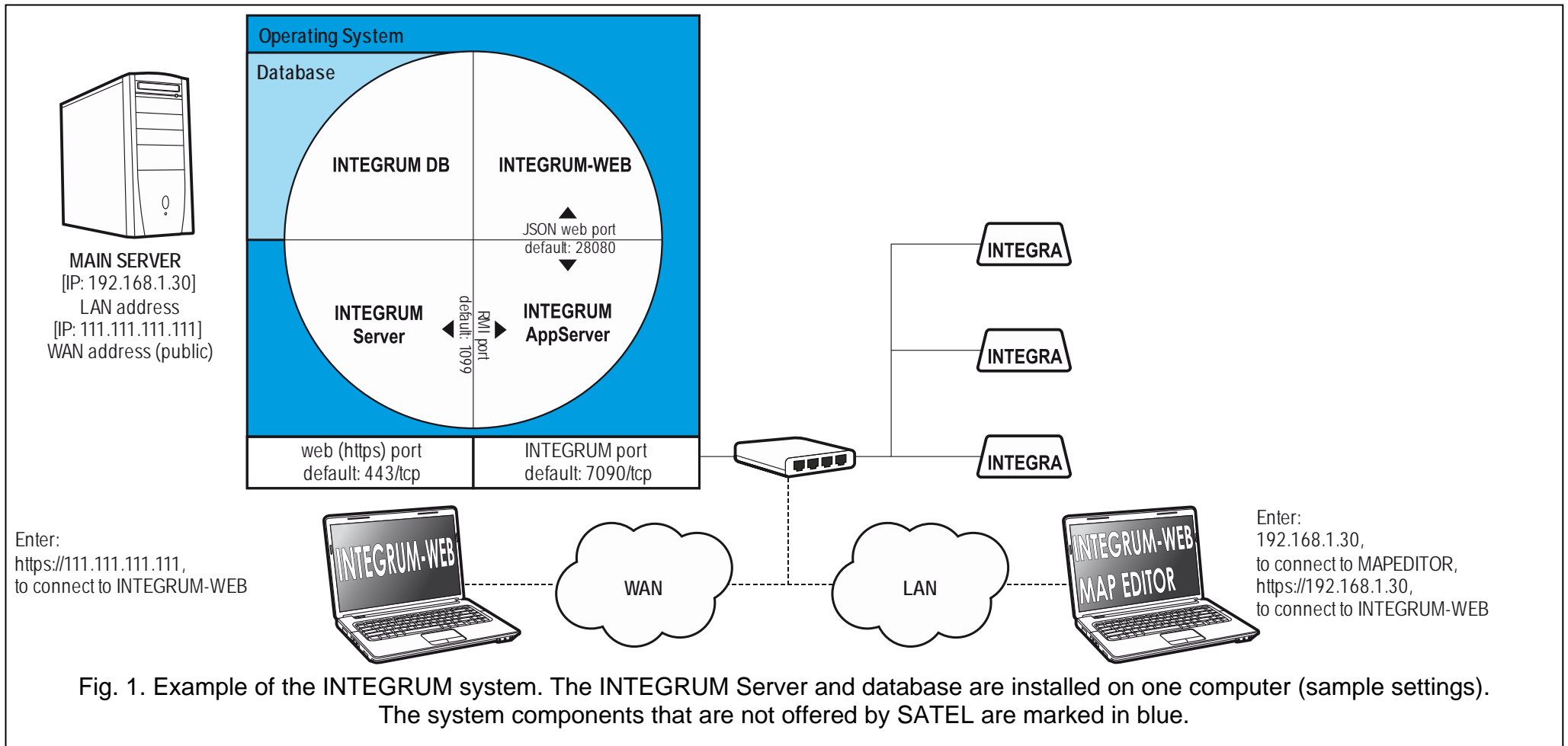


Fig. 1. Example of the INTEGRUM system. The INTEGRUM Server and database are installed on one computer (sample settings). The system components that are not offered by SATEL are marked in blue.

4. Network requirements

- Internet Protocol Version 4 (TCP/IPv4).
- IP address for each connected INTEGRA / ACSP-402 control panel.
- ACCO NET system and INTEGRUM installed on the same server.
- If the INTEGRUM-WEB application is to be accessible from another subnet, the Web port (https; default: 443/tcp) used for communication between the application and the client browser should be redirected.
- SATEL recommends that you purchase and install an SSL certificate to encrypt and validate the domain or organization in which the INTEGRUM-WEB application will run.



If the INTEGRUM system is connected to a public network, SATEL recommends that, in addition to standard encryption techniques (SSL), you also use extra security measures, such as firewall as well as intrusion detection and prevention systems (IDS / IPS).

5. Minimum hardware requirements

You can install the system on a prepared VMware ESX virtual machine or physical hardware.

- 2 core CPU with a performance comparable to devices obtaining 130 points for SPECint_rate_base2006 test,
- 4 GB of RAM,
- Gigabit Ethernet network adapter,
- operating system with Docker Engine version ≥ 20.10 installed.



The amount of RAM and disk resources depends on the type of control panels and their configuration. This amount is increased by 1 GB/user/process when tools for searching/reporting based on the event log are used at the same time. Additionally, the size of background maps used for visualization of the premises should be taken into account.

Disk resources are determined in multiples of 50 GB. As a starting size, you should assume +15 GB for each next 100 control panels/5 years and take into account the size of image files assigned to maps and users. The disk system must guarantee hardware data protection at least in the event of a single disk failure.

A hardware module for remote access to the server is required to provide support services.



If you are not sure if your computer meets the minimum hardware requirements, you can check it after installing the operating system – see “Verification of hardware requirements” p. 20.

For installation on the Windows system Hyper-V platform, the minimum requirements are:

- RAM: 16 GB,
- hard drive: 700 GB,
- 2 network adapters: one for the system, one Gigabit Ethernet standard for the Hyper-V virtual machine,
- operating system: Windows Server 2016, 2019 or 2022 Standard or Essential.

6. Installing the operating system

i | *We recommend installing the operating system on a computer with no operating system currently installed.*

INTEGRUM is provided as ready-to-use container images based on Linux x86_64 and started using the Docker Engine application. Check its availability at: <https://docs.docker.com/engine/install/> . Below is the installation process for the Rocky Linux 9.1 operating system.

In the case of installation on the Windows Server platform, installing the Hyper-V Platform is required to ensure start-up – see p. 18.

In the case of CPE units based on Windows 8, 10 <1903, Windows 2016, additional tools for connecting remotely to the system are required:

- Additional SSH client: Putty <https://putty.org/>
- In the case of offline installation, file transfer client: WinSCP <https://winscp.net/>

6-1. Go to <https://rockylinux.org/download/>. Select ISO: x86_64, type: boot and save it to disk. Once you have downloaded the ISO image, burn it to CD.

6-2. Insert the recorded CD into the computer CD drive. The installer splash screen will be displayed.

6-3. Install Rocky and set:

- language
- LOCATION – set Date & Time – set correct time zone
- SYSTEM:
 - network and host name – Configure button (IPv4 settings)
 - if the installation is running on a virtual machine, disable Kdump
- SOFTWARE – set the nearest mirror server and the minimal install option
- USER SETTINGS:
 - create the administrator user for integrum (remember the password you entered)
 - root password – leave the root account disabled

7. Installing the server environment



When you copy commands from this document, make sure that they are correctly moved to the console window. When the command exceeds the length of the line, a warning is added: Pay attention to the end of line characters. We recommended that you use a dedicated software instead of a web browser to open the PDF file.

7-1. On a computer with desktop environment (Windows, Linux), connect to the server.



```
ssh integrum@INTEGRUM_machine_IP
```



For older Windows systems, use Putty.

7-2. Enter the password and press ENTER.

7-3. Install Docker and configure user permissions.



```
sudo dnf check-update  
sudo dnf config-manager --add-repo https://download.docker.com/linux/centos/docker-ce.repo  
sudo dnf install -y docker-ce docker-ce-cli containerd.io docker-compose-plugin nano  
sudo systemctl enable docker  
sudo usermod -aG docker $USER  
newgrp docker
```



*After you use this command for the first time, enter the password given during installation. For the latest Docker installation manual, go to: <https://www.digitalocean.com/community/tutorials/how-to-install-and-use-docker-on-rocky-linux-9>
During installation on other Linux version, the server may not have the sudo command installed and configured. Run **su -l** and continue with the installation as administrator, skipping **sudo** at the beginning of the line.*



Make sure your computer meets the minimum hardware requirements (see p. 6).

7-4. Change the logging configuration for containers started by docker.

```
>_ | sudo nano /etc/docker/daemon.json ←
```

```
{  
  "log-driver": "local"  
}
```

Save and exit (Ctrl-X, Y, ENTER)

i | *By default, log rotation is not performed. As a result, you may run out of space on your disk. See <https://docs.docker.com/config/containers/logging/configure/> If nano is unavailable, you can install it: `sudo dnf install -y nano` or use `vi`.*

7-5. Start the service.

```
>_ | sudo systemctl start docker ←  
    | sudo systemctl status docker ←
```

7-6. Verify the installation of system packages.

7-6.1. Check available repositories.

```
>_ | dnf repolist enabled ←
```

A list of repositories used during installation will be displayed. Make sure that all of the items listed in the table below are included in the “repo ID” column.

i | *There may also be other repositories in the system.*

ID
baseos
docker-ce-stable

7-6.2. Check the installation of the components.

```
>_ | dnf list firewalld curl docker-ce docker-ce-cli containerd.io docker-compose-plugin ↵
```

A list of installed packages will be displayed.

Make sure that all of them are included in the “Installed packages” section and that there are no “Available packages” in the report. The following version numbers are the lowest supported by the software.

```
....  
Installed packages  
containerd.io.x86_64                1.6.9-3.1.el9                @docker-ce-stable  
curl.x86_64                        7.76.1-19.el9                @baseos  
docker-ce.x86_64                   3:20.10.21-3.el9             @docker-ce-stable  
docker-ce-cli.x86_64               1:20.10.21-3.el9             @docker-ce-stable  
docker-compose-plugin.x86_64       2.12.2-3.el9                 @docker-ce-stable
```

7-6.3. Check the logging configuration for the docker service.

```
>_ | docker info --format '{{.LoggingDriver}}' ↵
```

7-7. We recommend installing tools that may be useful in your everyday work and diagnostics.

```
>_ | sudo dnf install -y firewalld nano telnet chrony traceroute ↵  
sudo systemctl enable --now chronyd
```

8. Installing and updating the INTEGRUM system



The description below refers to a database installed as one of the containers. If you have purchased the support service, you can obtain procedures for installation on a dedicated database server.

You can install the INTEGRUM system using the console window.

When **[Update]** is added next to a step, do the step only when an older version of the program is installed.

8-1. **[Update]** Select the currently used images in order to be able to undo changes:



```
docker image tag cr.satel.pl/integrum/ee:3.1 cr.satel.pl/integrum/ee:3.1-prev ↵  
docker image tag cr.satel.pl/integrum/web:3.1 cr.satel.pl/integrum/web:3.1-prev ↵  
docker image tag cr.satel.pl/integrum/integrum:3.1 cr.satel.pl/integrum/integrum:3.1-prev ↵
```

8-2. Download and import the INTEGRUM container images.



```
export XZ_DEFAULTS="-T 0" && curl \[link to image\] | docker image load ↵
```

Instead of [\[link to image\]](#) enter the address provided with the license – repeat the command for each address.

8-3. In the case of offline installation, download the files on a computer with access to the Internet and store them in the home directory of the INTEGRUM server.



```
scp *.txz integrum@IP_maszyzny_INTEGRUM:/home/integrum/ ↵
```



For older Windows systems, use WinSCP.

Next, perform the import of container images on the INTEGRUM server.

```
>_ | export XZ_DEFAULTS="-T 0" && sudo find ~ -name 'integrum-*.txz' -exec docker image load -i {} \; ↵
```

8-4. Make sure the import was successful. There should be 6 Satel INTEGRUM images on the list.

```
>_ | docker image ls ↵
```

8-5. During the first installation, create a folder and unpack the default configuration files.

```
>_ | sudo mkdir /opt/integrum ↵  
    | sudo chown root:docker /opt/integrum ↵  
    | sudo chmod g+w /opt/integrum  
    | cd /opt/integrum/
```

In the case of online installation

```
>_ | curl \[link to file\] | tar xJ ↵
```

Instead of [\[link to file\]](#) enter the address provided with the license – repeat the command for each address.

In the case of offline installation, unpack the file you downloaded earlier.

```
>_ | tar xJf ~/pl-composer.txz ↵
```

We recommend installing SSL certificates. Obtain the files from the administrator in your organization. The files must have the following names: apache.crt – certificate; apache.key – corresponding private key. They must be located in the certs subdirectory.

You can generate local/untrusted SSL certificates. To do so, run the commands:

```
>_ | mkdir certs ↵  
    | openssl req -newkey rsa:4096 -nodes -sha256 -keyout certs/apache.key -addext "subjectAltName = DNS:[server name in your  
    | organization]" -x509 -days 3650 -out certs/apache.crt ↵
```

i | Pay attention to the domain name you enter in the openssl command.

Examine the configuration parameters.

```
>_ | nano .env ↵
    | nano docker-compose.yml ↵
```

If you are installing the system in a different time zone than CET / CEST, enter the name of your time zone.

To be able to use the ssl certificates, delete # in 2 lines of the docker-compose.yml file's web section:

```
# volumes:
  # - ./certs:/var/www/ssl/
```

8-6. Start the containers.

```
>_ | cd /opt/integrum/
    | docker compose build ↵
    | docker compose up -d ↵
```

8-7. Check the container status – after about 2 minutes.

```
>_ | docker compose ps -a ↵
```

Repeat the last command until the containers reach the status as in the table.

NAME	STATUS
integrum-integrum-web-server-1	Up [time] (healthy)
integrum-integrum-srv-server-1	Up [time] (healthy)
integrum-integrum-ejb-server-1	Up [time] (healthy)
integrum-integrum-db-server-1	Up [time] (healthy)
integrum-integrum-udb-server-1	Exited (0) (time)

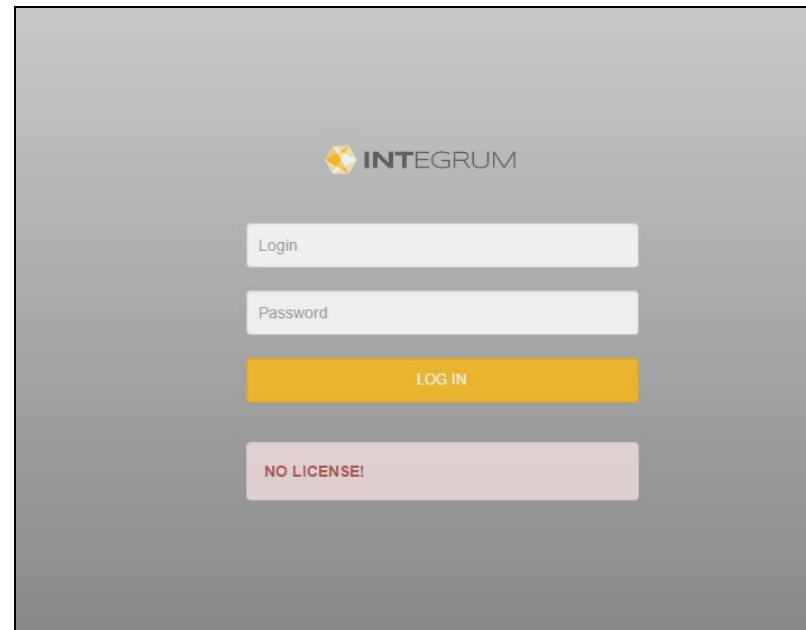
8-8. Configure remote access to INTEGRUM-WEB.

```
> sudo firewall-cmd --zone=public --add-service=https --permanent ↵  
sudo firewall-cmd --zone=public --add-service=https ↵
```

8-9. Make sure the program works correctly.

8-9.1. Enter the address of the INTEGRUM system server in the web browser address bar and press ENTER. The server address can be an IP address or a domain name.

8-9.2. The login page will open.



8-9.3. There is a text box below the “Log in” button in which, depending on the license status:

- if no license has been loaded yet – a message is displayed to inform you that there is no license,
- if at least one license has been loaded but has not yet been verified – a message is displayed to inform you that the license has not been verified,
- if at least one license has been loaded and verified – the license owner data are displayed.

-
- 8-9.4. Enter your login and password, then click “Log in”. You will gain access to the application. After system installation, the default login is “admin” and the password is “Satel.123”.
 - 8-9.5. Give the INTEGRUM system address to the system administrator.

9. Programming the settings

In the console window, you can configure the INTEGRUM container settings using the environment variables set in the configuration file.

 **Editing the files changes the system operation. Improper editing can lead to application errors. Edit only if necessary.**

9.1 INTEGRUM-WEB application

If you want to view the contents of the INTEGRUM-WEB configuration file, enter the following command in the console window:

```
>_ | cat /opt/integrum/docker-compose.yml ↵
```

and press ENTER.

If you want to edit the contents of this configuration file, enter the following command:

```
>_ | nano /opt/integrum/docker-compose.yml ↵
```

and press ENTER.

Shown below are the modifiable parameters of the INTEGRUM-WEB configuration file.

INTEGRUM_WEB_EVLIMIT	The number of events loaded in one operation
INTEGRUM_WEB_SOUNDONMAP	The value TRUE enables the alarm sound on the map
INTEGRUM_WEB_AUTHBEFOREACTION	The value TRUE enables additional authorization to perform actions on the map
INTEGRUM_WEB_DASHBOARDDEFAULT	The value TRUE sets the “Dashboard” screen as default after logging in
INTEGRUM_WEB_CONTROLWITHEVENTS	The value TRUE opens the “Events” tab on the control panel data screen

9.2 INTEGRUM-APPSERVER application

Shown below are the modifiable parameters of the configuration file of the INTEGRUM-APPSERVER application.

INTEGRUM_USELINKEDUSERFORINTEGRACOMMANDS	Modes of communication between INTEGRUM and INTEGRA control panel: 0 – default – the code entered in the “General” tab (control panel data screen) is used. 1 – logged in user code is used. If the application user is not linked to the control panel user, an error will be reported. 2 – same as 1, but if the application user is not linked to the control panel user, the code entered in the “General” tab (control panel data screen) will be used. 3 – same as 1, but if the application user is not linked to the control panel user and has the “Editing INTEGRA control panels” function, the code entered in the “General” tab (control panel data screen) will be used.
INTEGRUM_EVENT-EMAIL	List of addresses to which information about troubles and alarms will be sent.

10. Installing the Windows Server – Hyper-V platform

 | The following procedure will not work for installation of the Windows system without GUI.

10-1. Install the Windows system and configure the system network adapter.

10-2. Start PowerShell (Administrator).

Windows 2016

RMB Start => Command prompt (Administrator) => powershell <Enter>

Windows 2019 and Windows 2022


RMB Start => Windows PowerShell program (Administrator)

10-3. Enable the Hyper-V component.


 | *Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V -All* ↵

RESTART

10-4. Restart PowerShell (10.2) and install tools.

 | *Add-WindowsFeature Hyper-V-Tools* ↵
Add-WindowsFeature Hyper-V-PowerShell ↵

10-5. Configure the virtual network.

 | *New-VMSwitch -Name "VMNetwork" -NetAdapterName "Ethernet 2"* ↵

 | To download the network adapter name, use the command:

get-wmiobject win32_networkadapter -filter "netconnectionstatus = 2" | select netconnectionid,name

10-6. Configure the virtual machine (pay attention to the path and name of the ISO file in the fourth line).

```
>_ New-VM -Name "INTEGRUM" -MemoryStartupBytes 4GB -NewVHDPATH c:\INTEGRUM.vhdx -NewVHDSIZEBytes 500000000000↵  
Set-VMProcessor -VMName "INTEGRUM" -Count 4↵  
Connect-VMNetworkAdapter -VMName INTEGRUM -SwitchName VMNetwork↵  
Set-VMdvdDrive -VMName "INTEGRUM" -Path C:\Users\Administrator\Downloads\Rocky-9.1-x86_64-boot.iso ↵  
Start-VM -VMName "INTEGRUM"↵  
VMConnect.exe localhost "INTEGRUM" ↵
```

10-7. Continue with the installation in the INTEGRUM virtual machine window – see section 7.

11. Useful commands

You can manage the INTEGRUM system by entering commands in the console window (enter a command, then press ENTER).

11.1 Verification of hardware requirements

When you enter the command, you will see the number of cores, the total amount of RAM and the swap file size in MB.

```
>_ | cat /proc/cpuinfo | grep 'physical id|core id' | uniq | echo ' $(wc -l) Total\ cores && vmstat -s -S M | grep total --color=never ←
```

11.2 Checking the container status

System components are installed in the form of containers running continuously in the background. The operator can check their status.

Checking the status

```
>_ | docker ps -a ←
```

Stopping

```
>_ | docker stop container_name ←
```

Starting

```
>_ | docker start container_name ←
```

Shown below are the names of containers used by INTEGRUM:

integrum-integrum-db-server-1	Database server
integrum-integrum-ejb-server-1	Application server
integrum-integrum-web-server-1	Websites server
integrum-integrum-srv-server-1	INTEGRUM server

11.3 Collecting logs from system services and INTEGRUM components

```
>_ | cd /opt/integrum/ ↵  
    | docker compose logs | grep date_in_format_YYYY-MM-DD | gzip -c > /tmp/integrum-log-dzienny.gz ↵  
    | cat docker-compose.yml | gzip -c > /tmp/integrum-cfg.gz ↵↵
```

Additionally, detailed logs:

```
>_ | cd /opt/integrum/ ↵  
    | docker compose logs | gzip -c > /tmp/integrum-log-full.gz ↵
```

11.4 Remote access to the Wildfly application server management console

On a computer with GUI:

```
>_ | ssh -L 9990:localhost:9990 integrum@INTEGRUM_machine_IP ↵
```

Enter `http://localhost:9990` in the browser.

The default login is `integrum/Satel.123`

11.5 Verifying configuration of connection to the Wildfly application server database

Use the Wildfly application server management console.

Go to the Runtime tab. Then indicate Server -> Datasource -> SatelIntegrumDS and press Test.

11.6 Offline backup and restoring database



The solution described below is not optimal. We recommend using dedicated tools for creating backup and restoring database.

Creating backup.



```
cd /opt/integrum/ ↵  
docker compose stop ↵  
docker run --rm --volumes-from integrum-integrum-db-server-1 -v $(pwd):/backup busybox tar cvf /backup/backup.tar /var/lib/mysql ↵  
docker compose up -d ↵
```

Restoring from backup.



```
cd /opt/integrum/ ↵  
docker compose stop ↵  
docker run --rm --volumes-from integrum-integrum-db-server-1: -v $(pwd):/backup busybox tar xvf /backup/backup.tar --directory / ↵  
docker compose up -d ↵
```

11.7 Time server

The operating system allows the NTP service to be shared as a time server with other devices on the network, becoming a local time server. It is necessary to add a rule that makes this service port available on the network.



The command opens access to a network service and creates a potential vulnerability. Run the command only if necessary.



```
firewall-cmd --zone=public --add-port=123/udp ↵  
firewall-cmd --zone=public --add-port=123/udp --permanent ↵
```

12. Before you update the INTEGRA / INTEGRA Plus control panel firmware



Disconnect the control panel from the INTEGRUM system for the time of firmware update.

To disconnect the control panel from INTEGRUM, you can choose one of the following methods.

14-1. Method I

1. Login to the program (with Administrator privileges).
2. Go to the “Control panels” tab.
3. Click the name of the panel you want to disconnect.
4. Go to the “General” tab.
5. Click the “Active” button (switch it to “No”).
6. Click “Save”.
7. Refresh the page to make sure communication with the control panel has been terminated.

14-2. Method II

Unplug the Ethernet cable from the Ethernet module during firmware update.