

Installation Scout Enterprise Management Suite 15

Short Guide

Last edited: 2023-07-21

0. Legal information	3
1. Representation	4
2. System requirements	5
3. System limitations	8
4. Database support	9
4.1. Overview	9
4.2. SQL LocalDB	11
4.3. Authentication to SQL Server	12
4.4. SQL Server users and application roles	13
4.5. Scout Server cluster	16
4.6. Number of ODBC connections	18
5. Preparing for installation	19
5.1. Registering Scout Server in the network	19
5.2. Opening ports	24
5.3. Preparing SQL Server databases	25
5.4. Permissions and certificates	26
5.5. Downloading software	28
6. Installation: Scout Enterprise Management Suite	30
6.1. Features of the Scout Enterprise Management Suite	30
6.2. Installing Scout Enterprise Management Suite	33
6.3. After the initial installation	36
6.4. Unattended installation	37
6.5. Upgrading to newer versions	42
6.6. Modifying Scout Enterprise Management Suite	43
6.7. Uninstalling Scout Enterprise Management Suite	44

7. Installation: eLux Container	45
7.1. Installing a container	46
7.2. Updating to a later version	48
7.3. Uninstalling an eLux container	48
8. Installation: ELIAS 18	49
8.1. Installing ELIAS 18 / Windows	49
8.2. Installing ELIAS 18 / Linux	52
8.3. Starting ELIAS 18	56
8.4. Updating to newer ELIAS version	56
8. Database connections	57
9. Certificates	58
9.1. Certificate for Scout Keep Alive service	60
10. Management protocol	62
10.1. Certificate-based management protocol	62
10.2. Configuring the trust level on the devices	63
10.3. Configuring Scout Server for communication via CA certificates	65
11. Troubleshooting	66
12. Encrypting values	69
13. Appendix	70
13.1. Program and file directories	70
13.2. eLux partitions	70
13.3. IP ports	72
13.4. SNMP	77

0. Legal information

© 2023 Unicon GmbH

This document is copyrighted. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means, without our express consent. Information in this document is subject to change without notice. We disclaim all liability regarding correctness, completeness and topicality of the information contained herein and any errors or damage resulting from the information provided.

eLux® and Scout Enterprise Management Suite® are registered trademarks of Unicon GmbH in the European Union, GB and the United States.

ScoutaaS® is a registered trademark of Unicon GmbH in the European Union, GB, the United States and Japan.

All other product names are registered trademarks of their relevant owners.

Unicon GmbH
Ludwig-Erhard-Allee 26
76131 Karlsruhe
+49 (0)721 96451-0

1. Representation

The following representations and conventions for instructions are used throughout the documentation:

Representation	Description
Control element	All graphical user interface controls are displayed in bold
Menu > menu command	Whenever running a command involves clicking a series of menus, the single GUI controls such as menu commands or dialog tabs are linked by > .
Value	All data that have to be entered by the user or data that represent a field value are displayed in <code>Courier New</code> . Also, file names and path names are displayed in <code>Courier New</code> .
STRG	Keys to be pressed are displayed in CAPITAL LETTERS.
<Placeholder>	Placeholders in instructions and user input are displayed in <i>italics</i> and in <angle brackets>.
1. Instruction	Procedures to be carried out step by step are realized as numbered steps.
Result	System responses and results are displayed in <i>italics</i> .

Abbreviations and acronyms

Abbreviation	Description
AD	Active Directory , directory service of Microsoft Windows Server
EBKGUI	Interface of the eLux Builder Kit (Tool for creating eLux software packages)
EPM	eLux package module (<code>.epm</code> , software package)
FPM	Feature package module (<code>.fpm</code> , part of a software package)
FQDN	Fully qualified domain name
GB	Gigabyte
GHz	Gigahertz (processing speed)
HDD	Hard disk drive (flash memory)
IDF	Image Definition File (<code>.idf</code>)
IIS	Internet Information Services: Microsoft Web server
MB	Megabyte
OU	Organizational unit Unit or group within the organizational structure
VPN	Virtual Private Network

2. System requirements

Note

The following information refers to Scout Enterprise Management Suite 15.x.

Minimum requirements for Scout Server and Scout Console

- Hard disk space 600 MB (only Scout Enterprise Management Suite, the software container requires additional space)
- Scout Server and Scout Console: Microsoft Windows Server 2016, 2019 or 2022
- Scout Console only: Microsoft Windows 10 or 11

each including the relevant software updates provided by Microsoft at the time of installation

Note

We recommend operating the Scout Enterprise Management Suite on a Windows Server system. To run the Scout Console, a Windows workstation is sufficient.

- Microsoft .NET Framework version 3.5 and
Microsoft .NET Framework version 4.5.1 or later
- Suitable ODBC driver

Requirements for the database system

- Microsoft SQL Server 2016, 2017, 2019, 2022
- or for small installations:
MS SQL Server Express LocalDB as integrated DBMS based on SQL,
included in the Scout installation file

Minimum requirements for the eLux container:

- applies only if you use the legacy ELIAS, user-defined installation -

- FTP or HTTP server, locally installed or via network
- The required space depends on the number of provided operating system versions. For the current eLuxContainer installation, for example, we recommend an available disk space of 2.5 GB minimum.

Generally, the minimum requirement can be obtained from the size specified for the `AllPackages` archive on our myelux.com portal.

Recommended system requirements for ELIAS 18 and MongoDB on one computer

- applies only if you use ELIAS 18, to be installed separately -

- Hard disk space 30 GB (depending on container installations)
- RAM 8 GB minimum
- Microsoft Windows Server 2016 or later, 64-bit version
Microsoft Internet Information Service (IIS) 8.0 or later versions
including WebSocket Protocol for automatic page refresh

Minimum requirements for ELIAS 18 and MongoDB

- Hard disk space 10 GB
- RAM 6 GB
- Microsoft Windows 10, 64-bit version

Note

If you use your own MongoDB installation for ELIAS 18, make sure that you use a current and supported MongoDB version.

Minimum requirements for the web applications Scout Board, ELIAS 18 and Scout Cloud Gateway¹

- Web browser / minimum version
 - Mozilla Firefox ⇒ 96 ESR
 - Google Chrome ⇒ 96
 - Microsoft Edge ⇒ 96

¹see also [System requirements](#) for Scout Cloud Gateway in the **SCG** guide

Note

Some functions use pop-up windows. Make sure that pop-up windows are not blocked by your browser. This function can usually be found in the browser settings under **Privacy** or **Security**.

- Screen resolution Full HD

For [support periods](#) and the [compatibility matrix](#), see the whitepaper **Releases, Lifecycles and Compatibility**.

3. System limitations

There are no system restrictions known for any component of the Scout Enterprise Management Suite.

You can run additional services such as [Citrix XenApp](#) on the same system.

4. Database support

Scout requires database software such as Microsoft SQL Server or, for smaller environments, Microsoft SQL Server Express LocalDB.

4.1. Overview

Microsoft SQL Server

You can use any Microsoft SQL Server version with available product support as an SQL database. We recommend that you create the required databases before installing Scout Enterprise Management Suite.

A minimum of one **Scout database** is required to manage the following data:

- Device configuration
- Application definitions
- Asset data (static)
- Server settings
- Administrator management
- Console management
- License information
- Transaction logging

A Scout database requires about 50 MB free disk space per 1.000 devices.

For Scout versions up to Scout 15 2204, the Scout Statistics Service was included as an optional component of the Scout Enterprise Management Suite which required a dedicated statistics database. From Scout 15 2209, the Scout Statistics Service has been replaced by the Scout Keep Alive service. The keep alive data are now stored in the Scout database.

New databases can alternatively be created in Microsoft SQL Server during the installation process of the Scout Enterprise Management Suite, provided the required permissions are available.

Microsoft SQL Server Express LocalDB

Using Microsoft SQL Server Express is only recommended for less than 1.000 devices or for test and evaluation environments.

The Scout database is created automatically during the installation process:

The Scout installation file already includes Microsoft SQL Server Express LocalDB. If desired, during installation, the required database of the type `LocalDB` is created. The database name is defined by the system.

Multiple database connections

By using the database connection editor, you can define various database connections for the Scout Console. You then can select one or more of the defined connections when starting the console. From your console, you can use multiple connections to different databases at the same time.

The database connection editor is provided on the Windows Start menu. For further information, see "Database connections" on page 57.

Database cleanup

Outdated data can be deleted using the **Database cleanup** feature. For further information, see [Database cleanup](#).

4.2. SQL LocalDB

We only recommend using the integrated database Microsoft SQL Server Express LocalDB for less than 1.000 devices or for test and evaluation environments. The required software modules are included in the Scout installation file.

To use Microsoft SQL Server Express LocalDB, you are requested to specify a Scout Windows user during the installation process that acts as the owner of the LocalDB instance. We recommend using a technical user account that allows all users to access the LocalDB database and is provided with a non-expiring password. The account must be provided with the local user right **Log on as a service** and must be a member of the local administrator group.

Limitations of Microsoft SQL Server Express LocalDB compared to Microsoft SQL Server

- The Scout Console can only be operated in conjunction with the Scout service and the LocalDB database on the same server system. Dedicated Scout Consoles that can access the LocalDB database remotely are not supported.
- The **Configuration run** command to prepare the device configuration data is not available.

4.2.1. Performing a backup of SQL LocalDB before installing updates

Before you update an existing Scout Enterprise Management Suite installation to a newer version, we recommend performing a backup of the LocalDB database.

Method 1:

- ▶ Create a copy of the two files
`ScoutEnterpriseLocalDB.mdf` and
`ScoutEnterpriseLocalDB_log.ldf` located in the directory `C:\Users\<User name>\`

After having installed the Scout update version, copy the database files back to the specified directory.

Method 2 (requires SQL Server Management Studio):

1. In SQL Server Management Studio, connect to
 Database `ScoutEnterpriseLocalDB`
 Instance `(localdb)\.\ScoutEnterpriseManagementSuite_Shared`
2. Use the **Backup** feature to create a backup.

For further information, see the Microsoft documentation for SQL Server Management Studio such as <https://technet.microsoft.com/en-us/library/ms189621>.

After having installed the Scout update version, use the SQL Management Studio feature **Restore** to restore the database.

4.3. Authentication to SQL Server

When you select the **Microsoft SQL Server** database type during installation, you can choose between two authentication methods for the database engine, **Windows authentication** and **SQL Server authentication**.

The authentication requires either an SQL user or a Windows user. Each of them must be a member of certain database roles in SQL Server. For further information, see "SQL Server users and application roles" on the facing page.

Method	Description
Windows authentication	<p>'Trusted connection': The user identity is confirmed by Windows.</p> <p>The Scout service must be run with a user account equipped with the relevant permissions in SQL Server.¹</p> <ul style="list-style-type: none"> ▶ In the Scout installation dialog, specify the account name in the form <code>DOMAIN\username</code> (no case-sensitivity) <p>Example: <code>INT\mmi</code></p> <hr/> <p>Note</p> <p>For the Scout installation, either a user with the relevant permissions in SQL Server or the technical user account (Log on as a service) to be used must be logged on to the Windows server system.</p>
SQL Server authentication	<p>The username and password must refer to an SQL Server user account with the relevant user rights in SQL Server.</p> <ul style="list-style-type: none"> ▶ In the Scout installation dialog, specify the SQL username and password.

If you choose to install the Scout Enterprise Management Suite completely, three databases are required. You can configure access to the three databases in the following ways:

- If the same authentication method is used for all databases, you can configure different users for each database.
- If the same user is used for all databases, you can configure different authentication methods for accessing each database.

¹For Scout Enterprise Management Suite 15.5 and later versions, gMSA (Group Managed Service Accounts) are also supported.

4.4. SQL Server users and application roles

Below description gives a rough overview of the permissions required in SQL Server, as well as how to use an application role. An application role increases security by assigning operational administrators only the necessary permissions for the duration of a session.

Create databases

We recommend that you create the required databases in SQL Server before installing the Scout Enterprise Management Suite.

Please note the following:

- To create databases in SQL Server, you need the SQL Server role **dbcreator** as a minimum.
- The database names may be freely chosen.
- The tables within the databases are created by the installation routine of the Scout Enterprise Management Suite.

Important Do not delete the original database when backing up and restoring! The unique database ID must be preserved for the initialization of the license database. For further information, see "Troubleshooting" on page 66.

Permissions for users of the Scout Enterprise Management Suite

SQL server role

For the use of the Scout Enterprise Management Suite, the server role **public** in general is sufficient. Only if users are to perform additional tasks in SQL Server, extended permissions are necessary. For example, restoring databases requires the **dbcreator** server role.

SQL database role

On database level, for console-only users in standard environments, the database roles **db_datareader** and **db_datawriter** are sufficient.

db_owner is needed, for example, for database activities related to updating to a new Scout version. The same applies for performing any configuration and maintenance activities on the database.

The users must be mapped to the default schema `dbo`.

Note

For environments with SQL Server clusters, additional permissions such as `VIEW SERVER STATE` and `VIEW ANY DEFINITION` are required.

SQL application role

In the case of Windows authentication for SQL Server, users are authorized to also log on to the SQL Server Management Studio. For scenarios like this we recommend using a dedicated user group with limited database rights for console-only users.

Permissions to access SQL Server tables can additionally be controlled and restricted for all databases via a system-wide SQL application role. The name and password of the application role must be defined in the relevant database.

A console user for SQL Server then only needs the database role **public** in order to execute the stored procedure for activating the application role. Once the application role is active, the connection to SQL Server loses the user permissions and assumes the permissions of the application role. Other databases in which **guest** has been disabled will be inaccessible to the application role. The application role permissions remain active for the duration of a session.

Configuring console users and an application role in SQL Server Management Studio

The following instructions refer to the Scout database.

1. In SQL Server Management Studio, under **Security > Logins**, add a new user group (Example: **Console users**) with the following options:

Server role	Public
User mapping > Database role membership	db_datareader
Securables	Set non-required permissions to Deny . Example on server level: Alter any database > Deny

2. Below the Scout database, under **Security > Schemas**, add a new schema (Example: **Console users schema**).
Under **Schema owner**, select the **Console users**.
3. Below the Scout database, under **Security > Roles > Application roles**, add an application role (Example: **Console users role**) with the following options:

Default schema	Console users schema
Password	Choose freely
Securables	Select your Scout database and set all permissions except Connect to Grant

Defining the application role in the Scout database

1. To specify the application role data in encrypted mode, in a first step, encrypt the name and password of the role. For further information, see "Encrypting values" on page 69.
2. Back in SQL Server Management Studio, for the Scout database, edit the **System** table.
3. Add one row for the name and one row for the password of the application role. Paste the encrypted values into the table:

SystemID	ParamName	ParamVal
...		
<n>	RNameEx	<encrypted name of application role>
<n>	RPassEx	<encrypted password of application role>

When the Scout Console is started, the fields are read and the access rights of the application role are set.

4.5. Scout Server cluster

If you use an SQL database, several Scout Servers can connect to the same Scout database concurrently. Concurrent Scout Servers enable failure load balancing as well as the option to configure load balancing (ManagerLoadBalancing).

Client devices that connect to a Scout Server receive a list of all currently running servers that access the shared Scout database.

FailureLoadBalancing

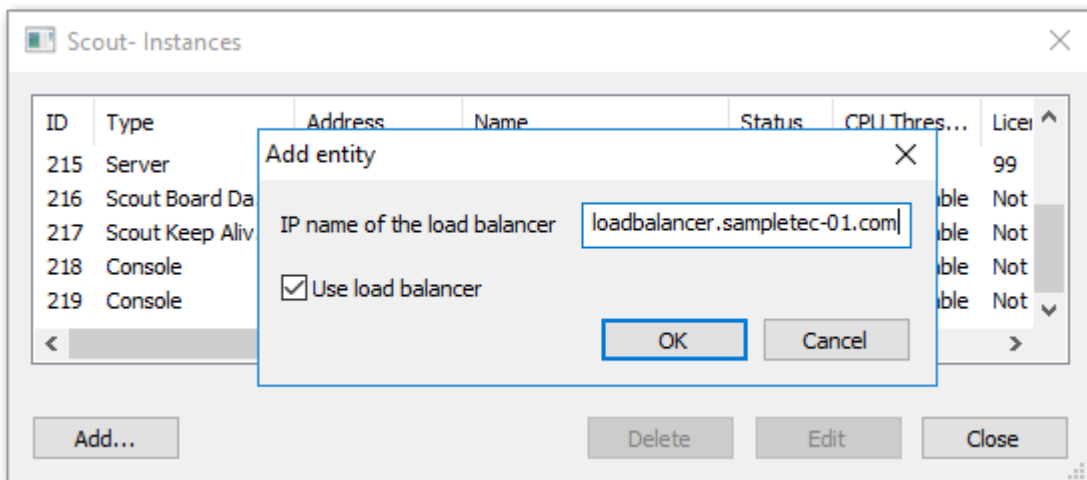
On start-up, a device tries to connect to the Scout Server it was connected to last time. If, however, that server is not available, it connects to the next server from the servers list which, subsequently, becomes the server the client tries to access by default from then on.

The FailureLoadBalancing mechanism restarts as soon as the client fails to connect to the same Scout Server.

ManagerLoadBalancing by dedicated load balancer

To define a dedicated load balancer, predefine the preferred manager address (IP address or name) for load balancing you want the devices to connect to:

- ▶ In the Scout Console, in **View > Scout entities**, add a new entity and select the option **Use load balancer**.



The load balancer entry refers to an existing load balancer pointing to the relevant Scout Server. The load balancer entry allows you to assign devices to a particular Scout Server without changing the Scout configuration.

The load balancer name is evaluated by the devices on each client restart.

Procedure:

- The device restarts
- The device connects to the load balancer and then is forwarded to the appropriate Scout Server

If, however, the Scout Server identified by the DNS entry `ManagerLoadBalancer` is not available, the `FailureLoadBalancing` mechanism described above is used and the client accesses the next server on the list.

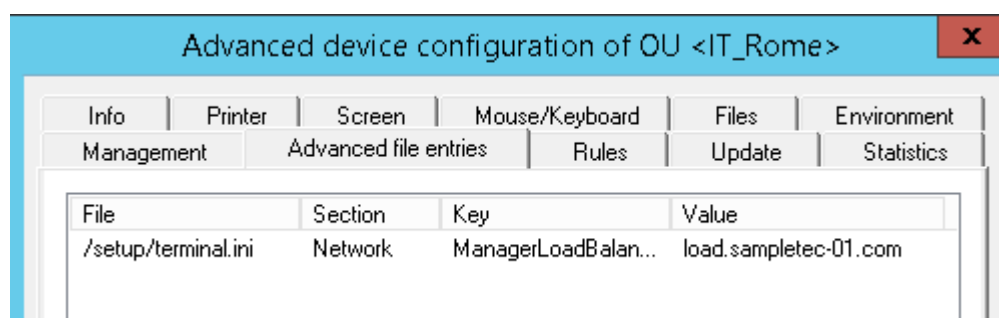
ManagerLoadBalancing by DNS entry

Alternatively, to predefine a preferred Scout Server you want the devices to connect to, you can use a DNS entry that you refer to in the advanced file entries.

- ▶ Use the Scout Console feature **Advanced file entries** for all devices, for an OU or an individual device:

File	/setup/terminal.ini
Section	Network
Entry	ManagerLoadBalancer
Value	<FQDN DNS entry>

For further information, see [Advanced file entries](#).



`ManagerLoadBalancer` refers to a DNS entry pointing to the relevant Scout Server. In a separate step, the DNS entry must be defined on the DNS server. The DNS entry allows you to assign devices to a particular Scout Server without changing the Scout configuration.

The `ManagerLoadBalancer` parameter is evaluated by the devices on each client restart.

Procedure:

- The device restarts
- DNS entry `ManagerLoadBalancer` is resolved
- The device connects to the appropriate Scout Server

If, however, the Scout Server identified by the DNS entry `ManagerLoadBalancer` is not available, the `FailureLoadBalancing` mechanism described above is used and the client accesses the next server on the list.

4.6. Number of ODBC connections

The number of ODBC connections between the Scout Server and Scout SQL database is defined dynamically on start-up of the server service. Normally, for each CPU kernel, two ODBC connections are defined and used.

The number of database connections currently used can be viewed by using the **system check** feature (Scout Console **View > System diagnostics > System check**).

System check		
Type	Result	Description
Scout server st...	Checking..	Checks whether the Scout service is running
✓ License status	All devices have a management license	Checks whether all clients will have a management license
✓ Subscription sta...	Ok.	Checks whether the subscription for the devices is valid
✓ Container access	All container directories are accessible	Checks whether the configured containers exist and are
✓ Recovery settings	The service is not installed.	Checks whether the recovery settings will work
✓ Database conne...	4	Checks how many database connections are used

From experience, two ODBC connections for each CPU kernel lead to good results considering

- maximum communication performance between Scout Server and SQL database and
- optimum CPU utilization.

Static versus dynamic ODBC connections

You can specify a fixed number of ODBC connections to meet the particular system requirements of a Scout installation. For this, you must define the following parameter in the `eluxd.ini` configuration file of the Scout Server:

File	%systemdrive%\Users\Public\Documents\UniCon\Scout\Server\eluxd.ini
Section	[ELUXD]
Parameter	DatabaseConnections=
Value	n (<i>n=1-128</i>)

Note

Increasing the number of database connections manually, can lead to CPU overload.

For further information on modifying `.ini` files, see [Advanced file entries](#) in the **Scout** guide.

5. Preparing for installation

Scout Server and the Scout Keep Alive service or Scout Statistics Service can be installed on the same machine or on different machines.

Make sure that the operating system is provided with up-to-date patches and the required software is installed. For further information, see "System requirements" on page 5.

Before you start the installation, read the following.

5.1. Registering Scout Server in the network

To allow automatic registration of the devices, assign the IP address of the Scout Server via DNS or DHCP.

- ▶ DNS: Assign the host name `ScoutSrv` to the IP address. This is the easiest way.
- Or:
- ▶ Configure one or more DHCP options. For further information, see [DHCP configuration](#).

Note

If you want to assign another Scout Server at a later time, use the Scout function **Client relocation**. Do not change the DHCP configuration while the devices are running.

Note

If you do not use DHCP options for Scout, we recommend that you select the option **Ignore Scout Server DHCP options** in the **Device configuration > Network**.

5.1.1. DHCP configuration

- optional -

Note

DHCP options can only be applied to eLux devices.

A new device booting for the first time can retrieve the following information from a DHCP server:

- IP address or name of the Scout Server (option 222)
- List of Scout Servers (option 224)
- ID of the destination OU on the Scout Server (option 223)

This requires configuring the DHCP server via one of the two following methods.

In method 1 (recommended), you define a new vendor class, set the new options, and then apply the values. Method 2 uses the DHCP Standard Options 222, 223 and 224.

The following instructions are based on the DHCP manager of Windows Server 2012.

Method 1: Defining user-defined vendor class



Requires

DHCP server compliant with RFC 2132, supporting user-defined vendor classes. Otherwise use method 2.

1. Open the DHCP manager.
2. Select the relevant DHCP server, and then click **Action > Define...**
3. Click **Add...** to create a new class:

Option	Value
Display name	eLux NG
Description	eLux specific options
Code (in ASCII column)	ELUXNG <i>The entry is automatically extended with the related hexadecimal number (45 4C 55 58 4E 47).</i>

4. Click **Action > Set Predefined Options....** Then, in the **Option class** list field, select eLux NG.
5. To define one Scout Server, click **Add...** and edit the new option as follows:

Option	Value
Name	Scout Server

Option	Value
Data type	String
Code	222
Description	Name or IP address of the Scout Server

6. To define more than one Scout Server, click **Add...** and edit the new option as follows:

Option	Value
Name	Scout Server list
Data type	String
Code	224
Description	Server names/IP addresses, comma-separated

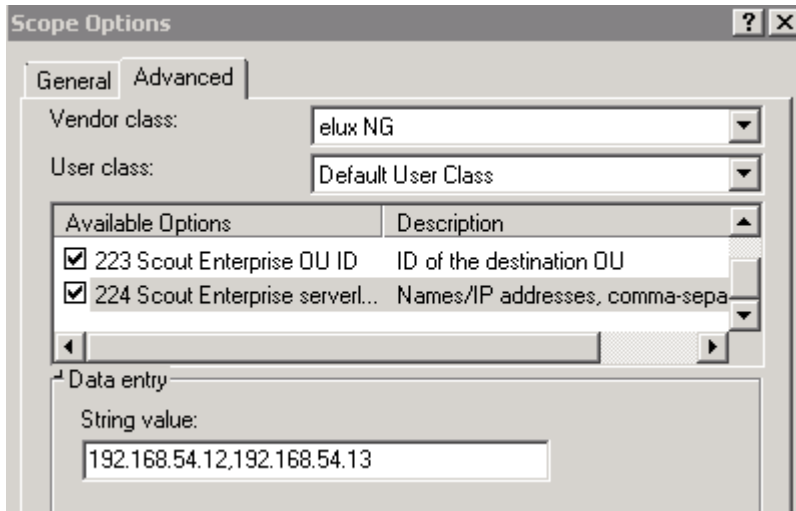
7. To define a specific OU that you can assign new devices to, click **Add...** and edit the new option as follows:

Option	Value
Name	Scout OU ID
Data type	Long
Code	223
Description	ID of the destination OU

8. To assign the options, for the relevant DHCP server, select either the **Server Options**, the **Scope options** or the **Reservations**. Then click **Action > Configure Options... > Advanced**.

In the **Vendor class** list field, select `elux NG`. Select each option defined and enter its value into the **Data entry** field:

Option	Value
222 Scout Server	<Name or IP address of the Scout Server>
223 Scout OU ID	<ID of the destination OU>
224 Scout Server list	<Names or IP addresses of the Scout Servers, separated by comma>



Method 2: Using DHCP Standard Options



Requires

The DHCP Standard Options 222, 223 and 224 must be available. Otherwise use Method 1.

1. Open the DHCP manager.
2. Select the relevant DHCP server, and then click **Action > Set Predefined Options....** In the **Option class** list field, select `DHCP Standard Options`.
3. Click **Add...** to create the following Standard Options, as described for Method 1:
 - Scout Server, String, 222
 - Scout Ernteprise server list, String, 224
 - Scout OU ID, Long, 223
4. To assign the options, for the relevant DHCP server, select either the **Server Options**, the **Scope options** or the **Reservations**. Then click **Action > Configure Options... > General**.

Select each option defined and enter its value into the **Data entry** field:

Option	Value
222 Scout Server	<Name or IP address of the Scout Server>
223 Scout OU ID	<ID of the destination OU>
224 Scout Server list	<Names or IP addresses of the Scout Servers, separated by comma>

Disabling DHCP option 12 as source for host names

If you have configured DHCP option 12 (host name), when connecting new devices, you can have the host names set via DHCP. To obtain the host name **not** via DHCP but from another source, such

as the name template defined in the Scout Console, prevent the take-over from DHCP option 12. To do so, use a `terminal.ini` parameter:

File	/setup/terminal.ini	
Section	Network	
Entry	IgnoreDHCPHostname	
Value	true	The default value is false.

5.1.2. Assign new devices to specific Scout Servers

If you use more than one Scout Server, you can specify in advance to which of them a device will be assigned during the onboarding process. A filter (regular expression) on the MAC address is used as a criterion for the assignment.

The filter rules are defined in an `.ini` file, which is then transferred to the devices as part of a custom feature package in the image. This way, new devices receive the information to which Scout Server they are to connect, even before the first contact to Scout.

The `.ini` file, for example `scoutmapping.ini`, is a text file that is structured according to the pattern below:

```
[Mapping1]
```

```

identifier=MAC    pattern=[AB][0-9A-F]$    scoutsrv=scout1.sampletec-01.com
[Mapping2]    identifier=MAC    pattern=[CD][0-9A-F]$    scoutsrv=scout2.sampletec-01.com
[Mapping3]    identifier=MAC    pattern=[EF][0-9A-F]$    scoutsrv=scout3.sampletec-01.com

```

Note the following:

- In Scout, the MAC address is displayed as a 12-digit number without separators (example: 901B0E01CE84)
- The filter must be a regular expression that filters on a substring of the MAC address.
- In a PostInstall script and PreUninstall script of the feature package, the `.ini` file must be referenced, example: `./setup/scoutmapping.ini`

For further details, please contact the Unicon support.

5.2. Opening ports

- ▶ Open the following ports in the firewall:¹

Port	Type	from	to
1433	TCP	Scout Server	MS SQL Server
1434	UDP	Scout Server	MS SQL Server (Browser service)
22123	TCP	Scout Server (Scout Management /secure)	eLux devices
22125	TCP	Scout Server (Scout Management / TLS 1.2)	eLux devices
22124	TCP	Scout Server	Scout Keep Alive service
5900	TCP	Scout Console (Mirroring eLux desktop)	devices
80/443	TCP	Clients (HTTP/HTTPS)	Web server
80/443	TCP	Clients (Firmware-updates via HTTP/HTTPS)	Web server

Note that, after the connection has been established, MS SQL Server assigns port numbers between 1024 and 5000 dynamically to its clients and that communication from 1433 to *ANY* must be allowed.

For further information, see [IP ports](#).

The firewall service must be started.

¹provided the default ports are used

5.3. Preparing SQL Server databases

Make sure that the following requirements are met:

- The Scout Server machines must be provided with suitable ODBC drivers to connect to the SQL database. For further information, see "System requirements" on page 5.
- We recommend that you create the required databases in Microsoft SQL Server before you install the Scout Enterprise Management Suite.¹

Note

For all databases, the database tables are created automatically by the Scout installer.

For further information, see "Database support" on page 9.

- SQL or AD users (**SQL server\Instance> / Security / Logins**) with relevant permissions for all databases

For further information, see "SQL Server users and application roles" on page 13.

- The Browser service on the SQL server must be started.

¹Alternatively, new Scout databases can be created in Microsoft SQL Server during the installation, relevant rights provided.

5.4. Permissions and certificates

Permissions for the Scout Enterprise Management Suite installation

- AD administrator account, member of the local administrators group on the target system
- The account must be provided with the local user right **Log on as a service** if you use LocalDB.

For information on how to authenticate to LocalDB, see "SQL LocalDB" on page 11.

For information on how to authenticate to SQL Server, see "Authentication to SQL Server" on page 12.

Note

The account of the installing administrator is the first active account of the Scout Console after the Administrator policies have been enabled.

Permissions for the web server

On the web server, one or more eLux containers provide eLux software packages and images.

- Web Server (IIS) role or relevant permissions for the web server used
- Administrator rights on the root directory for the installing administrator
- Write access on the eLux container directory for all users that are allowed to create or modify images in ELIAS

Permissions for Scout Board

Logon via Active Directory is already supported in the Technical Preview. The administrator rights are applied as defined in the Scout Console under **Security > Activate administrator policies**.

SSL certificates for Scout Keep Alive service and Scout Board

The communication between eLux and the Scout Keep Alive service¹ is based on the HTTPS protocol. For this, during installation, you are asked to specify a valid SSL certificate. Alternatively, you will be offered a self-signed certificate. For further information, see "Certificate for Scout Keep Alive service" on page 60.

For a secure connection to the Scout Board interface, also a valid SSL certificate is required. For further information, see **Installing Scout Board**.

¹from Scout 15 2209. Previous versions: Scout Statistics Service

eLux certificates for software packages

If you want to verify the signatures of the eLux software packages with ELIAS, you will need the relevant certificates:

- ▶ Download the package certificates from our myelux.com portal under **eLux Software Packages**.

5.5. Downloading software

Before you start the installation, download the .zip files required for the software you want to install:

- Scout Enterprise Management Suite
- Scout Enterprise ELIAS 18 for creating individual firmware images
- eLux software packages for the relevant operating system version
- USB stick image for the recovery installation of individual devices for the relevant operating system version
- ...

1. Sign in to our myelux.com portal.
2. On the **Download** menu, choose the relevant software:

Option	Description / Option	Download
eLux	eLux Software Packages Latest operating system versions, LTSR ¹ or CR ²	<ul style="list-style-type: none"> ■ Bundle: With eLuxRP-x.x.x AllPackages-x, you can install a container including all software packages in one step³ or import into ELIAS 18. ■ Individual packages: Under Release Packages, all available software packages of an eLux version are provided for download.
eLux	eLux USB Stick Images Ready-to-use images for USB installation of the latest eLux version	<ul style="list-style-type: none"> ■ <eLux CR version> Recovery Stick ■ <eLux LTSR version> Recovery Stick <p>includes the Citrix Workspace-App and the VMware Horizon client to connect against a backend</p>
eLux	eLux Portable eLux on a USB stick, based on latest eLux RP version	eLux Portable (no installation needed)

¹Long Term Service Release

²Current Release

³includes the installation file eLuxContainer.exe

Option	Description / Option	Download
Scout	Scout Enterprise Management Suite	<ul style="list-style-type: none"> ■ <Scout CR version> ■ <Scout LTSR version>
	Latest LTSR and CR versions	includes the installation file <code>ScoutInstaller.exe</code>
ELIAS		
	Latest ELIAS 18 version for creating and managing individual images	<ul style="list-style-type: none"> ■ ELIAS 18 <current version> for Windows ■ ELIAS 18 <current version> for Linux
	The Scout Enterprise Management Suite alternatively includes the legacy ELIAS program.	
	Scout Agent for Windows for managing Windows devices	Latest version
Scout Cloud Gateway	Gateway to connect your eLux devices through the Internet (latest version)	<ul style="list-style-type: none"> ■ Virtual Machine template (.ova) or ■ Debian package
Tools	StickWizz	Latest version (StickWizz is also included in the eLux USB Stick images)
	eLux Builder Kit (eLux SDK VM)	Please contact sales(at)unicon.com
	Development environment	
	Win2eLux	■ Win2eLux for 64-bit Windows
	Migrate from Windows to eLux	■ Win2eLux for 32-bit Windows

- To download the relevant file, click the file name or version number.
The software is downloaded in the form of .zip files.
- Unpack the .zip files.
- Provide the installation files such as `ScoutInstaller.exe` on a local hard drive.
- To create a recovery stick, connect an empty USB stick to a USB port. Start the `StickWizz.exe` application of the zip archive, and then write the image to the stick. For further information, see Creating a USB recovery stick in the **eLux recovery procedures** guide.

6. Installation: Scout Enterprise Management Suite

The Scout Enterprise Management Suite includes all features that are necessary or useful for managing a client infrastructure, in particular the Scout Server and the Scout Console.

To enable administrators to create individual firmware images, **one** of the following software components must be installed additionally:

- **ELIAS 18**

Here, you will import the eLux software packages for creating client firmware images later on. For further information, see "Installation: ELIAS 18" on page 49.

or

- If you use the legacy ELIAS included in the Scout Enterprise Management Suite:¹

eLux container with a compilation of software packages to be installed on a web server
For further information, see "Installation: eLux Container" on page 45.

6.1. Features of the Scout Enterprise Management Suite

Scout Enterprise Management Suite is the management solution for cloud devices, Hybrid Clients, mobile devices and PCs running the operating system eLux. In addition, Windows-based devices can be managed by using basic Scout management features.

Scout Enterprise Management Suite consists of several components. Most of the components listed below are included in the standard installation but can be optionally excluded when choosing custom installation.

Component	Description	Installation
Scout Server	The service controls and manages eLux devices as well as Windows devices on which Scout Agent for Windows has been installed.	ScoutInstaller.exe
Scout Console	User interface for the management of eLux devices and Windows-based devices on which Scout Agent for Windows has been installed Server communication only via database Multiple consoles can be managed with one Scout database.	ScoutInstaller.exe
Scout Board	Web user interface for the management of eLux devices and Windows-based devices on which Scout Agent for Windows has been installed	ScoutInstaller.exe

¹Choose user-defined installation and select it as a feature.

Component	Description	Installation
Recovery service	Customized TFTP service to realize a PXE recovery environment for eLux endpoints	ScoutInstaller.exe
ELIAS ¹	Legacy dialog program eLux Image Administration Service (ELIAS) for creating individual image definition files (.idf) for modular firmware updates of the eLux devices. The legacy ELIAS will be replaced by ELIAS 18.	ScoutInstaller.exe
ELIAS 18	New web-based platform-independent ELIAS application for creating individual image definition files (.idf)	separate (EliasInstaller.exe)
Scout Report Generator	Tool for creating freely definable reports across all currently existing devices, applications and OUs in the Scout Console Is launched from the Scout Console	ScoutInstaller.exe
Scout Keep Alive service ²	Windows service processing keep alive packets from eLux devices	ScoutInstaller.exe
Web API	Application programming interface for the management of eLux devices and for the management of Windows-based devices on which Scout Agent for Windows has been installed	ScoutInstaller.exe
Scout Command Interface	Command line interface for Scout commands	ScoutInstaller.exe
Scout Database Connection Editor	Tool for modifying database connection settings of the Scout Server and Scout Console	ScoutInstaller.exe

Further products

Scout Cloud Gateway	Cloud gateway with VPN backend for convenient connection of devices from the Internet to a Scout infrastructure	separate
Scout Agent for Windows	Service providing an interface for Windows-based devices to be managed through Scout Enterprise Management Suite	separate

The features are described in the following guides:

¹The legacy ELIAS is no more included in the standard installation. To include it, choose **User-defined**.

²Replaces the Scout Statistics Service from Scout 15 2209

- Scout Enterprise Management Suite:
Configuration, control and management of the eLux devices using the Scout Console
- Scout Board
- Scout Cloud Gateway
- ELIAS
- ELIAS 18
- Scout Report Generator
- Scout Command Interface

Recovery procedures for eLux devices are described in the **eLux Recovery procedures** short guide.

Note

To compose and use your own image files, in addition to the Scout Enterprise Management Suite installation, you need an ELIAS 18 installation. If you use the legacy ELIAS instead, you need an eLux container for the software packages, see [Installing a container](#).

6.2. Installing Scout Enterprise Management Suite

Note

Before you start to install, make sure you have read the topics "System requirements" on page 5 and "Preparing for installation" on page 19.

When you run the Scout Enterprise Management Suite installer, we recommend to choose the standard installation scope which includes all features except of the legacy ELIAS. Then install the new web-based ELIAS 18 separately.

Alternatively, choose the `user-defined` option and select the features to be installed. Here you can still add the legacy ELIAS. For further information on the provided components, see [Features of the Scout Enterprise Management Suite](#).

Note

Run the installer from a local hard drive. Do not use a USB stick, CD-R drive or a network drive.

Note

Anti-virus programs can have an impact on the installation. If required, disable the anti-virus program before you perform the installation.

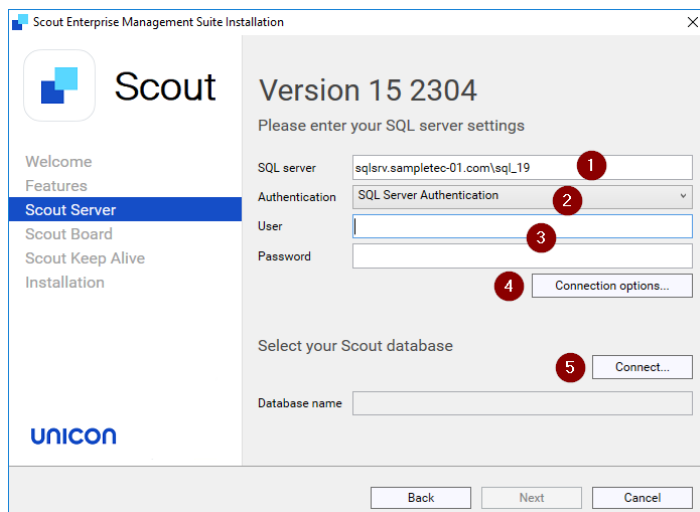
1. Run the `ScoutInstaller.exe` file as administrator.
2. Select the installation language. Subsequently, read and accept the license terms.
3. Select the database type you want to use:
 - Microsoft SQL Server
 - Microsoft SQL LocalDB

For further information, see "Database support" on page 9.

4. Select the type of installation. The `Service provider` option is only relevant for Managed Service Providers (MSPs) who want to offer Scout as a service and have an MSP account on our myelux.com portal. For further information, see the **Scout for MSPs** guide.
5. Choose the installation scope. To select individual features for installation or change the installation directory, select `User-defined`. For the standard installation, select `Standard`.
6. Specify the database connection data for your **Scout database**.

If you use Microsoft SQL LocalDB, enter the relevant Windows account name and password. For further information, see "SQL LocalDB" on page 11.

If you use Microsoft SQL Server, specify the required data to connect to the SQL Server machine:



- 1 <SQL Server machine\instance>
Example: sqlsrv.sampletec-01.com/sql_19
- 2 SQL Server authentication or Windows authentication
For further information, see "Authentication to SQL Server" on page 12.
- 3 SQL or Windows username and password for database access
- 4 SQL Server connection options:
 - For AlwaysOn Cluster: Faster reconnection after fail-over
 - Use encrypted ODBC connection
 - Trust server certificate (enabled by default)
- 5 Click to connect to the database server.

Click **Connect...**, and then, from the list-field, select your **Scout** database.

Note

To show the databases on the specified SQL server, the SQL Server Browser service must be active.

*Next to **Database name**, the selected database will be shown.*


7. In the next dialog, edit the **Scout Board** options.¹
Enter the port number for the Scout Board service, and then the computer name (FQDN) of the machine on which the database layer is to run. For further information, see **Installing Scout Board** in the **Scout Board** guide.
8. In the next dialog, edit the options for the **Scout Keep Alive service** database.²
Specify the TCP port.

¹optional component, from Scout 15 2209

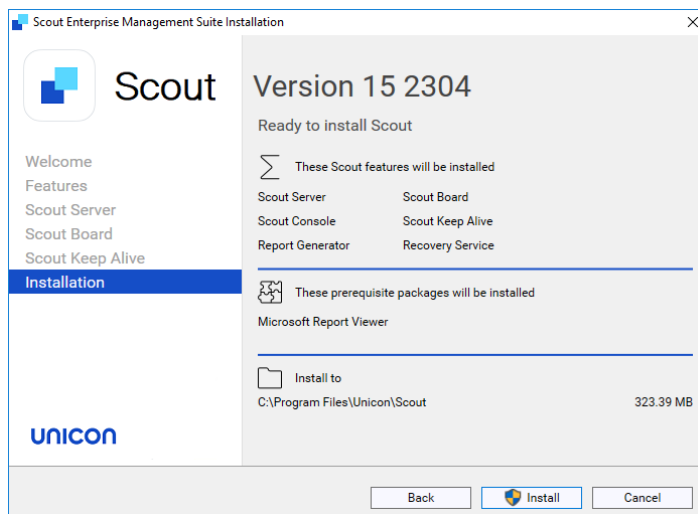
²optional component, from Scout 15 2209

With **HTTPS**, a secure connection to the interface is used. Specify a valid SSL certificate. Alternatively, let the system create a self-signed certificate, and then continue with the Scout installer.

Note

Click  to update the list-field content and select the newly created certificate. Any certificates available are shown with their assigned **friendly names**. If there is no friendly name or it is assigned more than once, their serial number is shown.

9. In the last step, check the overview of all features to be installed. To start the installation process, click **Install**.



If required software components such as Visual C++ Redistributable or Microsoft Report Viewer are not yet available on the target system, they will be installed by the installer.

Once the installation is completed, you will find shortcuts for the Scout Console and Scout Board on the desktop. In the Scout group of the Windows Apps view, you will find all Scout applications including the Scout Database Connection Editor.

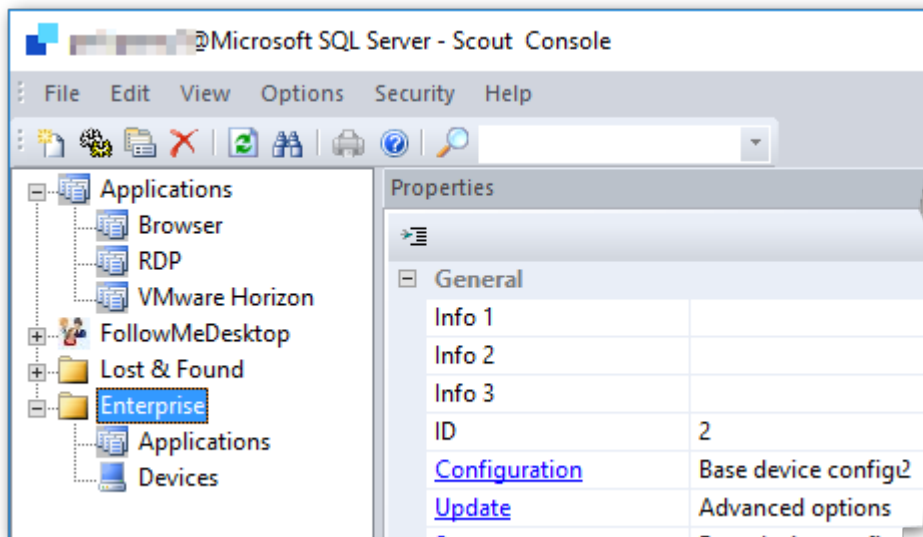
6.3. After the initial installation

The newly installed Scout Enterprise Management Suite can be evaluated without licenses for up to 5 devices and up to 3 months without functional limitations. After 3 months or with more than 5 devices, licenses must be added.

After you have completed the installation with an empty Scout database, for your Scout Console the following is provided:

- A default account `administrator` with password `elux`
 - ▶ Change the password immediately to prevent unauthorized access:
 - [Change console password](#) or
 - [Activate administrator policies](#)
- On the top level, three applications are predefined to connect to a back-end: **RDP**, **VMware Horizon** and the **Firefox** web browser.
 - ▶ To use one of the applications, modify the properties of an application definition and provide the relevant software by means of an IDF for the devices. For further information, see [Defining applications](#).
- A top-level organizational unit (OU) named **Enterprise** is created.
 - ▶ Under the top-level OU, add further OUs corresponding to your corporate structure. For further information, see [Organizational structure](#).

Note: The hyperlinks above are related to the sections of the **Scout** guide.



6.4. Unattended installation

Note

The following information refers to Scout Enterprise Management Suite 15.2302 and later. It includes the installation of Scout Board and Scout Keep Alive service. Information on earlier versions¹ can be found in the **Archive** section of the [PDF downloads](#) page.

Performing an unattended installation of the Scout Enterprise Management Suite

- ▶ Run the `ScoutInstaller.exe` file along with the required command-line parameters:
`"ScoutInstaller.exe" /s /v"<parameter>" /v"<parameter>"`
 You can add as many parameters as you like.

Creating a command line for unattended installation

Create a batch file for unattended installations by using a one-time manual installation according to the desired criteria.

1. Perform a manual installation of the Scout Enterprise Management Suite with the required components and options.
2. Open the log file created during the installation in a text editor:
`%LOCALAPPDATA%\Temp\Scout_Enterprise_Management_Suite_<time stamp>.log`
3. Under `Silent install command line`, copy the command line created by the manual installation.
4. Create a batch file that contains the copied command line.
Passwords have been removed and must be entered manually.
5. Replace the `<SET_PASSWORD>` strings for the database passwords by the relevant clear text passwords.
 If you want to use encrypted passwords, add `_CRYPTED` to the parameter names, see below.

List of parameters

The following tables summarize the available parameters and the values they can be given. On the left, **default values** are displayed in **bold**.

Note

To encrypt passwords, you can use environment variables. For further information, see "Encrypting values" on page 69.

Parameters for /v

¹including Scout Statistics Service and Scout Dashboard

Parameter	Description
UCPROP_DBTYPE=2	2 - Microsoft SQL Server 5 - Microsoft SQL LocalDB
UCPROP_DBNAME=Scout	Name of the Scout database
UCPROP_DBSERVER=sqlsrv.sampletec-01.com\sql_12	Database server (and instance) of the Scout database
DB_SCOUT_DB_AUTHENTICATION=Windows Authentication	Windows Authentication SQL Server Authentication
UCPROP_DBUSER=Scout-Admin	Only for SQL Server authentication: SQL username for the Scout database
UCPROP_DBPASSWORD_CRYPTED=u[D`Gqu[w_	Only for SQL Server authentication: Crypted password for the Scout database, see eluxd.ini
UCPROP_DBPASSWORD=My_Password	Only for SQL Server authentication: Unencrypted password for the Scout database
UCPROP_SERVICEUSER	Only for Windows authentication: Windows username
UCPROP_SERVICEPASSWORD_CRYPTED	Only for Windows authentication: Encrypted Windows password
UCPROP_TRUSTSERVERCERTIFICATE=1	Trust the database server certificate
UCPROP_ENCRYPT=0	0 - Use unencrypted ODBC connection 1 - Use encrypted ODBC connection
UCPROP_MULTISUBNETFAILOVER=0	0 - Default 1 - Faster reconnection after fail-over (AlwaysOn Cluster)
UCPROP_DBCREATE=0	0 - Scout database will not be recreated 1 - Scout database will be recreated
UCPROP_LANGUAGE=1	Display language 0 - German 1 - English If the parameter is not set, the language defined in the operating system is used.
RUNSCOUTSERVICE=true	true - Scout services will be started during installation false - Scout services will not be started

Default settings for the devices (base device configuration)

UCPROP_DESKTOP_ LANGUAGE=en_US	Display language for the desktop
UCPROP_KEYBOARD_ LANGUAGE=en	Keyboard language
UCPROP_TIMEZONE=US/Eastern	Time zone

Features

ADDLOCAL= Server,Console,Report	Only the specified Scout features will be installed. CommonFeature Server Console Recovery Elias Report
INSTALL_SCOUT_FEATURE=1	0 - Scout components will be skipped 1 - Scout components will be installed (as defined in ADDLOCAL)
INSTALL_SCOUTBOARD_ FEATURE=1	0 - Scout Board will be skipped 1 - Scout Board will be installed
INSTALL_SCOUTKEEPALIVE_ FEATURE=1	0 - Scout Keep Alive service will be skipped 1 - Scout Keep Alive service will be installed

Scout Board

UCPROP_SCOUTBOARD_ HOST=scout.sampletec-01.com	Computer name (FQDN) of the machine on which you want the database layer to run
UCPROP_SCOUTBOARD_ PORT=22160	Port number of the Scout Board service
UCPROP_SCOUTBOARD_ DBLAYER_ ADDRESS= tcp://scout.sampletec- 01.com:22150	Scout Board database layer address
UCPROP_SCOUTBOARD_ DBLAYER_ADDRESS_ PUBLISH=scout.sampletec- 01.com:22151	Public address of the Scout Board database layer

Scout Keep Alive service

UCPROP_SCOUTKEEPALIVE_ DBSERVER=sqlsrv.sampletec- 01.com	Database server (and instance) for the keepalive data These are normally stored in the Scout database, but can also be stored in a separate database.
--	---

UCPROP_SCOUTKEEPALIVE_
DBUSER

UCPROP_SCOUTKEEPALIVE_
DBNAME=Scout

UCPROP_SCOUTKEEPALIVE_
DBPASSWORD

UCPROP_SCOUTKEEPALIVE_ AUTHENTICATION=Windows	Windows SQL Server
--	-----------------------

UCPROP_SCOUTKEEPALIVE_
SERVICEUSER

UCPROP_SCOUTKEEPALIVE_
SERVICEPASSWORD

UCPROP_SCOUTKEEPALIVE_
TRUSTSERVERCERTIFICATE=1

UCPROP_SCOUTKEEPALIVE_
ENCRYPT=0

UCPROP_SCOUTKEEPALIVE_
MULTISUBNETFAILOVER=0

UCPROP_SCOUTKEEPALIVE_ CERTIFICATES=CREATESELF SIGN	Certificate name or automatically created self-signed certificate
--	--

UCPROP_SCOUTKEEPALIVE_PORT- T=22124	Port number of the Scout Keep Alive service
--	---

Further parameters

/s	Th installation will be performed in unat- tended (silent) mode.
/uninstall	The Scout Enterprise Management Suite will be uninstalled.
/I "%PUBLIC%\Documents\UniCon\scoutlog.txt"	The log file will be forwarded to the spe- cified file.

Example for an unattended installation

```
ScoutInstaller.exe /s /v"UCPROP_DBTYPE=2" /v"UCPROP_DBNAME=Scout"
/v"UCPROP_DBSERVER=sqlsrv.sampletec-01.com\sql_12"
/v"DB_SCOUT_DB_AUTHENTICATION=SQL Server Authentication"
/v"UCPROP_DBUSER=Scout-Admin"
/v"UCPROP_DBPASSWORD_CRYPTED=u[D`Gqu[w_ " /v"UCPROP_DESKTOP_LANGUAGE=de"
/v"INSTALL_SCOUTBOARD_FEATURE=1"
/v"UCPROP_SCOUTBOARD_HOST=scout.sampletec-01.com"
/v"UCPROP_SCOUTBOARD_PORT=22160"
/v"UCPROP_SCOUTBOARD_DBLAYER_ADDRESS=tcp:/scout.sampletec-01.com:22150"
/v"UCPROP_SCOUTBOARD_DBLAYER_ADDRESS_PUBLISH=tcp://scout.sampletec-
01.com:22151"
/v"ADDLOCAL=CommonFeature,Server,Console,Recovery,Report"
/v"INSTALL_SCOUTKEEPALIVE_FEATURE=0"
/v"INSTALLDIR=C:\Program Files\Unicon\Scout"
```

Note

When you perform an attended installation and select the required options, an `eluxd.ini` file will be created in the Scout Server directory. This file contains several Scout values that might be useful for unattended installation.

Performing unattended uninstall

- ▶ Run the following command:
"ScoutInstaller.exe" /s /uninstall

6.5. Upgrading to newer versions

An existing Scout Enterprise Management Suite installation can be updated to the latest version in just a few steps.

1. Perform a full database backup of your Scout databases.
For further information on backing up a Local DB, see "Performing a backup of SQL LocalDB before installing updates" on page 11.
2. Download the latest version of the Scout Enterprise Management Suite as a .zip file from our technical myelux.com portal.
3. Unpack the .zip file and provide the installation file on a local hard disk.
4. Run the `ScoutInstaller.exe` file as administrator.
5. Follow the instructions of the installation Wizard. Select your existing Scout databases.

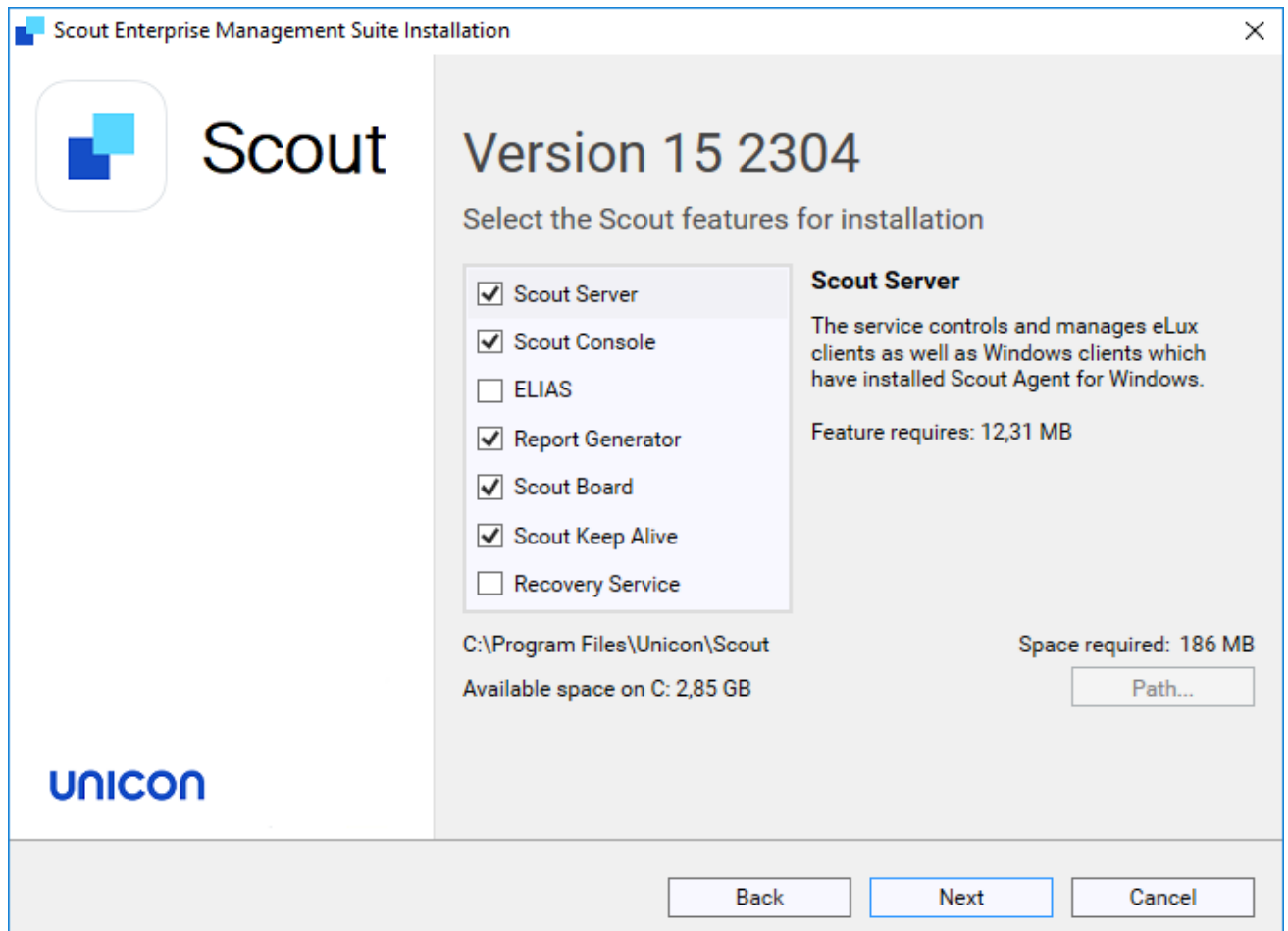
Depending on the extent of new features, upgrading to a new version might cause longer runtimes when the Scout database is converted.

Important To upgrade to Scout 15 2204 or later versions, the upgrade base must be Scout 15.2.0 or later. Any older databases cannot be converted and will not be accepted by the installer.

6.6. Modifying Scout Enterprise Management Suite

Installing additional features or uninstalling unneeded features

1. Use the control panel (Apps and Features) or run the `ScoutInstaller.exe` setup file as administrator.
2. In the Scout installation dialog, select the **Modify** option and click **Next**.



The installed features are shown with a checkmark.

3. Select the check boxes of the features you want to install. Clear the check boxes of the features you want to uninstall.

Note

If you clear the selection of an installed feature, it will be uninstalled.

Repairing installation

1. Use the control panel (Apps and Features) or run the `ScoutInstaller.exe` setup file as administrator.
2. In the Scout installation dialog, select the **Repair** option and click **Next**.

The Scout Enterprise Management Suite is checked for missing files, shortcuts and registry settings and will be repaired if necessary.

6.7. Uninstalling Scout Enterprise Management Suite

1. Use the control panel (Apps and Features) or run the `ScoutInstaller.exe` setup file as administrator.
2. In the Scout installation dialog, select the **Uninstall** option and click **Next**.

7. Installation: eLux Container

Note

If you use the web-based ELIAS 18, there is no need to install the eLux container. In ELIAS 18, you simply import the relevant software packages or the `AllPackages` bundle. For further information, see [Importing software packages](#) in the **ELIAS 18** guide.

The eLux container is a compilation of software packages used to create the firmware (IDF) of a client. The administrator selects a subset of the software package pool to define an IDF (Image definition file) that can be installed on the devices.

The software packages can be provided via the container installation on a web or FTP server (legacy ELIAS) or via the ELIAS 18 web service in a MongoDB (locally or in combination with IIS).

For the main operating system versions, eLux RP 6 / 32-bit and eLux RP 5, dedicated containers are provided. Current eLux RP 6 / 64-bit versions are installed under `...\eluxng\UC_RP6_X64`.

7.1. Installing a container

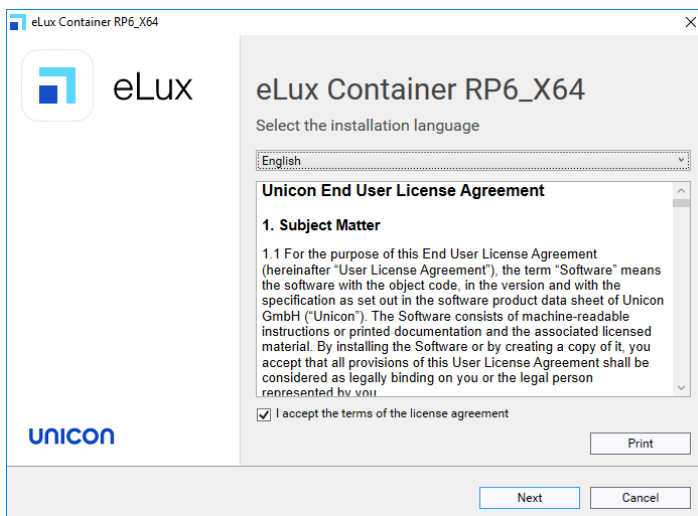
- applies only if you use the legacy ELIAS -

The following instructions show how to install an eLux container including all software packages that are provided on our portal for the selected operating system version.

Note

Before you start to install, make sure you have read the topics "System requirements" on page 5 and "Preparing for installation" on page 19.

1. Run the `eLuxContainer.exe`¹ file as administrator from a local drive.



2. Select the installation language. Subsequently, read and accept the license terms.
3. Select the type of server that you use as the source server for firmware updates:
 - ☒ HTTP
 - ☒ FTP
4. Specify the access data for the FTP or HTTP server:

Option	Description	Example
Root directory	Root directory of the server, local or network drive	W:\inetpub\wwwroot C:\Program Files\inetpub\ftproot
URL	complete URL to access the server	http://update.sampletec-01.com ftp://update.sampletec-01.com

¹Extracted Allpackages archive

5. If you use FTP, in addition, specify the logon data:

Option	Example
Username	anonymous
Password	elux@sampletec-01.com

The last dialog summarizes the required hard disk space.

6. To start the installation, click **Install**.

On the web or FTP server, a UC_RP6_X64 directory is created to hold the eLux RP 6 container. The `container.ini` file and the software packages (`.epm`, `.fpm` and signature files) are provided in the container. In ELIAS, you can create your own image now.

7. If the Scout Enterprise Management Suite is already installed, connect from the Scout Console to the eLux container in ELIAS: In the Scout Console, click **Options > ELIAS settings...** and specify the path pointing to the newly created container on the web/FTP server.

7.2. Updating to a later version

- applies only if you use the legacy ELIAS -

Updating the eLux container can become necessary when the latest operating system version or fixes are provided, or when new versions of the client applications are available.

Updating to new major or minor version

New major or minor versions of eLux are provided as releases on our portal.

- ▶ Use the latest `Allpackages` bundle to install a container.

If you upgrade to a new major version, a new container (Example: `UC_RP6_X64`) is created into which the software packages of the new eLux version are installed.

If you update to a new minor version, the new software packages are added to the existing container. The existing software packages remain unchanged.

Updating individual software packages

1. On our portal, from the relevant container, download the required package as a `.zip` file.
*The **Details** of each package in the container show the relevant enhancements and the history.*
2. Import the `.zip` file into your eLux container by using the ELIAS command **Container > Import Package**. For further information, see [Importing packages into a container](#) in the ELIAS guide.

7.3. Uninstalling an eLux container

- applies only if you use the legacy ELIAS -

1. Use the control panel or run the `eLuxContainer.exe` setup file as administrator.
2. In the installation dialog, select the **Uninstall** option and click **Next**.

8. Installation: ELIAS 18

Note

In ELIAS 18, you manage the eLux software packages for your firmware images. The ELIAS 18 installation replaces the container installation and the legacy ELIAS component of the Scout Enterprise Management Suite

ELIAS 18 is a web service that can be run stand-alone or in combination with Microsoft IIS.¹ ELIAS 18 can be operated on Windows or Linux.

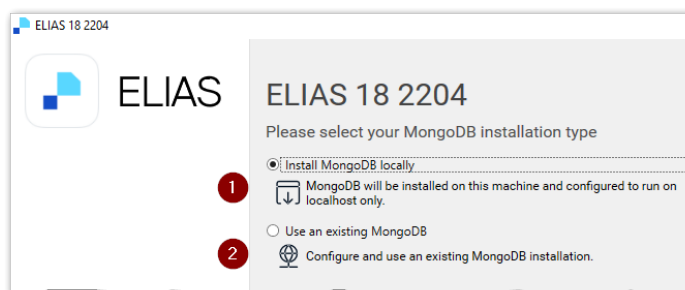
ELIAS 18 is platform-independent and offers more functionality and convenience than the legacy ELIAS. For further information, see [Overview](#) in the **ELIAS 18** guide.

8.1. Installing ELIAS 18 / Windows

Note

Before you start to install, make sure you have read the topics [System requirements](#) and [Preparing for installation](#).

1. Run the `EliasInstaller.exe` file as administrator.
2. Select the installation language. Subsequently, read and accept the license terms.
3. Select whether to install MongoDB locally or to use an existing MongoDB installation.



- 1 The database will only be available on the local host.
- 2 To use an existing MongoDB installation, in the next step, specify the MongoDB connection data.

For an **existing** MongoDB installation, note the following:

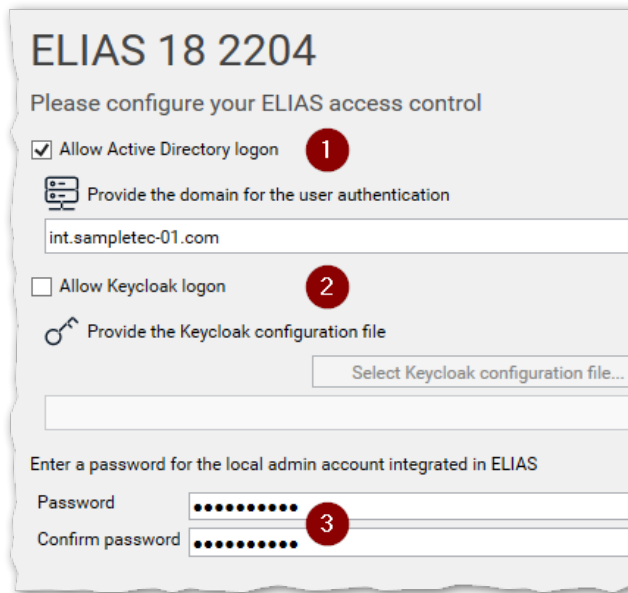
- If you want your administrators to access the same MongoDB installation from multiple web servers, use different databases within the MongoDB installation.
- Specify the MongoDB server address with its port number, and the user credentials. Depending on the configuration of your MongoDB installation, specify additional options, for example, to connect to a specific replica set with timeout. MongoDB creates a URL connection string from the information provided. For further information, see <https://docs.mongodb.com/manual/reference/connection-string/>

¹Other web servers can be used, but without configuration support.

Note

From ELIAS 18 2104, all containers are stored in one database. This allows administrators to create additional containers later on, independent of the database user. The database prefix is no longer required.

4. In the next step, enter a name for your ELIAS database.
5. Then specify your ELIAS access control:



- 1 AD domain for Active Directory user authentication

Example: `int.sampletec-01.com`

Domain users need to be registered in a specific AD group. For further information, see [Access management via AD](#) in the **ELIAS 18** guide.
- 2 Configuration file of the Keycloak server for Keycloak authentication¹

Example:
`C:\install\ELIAS\keycloak.json`

For further information, see [Access management via Keycloak](#) in the **ELIAS 18** guide.
- 3 Password for the local **admin** account

Note that the **Domain** and **Password** fields relate to two different logon types. For further information, see [Access management and logon](#) in the **ELIAS 18** guide.

6. Configure your web server settings:

¹If you add the Keycloak configuration file after the installation, subsequently restart the ELIAS service.

If there is no IIS on your system, the ELIAS web service is installed on port 80 unless you specify another port number.

If an IIS already exists on the system, select the option **Use IIS for ELIAS redirection**. In this case, ELIAS is installed on port 22130 to avoid a conflict with web server port 80. To make ELIAS accessible via the default ports 80/443, it is registered using the reverse proxy procedure and the specified sub-directory.

Specify the web site name and a path name for ELIAS.

To use HTTPS, an external web server such as IIS is required. The web site must be bound to port 443.

Note

To configure your devices for updates, specify the path name defined here on the **Firmware** tab of the device configuration in the Scout Console

7. Confirm or change the installation path.
8. To start the installation, click **Install**.

*After the installation is completed, you will find an **ELIAS** desktop icon containing the URL of your ELIAS 18 installation. Double-click it to open ELIAS in the default browser.*

Cross-origin requests

After installation, cross-origin resource sharing (CORS) is allowed only from the installation server network (FQDN) for security reasons. This server is set by the installation routine under **allowedOrigins**. Administrators outside this network cannot access the installation.

- ▶ To allow access from other networks, add additional servers with their FQDN in the `config.json` file under **allowedOrigins**. Optionally add a port number after the server name with a colon. Separate multiple entries by comma.

Using the wildcard character, you can also configure global access. However, we do not recommend this for security reasons. Example: `"allowedOrigins": ["*"]`

8.2. Installing ELIAS 18 / Linux

- The following instructions refer to ELIAS 18 2209 or later versions -

ELIAS 18 can also be used in a Linux environment. A Debian package (.deb) tested with Ubuntu 20.04 is available for this purpose.



Requires

A MongoDB database must be available either locally or remotely. The database requires sufficient hard disk space for container management, see also [System requirements](#).

1. From our myelux.com portal, under **Downloads > Scout> ELIAS**, download the provided Debian package of **ELIAS 18 <version> for Linux**.
2. Install the Debian package by using appropriate package management tools (Debian/Ubuntu).

Example: `sudo apt install ./elias-package.deb`

The files are installed to /opt/unicon/elias.

3. To configure the connection to MongoDB and the web service (back-end configuration), edit the file

`/opt/unicon/elias/server.json`:¹

Option	Description	Default
"server"	<p>MongoDB server name (as FQDN or IP address)</p> <p>For a local installation, use "localhost".</p> <p>Append the port number to the server name after a colon.</p>	"localhost:27017"
"mongoUser"	<p>MongoDB username</p> <p>If you do not use logon data, set an empty string.</p>	" "
"mongoPassword"	<p>MongoDB password</p> <p>If you do not use logon data, set an empty string.</p>	" "
"mongoPasswordEncrypted"	Encrypted MongoDB password	false
"mongoOptions"	optional: Additional MongoDB options	

¹This file remains local.

Option	Description	Default
"adminPassword"	Encrypted password for the local admin account To encrypt passwords, use the bcrypt method with 13 passes.	"elias"
"adGroup"	AD group users need to belong to for logon For further information on available logon types, see Access management and logon in the ELIAS 18 guide.	"ELIAS"
"logLevel"	Log level (debug info warn error)	"debug"
"port"	Port used by the ELIAS API	"22130"
"iisWebsite"	IIS redirection website name, not used on Linux	—

Note

To configure ELIAS for access via Keycloak, see [Access management via Keycloak](#) in the **ELIAS 18** guide.

- For the front-end configuration, edit the file `/opt/unicon/elias/config.json`:

Option	Description	Default/Example
"pollingInterval"	Interval in milliseconds for polling the API by the user interface	3000
"api"	Host name of the device ELIAS is running on (FQDN or IP address)	"<Host name>"
"domain"	AD domain for user authentication Domain users need to be registered in a specific AD group. To enable only the local admin account, set an empty string.	" "
"redirectPath"	Any path that redirects to the API (for example, if Apache is used) Must end in <code>api</code>	"api"

Note

This path must also be specified in the Scout Console, on the **Firmware** tab of the client device configuration.

"protocol"	Either "http" or "https"	"http"
"apiVersions"	Must be set to ["1.0"]	["1.0"]
"base.database"	Name of your ELIAS database If you create multiple containers, all of them will be stored in this database. ¹	"ELIAS-Database"
"port"	Port on which the ELIAS website is reachable externally	"8080"
"allowedOrigins"	List of URLs on which the ELIAS website is reachable externally (separated by comma) Example: "http://<Hostname or IP address>:8080"	

5. Restart the ELIAS service.

Example: `sudo systemctl restart scout-enterprise-elias`

Reverse proxy for the web server

For performance or security reasons, you can configure a simple reverse proxy to handle SSL encryption and decryption. A configuration for **Apache** might look like the following:

```
<IfModule mod_ssl.c>
<VirtualHost *:443>
    ServerName elias.dev.sampletec-01.com
    ProxyPreserveHost Off
    ProxyRequests off
    SSLProxyEngine On
    <Proxy *>
        Require all granted
    </Proxy>
    ProxyPass / http://localhost:22130/
    ProxyPassReverse / http://localhost:22130/

# Insert your certificate file names:
SSLCertificateFile /etc/ssl/private/ca-certificate.crt.pem
SSLCertificateKeyFile /etc/ssl/private/ca-certificate.key.pem

SSLEngine on

# Intermediate configuration, tweak to your needs:
SSLProtocol          all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
```

¹from ELIAS 18 2104

```
SSLCipherSuite          ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-
ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-
CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384
SSLHonorCipherOrder    off
SSLSessionTickets      off

SSLOptions +StrictRequire

# Add vhost name to log entries:
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\"" vhost_combined
LogFormat "%v %h %l %u %t \"%r\" %>s %b" vhost_common

</VirtualHost>
</IfModule>
```

Customize the data such as server name and certificate files to your configuration.

We also recommend creating a second configuration file to redirect communication arriving unencrypted via port 80 to port 443. Example:

```
<VirtualHost *:80>
RewriteEngine on
RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI} [END,NE,R=permanent]
</VirtualHost>
```

Again, customize the data to fit your configuration.

For the configuration files to be executed, proceed as follows:

1. Copy your **.conf** files to `/etc/apache2/sites-available`
2. Provide them to `/etc/apache2/sites-enabled`
for example with `a2ensite <filename>.conf`
or via symlink, for example `ln -s sites-available/<filename>.conf sites-enabled/<filename>.conf`
3. Restart the web server:
`systemctl reload apache2`

8.3. Starting ELIAS 18



Requires

ELIAS has been installed successfully. For further information, see [Installation: ELIAS 18](#) in the **Installation** guide.

ELIAS is started with an URL pointing to your installed ELIAS web service.

Without IIS:

- ▶ In the web browser, type the following URL:
`http://<host name>:<port number>` or
`https://<host name>:<port number>`
`<host name>` refers to the computer name or IP address of the computer ELIAS is installed on.
`<port number>` is the port you have specified for the ELIAS web service

With IIS redirection:

- ▶ In the web browser, type the following URL:
`http://<host name>/path` or
`https://<host name>/path`
`<host name>` refers to the computer name or IP address of the computer ELIAS is installed on / your web server.
`<path>` is the specified ELIAS path name under your web site (`elias` in the example above)

Note

The computer ELIAS is installed on provides an ELIAS desktop icon.

For access from outside the network, see [Installation: ELIAS 18](#) in the **Installation** guide.

8.4. Updating to newer ELIAS version

An existing ELIAS 18 installation can be updated to the latest version in just a few steps.

Note

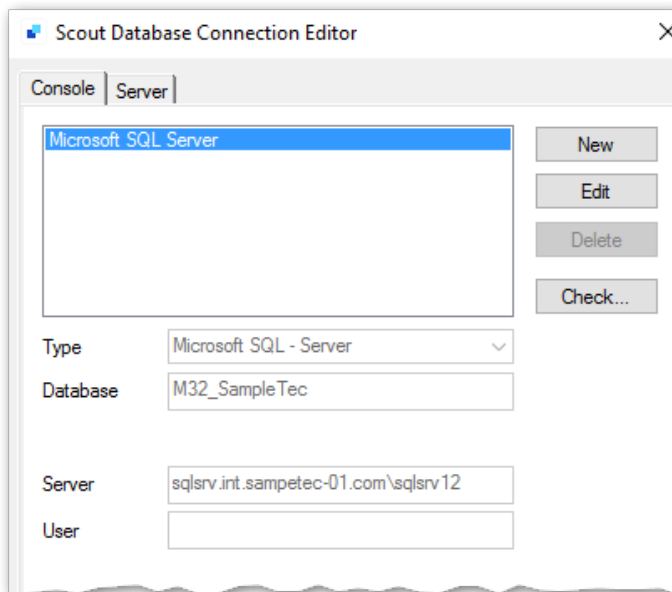
From ELIAS 18 2104, all containers are stored in one database. If you manage multiple containers in an earlier ELIAS-18 installation, the update installation will merge the corresponding databases into one database.

1. Download the latest ELIAS 18 version as a `.zip` file from our technical myelux.com portal (**Download > Scout > ELIAS**).
2. Unpack the `.zip` file and provide the installation file on a local hard disk.
3. Run the `EliasInstaller.exe` file as administrator and follow the instructions of the installation Wizard.

8. Database connections

When you install the Scout Enterprise Management Suite, you are asked to specify the Scout database. Check or modify the database connections at any point in time after the installation.

For the Scout Server and Scout Console, you can use the **Scout Database Connection Editor** to specify one or more connections to the Scout database. You can find the Scout Database Connection Editor as a stand-alone program within the Scout group of the Windows Apps view.



9. Certificates

Various features and applications require certificates to be provided. For (root) certificates on the client, note the following:

- Unless otherwise stated, the certificates must be Base64-encoded (ASCII) with file name extension `.crt`.
- To transfer certificates to the client, use the Scout feature **Files configured for transfer**. For further information, see [Files configured for transfer](#) in the **Scout** guide.
- On the client, the certificates are stored in the local certificate store `/setup/cacerts/` or in a sub-directory.

The following table provides an overview:

Feature	Component	Directory
Smart card user logon The certificates are specified in the Scout Console under Security > User authentication > Certificates	User authentication / AD+smart card	<code>/setup/cacerts/login</code>
Secure connection (TLS)	Firefox	<code>/setup/cacerts/browser¹</code>
Secure connection (TLS)	Chromium	<code>/setup/cacerts/browser</code>
Secure connection (TLS)	Builtin Browser Kiosk mode	<code>/setup/cacerts/browser</code>
Secure connection (TLS)	Citrix Workspace-App	<code>/setup/cacerts/</code> and <code>/setup/cacerts/intcerts</code>
Secure connection (TLS)	VMware Horizon client	<code>/setup/cacerts/</code>
Secure connection (TLS)	eLuxRDP	<code>/setup/cacerts</code>
Network logon	WLAN drivers / WPA-Supplicant (802.1X) X509/Radius Network Access Control / SCEP	<code>/setup/cacerts/</code> <code>/setup/cacerts/scep</code>
VPN / OpenVPN	BaseOS	<code>/setup/openvpn</code>

¹Earlier eLux versions have also used `/setup/cacerts/firefox`

Feature	Component	Directory
VPN / Cisco AnyConnect	Cisco AnyConnect	/setup/cacerts ¹ and /setup/cacerts/client
Firmware update including certificate check	BaseOS	/setup/cacerts

Note

StoreFront can be called using a Citrix session or a browser.

¹from eLux RP 6 2302. Earlier versions require the certificate in /setup/cacerts/ca

9.1. Certificate for Scout Keep Alive service

As the eLux devices and the Scout Keep Alive service communicate via HTTPS, for the installation of the Scout Keep Alive service, a valid SSL certificate for server authentication is required which is bound to port 22124 by default.

As soon as a certificate becomes invalid, you need to bind a new certificate to the port to keep the Scout Keep Alive service running. To do so, on the system the Statistics Service is running on, use the `netsh.exe` tool of the Windows command-line interface.

Note

If the computer has more than one network adapter, the certificate must be bound to all IP addresses.

Viewing the current SSL certificate bindings

1. Launch the command-line interface.
2. Use the following command:

```
netsh.exe http show sslcert
```

All ports with certificate bindings are shown including the relevant information.

Deleting an SSL certificate from a port

1. Launch the command-line interface.
2. Use the `netsh.exe` tool as shown in the following example:

```
netsh.exe http delete sslcert ipport=<IP address of host>:22124
```

Viewing the thumbprints of certificates

Note

Thumbprint corresponds to the certificate hash value.

1. Launch the Powershell. Note that the command is not supported by the normal command-line interface (cmd).
2. Use the following command depending on the certificate store:

```
dir cert:\LocalMachine\My
```

For all certificates available in the Microsoft Management Console, the thumbprints are shown under Local Computer\Personal (with and without binding).

Binding a new SSL certificate to a port

1. Launch the command-line interface.

2. Use the `netsh.exe` tool with the following command:

```
netsh.exe http add sslcert ipport=0.0.0.0:22124 certhash=<thumbprint  
of your certificate> appid={957ba029-e2a1-4a13-b426-645a5e3802e2}
```

The `ipport` parameter specifies the IP address and port.

The `certhash` parameter specifies the thumbprint of the certificate.

The `appid` parameter is the ID of the Scout Keep Alive service and must not be changed.

10. Management protocol

Communication between the Scout Server and the eLux devices can be established via port 22123 or port 22125.

If you are using a firewall, enable the relevant port.

10.1. Certificate-based management protocol

The certificate-based management protocol provides secure communication between the Scout Server and devices via end-to-end encryption with TLS 1.2.

Starting with Scout 15 2107, only devices with **eLux RP 6.2 or later** are supported. For further information, see [Compatibility client platform and Scout Enterprise Management Suite](#) in the **Whitepaper Releases, Lifecycles and Compatibility**.

The certificate-based encryption of the management protocol is carried out via a self-signed certificate automatically generated by the Scout service. Alternatively, you can use a CA certificate that must be configured on the Scout Server.

For the encrypted communication with the Scout Server, port 22125 is used.¹

For TLS 1.2 communication, the following requirements must be met:

- On the devices, the trust level must be specified by using **TlsVerifyOption**. By default, the trust level is set to 0 and the certificate check is disabled.

For further information, see "Configuring the trust level on the devices" on the facing page.

- If you are using a certificate issued by a CA (instead of self-signed), the certificate must be provided in the form of a `px` or `pem` file on the Scout Server. Note that the certificate must not be password-protected. The devices must be equipped with the corresponding root certificates.

For further information, see "Configuring Scout Server for communication via CA certificates" on page 65.

Note

To check the communication via TLS, view the `eluxd.log` log file of the Scout Server service.

¹Up to version Scout 15 2107, devices with earlier eLux versions could be used via port 22123 with AES-256 encryption.

10.2. Configuring the trust level on the devices

The certificate-based encryption of the management protocol for communication between the Scout Server and the eLux client requires the verification of the relevant certificates (Chain of trust). By default, encryption is carried out via a self-signed certificate automatically generated by the Scout Server.

Important If you use a certificate issued by a CA (CA certificate), make sure you transfer the corresponding root certificates to the devices. If the root certificate does not exist on a device and certificate check is enabled, the device can no longer be reached by the Scout Server.

To make it easier, you can perform both steps, enabling the certificate check and transferring certificates in one move.

Important In addition, the Scout Server must be configured accordingly and provide the certificate locally.

1. To enable the certificate check, configure the trust level for the relevant devices with the option **TlsVerifyOption**.

To do so, use the **Advanced file entries** feature of the Scout Console:

File	/setup/terminal.ini	
Section	Security	
Entry	TlsVerifyOption	
Value	0	Certificate is not verified
	1	Certificate is verified
	3	Certificate is verified with additional verification that the Scout Server name matches the Subject Common Name (CN) or Subject Alternative Name (SAN) in the certificate.

For further information, see [Advanced file entries](#) in the **Scout** guide.

2. If you use a CA certificate, make sure you transfer all corresponding root/intermediate certificates of your CA to the devices to `/setup/cacerts/scoutsrv`. This is where the system searches for the required certificates once the certificate check is enabled (Chain of trust).

For further information, see [Files configured for transfer](#) in the **Scout** guide.

3. If you use a CA certificate, in the next step, configure the Scout Server. For further information, see "Configuring Scout Server for communication via CA certificates" on page 65.
4. Restart the devices.

Note

After the `terminal.ini` file has been updated on the device, one more device restart might be required to enable the new setting.

Once you have enabled trust level 1 or 3 for a device, it can only communicate with its Scout Server by using valid certificates. With trust level 3, the device name is verified in addition.

10.3. Configuring Scout Server for communication via CA certificates

Note

This configuration is only required if you are using a certificate that has been issued by a CA.

1. Save the certificate file locally on the Scout Server.
2. On the server machine, in the file system under `%PUBLIC%\Documents\Unicon\Scout\Server\` open the `eluxd.ini` file for editing.

Add the following entries:

Section	Entry	Description
ELUXD	UseSelfsignedCertificate=0	Requires a certificate issued by a CA Use a certificate that is not protected by an additional password. If you set this option (with value 0), you are required to define the next values. Default: 1
ELUXD	CertificateFile= <i>Path to certificate file</i>	Path to the location of the certificate file Example: <code>C:\Users\Public\Documents\Unicon\Scout\Server\sampletec-01.pfx</code>
ELUXD	CertificateKeyFile= <i>Path to private key file</i>	Only required, if the certificate file is not in pfx format

3. Restart the Scout service.
4. Ensure that the certificate check is enabled and the required root/intermediate certificates of your CA are available on the devices (Chain of trust).
For further information, see "Configuring the trust level on the devices" on page 63.

From now on, the Scout Server will only communicate with devices that trust the CA certificate.

11. Troubleshooting

Error message / problem	Reason	Solution
Scout desktop icons are not displayed correctly.	Desktop icons are cached by Windows. This may lead to the fact that after you update Scout, new icons are not displayed correctly.	Delete the Windows icon cache. Please refer to the relevant documentation.
File access error while checking HTTP/FTP server (error number = 404)	Possibly caused by missing MIME type entries for the used file extensions on the web server	<p>In the MIME type settings of the web server, add the file extensions used in eLux containers and assign them to the relevant MIME types.</p> <p>When you install ELIAS 18 or an eLux container on Microsoft Internet Information Server (IIS), the mappings will be performed automatically.</p>

The following MIME types are required and installed with the container:

Extension	MIME type
.dd	text/plain
.epm	text/plain
.fpm	text/plain
.gz	application/x-gzip
.idf	text/plain
.ini	text/plain
.rdf	text/plain
.sig	text/plain
.xz	application/x-xz

The following additional assignments might become necessary:

Extension	MIME type	Description
.bin	application/octet-stream	BIOS update via Scout
.bup	text/plain	BIOS update via Scout
.cab	application/vnd.ms-cab-compressed	UEFI update via Scout

Extension	MIME type	Description
.mee	text/plain	Migration of eLux RP 5 devices to eLux RP 6 with whitelist ¹ Different images depending on the hardware model (for further information, see Different hardware models)
.udf	text/plain	UEFI updates in analogy to firmware updates ²

Troubleshooting for an installation with Microsoft SQL Server

Error message	Reason	Solution
Cannot initialize the license database.	When checking the database ID, a problem was identified. A database backup was restored on an SQL Server on which the database does not exist. Note: A unique database ID ensures that a Scout license database cannot be used more than once.	Preventive: Restore a database backup only on the SQL Server on which the database backup was created and the database still exists. In case of error: Contact Unicon Support. The Repair database button displays a checksum that can be used by Unicon Support to generate a validation code for repairing the license database.

Troubleshooting for an installation with LocalDB

Error message	Reason	Solution
Your Microsoft Jet Database Engine (MDB) database is not up-to-date	MDB databases are not supported by later versions of the Scout Enterprise Management Suite.	Use Microsoft SQL Server Express LocalDB.
User verification failed	The specified username or password is incorrect.	Make sure that the specified user is available. We recommend using a technical user account.

¹for current eLux versions done by the container installer

²from Scout 15 2107 and eLux RP 6 2107

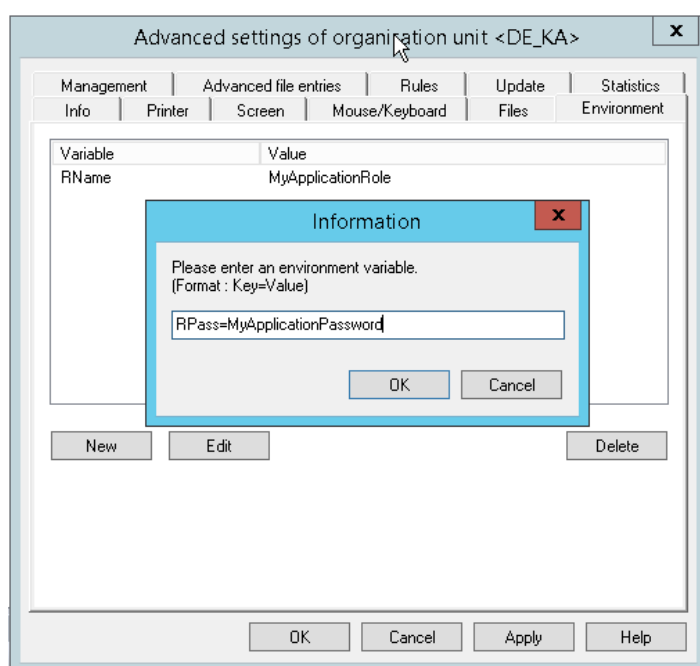
Error message	Reason	Solution
User does not have the right to log on as a service	The account must be provided with the local user right Log on as a service .	Use a technical user account provided with the right Log on as a service to access the LocalDB database.
User does not have administration rights	The user must be a member of the administrator group.	Make sure that the relevant account is provided with administrator rights.

For further information, see "SQL LocalDB" on page 11.

12. Encrypting values

Whenever you need to encrypt values, we recommend that you add and encrypt variables in a temporary OU, and then copy the encrypted values to their target position.

1. In the Scout Console, create a temporary OU such as `TEMP`.
2. For the `TEMP` OU, from the context menu, choose **Advanced device configuration > Environment**.
3. Add a new variable and its value. Confirm with **OK**.



*The new variable and its value is shown in the **Environment** tab.*

4. On the **Environment** tab, right-click the variable, and from the context menu, choose **Encrypt value**.

The value of the variable is shown in encrypted mode.

5. Select the variable and click **Edit**. Then, copy the encrypted value to the Clipboard and paste it on the target position.
6. Delete the temporary OU.

13. Appendix

13.1. Program and file directories

Program directory

The Scout Enterprise Management Suite by default is installed to

```
%PROGRAMFILES%\Unicon\Scout
```

ELIAS 18 is installed according to your specifications during installation, for example on the web server IIS.

The eLux container (only required for the legacy ELIAS) is installed on the web server to

```
<root directory>\eluxng
```

File path for Scout Server files

Scout log files, configuration files and more are saved to a subdirectory of

```
%PUBLIC%\Documents\Unicon
```

- ▶ To open the server files directory in the Windows Explorer, in the Scout Console, click **View > System diagnostics > Server files** (only if console and server are installed on the same machine).

File path for user files

User files are saved to a subdirectory of the local user directory in

```
%USERPROFILE%\Documents\Unicon
```

Diagnostic files that are requested via the console are saved to

```
%USERPROFILE%\Documents\Unicon\Scout\Console\Diag
```

Diagnostic files that are requested via Scout Board are downloaded by the browser used and saved and saved in the download directory, if configured.

Note

If you use anti-virus software on your Scout Server, we recommend that you exclude the specified directories from the virus scan to avoid side effects.

13.2. eLux partitions

An eLux device's flash memory is generally divided into three or four partitions when eLux is installed. Each partition is reserved for a dedicated purpose and is only touched when you perform special tasks that are related to this partition.

All partitions are created during a recovery installation.

Partition	Requires	Purpose	Recreated with	Other
System		Reserved for the firmware (software packages)	Scout Update command with option Format system partition before update	Size for eLux RP 6 2104 LTSR and earlier versions: 1,77 GB / 1,84 GB with/without encryption Size for eLux RP 6 2107 and later versions: 2,35 GB / 2.41 GB with/without encryption
Boot	only UEFI and USB	Boot section	-	
Setup		Device configuration Local application definitions	Factory reset command	Does not affect the system partition with installed firmware
Update	4 GB flash memory	Software delivery in advance (before firmware update) via Scout command or notification Signature check for eLux software packages Devices with update partition can be used as Dynamic Proxy (Provider) for firmware updates.	Scout Delivery command with option Format update partition before delivery	The size of the update partition complies with the storage space provided. The update partition is no larger than the storage space provided. Devices with less than 4 GB flash memory are not provided with an Update partition.

Note

In the Scout Console, in the Properties window of a device, the system, setup and update partitions are listed including their sizes.

Extended system partition starting with eLux RP 6 2107

When you perform an update installation or a new installation (recovery) to eLux RP 6 2107 or later, the system partition is created with 2,35 GB / 2.41 GB (with/without encryption) instead of the previous almost 2.0 GB. This creates more space for the firmware and allows larger images to be used.

■ Update installation

An update installation (firmware update) is still based on the previous partition sizes. The image size is thus still limited to the earlier values. Afterwards, the extended system partition is available and you can install images that may be up to 2.35 GB / 2.41 GB in size. This means, to install larger images on the freshly resized partition of the devices, a second firmware update is required.

■ Recovery installation

Provided an up-to-date recovery system is available, with a PXE or USB recovery installation the system partition can be partitioned to the new size directly during the installation process and a larger image with up to 2.35 GB / 2.41 GB can be written in the same process. A new installation or recovery installation thus allows the partition to be resized and used in one step.

Downgrade

Important To downgrade devices with the extended system partition (eLux RP 6 2107 or later) to an earlier version that only supports the previous system partition with less than 2 GB, you will have to go back to eLux RP 6 2104 LTSR.

We therefore recommend that you update test devices to eLux RP 6 2107 or later as the first step to thoroughly test functionality.

For further information, see Update from earlier partition layout in the **Scout** guide.

13.3. IP ports

eLux / required ports

Port	Type	Description	How to deactivate	In/Out
	ICMP	ping must be supported to verify the status of the eLux devices		In/Out
80	TCP	Firmware update by using HTTP (and proxy port, if used)		Outgoing
443	TCP	Firmware update via HTTPS/TLS		Outgoing
5900	TCP	Mirroring eLux desktop	In Config¹ > Security , disable mirroring or uninstall VNC server in X.Org package	Incoming
22123	TCP	Scout Server (Scout Manager / secure)		In/Out

¹Device configuration

Port	Type	Description	How to deactivate	In/Out
22125	TCP	Scout Server (Scout Manager / TLS 1.2)		In/Out
22129	TCP	VPN		Outgoing

eLux / optional ports

Port	Type	Description	How to deactivate	In/Out
	ESP	VPN (data transfer)	Uninstall package VPN System	In/Out
21	TCP	Update via FTP control port (dynamic data port)		Outgoing
22	TCP	SSH applications		Outgoing
23	TCP	5250 emulations and telnet sessions		Outgoing
53	TCP, UDP	DNS server		Outgoing
67	UDP	DHCP server	Configure a local IP address (Config > Network)	Outgoing
68	UDP	DHCP client (or: BootP client)	Configure a local IP address (Config > Network)	Incoming
69	UDP	TFTP server (only used during PXE recovery)		Outgoing
88	TCP, UDP	AD authentication (Kerberos)		Outgoing
111	TCP, UDP	TCP port mapper - RPC internal use only Works with lockd (random) UDP port mapper - drive access on NFS servers Works with NFSD drive access (port 2049) and mountd (random)	Uninstall Network Drive Share package	In/Out
123	UDP	Windows Time server (NTP)	Do not configure a time server (Config > Desktop)	In/Out

Port	Type	Description	How to deactivate	In/Out
139	TCP, UDP	SMB drive mapping, (NetBIOS) and SMB user authentication (CIFS)	Uninstall Network Drive Share package and User authentication modules package	Outgoing
161	UDP	SNMP	Uninstall SNMP Environment package	In/Out
162	UDP	SNMPTRAP	Uninstall SNMP Environment package	Outgoing
177	UDP	XCMCP protocol		Outgoing
389	TCP	AD authentication with user variables		Outgoing
443	TCP	VPN (connecting) via HTTPS/TLS	Uninstall package VPN System	In/Out
464	TCP, UDP	AD authentication (Kerberos) / Set password		Outgoing
514	TCP	Shell, X11 applications		Outgoing
515	TCP	Printing via LPD	Uninstall package Print environment (CUPS)	In/Out
631	TCP, UDP	CUPS (IPP) print client	Uninstall package Print environment (CUPS)	Outgoing
636	TCP	LDAPS authentication with user variables		Outgoing
2049	UDP	NFSD drive access NFS	Uninstall FPM NFS Support in Network Drive Share package	Outgoing
6000	TCP	Remote X11 application	In Config > Security, clear Allow remote X11 clients option	Incoming
7100	TCP	Font server can be assigned in (Config > Screen > Advanced		Outgoing
8080	TCP	Firmware update via Dynamic proxy (Provider and Consumer)	Set Config > Firmware > Proxy-Typ to None	In/Out

Port	Type	Description	How to deactivate	In/Out
9100	TCP	Printing directly to parallel port can be assigned in (Config > Printer)	In Config > Printer , clear TCP direct print option	Incoming
9101	TCP	Printing directly to USB port can be assigned in (Config > Printer)	In Config > Printer , clear TCP direct print option	Outgoing
20000	UDP	Wake On LAN		In/Out
22124	TCP	Scout Statistics		Outgoing

Scout Server

Port	Type	Description	In/Out
	ICMP	ping must be supported to verify the status of the eLux devices	In/Out
1433	TCP	MS SQL Server	Outgoing
1434	UDP	MS SQL Server (Browser service)	In/Out
22123	TCP	Clients (Scout Manager / secure)	In/Out
22124	TCP	Scout Statistics	Incoming
22125	TCP	Clients (Scout Manager / TLS 1.2)	In/Out

Scout Console

Port	Type	Description	How to deactivate	In/Out
1433	TCP	MS SQL Server		Outgoing
1434	UDP	MS SQL Server (Browser service)		Outgoing
5900	TCP	Mirroring the eLux desktop	In Config > Security , disable mirroring or uninstall VNC server in X.Org package	Outgoing

Scout Cloud Gateway

Port	Typ	Description	In/Out
22125	TCP	Scout Server (Scout Manager / TLS 1.2)	In/Out
22129	TCP	VPN	Incoming

13.4. SNMP

SNMP (Simple Network Management Protocol) is a network protocol for monitoring and controlling network devices.

For eLux RP 6, version SNMPv3 is used.

Note

The command line program **snmpget** is not included in the software package. To query SNMP status information, please use third party software.

13.4.1. Configuring SNMP

1. From our myelux.com portal, under **eLux Software Packages**, for your eLux version, under **Add-On**, download the package **SNMP Environment** and deploy it to the devices.
2. If there is no `/setup/snmp/snmpd.conf` on the devices, transfer the configuration file `snmpd.conf` to the devices to `/setup/snmp/snmpd.conf` by using the Scout feature **Configuring SNMP**.

Or:

Modify the `terminal.ini` file by using the **Configuring SNMP** feature of Scout. Example:

File	<code>/setup/terminal.ini</code>
Section	<code>SNMPD</code>
Entry	<code>rocommunity</code>
Value	<code>secret</code>

3. Optionally, to define further "SNMPD and SNMP Configuration Directives" on page 79, use the **Configuring SNMP** feature and modify the `terminal.ini` file under `SNMPD`. Examples:

```
syscontact=contact@sampletec.com
syslocation=testcenter
doDebugging=1
```

For further information on SNMPD Configuration Directives, see <http://www.net-snmp.org>.

The section `SNMPD` of the `terminal.ini` file is evaluated by the client and the file `/setup/snmp/snmpd.local.conf` is created. An existing `/setup/snmp/snmpd.conf` will be overwritten.

If the configuration file does not exist, the file `/setup/snmp/snmpd.local.conf` is created with default values.

Notes on configuring SNMP v3

- When you define users (**createUser**), set a password with at least 8 characters.
- For the authentication method, define `authPriv` or `authNoPriv`.

Note

For SNMP v2, you can use `noAuthNoPriv` as the authentication method.

13.4.2. SNMPD and SNMP Configuration Directives

The following table refers to the eLux software package **snmp**.

For further information on using SNMP with eLux, see "SNMP" on page 77.

For further information on SNMP commands, see <http://www.net-snmp.org>.

Application	Command
authtrapenable	1 2 (1 = enable, 2 = disable)
trapsink	host [community] [port]
trap2sink	host [community] [port]
informsink	host [community] [port]
trapsess	[snmpcmdargs] host
trapcommunity	community-string
agentuser	agentuser
agentgroup	groupid
agentaddress	SNMP bind address
syslocation	location
syscontact	contact-name
syservices	NUMBER
interface	name type speed
com2sec	name source community
group	name v1 v2c usm security
access	name context model level prefix read write notify
view	name type subtree [mask]
rwcommunity	community [default hostname network/bits] [oid]
rocommunity	community [default hostname network/bits] [oid]
rwuser	user [noauth auth priv] [oid]
rouser	user [noauth auth priv] [oid]
swap	min-avail
proc	process-name [max-num] [min-num]
procfix	process-name program [arguments...]
pass	miboid command

Application	Command
pass_persist	miboid program
disk	path [minspace minpercent%]
load	max1 [max5] [max15]
exec	[miboid] name program arguments
sh	[miboid] name program-or-script arguments
execfix	exec-or-sh-name program [arguments...]
file	file [maxsize]
dlmod	module-name module-path
proxy	[snmpcmd args] host oid [remoteoid]
createUser	username (MD5 SHA) passphrase [DES] [passphrase]
master	pecify 'agentx' for AgentX support
engineID	string
engineIDType	num
engineIDNic	string

SNMP Configuration Directives

Application	Command
doDebugging	(1 0)
debugTokens	token[,token...]
logTimestamp	(1 yes true 0 no false)
mibdirs	[mib-dirs +mib-dirs]
mibs	[mib-tokens +mib-tokens]
mibfile	mibfile-to-read
showMibErrors	(1 yes true 0 no false)
strictCommentTerm	(1 yes true 0 no false)
mibAllowUnderline	(1 yes true 0 no false)
mibWarningLevel	integerValue
mibReplaceWithLatest	(1 yes true 0 no false)
printNumericEnums	1 yes true 0 no false)
printNumericOids	1 yes true 0 no false)

Application	Command
escapeQuotes	(1 yes true 0 no false)
dontBreakdownOids	(1 yes true 0 no false)
quickPrinting	(1 yes true 0 no false)
numericTimeticks	(1 yes true 0 no false)
suffixPrinting	integerValue
extendedIndex	(1 yes true 0 no false)
printHexText	(1 yes true 0 no false)
dumpPacket	(1 yes true 0 no false)
reverseEncodeBER	(1 yes true 0 no false)
defaultPort	integerValue
defCommunity	string
noTokenWarnings	(1 yes true 0 no false)
noRangeCheck	(1 yes true 0 no false)
defSecurityName	string
defContext	string
defPassphrase	string
defAuthPassphrase	string
defPrivPassphrase	string
defVersion	1 2c 3
defAuthType	MD5 SHA
defPrivType	DES (currently the only possible value)
defSecurityLevel	noAuthNoPriv authNoPriv authPriv