UNICON

Installation Scout Enterprise Management Suite 15

Short Guide

Last edited: 2021-11-05

0. Legal information

Unicon Software Entwicklungs- und Vertriebsgesellschaft mbH
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 `Courier New`. Also, file names and path names are displayed in `Courier New`.
STRG	Keys to be pressed are displayed in CAPITAL LETTERS.
<Placeholder>	Placeholders in instructions and user input are displayed in *italics* 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 *italics*.

Abbreviations and acronyms

Abbreviation	Description
AD	Active Directory , directory service of Microsoft Windows Server
EBKGUI	Interface of the eLux Builder Kit (component of Scout Enterprise)
EPM	eLux package module (`.epm`, software package)
FPM	Feature package module (`.fpm`, 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 (`.idf`)
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 version 15.0 and later. Documentation for earlier versions can be found in the **Archive** section of the PDF downloads page.

Minimum requirements for the Scout Server

- Hard disk space 600 MB (only Scout Enterprise Management Suite, the software container requires additional space)
- Microsoft Windows Server 2012, 2012 R2, 2016, 2019 or Microsoft Windows 10

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

  > **Note**
  > We recommend operating Scout Enterprise Management Suite on a Windows Server system. If you use a Windows workstation instead, you cannot run Scout Dashboard.

- Microsoft .NET Framework version 3.5 and
  Microsoft .NET Framework version 4.5.1 or later
- Suitable ODBC driver
- In order to install the 64-bit version, first install the Microsoft SQL Server Native Client 11.0 on the Scout Server. The relevant `MSI` file (`sqlncli.msi`) can be downloaded from the Microsoft website either individually or as part of the Microsoft SQL Server Feature Pack. After successful installation of the Microsoft SQL Server Native Client, the driver is displayed in the ODBC data sources.

Minimum requirements for the Scout Statistics Service

For a maximum number of 200.000 devices, we recommend the following hardware

- Processor with 4 CPUs
- 8 GB RAM

For 200.000 up to 400.000 devices, we recommend the following hardware

- Processor with 8 CPUs
- 16 GB RAM

Minimum requirements for the Scout Dashboard

Hardware

- Processor with 2 GHz minimum, recommended 2.5 GHz or more (4 to 8 CPUs)
- 8 GB RAM
- Hard disk space 40 GB, recommended 80 GB

Operating system

- Microsoft Windows Server 2012, 2012 R2, 2016, 2019
  including the relevant software updates provided by Microsoft at the time of installation

Software

- Scout Server and Scout Statistics Service must be included in the Scout Enterprise Management Suite installation (same or different machine)
- Scout Report Generator must be installed if you want to use reports
- Microsoft Internet Information Service (IIS) 7.0 or later versions with the roles
  - Performance ⇒ Dynamic content compression
  - Application Development ⇒ ASP .NET 3.5
  - Application Development ⇒ ASP .NET 4.5

The following components are installed during the Scout Dashboard installation if they are not yet available:

- Microsoft Visual C++ Redistributable for Visual Studio 2012, Update 4
- Microsoft SQL Server 2012 Native Client
- Microsoft .NET Framework Version 4.5.2

Requirements for the database system

- Microsoft SQL Server 2012, 2014, 2016, 2017, 2019
- or for small installations:

  MS SQL Server Express LocalDB as integrated DBMS based on SQL,
  included in the Scout Enterprise installation file

> **Note**
> Scout Statistics Service and Scout Dashboard cannot be used with LocalDB.

Minimum requirements for the eLux container:

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

- FTP or HTTP server, locally installed or via network
- The required space depends on the number of provided operating system versions. For the installation of eLuxContainer for eLux RP 6.5 LTSR, for example, we recommend an available disk space of 2 GB minimum.

Recommended system requirements for ELIAS 18 and MongoDB on one computer

- to be installed separately -

- Hard disk space 30 GB (depending on container installations)
- RAM 8 GB minimum
- Microsoft Windows Server 2012 R2 or later, 64-bit version
  Microsoft Internet Information Service (IIS) 8.0 or later versions
  including WebSocket Protocol for automatic page refresh[1]
- Screen resolution 1366 x 768 or higher
- Web browser / minimum version
  - Mozilla Firefox ⇒ 78 ESR

    Note
    For Firefox 65 and later versions, pop-up windows are treated differently. To ensure that the **Create** and **Import** buttons in ELIAS work correctly, add an exception for the ELIAS URL in the Firefox settings under **Privacy & Security > Permissions > Block pop-up windows**.
  - Google Chrome ⇒ 77
  - Microsoft Edge ⇒ 77

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 its version is MongoDB 4.0.1 or later.

[1] from ELIAS 18.3

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

> **Note**
> The Microsoft JET Database (.mdb) can no longer be used with Scout Enterprise Management Suite 15.0 and later versions. Documentation for earlier versions can be found in the **Archive** section of the PDF Downloads page.

4.1. Overview

Microsoft SQL Server

- only for 64-bit installations[1] -

You can use any Microsoft SQL Server versions as an SQL database. We recommend that you create the required databases (any file name) before installing Scout Enterprise Management Suite.

Database		Description
Scout Enterprise	mandatory	Device configuration, (static) asset data, server settings, management of administrators, consoles and licenses, transaction logging requires about 50 MB free disk space per 1.000 devices
Scout Enterprise Statistics	mandatory if the Scout Statistics Service is to be installed (complete installation)	Asset data (dynamic, history)
Scout Dashboard	mandatory if the Scout Dashboard for web-based client management is to be installed (complete installation)	Dashboard settings, transaction logging

For further information, see Features of the Scout Enterprise Management Suite.

The databases can also be created in Microsoft SQL Server during the installation process of the Scout Enterprise Management Suite, if the required access rights are available.[2]

The database tables of all databases are created automatically by the installation routine of the Scout Enterprise Management Suite.[3]

---

[1] for Scout Enterprise Management Suite 15.0/14.9.1000 and later versions
[2] for Scout Enterprise Management Suite 15.0 and later versions
[3] For Scout Enterprise Management Suite 14.9 and earlier versions, the Scout Dashboard is installed separately.

Note
If you want to back up and restore the databases, ensure that you do not delete the original database. For further information, see Troubleshooting

Microsoft SQL Server Express LocalDB

- for Scout Enterprise Management Suite 14.7 and later versions -

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

Note
With Microsoft SQL Server Express LocalDB, you cannot use the Scout Statistics Service (keep alive messages and static asset data) nor Scout Enterprise-Dashboard (web console).

The Scout Enterprise database is created automatically during the installation process:

The Scout Enterprise installation file already includes Microsoft SQL Server Express LocalDB.[1] If desired, during installation, Scout Enterprise creates the required database of the type `LocalDB`. 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.

Database cleanup

Outdated data can be deleted using the **Database cleanup** feature. For further information, see Database cleanup.

[1] for Scout Enterprise Management Suite 14.7 and later versions

4.2. SQL LocalDB

- for Scout Enterprise Management Suite 14.7.0 and later versions -

We only recommend using the integrated database Microsoft SQL Server Express LocalDB for less than 1.000 clients or for test and evaluation environments. The required software modules are included in the Scout Enterprise 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 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 Enterprise service and the LocalDB database on a server system. Dedicated Scout Consoles that can access the LocalDB database remotely are not supported.
- The **Statistics** service (keep alive messages and static asset data) and Scout Enterprise **Dashboard** (web console) cannot be used.
- The **Configuration run** command to prepare the client 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 Enterprise update, 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 Enterprise update, use the SQL Management Studio feature **Restore** to restore the database.

4.3. Authentication to SQL Server

If 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 the `db_owner` fixed database role and the default schema for user mapping must be `dbo` in SQL Server. The `db_owner` role allows admins to perform the relevant configuration and maintenance activities on the database.

Method	Description
Windows authentication	'Trusted connection': The user identity is confirmed by Windows. The Scout Enterprise service must be run with a user account that has the required access rights in SQL Server (member of `db_owner`).[1] ▸ In the Scout Enterprise installation dialog, specify the account name in the form `DOMAIN\username` (no case-sensitivity) Example: `INT\mmi` The password can be entered subsequently.
SQL Server authentication	The username and password must refer to an SQL Server user account with the relevant user rights in SQL Server (member of `db_owner`). Note: For environments with SQL Server Clusters, `VIEW SERVER STATE` and `VIEW ANY DEFINITION` permissions are additionally required. ▸ In the Scout Enterprise 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.

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

4.4. Defining application roles for SQL Server

In order to control access to the SQL Server tables, for all Scout Enterprise databases, you can define an 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 the session.

Defining application role for Scout Enterprise database

1. In SQL Server, for the **Scout Enterprise** database, edit the **System** table.
2. Add one row for the name and one row for the password of the application role:

For Scout Enterprise 15.7 /15.5.1000 and earlier versions:

SystemID	ParamName	ParamVal
…		
<n>	RName	<encrypted name of application role>
<n>	RPass	<encrypted password of application role>

For Scout Enterprise 15.8 / 15.5.2000 and later versions:

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

3. To specify the application role data in encrypted mode, in a first step, encrypt the name and password of the role and then paste the encrypted values into the table. For further information, see Encrypting values.

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

Defining an application role for Scout Enterprise Dashboard database

1. In SQL Server, for the **Scout Dashboard** database, edit the **EnvironmentInfo** table.
2. Add one row for the name and one row for the password of the application role:

EnvironmentInfoID	Key	Value
…		
<n>	RName	<encrypted name of application role>
<n>	RPass	<encrypted password of application role>

3. Encrypt the name and password of the role and then paste the encrypted values into the table. For further information, see Encrypting values in the **Scout Enterprise** guide.

Each time Scout Dashboard connects to the database, the fields are read and the access rights of the application role are set.

Note
For the Scout Enterprise Statistics database, you can also define an application role in the **EnvironmentInfo** table as described above.

4.5. Scout Server cluster

If you use an SQL database, several Scout Servers can connect to the same Scout Enterprise 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 Enterprise database.

FailureLoadBalancing

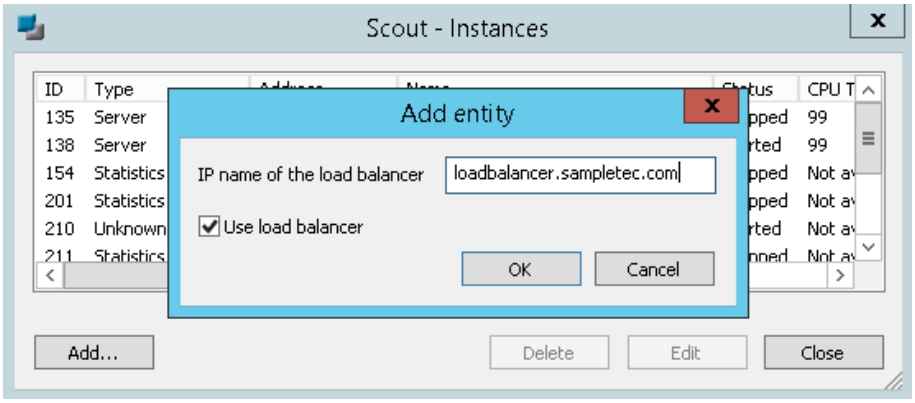
On start-up, the client tries to connect to the Scout Server it was connected to last time. If, however, that server is not available, it connects to the next server from the servers list which, subsequently, becomes the server the client tries to access by default from then on.

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 clients to connect to:

- In the Scout Console, in **View > Scout Enterprise 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 Enterprise configuration.

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

Procedure:

- Thin Client restarts
- Client 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.

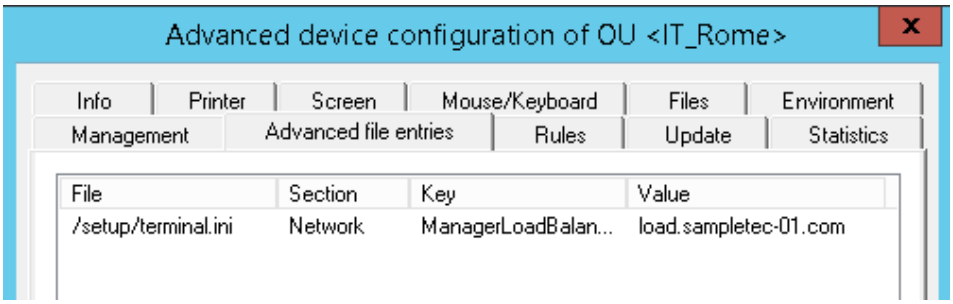
ManagerLoadBalancing by DNS entry

Alternatively, to predefine a preferred Scout Server you want the clients 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 Enterprise configuration.

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

Procedure:

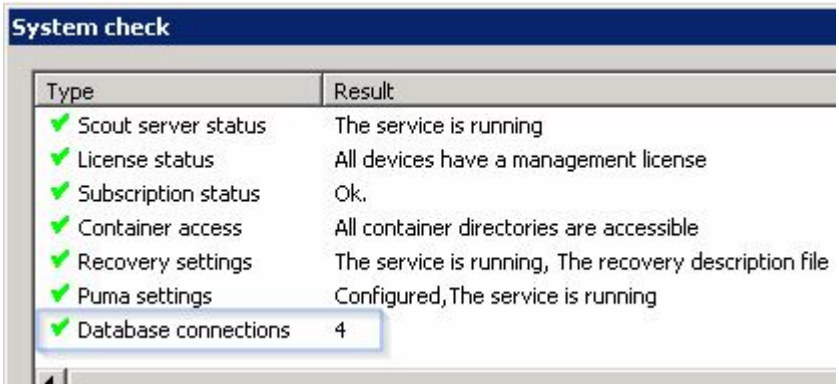
- Thin Client restarts
- DNS entry `ManagerLoadBalancer` is resolved
- Client connects to the appropriate Scout Server

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 Enterprise 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**).



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 Enterprise 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` *(n=1-128)*

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 Enterprise** guide.

4.7. Database compatibility mode for Dashboard

On login to the Scout Dashboard, the database versions of the Scout Enterprise database, the Scout Enterprise Statistics database and the Scout Enterprise Dashboard database are checked for compatibility.[1] If the version numbers do not match, the user cannot log in but receives a message.

Compatibility is additionally validated for the Dashboard service. The service is stopped as soon as one of the databases is found not to be compatible. By default, the validation is performed every 60 seconds.

Incompatibilities due to different database versions can arise if, for example, Scout Server has been updated to a newer version but Scout Enterprise Dashboard on another machine has not yet been updated.

Modifying the validation frequency of the Dashboard service

- Modify the values of the following parameters in the configuration file by using a text editor:

Path	<*Installation directory*>`\Scout Enterprise Dashboard Service` Example: `C:\Program Files\Unicon\Scout Enterprise Dashboard Service`
File	`ScoutDashboardService.exe.config`
Section	`databaseVersionConfigurationSection`
Parameter `occuringType`	`Periodically`|`Once` For `Once`, validation is performed only once on the start of the service
Parameter `schedulePeriodInSeconds`	<*Integer value for the number of seconds for `Periodically`*> A minimum period of 60 seconds (default) is recommended.

[1] for Scout Enterprise Management Suite 15.0 / Scout Enterprise Dashboard 2.0 and later versions

5. Preparing for installation

The Scout Server, the Scout Statistics Service and the Scout Dashboard 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.

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 Enterprise function **Client relocation**. Do not change the DHCP configuration while the clients are running.

Note

If you do not use DHCP options for Scout Enterprise, 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 clients.

A new client 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 *The entry is automatically extended with the related hexadecimal number (45 4C 55 58 4E 47).*

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
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

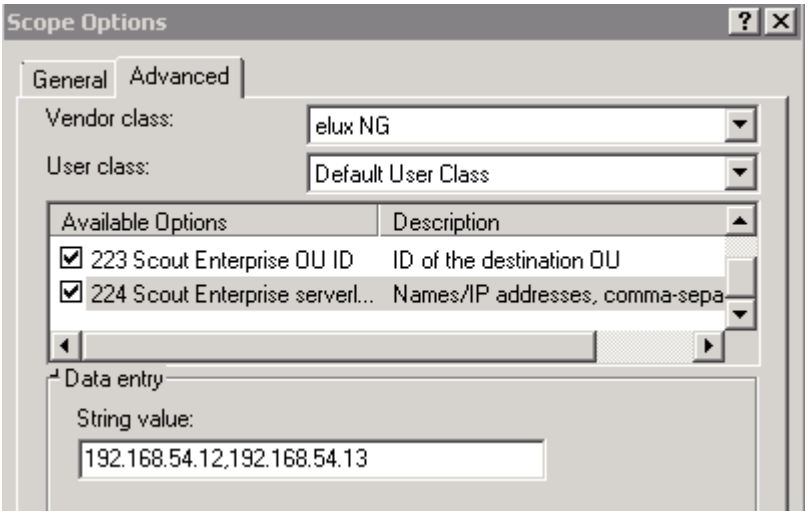
7. To define a specific OU that you can assign new devices to, click **Add...** and edit the new option as follows:

Option	Value
Name	Scout Enterprise 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 Enterprise 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 Enterprise 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 Enterprise 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`	By default, the 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 Enterprise.

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 Enterprise, 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 software support.

5.2. Opening ports

- Open the following ports in the firewall:

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 Enterprise Management /secure)	eLux clients
22125	TCP	Scout Server (Scout Enterprise Management / TLS 1.2)[1]	eLux-Clients
22124	TCP	Scout Server	Scout Statistics Service
5900	TCP	Scout Console (Mirroring eLux desktop)	Clients
80/443	TCP	Clients (HTTP/HTTPS)	Dashboard server/ 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.

[1] for Scout Enterprise Management Suite 15.1 / eLux RP 6.1 and later versions

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.
- We recommend creating the required databases (file names can be selected freely) 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 Enterprise Management Suite installer.

  For further information, see Database support.
- SQL or AD user (**<SQL server\Instance> / Security / Logins**) with membership `db_owner` for all databases (**<Database name> / Security / User**)
- The Browser service on the SQL server must be started.

[1] For Scout Enterprise Management Suite 15.0 and later versions, the Scout Enterprise databases can be created in Microsoft SQL Server during the installation, relevant rights provided.

5.4. Permissions and certificates

Permission 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 Local DB, see SQL LocalDB.

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

> **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

- Web Server (IIS) role or relevant permissions for the web server used
- Administrator rights on the root directory for the installing administrator
- For Scout Dashboard: Web Server (IIS) role including
  - Performance ⇒ Dynamic content compression
  - Application Development ⇒ ASP .NET 3.5
  - Application Development ⇒ ASP .NET 4.5
- Write access on the eLux container directory for all users that are allowed to create or modify IDFs in ELIAS

Permissions for Scout Dashboard

- Active Directory integration for the Scout Dashboard server and all administrators who log in to Scout Dashboard
- After the installation, in the Scout Console, the relevant administrators must be authorized to use Scout Dashboard. For further information, see Changing base permissions in the **Scout Enterprise** guide.

SSL certificates for Scout Statistics Service and Scout Dashboard

The communication between eLux and the Scout Statistics Service is based on the HTTPS protocol. Therefore, for the installation of the Scout Statistics Service, an SSL certificate for server authentication is required which is bound to port 22124 by default. For further information, see Certificate for Scout Enterprise Statistics Service.

If you intend to operate Scout Dashboard over HTTPS, a valid SSL certificate is required for Dashboard as well.

Note
For the certificate-based encryption of the management protocol in Scout Enterprise Management Suite 15.1 and eLux RP 6.1, the Scout Enterprise service creates a self-signed certificate automatically on start-up.

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 of the package certificates from our portal www.myelux.com 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 Enterpise 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 portal www.myelux.com.
2. On the **Download** menu, choose the relevant software:

Option	Description / Option	Download
eLux Portable	eLux on USB stick, based on latest eLux RP version	eLux Portable (no installation needed)
eLux Software Packages	Latest operating system versions, LTSR and CR, divided into containers according to platform	■ Bundle: With `AllPackages-x eLuxRP-x.x.x`, you can install a container including all software packages in one step[1] or import into ELIAS 18. ■ Individual packages: For each eLux version, under **Release Packages**, all available software packages are provided for download.
eLux USB Stick Images	Ready-to-use images for USB installation of the latest eLux versions	Stick image for the required eLux version includes the Citrix Workspace app and the VMware Horizon client to connect against a backend
Scout Enterprise	Scout Enterprise Management Suite	■ Latest versions ■ Version required to convert an `.mdb` database includes the installation file `Scout Enterprise.exe`

[1] includes the installation file `eLuxContainer.exe`

Option	Description / Option	Download
	ELIAS 18	Latest ELIAS 18 version for creating and managing individual images The Scout Enterprise Management Suite alternatively includes the legacy ELIAS program.
	Scout Cloud Gateway	Management of remote eLux clients via the Internet contains a virtual machine template (`.ova`)
	Scout Agent for Windows	Scout Agent for managing Windows devices
Tools	StickWizz	Latest version (StickWizz is also included in the eLux USB Stick images)
	eLux Builder Kit	For the development environment, please contact sales(at)unicon-software.com
	Win2eLux	Version per eLux platform for migration from Windows

3. To download the relevant file, click the file name or version number.

   The software is downloaded in the form of `.zip` files.

4. Unpack the `.zip` files.
5. Provide the installation files such as `Scout Enterprise.exe` on a local hard drive.
6. 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.

  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.

6.1. Features of the Scout Enterprise Management Suite

Scout Enterprise Management Suite is the management solution for Thin Clients or 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 clients as well as Windows clients on which Scout Agent for Windows has been installed.	`Scout Enterprise.exe`
Scout Console	User interface for the management of eLux clients and for the management of Windows-based clients clients on which Scout Agent for Windows has been installed Server communication only via database Multiple consoles can be managed with one Scout database.	`Scout Enterprise.exe`
Recovery service	Customized TFTP service to realize a PXE recovery environment for eLux endpoints	`Scout Enterprise.exe`

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

Component	Description	Installation
ELIAS	Legacy dialog program eLux Image Administration Service (ELIAS) for creating individual image definition files (`.idf`) for modular firmware updates of the eLux clients. The legacy ELIAS will be replaced by ELIAS 18.	`Scout Enterprise.exe`[1]
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	`Scout Enterprise.exe`
Scout Statistics Service	Service for the evaluation of device status information and dynamic asset details	`Scout Enterprise.exe`
Scout Dashboard	Web-based console for the management of eLux clients and for the management of Windows-based clients on which Scout Agent for Windows has been installed	`Scout Enterprise.exe`
Web API[2]	Application programming interface for the management of eLux clients and for the management of Windows-based clients on which Scout Agent for Windows has been installed	`Scout Enterprise.exe`
Scout Agent for Windows	Service providing an interface for Windows-based clients to be managed through Scout Enterprise Management Suite	separate
Scout Command Interface	Command line interface for Scout commands	`Scout Enterprise.exe`
Scout Database Connection Editor	Tool for modifying database connection settings of the Scout Server and Scout Console	`Scout Enterprise.exe`

The features are described in the following guides:

- Scout Enterprise Management Suite:
  Configuration, control and management of the client devices using the Scout Console
  Scout Statistics Service
- ELIAS

[1]for Scout Enterprise Management Suite Version 15.7 and later versions, the legacy ELIAS is no longer included in the standard installation. To install the feature, select **User-defined**.
[2]for Scout Enterprise Management Suite 15.0 and later versions

- ELIAS 18
- Scout Report Generator
- Scout Command Interface
- Scout Dashboard

Recovery procedures for eLux clients 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 eLux container for the software packages.
For further information, see Installing a container.

6.2. Installing Scout Enterprise Management Suite

Note

Before you start to install, make sure to have read the following topics:

- System requirements
- Preparing for installation

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[1]. 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.

The following instructions refer to the standard installation.

Note

- Run the installer from a local hard drive. Do not use a USB stick, CD-R drive or a network drive.
- Anti-virus programs can have an impact on the installation. If required, disable the anti-vrus program before you perform the installation.

1. Run the `Scout Enterprise.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 Support of databases.
4. Select the installation type.[2] The `Service provider` option is only relevant for service providers who want to use Scout as a Service and have a service provider account on myelux.com. For further information, see the **Service Provider Mode** guide.
5. Select the type of installation. To select individual features for installation or change the installation directory, select `User-defined`. For the standard installation, select `Standard`.[3]

[1] included up to Scout Enterprise Management Suite 15.5
[2] ab Scout Enterprise 15.8
[3] formerly Complete

6. Specify the database connection data for your **Scout Enterprise database**. If you use Microsoft SQL LocalDB, enter the relevant Windows account name and password. For further information, see SQL LocalDB.
7. If you use Microsoft SQL Server, enter the required data to connect to the SQL server:

Legend to numbers	
1	*<SQL server\instance>* Example: `sqlsrv.dev.sampletec-01.com\sql_19`
2	`SQL Server authentication` or `Windows authentication` For further information, see Authentication to SQL Server.
3	SQL or Windows username and password for database access
4	SQL Server connection options: • For AlwaysOn Cluster: Faster reconnection after failover • Use encrypted ODBC connection
5	Click to connect to the database server.

8. Click **Connect...**, and then in the list-field, select your **Scout Enterprise** 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.*

9. In the next dialog, verify or modify the required data to connect to the **Scout Enterprise Statistics** database and click **Connect...**. In the list-field, select your **Scout Enterprise Statistics** database.

10. In the next dialog, for the Scout Statistics Service, specify the TCP port and the certificate of the Statistics service.

    If there is no valid SSL certificate available, create a self-signed certificate. Then continue with the Scout Enterprise Management Suite installer.

    Note

    By using , you can update the list-field contents and select the newly created certificate.
    Any certificates available are shown with their assigned **friendly name**. If there is no friendly name or it is assigned more than once, with their serial number is shown.

    Optionally, go back in the installer and cancel the selection of the Scout Statistics Service.

11. In the next dialog, verify or modify the required data to connect to the **Scout Dashboard database** and click **Connect...**. In the list-field, select your **Scout Dashboard database**.
12. In the next dialog, configure your Dashboard website:

Application name	is shown in the Dashboard URL
HTTP or HTTPS port	port number for Dashboard must correspond to the port number configured on the web server
Enable HTTPs	uses the secure HTTPS protocol
SSL Encryption	for HTTPS only Select a valid SSL certificate or create a self-signed certificate.

    The last dialog summarizes the features that will be installed.

13. 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 Dashboard on the desktop. In the Scout Enterprise group of the Windows Apps view, you will find all Scout Enterprise applications including the Scout Enterprise Database Connection Editor.

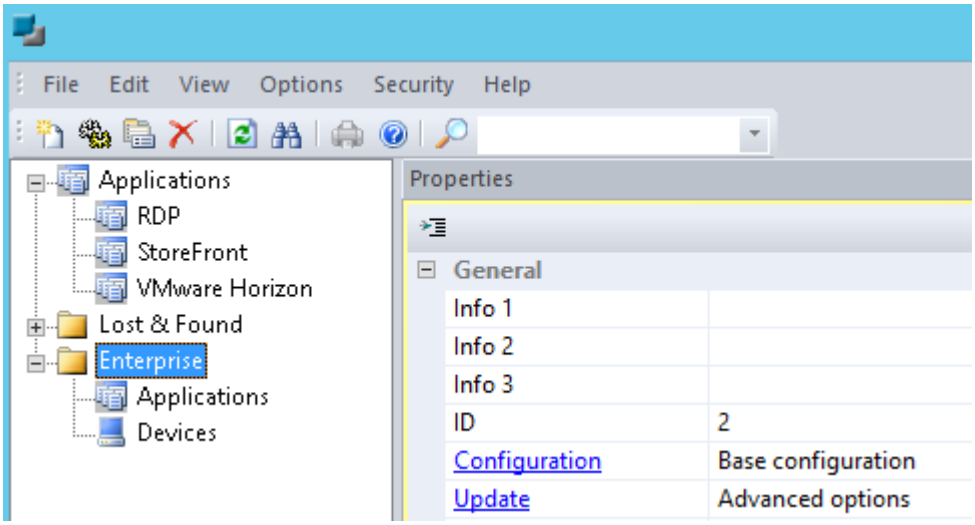
6.3. After the initial installation

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

After you have completed the installation with an empty Scout Enterprise 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:[1] **RDP**, **VMware Horizon** and the **Firefox** web browser.[2]
  - 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 clients. For further information, see Defining applications.
- A top-level organizational unit (OU) named **Enterprise** is created[3].
  - Under the top-level OU, add further OUs correspondig to your corporate structure. For further information, see Organizational structure.

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



[1] for Scout Enterprise Management Suite 15.0 and later versions
[2] for Scout Enterprise Management Suite 15.0 to 15.4 StoreFront instead of Firefox
[3] for Scout Enterprise Management Suite 15.0 and later versions

6.4. Unattended installation

> **Note**
> The following information refers to Scout Enterprise Management Suite 15.0 and later versions. Documentation for earlier versions can be found in the **Archive** section of the PDF downloads page.

Performing an unattended installation of the Scout Enterprise Management Suite

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

  > **Note**
  > Scout Statistics Service and Scout Dashboard can only be used if the database is based on Microsoft SQL Server.

Create command line for unattended installation

- for Scout Enterprise 15.7 and later versions -

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 with a text editor:
   `%LOCALAPPDATA%\Temp\Scout_Enterprise_(64_bit)_<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 manuallly.
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** and *example values* are displayed in *italics*.

Note
To encrypt passwords, you can use environment variables. For further information, see Encrypting values.

Parameters for /v

Parameter	Description
UCPROP_DBTYPE=**2**	`2` - Microsoft SQL Server `5` - Microsoft SQL LocalDB
UCPROP_DBNAME=*Scout*	Name of Scout Enterprise database
UCPROP_DBSERVER=*sqlsrv.dev.sampletec-01.com\sql_12*	Database server and instance of the Scout Enterprise database
UCPROP_DBUSER=Scout-Admin	Only for SQL Server authentication: SQL username for Scout Enterprise database
UCPROP_DBPASSWORD_CRYPTED=u[D``Gqu[w_	Only for SQL Server authentication: Crypted password for Scout Enterprise database, see `eluxd.ini`
UCPROP_DBPASSWORD=*My_Password*	Only for SQL Server authentication: Uncrypetd password for Scout Enterprise database
UCPROP_SERVICEUSER	Only for Windows authentication: Windows username
UCPROP_SERVICEPASSWORD_CRYPTED	Only for Windows authentication: Crypted Windows password
UCPROP_DBNAME_STATISTIC=*Scout_Statistics*	Name of Scout Enterprise Statistics database
UCPROP_DBSERVER_STATISTIC=*sqlsrv.dev.sampletec-01.com\sql_12*	Database server and instance of Scout Enterprise Statistics database
UCPROP_DBUSER_STATISTIC=*Scout-Admin*	Only for SQL Server authentication: SQL username for Scout Enterprise Statistics database
UCPROP_DBPASSWORD_CRYPTED_STATISTIC=*u[D``Gqu[w_*	Only for SQL Server authentication: Crypted password for Scout Enterprise Statistics database, see `eluxd.ini`
UCPROP_DBPASSWORD_STATISTIC=*My_Password*	Only for SQL Server authentication: Uncrypted password for Scout Enterprise Statistics database
UCPROP_SERVICEUSER_STATISTIC=*Scout-Admin*	Only for Windows authentication: Windows username for Scout Enterprise Statistics database

UCPROP_SERVICEPASSWORD_CRYPTED_STATISTIC=*u[D``Gqu[w_*	Only for Windows authentication: Crypted Windows password for Scout Enterprise Statistics database
UCPROP_SERVICEPASSWORD_STATISTIC=*My_Password*	Only for Windows authentication: Uncrypted password for Scout Enterprise Statistics database
UCPROP_STATISTIC_SERVER_PORT=*22124*	TCP port of the Scout Statistics Service
UCPROP_STATISTIC_CERTIFICATES=\"*MyCert_ServAuth*\"	Certificate of the Scout Statistics Service

UCPROP_DBCREATE=**0**	`0` - Scout Enterprise database will not be recreated `1` - Scout Enterprise database will be recreated
UCPROP_DBCREATE_STATISTIC=**0**	`0` - Scout Enterprise Statistics database will not be not recreated `1` - Scout Enterprise Statistics database will be recreated
UCPROP_CREATE_CERT_STATISTIC=**0**	`0` - No certificate will be created for Scout Statistics Service `1` - Self-signed certificate for Scout Statistics Service will be created
RUNSCOUTSERVICE=**true**	`true` - Scout Enterprise services will be started during installation `false` - Scout Enterprise services will not be started
CHECKIMPERSONATION=**true**[1]	`true` -For Windows authentication, the specified user account is verified `false` - No verification

UCPROP_LANGUAGE=*de*	Language setting for the client desktop `de` - German `en` - English If the parameter is not set, the language defined in the operating system is used.

Dashboard

[1] from Scout Enterprise Management Suite 15.5.2000 and 15.8

DB_SCOUT_USER=*Scout-Admin*	Username for Scout Enterprise database corresponds to UCPROP_DBUSER for SQL Server authentication corresponds to UCPROP_SERVICEUSER for Windows authentication
DB_STATISTIC_USER=*Scout-Admin*	Username for Scout Enterprise Statistics database corresponds to UCPROP_DBUSER_STATISTICfor SQL Server authentication corresponds to UCPROP_SERVICEUSER_STATISTIC for Windows authentication
DB_DASHBOARD_USER=*Scout-Admin*	User name for Scout Enterprise Dashboard database
DB_DASHBOARD_PASSWORD_CRYPTED=*u[D``Gqu[w_*	Crypted password for Scout Enterprise Dashboard database, see `eluxd.ini`
DB_DASHBOARD_PASSWORD=*My_Password*	Uncrypted password for Scout Enterprise Dashboard database
DB_DASHBOARD_SERVER	Database server and instance of Scout Dashboard database
DB_DASHBOARD_DATABASE	Name of Scout Dashboard database

DB_DASHBOARD_DB_AUTHENTICATION= **Windows Authentication**	Type of authentication:
	`Windows Authentication`
	`SQL Server Authentication`

DB_DASHBOARD_CREATE_CERT=**0**	`0` - No certificate will be created `1` - Self-signed certificate for Scout Dashboard is created
WEBSITE_HTTP_PORT=**80**	Port number for Dashboard web site (HTTP) must correspond to the port number configured on the web server
WEBSITE_HTTPS_PORT=**443**	Port number for Dashboard web site (HTTPS) must correspond to the port number configured on the web server
WEBSITE_SSL=**0**	`0` - SSL will not be used `1` - SSL will be used
SELECTED_CERTIFICATE	Certificate of Scout Dashboard: `Create Self-Signed Certificate` *<Friendly name or serial number of certificate>*
ENABLE_HTTP_FIREWALLRULE=**1**	`0` | `1`
ENABLE_HTTPs_FIREWALLRULE=**1**	`0` | `1`

Features

ADDLOCAL=*Server,Console,Report*	Only the specified features will be installed.
	`Server`
	`Console`
	`Recovery`
	`Elias`
	`Report`
	`ScoutStatistic`

ADDLOCAL_ DASHBOARD=*Feature.Scout.Dashboard*	The specified Dashboard features will be installed:
	`Feature.Scout.Dashboard`
	`Feature.Scout.Dashboard.Api`

INSTALL_SCOUT_DASHBOARD_ FEATURE=**0**[1]	`0` - Scout Dashboard and/or Web API will not be installed `1` - Scout Dashboard and/or Web API will be installed (as defined in ADDLOCAL_DASHBOARD)
INSTALL_SCOUT_FEATURE=**1**	`0` - The Scout Enterprise components will not be installed `1` - The Scout Enterprise components will be installed (as defined in ADDLOCAL)

Further parameters

/s	Th installation will be performed in unattended (silent) mode.
/uninstall	The Scout Enterprise Management Suite will be uninstalled.
/l *"%PUBLIC%\Documents\UniCon\scoutlog.txt"*	The log file will be forwarded to the specified file.

[1] obsolete for Scout Enterprise Management Suite 15.2 and later versions: This parameter is set internally based on the database information specified.

Example for an unattended installation

```
Scout Enterprise.exe /s /v"UCPROP_DBTYPE=2" /v"UCPROP_DBNAME=Scout"
/v"UCPROP_DBSERVER=sqlsrv.dev.sampletec-01.com\sql_12" /v"UCPROP_
DBUSER=Scout-Admin"
/v"UCPROP_DBPASSWORD_CRYPTED=u[D``Gqu[w_" /v"UCPROP_DESKTOP_
LANGUAGE=en"
/v"UCPROP_DBNAME_STATISTIC=Scout_Statistics"
/v"UCPROP_DBSERVER_STATISTIC=sqlsrv.dev.sampletec-01.com\sql_12"
/v"UCPROP_DBUSER_STATISTIC=Scout-Admin" /v"UCPROP_DBPASSWORD_CRYPTED_
STATISTIC=u[D``Gqu[w_"
/v"UCPROP_STATISTIC_SERVER_PORT=22124"
/v"UCPROP_STATISTIC_CERTIFICATES=\"MyCert_ServAuth\""
/v"ADDLOCAL=Console,Server,Report,Elias,ScoutStatistic"
```

Note

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

Performing unattended uninstallation

- Run the following command:
  `"Scout Enterprise.exe" /s /uninstall`

6.5. Updating 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 Enterprise databases.

   For further information on backing up a Local DB, see Backing up SQL LocalDB before installing updates.

2. Download the latest version of the Scout Enterprise Management Suite as a `.zip` file from our technical portal www.myelux.com.
3. Unpack the `.zip` file and provide the installation file on a local hard disk.
4. Run the `Scout Enterprise.exe` file as administrator.
5. Follow the instructions of the installation Wizard. Select your existing Scout Enterprise databases.

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

Note

From Scout Enterprise Management Suite 14 to 15, the license management procedure has changed. Before you perform an upgrade to version 15, see the notes in our Whitepaper **Licensing and Subscription Scout15 and eLux RP 6** under FAQs.

6.6. Changing Scout Enterprise Management Suite installation

Installing additional features or uninstalling unneeded features

1. Use the control panel or run the `Scout Enterprise.exe` setup file as administrator.
2. In the Scout Enterprise 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 cancel the selection of an installed feature, it will be uninstalled.

Repairing installation

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

7. Installation: eLux Container

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 clients.

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).

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.

For the operating system versions eLux RP 6 / 64-bit, eLux RP 6 / 32-bit and eLux RP 5, dedicated containers are provided.

If you install the eLux container to be used by the legacy ELIAS, the containers are stored on the FTP or HTTP server root directory as follows:

- `…\eluxng\UC_RP6_X64` (for eLux RP 6.3 and later versions)
- `…\eluxng\UC_RP6` (eLux RP 6.1 and 6.2)
- `…\eluxng\UC_RP5`

7.1. Installing a container

- applies only if you use the legacy ELIAS -

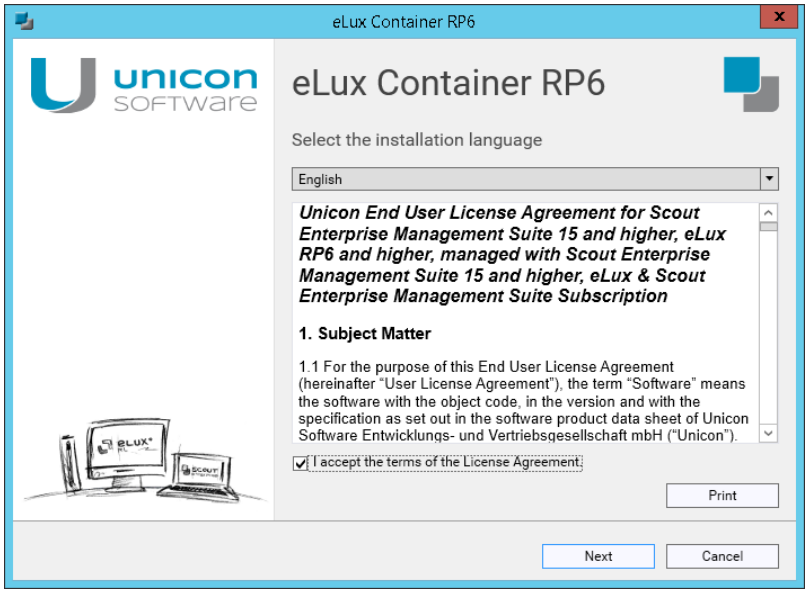
The following instructions show how to install an eLux container including all software packages that are provided on our portal for the selected operating system version. The eLux RP 6 container installation is used as an example.[1]

Note

Before you start to install, make sure to have read the following topics:

- System requirements
- Preparing for installation.

1. Run the `eLuxContainer.exe` 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 source server for firmware updates:
   - `HTTP`
   - `FTP`
4. Specify the access data for the FTP or HTTP server:

[1] The instructions refer to the installer available from July 2017 onwards. The instructions for earlier versions might be slightly different.

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 for access the server	`http://update.sampletec-01.com` `ftp://update.sampletec-01.com`

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 IDF now.

7. If 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 newer 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 update 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 eLux container

- applies only if you use the legacy ELIAS -

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

[1] for eLux RP 5.6 and earlier versions: `setup.exe`

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.[2]

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 to have read the following topics:

- System requirements
- 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] Other web servers can be used, but without configuration support.
[2] for ELIAS 18.2 and later versions

1 The database will only be available on the local host.

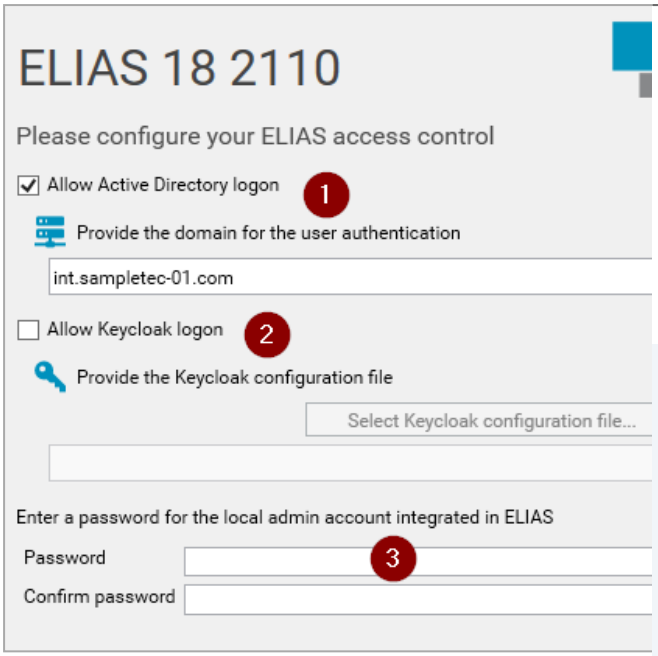
2 To use an existing MongoDB installation, in the next step, specify the MongoDB connection data.

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/

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 1 Configuration file of the Keycloak server for Keycloak authentication[2]

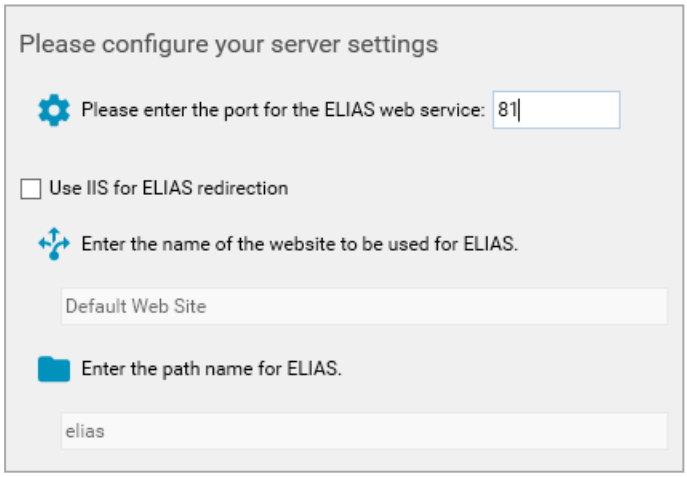
Example: `C:\install\ELIAS\keycloak.json`

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:



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

[1] from ELIAS 18.3

[2] If you add the Keycloak configuration file after installation, subsequently restart the ELIAS service.

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 clients for updates, specify the path name defined here on the **Firmware** tab of the clients' 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.*

8.2. Installing ELIAS 18 / Linux

- The following instructions refer to ELIAS 18 2104 or later versions -

ELIAS 18 can also be used in a Linux environment.[1] A Debian package (`.deb`) tested with Ubuntu 18.04 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 portal www.myelux.com, under **Downloads > Scout Enterprise > ELIAS**, download the provided Debian package of **ELIAS 18 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, edit the file `/opt/unicon/elias/server.json`:[2]

Option	Description	Default
"server"	MongoDB server name (as FQDN or IP address) For a local installation, use `"localhost"`.	`"localhost"`
"mongoPort"	MongoDB port	`"27017"`
"mongoUser"	MongoDB username If you do not use logon data, set an empty string.	`""`
"mongoPassword"	MongoDB password If you do not use logon data, set an empty string.	`""`
"mongoPasswordEncrypted"	Encrypted MongoDB password	false
"mongoOptions"	optional: Additional MongoDB options	
"adminPassword"	Encrypted password for the local **admin** account	`"elias"`
"adGroup"	AD group users need to belong to for logon	`"ELIAS"`

[1] from ELIAS 18.2
[2] This file remains local.

For further information on the logon types, see Access management and logon in the **ELIAS 18** guide.

"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	–

4. To complete the configuration, also 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 `api`	`"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-123"`
"port"	Port on which the ELIAS website is reachable externally	`"22130"`
"allowedOrigins"	List of URLs on which the ELIAS website is reachable externally Example: `"http://<Hostname or IP address>:22130"`	

[1] from ELIAS 18 2104

5. Restart the ELIAS service.

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

> **Note**
> To configure ELIAS for access via Keycloak,[1] see Access management via Keycloak in the **ELIAS 18** guide.

[1] from ELIAS 18.3

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.

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 portal www.myelux.com (**Download > Scout Enterprise > 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.

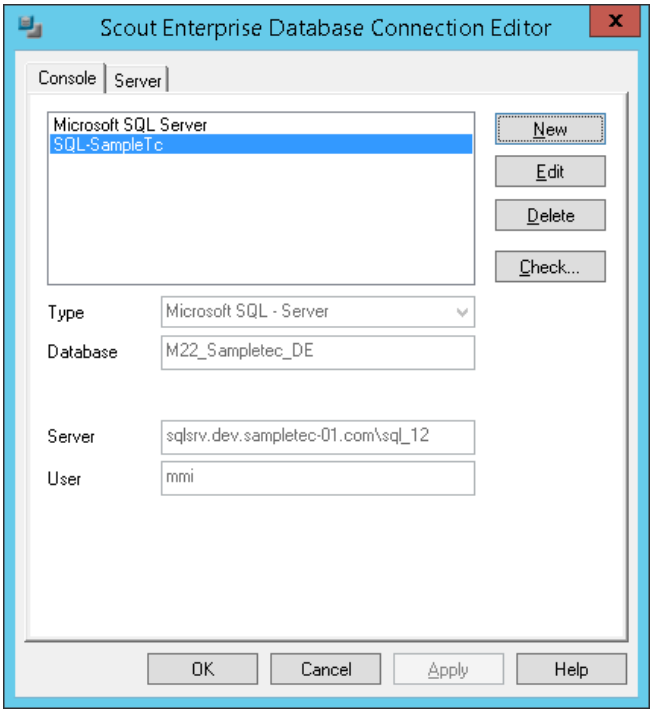
9. Database preferences

9.1. Database connections

When you install the Scout Enterprise Management Suite, you are asked to specify the Scout Enterprise database, the Scout Enterprise Statistics database, and the Scout Dashboard database. To check or modify the database connections at any point in time after the installation, see the following information.

Scout Enterprise database

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



Connections to the Scout Enterprise Statistics database and the Scout Dashboard database can only be modified in the relevant configuration file:

Modifying further database connections

1. Open the relevant configuration file by using a text editor. For the directory and file name of all configuration files, see Database preferences for Scout Enterprise Dashboard, API and Statistics database.
   Edit the parameter `connectionString`:

Section	`connectionStrings`
Parameter `connectionString`	Example: `"data source=sqlsrv.dev.sampletec-01.com\sql_12;initial catalog=M22_Sampletec_DE;persist security info=True;user id=mmi;password=~Yp{wQ[wUsX@;MultipleActiveResultSets=True;"`

2. To modify the user password, if in the section `database Connection ConfigurationSection` the parameter `passwordFormat="Encrypted"` is defined, you are required to enter the password in encrypted mode. Use the **Environment Variables** feature of the Scout Console to encrypt it. For further information, see Encrypting values.

   To define the password without encryption, in the section `database Connection ConfigurationSection`, set the parameter `passwordFormat=""`

3. If in the section `database Connection ConfigurationSection` Windows authentication is defined, you can specify a separate Windows user with domain and password for each database connection.

Note

The authentication values must always be defined accordingly in both sections. If the parameter `passwordFormat="Encrypted"` is defined, the password must be specified in encrypted mode in the database connection.

Example:

```
<databaseConnectionConfigurationSection>
  <databaseConnectionConfiguration passwordFormat="Encrypted" />
  <databaseConnectionAuthentication authentication="SQL Server Authentication" />
  <databaseScoutServerWindowsAuthentication windowsUser="" windowsDomain="" windowsPassword="" />
  <databaseScoutStatisticWindowsAuthentication windowsUser="" windowsDomain="" windowsPassword="" />
  <databaseScoutDashboardWindowsAuthentication windowsUser="" windowsDomain="" windowsPassword="" />
</databaseConnectionConfigurationSection>


<connectionStrings>
  <add name="ScoutServer" connectionString="data source=[redacted] SQL2014;initial catalog=[redacted]-Scout900;persist security info=True;user id=[redacted];password=[redacted];MultipleActiveResultSets=True;" />
  <add name="ScoutStatistic" connectionString="data source=[redacted] SQL2014;initial catalog=[redacted]-ScoutStatistic900;persist security info=True;user id=[redacted];password=[redacted];MultipleActiveResultSets=True;"
  <add name="ScoutDashboard" connectionString="data source=[redacted] SQL2014;initial catalog=[redacted]-Dashboard;persist security info=True;user id=[redacted];password=[redacted];MultipleActiveResultSets=True;" />
</connectionStrings>
```

9.2. Configuration files for Scout Enterprise Dashboard, API and Statistics database

To modify preferences for one of the databases, edit the relevant configuration file by using a text editor.

Preferences can be found in the following configuration files:

Component	Directory	Configuration file
Statistics service	*<Installation directory>*\Scout\Statistic	StatisticService.exe.config
Dashboard website	*<Web server root directory>*\Scout*<YourWebsiteName>*	Web.config
API[1]	*<Web server root directory>*\Scout*<YourWebsiteName>*\Api	Web.config
Dashboard service	*<Installation directory>*\Scout Enterprise Dashboard Service	ScoutDashboardService.exe.config
Dashboard plugin	*<Installation directory>*\Scout Enterprise Dashboard Service\Plugins\Configuration	ManagedThinClientMonitor.config
Dashboard plugin	*<Installation directory>*\Scout Enterprise Dashboard Service\Plugins\Configuration	ScoutServerViews.config
Dashboard plugin	*<Installation directory>*\Scout Enterprise Dashboard Service\Plugins\Configuration	SyncScoutServerLog.config

[1] for Scout Enterprise Management Suite 15.0 and later versions

9.3. Showing company logos on the website

In place of the Unicon logo, you can show your own company logo on the Scout Dashboard website or API website.[1] In addition, you can show your own website icon (Favicon).

Requires
The picture files must be provided in a suitable size. The `.ico` format is not supported.

1. Save the picture files to the following directory:

Dash-board	*<WebserverRootDirectory>*`\Scout\`*<YourWebsiteName>*`\Content\images\CompanyLogo` Example: `C:\inetpub\wwwroot\Scout\Dashboard\Content\images\CompanyLogo`
API	`<WebserverRootDirectory>\Scout\`*<YourWebsiteName>*`\Api\Areas\HelpPage\Content\images\CompanyLogo`

2. Open the configuration file `Web.config` using a text editor:

Dashboard	*<WebserverRootDirectory>*`\Scout\`*<YourWebsiteName>*`\Web.config`
API	*<WebserverRootDirectory>*`\Scout\`*<YourWebsiteName>*`\Api\Web.config`

3. In the configuration file `Web.config`, enter the names of the picture files:

Section	`companyLogoConfigurationSection`
Parameter	`companyLogoConfiguration`

Entry	`logoName="<`*logo file*`>" urlIcon="<`*favicon file*`>"`
	Example:
	`logoName="sampleteclogo.png" urlIcon="sampletecicon.png"`

[1] for Scout Enterprise Management Suite 15.0 / Scout Enterprise Dashboard 2.0 and later versions

9.4. Database compatibility mode for Dashboard

On login to the Scout Dashboard, the database versions of the Scout Enterprise database, the Scout Enterprise Statistics database and the Scout Enterprise Dashboard database are checked for compatibility.[1] If the version numbers do not match, the user cannot log in but receives a message.

Compatibility is additionally validated for the Dashboard service. The service is stopped as soon as one of the databases is found not to be compatible. By default, the validation is performed every 60 seconds.

Incompatibilities due to different database versions can arise if, for example, Scout Server has been updated to a newer version but Scout Enterprise Dashboard on another machine has not yet been updated.

Modifying the validation frequency of the Dashboard service

- Modify the values of the following parameters in the configuration file by using a text editor:

Path	*<Installation directory>*`\Scout Enterprise Dashboard Service` Example: `C:\Program Files\Unicon\Scout Enterprise Dashboard Service`
File	`ScoutDashboardService.exe.config`
Section	`databaseVersionConfigurationSection`
Parameter `occuringType`	`Periodically` | `Once` For `Once`, validation is performed only once on the start of the service
Parameter `schedulePeriodInSeconds`	*<Integer value for the number of seconds for `Periodically`>* A minimum period of 60 seconds (default) is recommended.

9.5. Dashboard / Limited functionality

Hiding views

- for Scout Enterprise Management Suite 15.2 and later versions -

By default, Scout Dashboard provides five views. If required, you can hide individual pages:

[1] for Scout Enterprise Management Suite 15.0 / Scout Enterprise Dashboard 2.0 and later versions

Path	*<Web server root directory>*\Scout*<YourWebsiteName>* Example: C:\inetpub\wwwroot\Scout\Dashboard
File	Web.config
Section	grantedPageConfigurationSection
Parameter	grantedPageConfiguration
Entry	pages="Home,Device,Log,ReportDefinition,CommandHistory"

- Delete the relevant pages from the entry.

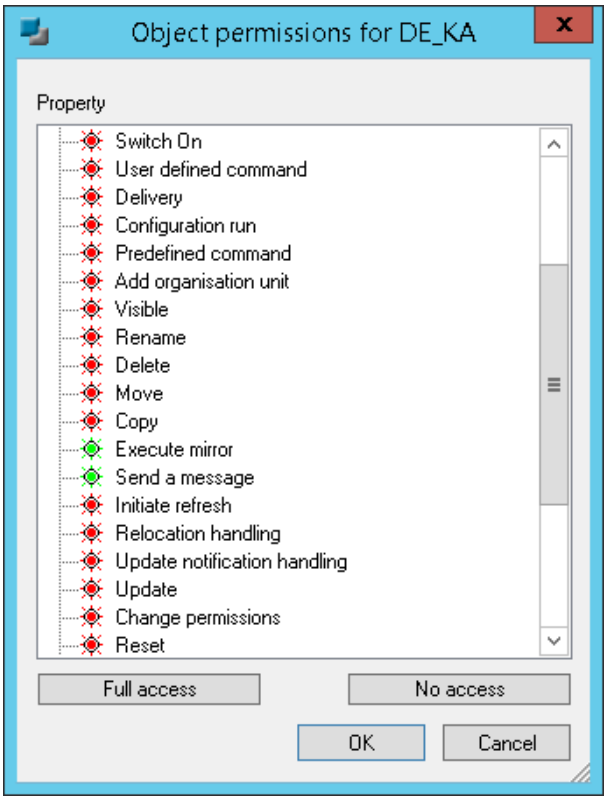
Example:

```
<grantedPageConfigurationSection>
  <grantedPageConfiguration pages="Device" />
</grantedPageConfigurationSection>
```

The configuration of the example shows only the **Devices** page in the Scout Dashboard. The remaining pages cannot be displayed, either via the interface or the URL.

Disabling further functions

You can disable more functions by restricting the administrator object rights in the Scout Console. For example, you can authorize an administrator only to mirror devices. For further information, see Changing object rights.



9.6. Dashboard / Obsolete diagnostic files

Diagnostic files that have been requested via Scout Dashboard are stored on the web server under `<web server root directory>\Scout\<YourWebsiteName>\Content\Diagnostic` and are deleted after 30 days by default.[1]

You can modify the time period after which downloaded diagnostic files are deleted:

Path	`<Web server root directory>\Scout\<YourWebsiteName>\Api`
	Example:
	`C:\inetpub\wwwroot\Scout\Dashboard\Api`

File	`Web.config`
Section	`deviceDiagnosticConfigurationSection`
Parameter	`numberOfDaysUntilDeleted`
Entry	*<integer value for the number of days>* default = 30

For further information, see Diagnostic files in the **Dashboard** guide.

[1] for Scout Enterprise Management Suite 15.0 / Scout Enterprise Dashboard 2.0 and later versions

10. 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 Enterprise feature **Files configured for transfer**. For further information, see Files configured for transfer in the **Scout Enterprise** 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	/setup/cacerts/login
Secure connection (TLS)	Firefox	/setup/cacerts/firefox[1] /setup/cacerts/browser[2]
Secure connection (TLS)	Chromium	/setup/cacerts/browser
Secure connection (TLS)	Builtin Browser Kiosk mode	/setup/cacerts/browser[3]
Secure connection (TLS)	Citrix Workspace app	/setup/cacerts/ and /setup/cacerts/intcerts
Secure connection (TLS)	VMware Horizon client	/setup/cacerts/
Secure connection (TLS)	eLuxRDP	/setup/cacerts
Network logon	WLAN drivers / WPA-Supplicant (802.1X) X509/Radius Network Access Control / SCEP	/setup/cacerts/ /setup/cacerts/scep

[1] for eLux RP 6.4 and earlier versions
[2] For eLux RP 6.5/Firefox 60.5 and later versions, the certificates can be located in either directory.
[3] for eLux RP 6.5 and later versions

Feature	Component	Directory
VPN / OpenVPN	VPN System[1] / BaseOS	/setup/openvpn
VPN / Cisco AnyConnect	VPN System[2] / Cisco AnyConnect	/setup/cacerts/ca and /setup/cacerts/client
Firmware update including certificate check	BaseOS	/setup/cacerts

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

[1] up to eLux RP 5.7 and eLux RP 6.5
[2] up to eLux RP 5.7 and eLux RP 6.5

10.1. Certificate for Scout Statistics Service

As the eLux clients and the Scout Statistics Service communicate via HTTPS, for the installation of the Scout Statistics 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 Statistics 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 Statistics Service and must not be changed.

11. Management protocol

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

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

11.1. Certificate-based management protocol

Beginning with Scout Enterprise Management Suite 15.1 and eLux RP 6.1, the certificate-based management protocol provides secure communication between the Scout Server and the clients via end-to-end encryption with TLS 1.2.

To manage eLux RP devices running eLux RP 6.1 and later versions, Scout Enterprise 15.1 or later is required. 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 White-paper **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 Enterprise service. Alternatively, you can use a CA certificate that must be configured on the Scout Server.

For eLux RP 6.1 and later versions, port 22125 is used for encrypted communication with the Scout Server.[1]

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

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

  For further information, see Configuring Scout Server for communication via CA certificates.

Note
You can check the communication via TLS in the log file for the Scout Server service `eluxd.log`.

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

11.2. Configuring the trust level on the clients

- for Scout Enterprise Management Suite 15.1 / eLux RP 6.1 and later versions -

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 clients. If the root certificate does not exist on the 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.

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 Enterprise** 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 Enterprise** 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 74.

4. Restart the clients.

> **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.

11.3. 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=`*Path to certificate file*	Path to the location of the certificate file Example: `C:\Users\Public\Documents\Unicon\Scout\Server\sampletec-01.pfx`
`ELUXD`	`CertificateKeyFile=`*Path to private key file*	Only required, if the certificate file is not in `pfx` format

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

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

12. Troubleshooting

Error message	Reason	Solution
File access error while checking HTTP/FTP server (error number = 404)	Possibly caused by missing MIME type entries for the used file extensions s on the web server	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. For Scout Enterprise Management Suite 15.x, the assignments are carried out automatically during the installation of the eLux container in Microsoft Internet Information Server (IIS).

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
.xz	application/x-xz

The following additional assignments might become necessary:

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

Extension	MIME type	Description
.mee	text/plain	Migration of eLux RP 5 clients to eLux RP 6 with whitelist[1] (for further information, see Limited migration) 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 Enterprise 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 Scout Enterprise Management Suite. To convert them to LocalDB, Scout Enterprise 14.6.1 is required.	First, install Scout Enterprise Management Suite version 14.6.1 with your `.mdb` database and start the console. Subsequently, install a later version with the same database. On the first start, the database is automatically converted to Local DB.
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.

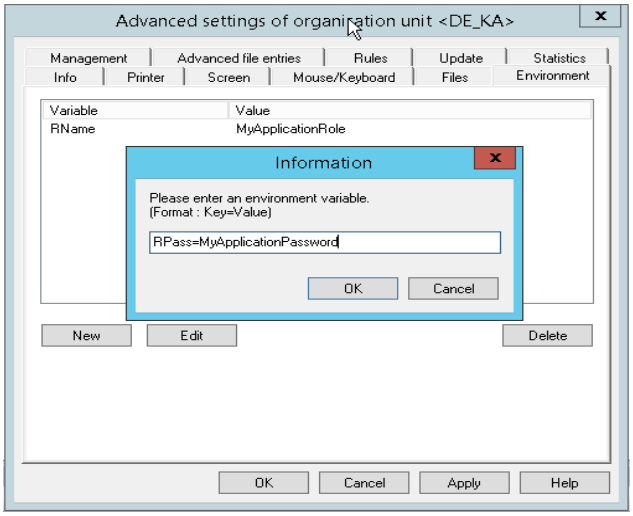
[1] for eLux RP 6.2.3 and later versions done by the container installer
[2] from Scout 15 2107 and eLux RP 6 2107

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.

13. 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, on the context menu, click **Advanced device configuration**[1] **> 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 on the context menu, click **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.

[1] formerly **Advanced settings**

14. Appendix

14.1. Program and file directories

Program directory

Scout Enterprise Management Suite by default is installed to

`%PROGRAMFILES%\Unicon\Scout`

Scout Dashboard is installed on the web server (IIS) by default to

`<root directory>\Scout\Dashboard`
The directory name `Dashboard` is the application name shown in the URL and can be modified during installation.

The eLux container is installed on the web server to

`<root directory>\eluxng`

File path for Scout Server files

Scout Enterprise 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 Dashboard are saved on the web server to

`<root directory>\Scout\Dashboard\Content\Diagnostic`

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.

14.2. eLux partitions

A thin client'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 Enterprise **Update** command with option **Format system partition before update**	Size 2 GB up to bis eLux RP 6 2104 LTSR CU1 Size 2.8 GB starting with eLux RP 6 2107
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 Enterprise command or notification Signature check for eLux software packages Devices with update partition can be used as Dynamic Proxy (Provider) for firmware updates.	Scout Enterprise **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.

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 to eLux RP 6 2107 or later, the system partition is created with 2.8 GB instead of the previous 2.0 GB. This creates more space for the firmware and allows larger images to be used.

If an up-to-date recovery system is available, you can partition the system partition to fit the new size of 2.8 GB during the installation process. Otherwise, the devices will need to be restarted after the installation.

To ensure you have an up-to-date recovery system for eLux RP 6 2107, choose to use one of the following options:

- Ready-to-use eLux USB stick image **eLux RP 6 2107 Recovery Stick** available for download on our technical portal
- Recovery system for creating individual USB recovery images in ELIAS as a `.dd` file[1]
  - ELIAS 18: **eLux USB Recovery system for ELIAS 18** package, available for download on our technical portal in the eLux RP 6 2107 container, can be imported into ELIAS 18 installations / containers
  - Legacy ELIAS: by installing Scout Enterprise Management Suite 15 2107 including ELIAS[2]
- Recovery system for PXE installations through installation of Scout Enterprise Management Suite 15 2107 including recovery service

Important

To downgrade devices with the extended system partition of 2.8 GB (eLux RP 6 2107 or later) to an earlier version that supports a 2 GB system partition, you will have to go back to eLux RP 6 2104 LTSR CU1.
We therefore recommend that you update test devices to eLux RP 6 2107 as the first step to thoroughly test functionality.

14.3. 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 **Config**[3] **> Security**, disable mirroring or uninstall `VNC server` in `X.Org` package	Incoming
22123	TCP	Scout Server (Scout Enterprise Manager / secure)		In/Out

[1] For further information, see Image as a USB recovery system in the ELIAS 18 guide
[2] `.dd` file can be found in the ELIAS program directory
[3] Device configuration, formerly Setup

Port	Type	Description	How to deactivate	In/Out
22125	TCP	Scout Server (Scout Enterprise Manager / TLS 1.2) [1]		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

[1] for Scout Enterprise Management Suite 15.1 / eLux RP 6.1 and later versions

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
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

Port	Type	Description	How to deactivate	In/Out
20000	UDP	Wake On LAN		In/Out
22124	TCP	Scout Enterprise 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 Enterprise Manager / secure)	In/Out
22124	TCP	Scout Enterprise Statistics	Incoming
22125	TCP	Clients (Scout Enterprise Manager / TLS 1.2) [1]	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 Dashboard

Scout Dashboard can be installed with HTTP or HTTPS.

Port	Typ	Description	How to deactivate	In/Out
80	TCP	Dashboard service / web server via HTTP		Incoming
443	TCP	Dashboard service / web server via HTTPS/TLS		Incoming

[1] for Scout Enterprise Management Suite 15.1 / eLux RP 6.1 and later versions

Port	Typ	Description	How to deactivate	In/Out
5901	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 Enterprise Manager / TLS 1.2)	In/Out
22129	TCP	VPN	Incoming

14.4. SNMP

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

For eLux RP 5 and 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.

14.4.1. Configuring SNMP

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

   Or:

   Modify the `terminal.ini` file by using the Advanced file entries feature of Scout Enterprise. Example:

File	`/setup/terminal.ini`
Section	`SNMPD`
Entry	`rocommunity`
Value	`secret`

3. Optionally, to define further SNMPD Configuration Directives, use the Advanced file entries 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.

14.4.2. SNMPD and SNMP Configuration Directives

The following table refers to the software package **snmp-5.6.1.1-2** for eLux.
For further information on using SNMP with eLux, see SNMP.

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
sysservices	NUMBER
interface	name type speed
com2sec	name source community
group	name v1|v2c|usm security
access	name context model level prefx 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