primos

— Print. Mobile. Secure. —

by SEH

User Manual

Manufacturer and Contact

SEH Computertechnik GmbH
Suedring 11
33647 Bielefeld
Germany

Phone: +49 (0)521 94226-29
Fax: +49 (0)521 94226-99
Support: +49 (0)521 94226-44
Email: info@seh.de
Web: http://www.seh.de

Scan this QR code (meCard) using your smart phone.

Document

Type: User Manual
Title: primos
Version: 1.1

Legal Notices

Contents

1   General Information

This chapter contains information concerning the device and the documentation as well as notes about your safety.
You will learn how to benefit from your primos and how to operate the device properly.

What Information Do You Need?

- 'primos' ⇨ 🖹2
- 'Documentation' ⇨ 🖹3
- 'Support And Service' ⇨ 🖹5
- 'Your Safety' ⇨ 🖹6
- 'First Steps' ⇨ 🖹6
- 'Find IP address of primos' ⇨ 🖹7

1.1   primos

Purpose

primos is a mobile printing solution for printing content such as documents and graphics from iOS devices (iPhone, iPad etc.). Print jobs that go through primos stay in the network, they are processed locally and do not get transferred via the Internet or cloud mechanisms. Up to 10 printers can be made available for iOS devices with primos.

primos has mainly been developed for professional business use (enterprise environments).

Mode of Operation

primos is connected to your network by cable. The iOS devices are connected to this network via WLAN. Print jobs are sent from iOS apps with AirPrint™ support to primos via your network. primos forwards the print job to wired or wireless printers with or without AirPrint™ support for printing. In doing so primos is manufacturer-independent.

Optionally, a USB printer can be connected to the USB port of primos and thus be AirPrint™ enabled.
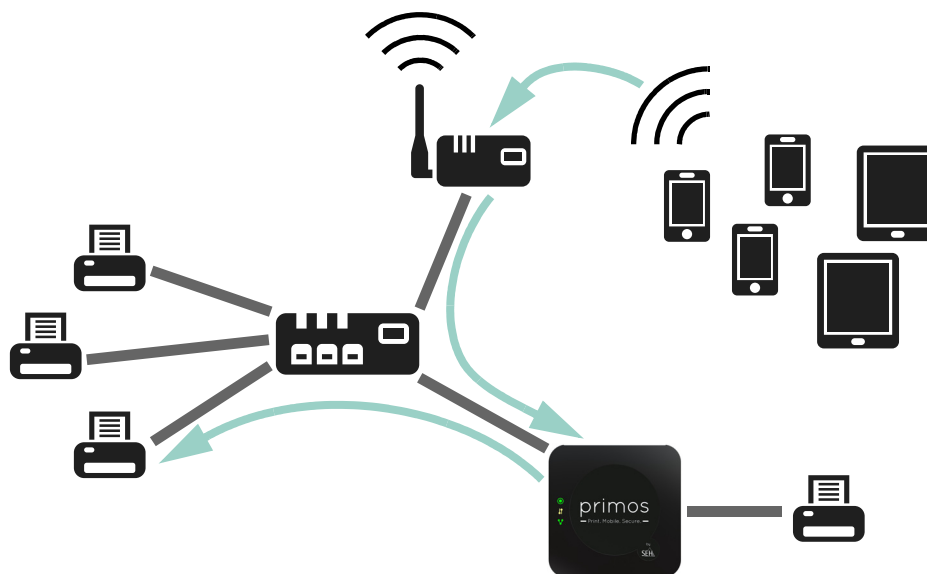
Figure 1:   Topology

In addition, primos enhances AirPrint™with various features (Wide-Area AirPrint™, directory services support and much more).

Requirements

Network
Wired TCP/IP network (LAN) with wireless access point (WLAN).

Supported iOS Devices
primos supports all iOS devices with AirPrint™ support. All iOS devices with iOS 4.2 or later come with AirPrint™. The iOS devices are connected to the wired network via WLAN.

Supported Printers
Network printers (wired or wireless) which support at least one of the following printing protocols: IPP, IPP Secure, LPD or Socket Printing (JetDirect Printing).

1.2 Documentation

Information about the features of your product can be found in the data sheet of your primos.

Structure of the Documentation

The primos documentation consists of the following documents:

User Manual	PDF	Detailed description of the primos configuration and administration.
Quick Installation Guide	Printed PDF	Information about hardware installation and the initial operation procedure.
Important Product Information	Printed PDF	Information about security, regulatory compliance, and disposal.
Online Help (primos Control Center)	HTML	The Online Help contains detailed information about how to use the 'primosControl Center'.

Document Features

This documentation has been designed as an electronic document for screen use. Many programs (e.g. Adobe® Reader®) offer a bookmark navigation feature that allows you to view the entire document structure.

This document contains hyperlinks to the associated information units. If you want to print this documentation, we recommend using the printer setting 'Duplex' or 'Booklet'.

Terminology Used in this Document

The explanation of technical terms used in this document is summarized in a glossary. The glossary provides a quick overview of technical matters and background information ⇨ 🖹66.

Symbols and Conventions

A variety of symbols are used within this document. Their meaning is listed in the following table:

——— **Warning** ——— **Warning**	A warning contains important information that must be heeded. Non-observance may lead to malfunctions.
——— **Note** ——— Note	A notice contains information that should be heeded.
1. Mark ...	Numbers guide you through instructions.
↳ Confirmation	The arrow confirms the consequence of an action.
✓ Requirements	Hooks mark requirements that must be met before you can begin the action.
☐ Option	A square marks procedures and options that you can choose.
•	Eye-catchers mark lists.
🛈	This sign indicates the summary of a chapter.
⇨ 🖹	The arrow marks a reference to a page within this document. In the PDF file, you can jump to this page by clicking the symbol.
💡	The light bulb signals tips.
Bold	Established terms (of buttons or menu items, for example) are set in bold.
Courier	Command lines are set in Courier font.
'Proper names'	Proper names are put in inverted commas

1.3 Support And Service

Contact SEH Computertechnik GmbH offers extensive support. If you have any questions, please contact our hotline.

Monday – Thursday	8:00 a.m. – 4:45 p.m.
Friday	8:00 a.m. – 15:15 p.m.

+49 (0)521 94226-44   USA: +1-610-943-3226

support@seh.de

http://www.seh.de/

Downloads Downloads can be found on the SEH Computertechnik GmbH homepage:

http://www.seh-technology.com/services/downloads/
download-mobility-solutions/primos.html

For primos you will find:

- current firmware/software
- current tools
- current documentation
- current product information
- product data sheets
- and much more

1.4   Your Safety

Read and observe all safety regulations and warnings found in the documentation, on the device and on the packaging. This will avoid potential misuse and prevent damages to people and devices.

SEH Computertechnik GmbH will not accept any liability for personal injuries, property damages and consequential damages resulting from the non-observance of the mentioned safety regulations and warnings. SEH Computertechnik GmbH will not accept any liability for loss of data, property damages and consequential damages resulting from the non-observance of the mentioned safety regulations and warnings.

Intended Use   primos is used in TCP/IP networks and has been designed for use in office environments. primos allows for printing from iOS devices on printers with or without AirPrint™ support.

Improper Use   All uses of the device that do not comply with the primos functionalities described in the documentation are regarded as improper uses. It is not allowed to make modifications to the hardware and software or to try to repair the device.

Safety Regulations   Before starting the initial operation procedure of primos, read and follow the safety regulations in the document 'Important Product Information'. This document is enclosed in the packaging in printed form.

Warnings   Read and observe all warnings mentioned in this document. Warnings are found before any instructions known to be dangerous. They are presented as follows:

--------- **Warning** ---------
Warning!

1.5   First Steps

This section provides all the information that you need for a fast operational readiness.

1. Read and observe the security regulations in order to avoid damages to people and devices ⇨🗎6.
2. Carry out the hardware installation. The hardware installation comprises the connection of primos to the network and the mains supply; see: 'Quick Installation Guide'.
3. Find the IP address of primos; see: ⇨🗎7.
4. Configure print queues on primos ⇨🗎22.
↳ primos is now operational. You can print from iOS devices ⇨🗎36.

1.6 Find IP address of primos

Why IP Addresses?

An IP address is used to address network devices in an IP network. TCP/IP network protocols require the storing of the IP address in primos so that the device can be addressed within the network.

How Does primos Obtain its IP Address?

primos is shipped without IP address. After primos has been connected to the network, it receives an IP address via DHCP. If this is not the case, primos seeks a ZeroConf IP address from the ZeroConf address range (169.254.0.0/16).

You can change the IP address settings later on:

- 'How to Configure IPv4 Parameters' ⇨🗎13
- 'How to Configure IPv6 Parameters' ⇨🗎14

How Do I Find the IP Address?

The primos IP address can be determined using the SEH primos App.

System Requirements of the SEH primos App:
- Windows 7, Windows 8, Windows 10;
  OS X 10.7.x – 10.11.x
- The installation can only be carried out by users with administrative rights.

Requirements

✓ primos is connected to your network; see: 'Quick Installation Guide'.

1. Write down the hardware address of you primos. You can find the hardware address in the type plate at the bottom of primos.
2. Download the SEH primos App for your operating system from the SEH Computertechnik GmbH website.

http://www.seh-technology.com/services/downloads/
download-mobility-solutions/primos.html

3. Install the SEH primos App on your client.
4. Start the SEH primos App.
   All primos devices found in the network are displayed.
5. Find your primos using the hardware address.

Note

The IP address can also be found via Bonjour. primos is advertised under the name 'primos@ICxxxxxx' (wherein ICxxxxxx is the default name ⇨ 🖹66). All devices with iOS and OS X support Bonjour natively. On devices with other operating systems, such as Windows, the Bonjour service must be installed manually.

---

2   Administration Methods

You can administer and configure primos in a number of ways. The following chapter gives you an overview of the various administration options.

You will get information on when to use these methods and which functions these methods support.

What Information Do You Need?

- 'Administration via the primos Control Center' ⇨🖹9
- 'Administration via SEH primos App' ⇨🖹12

2.1   Administration via the primos Control Center

What Is the primos Control Center?

primos can be configured and monitored via the primos Control Center. The primos Control Center is stored in primos and can be displayed by means of a browser software (Internet Explorer, Mozilla Firefox, Safari).

Security

The access to the primos Control Center is protected (⇨🖹45). The default user profile is:
User name: admin
Password: admin

—— **Note** ——
Change the default password as soon as possible (⇨🖹45)!

For further information on user profiles see ⇨🖹45.

Starting the primos Control Center

You can open the primos Control Center directly in the browser or via the SEH primos App:

- 'Open primos Control Center in Browser' ⇨🖹10
- 'Open primos Control Center via SEH primos App' ⇨🖹10

—— **Note** ——
If the primos Control Center is not displayed, check the proxy settings of your browser.

Open primos Control Center in Browser

Requirements
- ✓ primos is connected to the network and the mains voltage.
- ✓ primos has a valid IP address.

1. Open your browser.
2. Enter the IP address of primos as the URL.
↳ The primos Control Center is displayed in the browser.

Open primos Control Center via SEH primos App

Requirements
- ✓ primos is connected to the network and the mains voltage.
- ✓ primos has a valid IP address.
- ✓ Your primos is displayed in the SEH primos App (⇨ 🖺12).

1. In the list, double-click on your primos.
↳ Your standard browser opens and the primos Control Center is displayed.

Structure of the primos Control Center

Figure 2:   primos Control Center

You can choose your language by clicking the relevant flag.

The available menu items are located in the navigation bar (top). After selecting a menu item (simple mouse click), the available submenu items are displayed at the left. After selecting a submenu item, the corresponding page with its content is displayed (at the right).

The manufacturer's contact details and additional information regarding the product are displayed under **Product & Company**. The **Sitemap** provides an overview of and direct access to all pages of the primos Control Center.

All other menu items refer to the configuration of primos. They are described in the Online Help of the primos Control Center. To start the Online Help, click the (?) icon.

Logout   For security reasons, always logout of the primos Control Center after having configured settings.

1.   Click **Logout**.
↳ The login page appears. You have successfully logged out.

2.2   Administration via SEH primos App

The SEH primos App has been developed by SEH Computertechnik GmbH for the administration of primos devices.

Mode of Operation

After the SEH primos App is started, the network will be scanned for connected primos devices. The network range to be scanned is freely definable. All primos devices found will be displayed in a list. All devices found can be selected and administrated.

Installation

In order to use the SEH primos App, the program must be installed on a computer with a Windows or Mac OS X operating system. Different installation files are available, depending on the operating system.

System requirements

– Windows 7, Windows 8, Windows 10;
   OS X 10.7.x – 10.11.x
– The installation can only be carried out by users with administrative rights.

1. Download the SEH primos App for your operating system from the SEH Computer-technik GmbH website.

    http://www.seh-technology.com/services/downloads/
    download-mobility-solutions/primos.html

2. Install the SEH primos App on your client.
↳ The SEH primos App is installed on your client.

Start

You can identify the SEH primos App by its icon: . The SEH primos App can be started with the usual mechanisms of your operating system.

3   Network Settings

You can define various settings for an ideal integration of primos into a network.
This chapter describes which network settings are supported.

3.1   How to Configure IPv4 Parameters

You can define various IPv4 parameters for an ideal integration of primos into a TCP/IP network. By default, the IP address is assigned dynamically to primos via DHCP. However, you can manually assign a static IP address to primos.

1. Start the primos Control Center.
2. Select **NETWORK – IPv4**.
3. Configure the IPv4 parameters; table 1 ⇨ 13.
4. Click **Save** to confirm.
↳ The settings are saved.

Table 1: IP parameters

Parameters	Description
DHCP	Enables/disables the DHCP protocol. *TCP/IP parameters can be assigned automatically to primos via DHCP.*
Static	Enables/disables the manual assignment of static TCP/IP parameters for primos. *Define the IP address, subnet mask and gateway.*
IP address	Defines a manually assigned IPv4 address for primos.
Subnet mask	Defines a manually assigned subnet mask for primos.
Gateway	Defines a manually assigned gateway address for primos.

3.2   How to Configure IPv6 Parameters

You can integrate primos into an IPv6 network.

What Are the Advantages of IPv6?

IPv6 (Internet Protocol version 6) is the successor of the more common IPv4. Both protocols are standards for the network layer of the OSI model and regulate the addressing and routing of data packets via a network. The introduction of IPv6 has many benefits:

- IPv6 increases the IP address space from 2^{32} (IPv4) to 2^{128} (IPv6) IP addresses
- Auto Configuration and Renumbering
- Efficiency increase during routing due to reduced header information
- Integrated services such as IPSec, QoS, Multicast
- Mobile IP

What is the Structure of an IPv6 Address?

An IPv6 address consists of 128 bits. The normal format of an IPv6 address is eight fields. Each field contains four hexadecimal digits representing 16 bits.

Each field is separated by a colon (:). Example:

`fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4`

Leading zeros in a field can be omitted. Example:

`fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4`

An IPv6 address may be entered or displayed using a shortened version when successive fields contain all zeros (0). In this case, two colons (::) are used. However, the use of two colons can be used only once in an address. Example:

`fe80 :                          : 10 : 1000 : 1a4`

As a URL in a Web browser, an IPv6 address must be enclosed in brackets. This prevents port numbers from being mistakenly regarded as part of an IPv6 address. Example:

`http://[2001:608:af:1::100]:443`

Note

The URL will only be accepted by browsers that support IPv6.

Which Types of IPv6 Addresses Are Available?

There are different types of IPv6 addresses. The prefixes of the IPv6 addresses provide information about the IPv6 address types.

- Unicast addresses can be routed globally. These addresses are unique and therefore unambiguous. A packet that is sent to a unicast address will only arrive to the interface that is assigned to this address. Unicast addresses have the prefixes '2' or '3'.
- Anycast addresses are assigned to more than one interface. This means that a data packet that is sent to this address will arrive at various devices. The syntax of anycast

addresses is the same as the one of unicast addresses. The difference is that anycast addresses choose one interface out of many.

- A packet that is dedicated to an anycast address arrives at the nearest interface (in line with the router metrics). Anycast addresses are only used by routers.

- Multicast addresses allow you to send data packets to different interfaces at the same time without a proportional increase of the bandwidth. A multicast address can be recognized by the prefix 'ff'.

1. Start the primos Control Center.
2. Select **NETWORK – IPv6**.
3. Configure the IPv6 parameters; table 2 ⇨ 📄15.
4. Click **Save** to confirm.
↳ The settings are saved.

Table 2: IPv6 parameters

Parameters	Description
IPv6	Enables/disables the IPv6 functionality of primos.
Automatic configuration	Enables/disables the automatic assignment of the IPv6 address for primos.
IPv6 address	Defines a manually assigned IPv6 unicast address in the n:n:n:n:n:n:n:n format for primos. *Every 'n' represents the hexadecimal value of one of the eight 16 bit elements of the address.*
Router	Defines the IPv6 unicast address of the router. primos sends its 'Router Solicitations' (RS) to this router.
Prefix length	Defines the length of the subnet prefix for the IPv6 address. The value 64 is preset. *Address ranges are indicated by prefixes. The prefix length (number of bits used) is added to the IPv6 address and specified as a decimal number. The decimal number is separated by '/'.*

3.3 How to Configure the DNS

DNS is a service that translates domain names into IP addresses. Using DNS, names can be assigned to IP addresses and vice versa.

With the help of DNS, some settings can be made more easily (input of host names instead of IP addresses when specifying servers).

Note

If your network in configured accordingly, primos receives the DNS settings automatically via DHCP.

---

1. Start the primos Control Center.
2. Select **NETWORK – DNS**.
3. Configure the DNS parameters; table 3 ⇨🖹16.
4. Click **Save** to confirm.
↳ The settings are saved.

Table 3: DNS parameters

Parameters	Description
Primary DNS server	Defines the IP address of the primary DNS server.
Secondary DNS server	Defines the IP address of the secondary DNS server. *The secondary DNS server is used if the primary DNS server is not available.*
Domain name (suffix)	Defines the domain name of an existing DNS server.

3.4 How to Configure Bonjour

Bonjour allows the automatic recognition of computers, devices, and network services in TCP/IP-based networks.

primos uses Bonjour to:

- search for printers in the network (⇨🖹22).
- check the IP address assigned via ZeroConf (⇨🖹7).
- announce its Bonjour services.

Bonjour is always active in primos. You can configure the name that primos uses to announce its Bonjour services. By default, primos advertises under the name 'primos@ICxxxxxx' (wherein ICxxxxxx is the default name ⇨🖹66).

1. Start the primos Control Center.
2. Select **NETWORK – Bonjour**.
3. Configure the Bonjour name.

4.   Click **Save** to confirm.
↪ The setting will be saved.

3.5   How to Configure Directory Services

You can embed primos into a directory service. Via the directory service user data is managed centrally and can be provided to primos. You can use this to control who can print ⇨▤35.

───────── **Note** ─────────
Settings for the Active Directory user login (⇨▤45) are made independent of the settings for embedding primos into Active Directory described in this chapter.
─────────────────────────────

primos supports the following directory service:

• Active Directory®
• LDAP

What Do You Want to Do?

☐   'Embedding primos into an Active Directory' ⇨▤17
☐   'Embedding primos into an LDAP directory' ⇨▤18

Embedding primos into an Active Directory
primos is embedded into an Active Directory by making it member of a domain.

Requirements

✓   A DNS server is configured in primos ⇨▤16.
✓   primos was entered with a type A resource record (IPv4 address of the host) on the DNS server used.
✓   A time server is configured in primos ⇨▤19.

1.   Start the primos Control Center.
2.   Select **NETWORK – Directory services**.
3.   Configure the Active Directory parameters; table 4 ⇨▤17.
4.   Click **Save** to confirm.
↪ primos is member of a domain and thus embedded into the Active Directory.

Table 4:   Active Directory parameters

Parameters	Description
Active Directory	Enables/disables the embedding of primos into an existing Active Directory.
Active Directory name	Defines the name of the Active Directory into which primos is embedded. *Enter the full name of the domain (Fully Qualified Domain Name – FQDN).*

Parameters	Description
Workgroup	Defines the name of the workgroup. *Enter the NetBIOS domain name.*
Password server	Defines the password server of the Active Directory via the IP address or the host name. (Optional) *The host name can only be used if a DNS server was configured beforehand.*
WINS server	Defines the WINS server of the Active Directory via the IP address or the host name. *A WINS server should be specified to allow the communication between participants of different network segments.* *The host name can only be used if a DNS server was configured beforehand.*
Administrator account	Defines the name of the administrator account that was created for primos on the Domain Controller.
Password	Password of the administrator account that was created for primos on the Domain Controller of the Active Directory.

Embedding primos into an LDAP directory

Requirements

✓ A DNS server is configured in primos ⇨ 🗎16.
✓ primos was entered with a type A resource record (IPv4 address of the host) on the DNS server used.
✓ A time server is configured in primos ⇨ 🗎19.

1. Start the primos Control Center.
2. Select **NETWORK – Directory services**.
3. Configure the LDAP parameters; table 5 ⇨ 🗎18.
4. Click **Save** to confirm.
↳ primos is embedded into the LDAP directory.

Table 5: LDAP parameters

Parameters	Description
LDAP	Enables/disables the embedding of primos into an existing LDAP directory service.
LDAP server	Defines the LDAP server via the IP address or the host name. *The host name can only be used if a DNS server was configured beforehand.*
Base DN	Defines the base DN (distinguished name). The base DN defines the starting point in the directory for the downwards search of users. *Domain components are to be separated by commas (example: dc=mydomain,dc=com).*

4 Device Settings

You configure descriptions and the device time for primos. This chapter describes these device settings.

4.1 How to Determine a Description

You can assign freely definable descriptions to primos. This gives you a better overview of the devices available in your network.

1. Start the primos Control Center.
2. Select **DEVICE** - **Description**.
3. Enter freely definable names for **Host name**, **Description**, and **Contact person**.
4. Click **Save** to confirm.
↳ The descriptions are saved.

4.2 How to Configure the Device Time

You can control the device time of primos via a time server (SNTP server) in the network. A time server synchronizes the time of devices within a network.

Benefits and Purpose

primos needs the device time to join directory services (⇨ 🖹17) and to provide the print jobs in the job history (⇨ 🖹29) with time stamps amongst other things.

UTC

primos uses 'UTC' (Universal Time Coordinated) as a basis. UTC is a reference time and used as a time standard.

Time Zone

The time received by the time server does not necessarily correspond to your local time zone. Deviations from your location and the resulting time difference (including country-specific particularities such as Daylight Saving Time) can be handled by means of the 'Time zone' parameter.

―――― **Note** ――――
Time servers can be assigned automatically via DHCP. A time server assigned via DHCP always takes priority over a manually defined time server.

Requirements

✓ A time server is integrated into the network.

1. Start the primos Control Center.
2. Select **NETWORK – Date/Time**.
3. Tick **Date/Time**.
4. Into the **Time server** box, enter the IP address or the host name of the time server
   (The host name can only be used if a DNS server was configured beforehand.)
5. Select the code for your local time zone from the **Time zone** list.
6. Click **Save** to confirm.
↳ The settings are saved.

5   Print

This chapter explains how you set up primos for printing and how you configure enhanced settings for printing.

In order to print from iOS devices via primos, you have to create a print queue for the respective printer in primos. For each queue you then define numerous settings (driver, print protocol, access control and much more). In addition, you can define general print options.

What Information Do You Need?

- 'How to Configure Printers on primos (Creating Queues)' ⇨📄22
- 'How to Manage Queues' ⇨📄27
- 'How to View the Job History' ⇨📄29
- 'How to Define the Printer Name That Is Displayed on the iOS Devices' ⇨📄30
- *'How to Manage Drivers in primos'* ⇨📄31
- 'How to Maintain or Test a Printer via primos' ⇨📄33
- 'How to Configure Advanced Print Settings' ⇨📄33
- 'How to Encrypt Print Data Transmission' ⇨📄34
- 'How to Control Who Can Print' ⇨📄35
- 'How to Print from iOS Devices' ⇨📄36
- 'How to Print Across Subnets (Wide-Area AirPrint™)' ⇨📄37

5.1   How to Configure Printers on primos (Creating Queues)

In order to print from iOS devices via primos, you have to create a print queue, queue for short, for the respective printer in primos.

What Is a Queue?   Queues are used to communicate with printers and transmit print jobs. The prints jobs are collected in the queue and processed one after another. This way several persons can share a printer without conflict.

———— **Note** ————
Up to 10 queues can be created in primos.

How to Create a Queue   There are 3 possibilities to create queues in primos:

- **Smart Printer Setup**: Starts a search for network printers. Subsequently up to 10 queues will be created automatically.
- **Expert Printer Setup**: Starts a search for network printers. You will then get a list of printers found and queue proposals for those printers. You can edit those and create up to 10 queues.
  (Knowledge of printer settings required.)
- **Manually create** a queue: If you create a queue manually, you need to configure all settings for one single queue. When you are doing this, the network is searched for printers in the background. You either choose the printer for which you want to create the queue from the list of search results or define a printer connection manually.
  (This method of creating a queue is especially suited for when you only want to create a single queue or create a queue for a specific printer.)

———— **Note** ————
The Smart Printer Setup is only available if no queues are created in primos.

What Do You Want to Do?
- ☐ 'Using the Smart Printer Setup' ⇨🖹23
- ☐ 'Using the Expert Printer Setup' ⇨🖹23
- ☐ 'Creating a Queue Manually' ⇨🖹25

Using the Smart Printer Setup

If you open the primos Control Center START page and if no queues are created in primos, e.g. when you install primos for the first time, an automatic pop-up that allows you to start the Smart Printer Setup appears. Alternatively, you can start the Smart Printer Setup manually.

Which Queues are Created?

In primos up to 10 queues are created automatically for printers. If a USB printer is connected to the USB-Port of primos, a queue is created for this printer first of all.

✓ No queue has been created in primos.

1. Start the primos Control Center.
2. Select **PRINTING – Printer Setup**.
3. In the **Default settings for discovery results** area, define the default settings for creating queues on the basis of the discovery results.
4. Click **Smart Printer Setup**.
↳ The Smart Printer Setup starts. primos searches for network printers and automatically creates queues for up to 10 printers found. Then an overview of the queues created is displayed.

Note

Depending on the size of your network, running the Smart Printer Setup may take a few minutes.

Note

If a queue is marked with a yellow pencil icon, check if the assigend manufacturer and model are correct.

Using the Expert Printer Setup

✓ A maximum of 9 queues are created in primos.

1. Start the primos Control Center.
2. Select **Printing – Printer discovery**.
3. In the **Default settings for discovery results** area, define the default settings for creating queues on the basis of the discovery results.
(You can change queues individually when editing the discovery results.)
4. Click **Expert Printer Setup**.
The printer discovery starts. After the printer discovery has finished, a list of the printers found is displayed.

Note

Depending on the size of your network, the printer discovery may take a few minutes.

---

5. Define the queue settings for the desired printers; table 6 ⇨ 🖹24.
   - Use the checkbox in front of the printer to select one or more printers for which a queue is to be created.
   - You can filter the search results according result type (only newly discovered printers / all printers) and printer connection (IPP, socket, etc.)

Note

Do not filter the discovery results after you already have defined settings. Hidden queues will automatically be reset to their default values.

---

6. Click **Save all** or **Save selected**.
   ↳ The queues are created in primos.

Note

Only after the queue has been created, you can define enhanced settings for the queue. See 'Edit Queue' ⇨ 🖹27.

Tabelle 6: Queue parameters

Parameters	Description
Driver	primos tries to assign correct printer drivers to the printers discovered in the network. color mark following the printer name indicates if a suitable driver was found for the respective printer: - green: a suitable driver was assigned - green with check mark: the driver has been assigned to this printer type once before by the administrator - yellow: a driver was assigned but it must be checked if it is suitable - red: no suitable driver was found If a incorrect or no driver was assigned, a driver can be chosen and assigned to printers via the button 'Apply the driver chosen above'.
Name	Freely definable queue name. The queue name and the AirPrint™ identifier together make up the printer name that is displayed in the printer dialog of the iOS devices. *Up to 50 ASCII characters (except for spaces, slashes, quotation marks and the pound sign) can be entered.* *The queue name cannot be changed afterwards!*
Description	Freely definable description of the queue. *You can enter a maximum of 50 ASCII characters.*
Connection type	Defines the printing protocol (IPP, socket and so on).

Parameters	Description
Upload driver (PPD)	Loads a printer driver onto primos and assigns it to the queue. *If the pre-installed printer drivers do not suffice, you can load a suitable driver onto primos. The driver must be in 'PPD' format. For further information; see: ⇨ 📄31.*
Paper size	Defines the paper size for printouts.

Creating a Queue Manually

1. Start the primos Control Center.
2. Select **Printing – Create queue**.
3. Configure the queue parameters; table 7 ⇨ 📄25.
4. Click **Create queue**.
↳ The queue is created in primos.

Tabelle 7: Create queue – parameters

Parameters	Description
Name	Freely definable queue name. The queue name and the AirPrint™ identifier (⇨ 📄30) together make up the printer name that is displayed in the printer dialog of the iOS devices. *Up to 50 ASCII characters (except for spaces, slashes, quotation marks and the pound sign) can be entered.* *The queue name cannot be changed afterwards!*
Description	Freely definable description of the queue. *You can enter a maximum of 50 ASCII characters.*
Select Printer	Defines the printer. *The list shows printers automatically discovered in the network. You may also define a printer connection manually ('Connection').*
Connection type	Defines the printing protocol (IPP, socket and so on) for the printer selected from the list. *You can only select printing protocol which the printer chosen supports.*

Parameters	Description
Connection	Defines the connection to a printer in the form of a device URI (uniform resource identifier).
	- IPP / IPPS: In IPP (Internet Printing Protocol) the print data is transmitted via HTTP to the printer. The connection between primos and the printer can be encrypted via SSL/TLS (IPPS). Standard port IPP: 631. Standard port IPPS: 443.
	`ipp://<IP address or host name of the printer>:<port number>/ipp`
	`ipp://<IP address or host name of the printer>/ipp/`
	`ipps://<IP address or host name of the printer>:<port number>/ipp`
	`ipps://<IP address or host name of the printer>/ipp/`
	- LPR/LPD protocol: In Line Printer Daemon printing the print data is sent to the IP address of the printer by means of an LPD queue.
	`lpd://<IP address or host name of the printer>/<queue>`
	- Socket printing (Jetdirect printing): The data is transferred to the TCP/IP port via a raw/socket connection. Standard port: 9100.
	`socket://<IP address or host name of the printer>:<port number>`
	Alternatively, you can choose a printer automatically discovered in the network from the list and select a connection type.
Paper size	Defines the paper size for printouts.
Select driver	Defines the printer driver.
Upload driver (PPD)	Loads a printer driver onto primos and assigns it to the queue. *If the pre-installed printer drivers do not suffice, you can load a suitable driver onto primos. The driver must be in 'PPD' format. For further information; see:* ⇨ 📄31.

5.2   How to Manage Queues

After you have created queues for your network printer in primos, you can edit or delete those queues.

Edit Queue

1. Start the primos Control Center.
2. Select **PRINTING – Queues**.
3. Select the queue to be edited by clicking the icon ✐.
4. Configure the queue parameters; table 8 ⇨ 🖹27.
5. Click **Save** to confirm.
↳ The settings are saved.

Table 8:   Edit queue – parameters

Parameters	Description
Description	Freely definable description of the queue. *You can enter a maximum of 50 ASCII characters.*
Connection	Defines the connection to a printer in the form of a device URI (uniform resource identifier).
	- IPP/IPPS: In IPP (Internet Printing Protocol) the print data is transmitted via HTTP to the printer. The connection between primos and the printer can be encrypted via SSL/TLS (IPPS). Standard port IPP: 631. Standard port IPPS: 443. `ipp://<IP address or host name of the printer>:<port number>/ipp` `ipp://<IP address or host name of the printer>/ipp/` `ipps://<IP address or host name of the printer>:<port number>/ipp` `ipps://<IP address or host name of the printer>/ipp/`
	- LPR/LPD protocol: In Line Printer Daemon printing the print data is sent to the IP address of the printer by means of an LPD queue. `lpd://<IP address or host name of the printer>/<queue>`
	- Socket printing (Jetdirect printing): The data is transferred to the TCP/IP port via a raw/socket connection. Standard port: 9100. `socket://<IP address or host name of the printer>:<port number>`
Make	Defines the printer manufacturer. Via make and model the printer driver is defined.

Parameters	Description
Model	Defines the printer model. Via model and make the printer driver is defined.
Upload driver (PPD)	Loads a printer driver onto primos and assigns it to the queue. *If the pre-installed printer drivers do not suffice, you can load a suitable driver onto primos. The driver must be in 'PPD' format. For further information; see: 'How to Manage Drivers in primos'* ⇨🖹31.
Paper size	Defines the paper size for printouts.
Action	See 'How to Maintain or Test a Printer via primos' ⇨🖹33.
Secure AirPrint™	See 'How to Encrypt Print Data Transmission' ⇨🖹34.
User authentication	See 'How to Control Who Can Print' ⇨🖹35.
Access	See 'How to Control Who Can Print' ⇨🖹35.
Advanced print settings	*See 'How to Configure Advanced Print Settings'* ⇨🖹33.

Delete Queue

Note

Deleted queues might appear on the iOS devices for some time after a queue has been deleted. The iOS device will update its information over time so that the deleted queues will no longer appear.

---

1. Start the primos Control Center.
2. Select **PRINTING – Queues**.
3. Click the symbol ✖ for the file to be deleted.
4. Confirm the security query.
↳ The queue will be deleted.

5.3   How to View the Job History

The 'Job History' displays information on the print jobs that have been processed by primos.

A maximum of 100 print jobs are displayed. From the 101rd print job onwards the FIFO method (first-in, first-out) is applied. The recorded print jobs will be deleted when primos is reset.

───────────── **Note** ─────────────

A time server (⇨🖹19) must be configured in primos so that the date and time can be displayed correctly. If no time server is configured, the time stamp corresponds to the default time.

───────────────────────────────────────

Filter   The print jobs displayed can be filtered:

  – all jobs
  – completed jobs
  – active jobs

What Do You Want to Do?
  ☐ 'Having a Look at the Job History' ⇨🖹29
  ☐ 'Filtering the Job History' ⇨🖹29

Having a Look at the Job History

1. Start the primos Control Center.
2. Select **PRINTING – Job history**.
↳ The job history is displayed.

Filtering the Job History

1. Start the primos Control Center.
2. Select **PRINTING – Job history**.
   The job history is displayed.
3. Click the filter button.
↳ The job history entries are displayed according to the filter.

5.4 How to Define the Printer Name That Is Displayed on the iOS Devices

In the print dialog on the iOS device, the printer name is displayed according to the following make up: '<AirPrint™ identifier> <queue name>'. Both elements can be named according to your wishes.

Queue Name The queue name is defined individually when the queue is created (⇨ 🖹22) and cannot be changed afterwards.

AirPrint™
Identifier The AirPrint™ identifier is a prefix that marks printers made available via primos on iOS devices. The AirPrint™ identifier is applied to all queues. It can be changed at any time. The default is 'air '.

> Chose an identifier that begins with a letter that from the beginning of the alphabet. This way you can ensure that the printers made available via primos appear at the beginning of the printing dialog on the iOS devices.

Example: You are using the default AirPrint™ identifier 'air ' and the name of the department in which the printer is located:
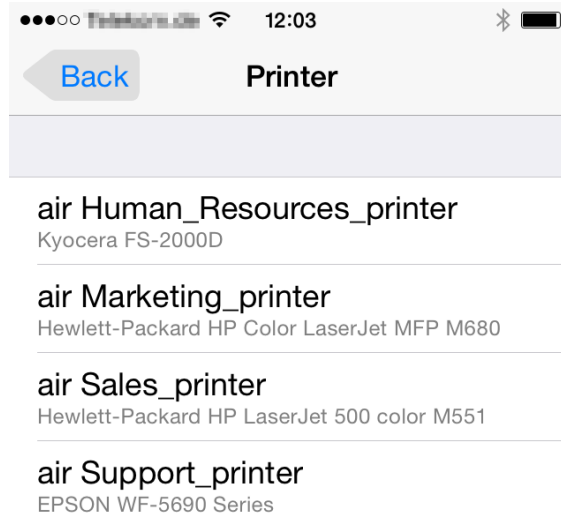

Figure 3: Printer name in the printing dialog on the iOS device

1. Start the primos Control Center.
2. Select **PRINTING – Settings**.
3. Into the **AirPrint™ identifier** box, enter a freely definable ID.
4. Click **Save** to confirm.
↳ The setting will be saved.

5.5   How to Manage Drivers in primos

In primos, a suitable printer driver must be installed and assigned to the queue. A big number of printer drivers for the most common printer models is alread installed in primos. In case that the driver required for your printer is not available, you can load and manage drivers on primos.

PPD

primos uses printer drivers in PPD (PostScript Printer Description) format. PPDs are text files that describe printer properties. Please ask your printer manufacturer for a PPD suitable for your printer.

Driver Management

primos comes with a driver management. You can up- or download one or more drivers. When downloading the drivers are combined into a compressed file. This file can then be loaded into another primos. If the driver is no longer required, it can be deleted.

————— **Note** —————

Only user-defined drivers can be managed. The drivers that come with primos cannot be managed in the driver management.

Assign Drivers

After you have loaded a driver onto primos, you can assign it to a queue. This can be done when creating a queue or later on when editing a queue.

- 'How to Configure Printers on primos (Creating Queues)' ⇨🖹22
- 'Edit Queue' ⇨🖹27

————— **Note** —————

Drivers loaded onto primos appear in the driver selection box under the filter 'Uploaded'.

What Do You Want to Do?

- ☐ 'Load Driver into primos' ⇨🖹31
- ☐ 'Loading a Driver Package into primos' ⇨🖹32
- ☐ 'Download Driver' ⇨🖹32
- ☐ 'Delete Driver' ⇨🖹32

Load Driver into primos
- ✓ The driver must be in 'PPD' format.
- ✓ The PPD must not contain code (compiled or binary parts).

1. Start the primos Control Center.
2. Select **PRINTING – Drivers**.
3. Click **Browse**.

4. Specify the driver.
5. Click **Upload**.
↳ The driver is saved in primos.

Loading a Driver Package into primos
✓ The driver package has been previously downloaded from a primos ⇨🖹32.

1. Start the primos Control Center.
2. Select **PRINTING – Drivers**.
3. Click **Browse**.
4. Specify the driver package.
5. Click **Upload**.
↳ All drivers contained in the package are saved in primos.

Download Driver
✓ One or more user-defined drivers have been saved in primos.

1. Start the primos Control Center.
2. Select **PRINTING – Drivers**.
3. In the **Download / delete drivers** area, select the desired driver(s) from the list.
4. Click **Download selected drivers**.
↳ The drivers are saved to your client in a compressed file.

Delete Driver

—————— **Note** ——————
Drivers that are assigned to a queue cannot be deleted.
——————————————————————————————

✓ One or more user-defined drivers have been saved in primos ⇨🖹31 /⇨🖹32.

1. Start the primos Control Center.
2. Select **PRINTING – Drivers**.
3. In the **Download / delete drivers** area, select the desired driver(s) from the list.
4. Click **Delete selected drivers**.
↳ The driver(s) are deleted.

5.6   How to Configure Advanced Print Settings

You can define advanced print settings. These settings are to be defined for each queue individually and depend on printer and driver.

The default print settings are preset. You can change individual settings and, if necessary, reset them by querying the printer for the default settings.

1. Start the primos Control Center.
2. Select **PRINTING – Queues**.
3. Select the desired queue by clicking the icon ✏.
4. In the **Advanced print settings** area, configure the settings.
   (Which settings can be configured depends on printer model and driver).
↳ The settings are saved.

5.7   How to Maintain or Test a Printer via primos

You can trigger certain actions for a queue, i.e. printer:

– Print test page
– Stop or restart printer
  (If the printer is stopped, print jobs are accepted but not printed. As soon as the printer is started, all print jobs that have accumulated meanwhile will be printed.)
– Reject or accept again all print jobs
– Delete all print jobs

Benefits and Purpose

The actions help with testing and maintenance of the printer. Examples:

– Print a test page in order to check the printer connection or test a new driver.
– Stop the printer if maintenance is briefly performed on the printer (e.g. if toner is exchanged or paper added). As soon as you restart the printer, all print jobs that have accumulated meanwhile will be printed.)
– If a long downtime of the printer is foreseeable, e.g. for repairs, all print jobs should be rejected. This way print jobs will not accumulate in the queue if they cannot be printed.
– If a printer error causes a long downtime and many print jobs have accumulated in the queue which are not to be printed after the error has been fixed, delete all print jobs. This way you will not waste resources and the printer will not be occupied with printing for a long time.

Requirements

✓ A queue has been created on primos ⇨ 🗎22.

1. Start the primos Control Center.

2. Select **PRINTING – Queues**.
3. Select the desired queue by clicking the icon ✏.
4. In the **Device** area, select the desired printer action from the **Action** list.
5. Click **Save** to confirm.
↳ The printer action is triggered.

5.8   How to Encrypt Print Data Transmission

The print data is sent from the iOS device via primos to the printer. The print data stream can be divided into two ways:

- Print data is sent from the iOS device to primos
  (By default print data is transmitted unencrypted. Die transmission can be encrypted by using Secure AirPrint™. See below.
- The print data is sent from primos to the printer
  (The connection type that has been specified for the queue defines the protocol which is used to send the print data from primos to the printer. Depending on the protocol chosen the print data is send with or without encryption. See ⇨ 🖹22.)

Secure AirPrint™   You can encrypt the print data transmission from the iOS device to primos by using an SSL/TLS encryption method. The cipher strength is defined via the encryption level ⇨ 🖹43. The encryption is to be defined for each queue separately.

Requirements   ✓ A queue has been created on primos ⇨ 🖹22.
✓ A certificate has been installed on primos ⇨ 🖹49.

1. Start the primos Control Center.
2. Select **PRINTING – Queues**.
3. Select the desired queue by clicking the icon ✏.
4. Tick/clear **Secure AirPrint™**.
5. Click **Save** to confirm.
↳ The setting will be saved.

——————— **Note** ———————
To completely encrypt the print data transmission, we recommend to encrypt the transmission from primos to printer using an IPPS connection ⇨ 🖹22.

5.9 How to Control Who Can Print

You can restrict the access to queues and therefore printing on the corresponding printer. In order to do this, you define print authorizations for individual queues.

Mode of operation

The authentication of users is done via a directory service. In a first step you can limit the access to users defined in a directory service only. Only users defined in the directory service are allowed to print. If a stricter limitation is desired, you can limit users further with the help of a list in a second step. There are two types of list:

- Allow list: Only users on the list can print.
- Deny list: Users on the list cannot print. All other users can print.

You can add users or user groups to the list.

> For a large number of users we recommend to create groups in the directory service. Groups are more easy to enter on primos than single users.

Print

Queues with limited access are marked with the icon 🔒 on the iOS device.

Before printing, a user name and corresponding password as defined in the directory service must be entered on the iOS device.

Note

iOS devices store this information automatically; the authentication must only be done when printing via this queue for the first time.

Requirements

- ✓ primos is embedded into a directory service ⇨ 🖹17.
- ✓ Users and/or groups are defined in a directory service.
- ✓ A queue has been created on primos ⇨ 🖹22

1. Start the primos Control Center.
2. Select **PRINTING – Queues**.
3. Select the desired queue by clicking the icon ✏.
4. Tick **User authentication**.
5. Decide on the restriction:
   - Access for all users: All users defined in the directory can print after entering their user name and password.
   - Restricted access: Print permissions are defined via a list.
6. In case you have chosen restricted access, choose the **Type of list**.
   - Allow list: Only users on the list can print.
   - Deny list: Users on the list cannot print. All other users can print.

   Into the **Add users/groups to list** box, then enter the desired users and groups and

confirm with **Add**. Please note the conventions for entering users and groups:
- The convention for entering users and groups depends on the directory service into which primos is embedded.
Active Directory: DOMAIN\User name and DOMAIN\Group
LDAP: User respectively group
- Several users are to be separated by comma.
7. Click **Save** to confirm.
↳ The settings are saved.

5.10 How to Print from iOS Devices

Simply and flexibly print content such as documents and pictures from iOS devices (iPhone, iPad, and so on). To do so, print jobs are sent from iOS apps with AirPrint™ support to primos via your network. primos forwards the print job to the printer for printing.

―――――――――― **Note** ――――――――――
If the print permissions have been restricted (⇨ 🖹 35), a user name and password are queried on the iOS device before printing. iOS devices store this information automatically; the authentication must only be done when printing via this queue for the first time.

Requirements
- ✓ In primos a queue has been created for the printer ⇨ 🖹 22.
- ✓ Your iOS device is connected to the network via WLAN.
- ✓ Your iOS device supports AirPrint™.
- ✓ The app selected supports AirPrint™.

1. On your iOS device, open the app you want to print from.
2. Choose the content you want to print.
3. Open the print menu.
4. Tap **Printer**.
All available printers are displayed. Printers made available by primos are per default tagged with AirPrint™-Identifier ⇨ 🖹 30
5. From the list, select the desired printer.
6. Define the print options, e.g. the number of copies.
7. Tap **Print**.
↳ You content is printed.

While printing, you can check the printing status in the Print Center on your iOS device. To open the Print Center, double-click the Home button and tap **Print Center**.

5.11 How to Print Across Subnets (Wide-Area AirPrint™)

AirPrint™ uses the Bonjour protocol (⇨🖹16) to find printers and make them available in the network.

However, Bonjour is limited to local network segments. You have to set up primos in such a way that searching for and finding printers is possible across network segments. Then you can print from the entire network. Follow the instructions below in the indicated order.

Procedure
- Enable Wide-Area AirPrint™ on primos: 'Configuring Wide-Area AirPrint™ on primos' ⇨🖹38.
- Define a subdomain for primos, e.g. primos.mydomain.com. Configure this subdomain on primos: 'Configuring Wide-Area AirPrint™ on primos' ⇨🖹38.

Warning

The primos subdomain must not end with '.local'. This domain is reserved for multicast Bonjour (mDNS).

- On primos, define the printer which are to be used with Wide-Area AirPrint™: 'Configuring Wide-Area AirPrint™ on primos' ⇨🖹38.
- Optionally, you can deactivate the standard mechanism (multicast) for publishing printers in the network. Printers will then only be made available via Wide-Area AirPrint™. (See 'Configuring Wide-Area AirPrint™ on primos' ⇨🖹38.)
- On your DNS server, configure a conditional forwarder. Request which contain the primos subdomain must be forwarded to primos: ⇨🖹38.
- Tell the iOS devices which are to use Wide-Area AirPrint™ how to search for and find printers in the primos subdomain. To do this, the primos subdomain must be defined as search domain on the iOS devices. You can either set this up manually or automatically on all iOS devices in the domain.
  - 'Configuring the primos Subdomain as Search Domain on iOS Devices Automatically' ⇨🖹39
  - 'Configuring the primos Subdomain as Search Domain on iOS Devices Manually' ⇨🖹40

Configuring Wide-Area AirPrint™ on primos

Requirements
- ✓ A DNS server is operated in your network.
- ✓ A DNS server is configured in primos ⇨ 🖹16.

1. Start the primos Control Center.
2. Select **PRINTING – Settings**.
3. Configure the Wide-Area AirPrint™ parameters; table 9 ⇨ 🖹38.
4. Click **Save** to confirm.
↳ The settings are saved.

Table 9: Wide-Area AirPrint™ parameters

Parameters	Description
Wide-Area AirPrint™	Enables/disables Wide-Area AirPrint™.
primos subdomain	Wide-area AirPrint™ domain name for which a conditional forwarder to primos is configured on the DNS server.
Printers to be published via wide-Area AirPrint™	Defines the printers that can be used via wide-Area AirPrint™.
Multicast publishing	Enables/disables the standard mechanism for publishing queues in the network (via multicast). *If you deactivate this option, printers will only be made available via Wide-Area AirPrint™.*

Configuring a Conditional Forwarder on the DNS Server
As an example the configuration procedure on Windows Server 2012 is described.

Requirements
- ✓ In primos Wide-Area AirPrint™ has been configured ⇨ 🖹38.
- ✓ A DNS server is operated in your network.
- ✓ You are logged on to Windows Server 2012 as administrator.

1. Start the **DNS Manager**.
2. Rightclick on **Conditional Forwarders** and from the context menu choose **New Conditional Forwarder**.
   The dialog **New Conditional Forwarder** appears.
3. In the **DNS Domain** box, enter the primos subdomain.
4. In the area **IP addresses of the master servers** enter in the field IP Address the **IPv4 address** of primos.
   Windows server 2012 validates your input. If the validation is successful, a green check mark appears and you can click 'OK'.
5. Click **OK** to confirm.
↳ The conditional forwarder is saved.

Configuring the primos Subdomain as Search Domain on iOS Devices Automatically

The primos subdomain can be defined as search domain automatically on all iOS devices using your DHCP server. In order to do so, the primos subdomain is entered on the DHCP server as option 119. As soon as an iOS sends a request to the DHCP server, it will automatically receive the primos subdomain as search domain in the answer. The iOS device will save this information automatically.

Preparation   As an example the configuration procedure on Windows Server 2012 is described. On the DHCP server on Windows 2012, subdomain must be entered in coded form (according to RFC 3397). As this coding is difficult, the primos Control Center provides a coding tool. If you enter your IPv4 DHCP range and primos subdomain, it will give you the command line command which contains your primos subdomain and IPv4 DHCP range in coded form.

1. Start the primos Control Center.
2. Select **MAINTENANCE – Service**.
3. In the **DHCP option 119** area, enter your IPv4 DHCP range in the **DHCP range** box.
4. In the **DHCP option 119** area, enter your primos subdomain in the **primos subdomain** box.
↳ The Command box will show the command line commands. Save the command line commands (e.g. as text file or in the clipboard).

Configuration   The Windows Server graphical user interfaces do not offer a user-friendly configuration interface for the DHCP option 119. Therefore the configuration on Windows Server 2012 is described below using the command line.

Example   To illustrate the configuration, the following example is used.

Your primos subdomain is: primos.mydomain.com

Your IPv4 DHCP range is: 10.168.0.0

Command line commands:

```
REM entered DHCP range is 10.168.0.0
REM entered primos subdomain is primos.mydomain.com
netsh dhcp server V4 delete optiondef 119
netsh dhcp server V4 add optiondef 119 "DNS Search Path" BYTE 1
netsh dhcp server V4 scope 10.168.0.0 set optionvalue 119 BYTE 06 70 72 69
6d 6f 73 08 6d 79 64 6f 6d 61 69 6e 03 63 6f 6d 00
```

Note

The first two lines are for information only. Therefore they are labeled as comment with 'REM' and thus excluded from execution.

Requirements	✓ In primos Wide-Area AirPrint™ has been configured ⇨▤38.
	✓ A DNS server is operated in your network.
	✓ On your DNS server a conditional forwarder to the primos subdomain has been set up ⇨▤38.
	✓ A DHCP server is operated in your network.
	✓ You are logged on to Windows Server 2012 as administrator.
	✓ You have the command line commands; see: 'Preparation' ⇨▤39.

1. Start the command prompt.
   The box **Administrator: Command Prompt** appears.
2. Execute the command line commands created in preparation one after another.
   Example:
   ```
   netsh dhcp server V4 delete optiondef 119
   ```
   (Deletes a preconfigured option 119, if applicable.)
   ```
   netsh dhcp server V4 add optiondef 119 "DNS Search Path" BYTE 1
   ```
   (Activates option 119.)
   ```
   netsh dhcp server V4 scope 10.168.0.0 set optionvalue 119 BYTE 06 70 72
   69 6d 6f 73 08 6d 79 64 6f 6d 61 69 6e 03 63 6f 6d 00
   ```
   (Configures option 119.)

   After each execution, the successful execution of the command is confirmed.

↳ The primos subdomain is created on the DHCP server as option 119. The DHCP server will automatically set up the primos subdomain as search domain on all iOS devices.

💡 Check if the entry appears on the DHCP server. In order to do so, start the DHCP server and check if the entry appears under **<your domain>** - **IPv4** - **<range>** - **Scope Options**. If necessary, refresh the display.

Configuring the primos Subdomain as Search Domain on iOS Devices Manually
You can enter the primos subdomain as search domain directly on your iOS device.

Requirements	✓ In primos Wide-Area AirPrint™ has been configured ⇨▤38.
	✓ A DNS server is operated in your network.
	✓ On your DNS server a conditional forwarder to the primos subdomain has been set up ⇨▤38.

1. On your iOS devices open the menu **Settings**.
2. Select **Wi-Fi**.
   The Wi-Fi menu is displayed.
3. Select your Wi-Fi from the list.
   The Wi-Fi settings are displayed.

4. Select the option **Search Domains**.
   The keyboard appears.
5. Add the primos subdomain.
   (Several search domains are to be separated comma.)
6. Let the key board fade out.
↳ The primos subdomain has been configured as search domain on the iOS device. The iOS device will search for and find printers in the primos subdomain.

6   Security

A number of security mechanisms are available to ensure optimum security for primos. This chapter describes how to make use of these security mechanisms.

6.1   How to Define the Encryption Level for SSL/TLS Connections

The following connections in primos can be encrypted via SSL/TLS:

- Web access to the primos Control Center: HTTPS (⇨📄44)
- print data transmission: IPPS and Secure AirPrint™ (⇨📄34)

Encryption Level   The encryption strength and thus the safety of the connection is defined via the encryption level.

Cipher Suite   Each encryption level is a collection of so-called cipher suites. A cipher suite is a standardized sequence of four cryptographic algorithms that are used to establish a secure connection. Depending on their cipher strength (in bit), cipher suites are grouped to form an encryption level. Which cipher suites are supported by primos, i.e. are part of an encryption level, depends on the SSL/TLS protocol used.

Establishing Connections   When establishing a secure connection, a list of supported cipher suites is sent to the communicating party. A cipher suite is agreed upon that will be used later on. The strongest cipher suite that is supported by both parties will be used by default. If there is no cipher suite that is supported by both parties, no SSL/TLS connection will be established.

Warning

The communicating parties of primos (e.g. browser) must support the cipher suites of the selected encryption level in order to successfully establish a connection. When problems occur, select a different level or reset the primos configuration settings (⇨📄61).

The following encryption levels can be selected:

- Compatible: Cipher suites with an encryption of 40 to 256 bit are used.
- Low: Only cipher suites with a low encryption of 56 bit are used. (Fast connection)
- Medium: Only cipher suites with an encryption of 128 bit are used.
- High: Only cipher suites with a strong encryption of 128 to 256 bit are used. (Slow connection)

Warning

Do <u>not</u> use the encryption level 'Low' if only HTTPS is defined as the permitted connection type for the web access to the primos Control Center.

---

1. Start the primos Control Center.
2. Select **SECURITY – SSL connections**.

3. From the **Encryption** area select the desired encryption level.
4. Click **Save** to confirm.
↳ The setting will be saved.

Note

Detailed information about the individual SSL/TLS connection status (e.g. supported cipher suites) can be found on the Details page at **SSL connection status – Details**.

6.2   How to Control the Access to the primos Control Center

The web access to the primos Control Center can be secured by selecting the permitted types of connection (HTTP/HTTPS).

If HTTPS is exclusively chosen as the connection type, the administrative web access to the primos Control Center is protected by SSL/TLS. The cipher strength is defined via the encryption level ⇨ 🖹43.

Note

When logging into the primos Control Center (⇨ 🖹45), the password is transmitted in plain text. We recommend to only use the HTTPS connection.

SSL/TLS requires a certificate to check the identity of primos. During a so-called 'handshake', the client asks for a certificate via a browser. This certificate must be accepted by the browser. Please refer to the documentation of your browser software. URLs that require an SSL/TLS connection start with 'https'.

1. Start the primos Control Center.
2. Select **SECURITY – Device access**.
3. In the **Connection** area, tick **HTTP/HTTPS** or **HTTPS only**.
4. Click **Save** to confirm.
↳ The setting will be saved.

6.3   How to Manage User Profiles (Access Control)

The access to the primos is controlled by means of user accounts. You will need a user name and a password to get access to the program.

<hr>

Note

When logging in, the password is transmitted in plain text. We recommend to encrypt the connection to the primos Control Center (HTTPS ⇨🗎44).

<hr>

Administrator   By default the administrator user profile is configured.

| User name: | admin |
| Password: | admin |

The password for the administrator user profile can be modified, the user name is unchangeable.

<hr>

Note

Change the default password as soon as possible!

<hr>

Directory service   You can embed primos into an Active Directory so that users defined in the Active Directory can log into primos. The users defined can then authenticate themselves with their Active Directory user name and password to gain access to the primos Control Center.

<hr>

Note

Only system administrators should have access to the primos Control Center because this is where security-related settings can be configured.

<hr>

Session timeout   With the session timeout you can define that the connection to the primos Control Center is terminated for security reasons if there is no user activity during the defined period. The logged in user will be logged out and has to log in again.

Logout   For security reasons, always logout of the primos Control Center after having configured settings ⇨🗎9.

What Do You Want to Do?
- ☐ 'Changing the Administrator Password' ⇨🗎46
- ☐ 'Configuring Active Directory User Login' ⇨🗎46
- ☐ 'Configuring the Session Timeout' ⇨🗎46

Requirements

Changing the Administrator Password

1. Start the primos Control Center.
2. Select **SECURITY – Device access**.
3. Into the **Password** box, enter a password.
4. Repeat the password.
5. Click **Save** to confirm.
↳ The setting will be saved.

Configuring Active Directory User Login

✓ There is an Active Directory in your network.

Note

The settings for the Active Directory user login are independent of the general Active Directory settings (⇨ 17).

1. Start the primos Control Center.
2. Select **SECURITY – Device access**.
3. Tick **Active Directory user login**.
4. Into the **Active Directory server** box, enter the IP address or host name of the Active Directory server.
   (The host name can only be used if a DNS server was configured beforehand.)
5. Into the **Active Directory suffix** box, enter the suffix preceded by '@'.
   Example: @Domain.
6. Into the **Users having access to this device** box, enter the Active Directory users which are to log into the primos Control Center.
7. Enable optionally the encryption of the Active Directory connection.
   (Recommended)
8. Click **Save** to confirm.
↳ The settings are saved.

Configuring the Session Timeout

1. Start the primos Control Center.
2. Select **SECURITY – Device access**.
3. Tick **Session Timeout**.
4. Into the **Session duration** box, enter the time in Minutes after which the timeout is to be effective.
↳ The setting will be saved.

6.4   How to Protect primos from Cross-Site Scripting

What is Cross-Site Scripting?

Cross-site scripting (XSS) is a form of attack which uses a security vulnerability in websites: By default the user input entered on a website is submitted to the browser. An attacker may use this to transmit malicious code (e.g. scripts). The objective is e.g. to steal user data such as user profiles.

To prevent cross-site scripting attacks values can be checked and only trusted values accepted.

1. Start the primos Control Center.
2. Select **SECURITY – Device access**.
3. In the **Cross-Site-Scripting (XSS)** area, enable/disable **Value check**.
↳ The setting will be saved.

6.5   How to Control the Access to primos (TCP Port Access Control)

TCP Port Access Control

You can control the access to primos. To do so, all TCP ports on primos can be blocked. Network elements that are to have permission to access primos, can be defined as exceptions and excluded from locking. primos only accepts data packets from network elements defined as exceptions. Please note: This also applies to iOS devices. If the TCP port access control is enabled, you can only print from iOS devices which have been defined as exceptions.

Exceptions

In order to exclude network elements (e.g. iOS devices, clients, DNS server, SNTP server) from port locking, they must be defined as exceptions. To do so, the IP addresses or MAC addresses (hardware addresses) of the network elements with access rights must be entered in the 'Exceptions' area. Please note:

• MAC addresses are not delivered through routers!
• Address ranges can be defined using CIDR notation.

printers for which a queue has been created in primos are automatically excluded from port locking.

Test Mode

The 'test mode' allows you to check the configured access protection. If the test mode is activated, access protection remains active until primos is rebooted. After restarting, the protection is no longer effective.

The 'test mode' option is activated by default. After a successful test, you must deactivate the test mode so that access protection remains permanently active.

1. Start the primos Control Center.
2. Select **SECURITY – TCP port access**.
3. Tick **Port access control**.
4. In the **Exceptions** area, define the network elements which are excluded from port locking. Enter the IP or MAC addresses and tick the options.
5. Make sure that the test mode is enabled.
6. Click **Save** to confirm.
   The settings are saved.
   The port access control is activated until the device is restarted.
7. Check the port access and configurability of primos.

———— **Note** ————
If primos can no longer be reached using the primos Control Center, restart the device (⇨🖹64).

8. Clear **Test mode**.
9. Click **Save** to confirm.
↳ The settings are saved. The port access control is active. Access to the ports is restricted.

6.6 How to Use Certificates Correctly

primos has its own certificate management. This section explains how certificates are used and when the use of certificates is recommended.

What are Certificates?

Certificates can be used in TCP/IP-based networks to encrypt data and to authenticate communication partners. Certificates are electronic messages containing a key (public key) and a signature.

Benefits and Purpose

The use of certificates allows for various security mechanisms. Use certificates in primos

- to check the identity of primos in the network (⇨ 🖹55).
- to authenticate the client if the connection to the primos Control Center is protected via HTTPS (SSL/TLS) (⇨ 🖹44).
- to encrypt print data (IPPS and Secure AirPrint™ ⇨ 🖹34).

Which Certificates are available?

Both self-signed certificates and CA certificates can be used with primos. The following certificates can be distinguished:

- Upon delivery, a certificate (the so-called **default certificate)** is stored in primos. It is recommended that you replace the default certificate by a self-signed certificate or a requested certificate as soon as possible.
- **Self-signed certificates** have a digital signature that has been created by primos.
- A **requested certificate** is created by a certification authority (CA) for primos on the basis of a certificate request.
- **CA certificates** are certificates that have been issued for a certification authority (CA). They are used for verifying certificates that have been issued by the respective certification authority.

The following certificates can be installed at the same time in primos:

– 1 Self-signed certificate
– 1 client certificate, i.e. 1 requested certificate OR 1 PKCS#12 certificate
– 1to 32 CA certificates

All certificates can be deleted separately.

What Do You Want to Do?

☐ 'Displaying Certificates' ⇨ 🖹50

☐ 'Creating a Self-Signed Certificate' ⇨ 🖹50

☐ 'Creating a Certificate Request for a Requested Certificate' ⇨ 🖹51

☐ 'Installing a Requested Certificate in primos' ⇨ 🖹52

☐ 'Installing a PKCS#12 Certificate in primos' ⇨ 🖹52

☐ 'Installing a CA Certificate in primos' ⇨📄53
☐ 'Deleting Certificates' ⇨📄53

Displaying Certificates
Certificates installed in primos and certificate requests can be displayed and viewed.

Requirements   ✓ A certificate is installed in primos .

1. Start the primos Control Center.
2. Select **SECURITY – Certificates**.
3. Select the certificate via the icon Q.
↳ The certificate is displayed.

Creating a Self-Signed Certificate

—————— **Note** ——————
If a self-signed certificate has already been created in primos, you must first delete the
certificate (⇨📄53).
————————————————

1. Start the primos Control Center.
2. Select **SECURITY – Certificates**.
3. Click **Self-signed certificate** an.
4. Enter the relevant parameters; table 10 ⇨📄50.
5. Click **Create/Install**.
↳ The certificate will be created and installed. This may take a few minutes.

Table 10: Parameters for the Creation of Certificates

Parameters	Description
Common name	Is used to clearly identify the certificate. It is advisable to use the IP address or the host name of primos to allow a clear assignment of the certificate to primos. *You can enter a maximum of 64 characters.*
Email address	Specifies an email address. *You can enter a maximum of 40 characters.* *(Optional entry)*
Organization name	Specifies the company that uses primos. *You can enter a maximum of 64 characters.*
Organizational unit	Specifies the department or subsection of a company. *You can enter a maximum of 64 characters.* *(Optional entry)*

Parameters	Description
Location	Specifies the locality where the company is based. *You can enter a maximum of 64 characters.*
State name	Specifies the state in which the company is based. *You can enter a maximum of 64 characters.* *(Optional entry)*
Domain component	Allows you to enter additional attributes. *(Optional entry)*
Country	Specifies the country in which the company is based. Enter the two-digit country code according to ISO 3166. Examples: DE = Germany, GB = Great Britain, US = USA
Expires on	Specifies the date from which on the certificate becomes invalid.
RSA key length	Defines the length of the RSA key used: - 512 bit (fast encryption and decryption) - 768 bit - 1024 bit (standard encryption and decryption) - 2048 bit (slow encryption and decryption)

Creating a Certificate Request for a Requested Certificate

As preparation for using a certificate which is issued by a certification authority for primos, a certificate request can be created in the primos. The request must be sent to the certification authority which creates an certificate on the basis of this request. The certificate must be in 'base64' format.

———— **Note** ————

If a certificate request has already been created in primos, you must first delete the certificate request (⇨🖹53).

1. Start the primos Control Center.
2. Select **SECURITY – Certificates**.
3. Click **Certificate request**.
4. Enter the required parameters, table 10 ⇨🖹50.
5. Click **Create a request**.
   The creation of the certificate request is in progress. This may take a few minutes.
6. Select **Upload** and save the requests in a text file.
7. Click **OK**.
8. Send the text file as certificate request to a certification authority.

When the certificate has been received, it must be saved in the device ⇨🖹52.

Installing a Requested Certificate in primos

Requirements
- ✓ A certificate request has been created at an earlier date ⇨🗎51.
- ✓ The certificate must be in 'base64' format.

———— **Note** ————
If a PKCS#12 certificate has already been installed in primos, you must first delete the certificate (⇨🗎53).

1. Start the primos Control Center.
2. Select **SECURITY – Certificates**.
3. Click **Requested certificate**.
4. Click **Browse**.
5. Specify the requested certificate.
6. Click **Install**.
↪ The requested certificate is installed in primos.

Installing a PKCS#12 Certificate in primos
PKCS#12 certificates are used to save private keys and their respective certificates and to protect them by means of a password.

———— **Note** ————
If a PKCS#12 or a requested certificate has already been installed in primos, you must first delete the certificate (⇨🗎53).

Requirements
- ✓ The certificate must be in 'base64' format.

1. Start the primos Control Center.
2. Select **SECURITY – Certificates**.
3. Click **PKCS#12 certificate**.
4. Click **Browse**.
5. Enter the PKCS#12 certificate.
6. Enter the password.
7. Click **Install**.
↪ The PKCS#12 certificate is installed in primos.

Installing a CA Certificate in primos

In order to check the identity of the network communicating parties of primos, it is necessary to validate their certificates. For this, the root CA certificates of the certification authorities that have issued the certificates of said communicating parties are installed in primos.

Up to 32 CA certificates can be installed. Thus multi-level public key infrastructures (PKIs) are supported.

Example: primos offers a number of authentication methods to verify its identity in a network. If you use the authentication method 'EAP-TLS' (⇨ 📄55), you must install the root CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS) in primos.

Requirements   ✓ The certificate must be in 'base64' format.

1. Start the primos Control Center.
2. Select **SECURITY – Certificates**.
3. Click **CA certificate**.
4. Click **Browse**.
5. Specify the CA certificate.
6. Click **Install**.
↳ The CA certificate is installed in primos.

Deleting Certificates

———— **Warning** ————

Do not delete the certificate (CA/self-signed/PKCS#12) if only HTTPS is defined as the permitted connection type for the web access to the primos Control Center. If the corresponding certificate is deleted, the primos Control Center can no longer be reached. In this case you have to reset the configuration settings of primos (⇨ 📄61).

Requirements   ✓ A certificate is installed in primos .

1. Start the primos Control Center.
2. Select **SECURITY – Certificates**.
3. Select the certificate to be deleted via the icon 🔍. The certificate is displayed.
4. Click **Delete**.
↳ The certificate is deleted.

6.7   How to Use Authentication Methods

By means of authentication, a network can be protected against unauthorized access. primos can participate in various authentication procedures. This section describes which procedures are supported and how these procedures are configured in primos.

What is IEEE 802.1X?

The IEEE 802.1X standard provides a basic structure for various authentication and key management protocols. IEEE 802.1X allows you to control the access to networks. Before users gain access to a network via a network device, they must authenticate themselves in the network. After the authentication was successful, the access to the network will be freed.

What is EAP?

The standard IEEE 802.1X is based upon the EAP (Extensible Authentication Protocol). EAP is a universal protocol for many authentication procedures. EAP allows for a standardized authentication procedure between the network device and an authentication server (RADIUS). First you must define the authentication procedure (TLS, PEAP, TTLS, etc.) to be used and configure it on all network devices involved.

What is RADIUS?

RADIUS (Remote Authentication Dial-In User Service) is an authentication and account management system that validates user login information and grants access to the desired resources.

primos supports various EAP authentication methods in order to authenticate itself in a protected network.

What Do You Want to Do?

Configuring EAP-MD5

Benefits and Purpose

EAP-MD5 validates the identity of devices or users before they gain access to network resources. You can configure primos for the EAP-MD5 network authentication. This makes sure that primos gets access to protected networks.

Mode of Operation

EAP-MD5 describes a user-based authentication method via a RADIUS server. primos must be defined as user (with user name and password) on a RADIUS server. The authentication method EAP-MD5 must then be enabled in primos and the user name and password need to be entered.

Requirements   ✓ primos is defined as user (with user name and password) on a RADIUS server.

1. Start the primos Control Center.
2. Select **SECURITY – Authentication**.
3. Select **MD5** from the **Authentication method** list.
4. Enter the **User name** and **Password** that are used for the configuration of primos on the RADIUS server.
5. Click **Save** to confirm.
↳ The settings are saved.

Configuring EAP-TLS

Benefits and Purpose   EAP-TLS (Transport Layer Security) validates the identity of devices or users before they gain access to network resources. You can configure primos for the EAP-TLS network authentication. This makes sure that primos gets access to protected networks.

Mode of Operation   EAP-TLS describes a certificate-based authentication method via a RADIUS server. For this purpose, certificates are exchanged between primos and the RADIUS server. An encrypted TLS connection between primos and the RADIUS server is established in this process. Both RADIUS server and primos need a valid, digital certificate signed by a CA. The RADIUS server and primos must validate the certificate. After the mutual authentication was successful, the access to the network will be freed.

Since each device needs a certificate, a PKI (Public Key Infrastructure) must be available. User passwords are not necessary.

If you want to use the EAP-TLS authentication, you must observe the instructions below in the indicated order. If this procedure is not adhered to, primos may not be addressable in the network. In this case you have to reset the configuration settings of primos (⇨🖹61).

Procedure   • Create a certificate request in primos ⇨🖹51.

• Create a certificate using the certificate request and the authentication server.

• Install the requested certificate in primos ⇨🖹52.

• Install the root CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS) in primos ⇨🖹53.

• Enable the authentication method 'EAP-TLS' in primos.

1. Start the primos Control Center.
2. Select **SECURITY – Authentication**.
3. Select **TLS** from the **Authentication method** list.
4. From the list **EAP root certificate**, select the root CA certificate.
5. Enter the password that is used for the configuration of primos on the RADIUS server.

6. Click **Save** to confirm.
↳ The settings are saved.

Configuring EAP-TTLS

Benefits and Purpose

EAP-TTLS (Tunneled Transport Layer Security) validates the identity of devices or users before they gain access to network resources. You can configure primos for the EAP-TTLS network authentication. This makes sure that primos gets access to protected networks.

Mode of Operation

EAP-TTLS consists of two phases:

In phase 1, a TLS-encrypted channel between primos and the RADIUS server will be established. Only the RADIUS server authenticates itself to primos using a certificate that was signed by a CA. This process is also referred to as 'outer authentication'.

In phase 2, an additional authentication method is used for the communication within the TLS channel. EAP-defined methods and older methods (CHAP, PAP, MS-CHAP and MS-CHAPv2) are supported. This process is also referred to as 'inner authentication'.

The advantage of this procedure is that only the RADIUS server needs a certificate. Therefore no PKI is needed. Moreover, TTLS supports most authentication protocols.

Requirements

✓ primos is defined as user (with user name and password) on a RADIUS server.

1. Start the primos Control Center.
2. Select **SECURITY – Authentication**.
3. Select **TTLS** from the **Authentication method** list.
4. From the list **EAP root certificate** choose the root CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS). (Optional) The certificate increases the security when establishing the connection. **(The root CA certificate must have been installed in primos previously** ⇨ 🖹53**.)**
5. In the **Anonymous name** box enter the name for the unencrypted part of the EAP-TTLS authentication.
6. From the list **Inner authentication** choose the method intended to secure the communication in the TLS channel.
7. Enter the **User name** and **Password** that are used for the configuration of primos on the RADIUS server.
8. Install a WPA add-on. (Optional)
9. Click **Save** to confirm.
↳ The settings are saved.

Configuring PEAP

Benefits and Purpose

The PEAP (Protected Extensible Authentication Protocol) validates the identity of devices or users before they gain access to network resources. You can configure primos for the PEAP network authentication. This makes sure that primos gets access to protected networks.

Mode of Operation

In the case of PEAP, an encrypted TLS (Transport Layer Security) channel is established between the print server and the RADIUS server (as is the case for EAP-TTLS, see ⇨ 🖹 56). Only the RADIUS server authenticates itself to primos using a certificate that was signed by a CA.

The TLS channel is then used to establish another connection that can be protected by means of additional EAP authentication methods (e.g. MSCHAPv2).

The advantage of this procedure is that only the RADIUS server needs a certificate. Therefore no PKI is needed. PEAP uses the advantages of TLS and supports various authentication methods, including user passwords and one-time passwords.

Requirements

✓ primos is defined as user (with user name and password) on a RADIUS server.

1. Start the primos Control Center.
2. Select **SECURITY – Authentication**.
3. Select **PEAP** from the **Authentication method** list.
4. From the list **EAP root certificate** choose the root CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS). (Optional) The certificate increases the security when establishing the connection. **(The root CA certificate must have been installed in primos previously ⇨ 🖹 53.)**
5. In the **Anonymous name** box enter the name for the unencrypted part of the PEAP authentication.
6. From the list **Inner authentication** choose the method intended to secure the communication in the TLS channel.
7. From the list **PEAP version** choose the PEAP protocol version to be used.
8. From the list **PEAP label** choose the PEAP label version to be used.
9. Enter the **User name** and **Password** that are used for the configuration of primos on the RADIUS server.
10. Install a WPA add-on. (Optional)
11. Click **Save** to confirm.
↳ The settings are saved.

Configuring EAP-FAST

Benefits and Purpose

EAP-FAST (Flexible Authentication via Secure Tunneling) validates the identity of devices or users before they gain access to network resources. You can configure primos for the EAP-FAST network authentication. This makes sure that primos gets access to protected networks.

Mode of Operation

EAP-FAST uses (as in the case of EAP-TTLS ⇨ 🖹56) a channel in order to protect the data transfer. The main difference is that EAP-FAST does not require certificates for authentication purposes. (The use of certificates is optional.)

PACs (Protected Access Credentials) are used to build the channel. PACs are credentials that comprise up to three components.

- A shared secret key that contains the preshared key between primos and the RADIUS server.
- An opaque part that is provided to primos and presented to the RADIUS server when primos wishes to obtain access to network resources.
- Other information that may be useful to the client. (Optional)

EAP-FAST uses two methods to generate PACs:

- The manual delivery mechanism can be every mechanism that the administrator configures and considers to be safe for the network.
- In the case of the automatic delivery, an encrypted channel is established in order to protect the authentication of primos as well as the delivery of the PACs.

Requirements ✓ primos is defined as user (with user name and password) on a RADIUS server.

1. Start the primos Control Center.
2. Select **SECURITY – Authentication**.
3. Select **FAST** from the **Authentication method** list.
4. From the list **EAP root certificate** choose the root CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS). (Optional) The certificate increases the security when establishing the connection. **(The root CA certificate must have been installed in primos previously ⇨ 🖹53.)**
5. In the **Anonymous name** box enter the name for the unencrypted part of the EAP-FAST authentication.
6. From the list **Inner authentication** choose the method intended to secure the communication in the TLS channel.
7. From the **FAST provisioning** box choose the provisioning mechanism for PACs.
8. Enter the **User name** and **Password** that are used for the configuration of primos on

the RADIUS server.
9.   Install a WPA add-on. (Optional)
10. Click **Save** to confirm.
↪ The settings are saved.

7   Maintenance

Various maintenance activities can be carried out for primos. This chapter gives a short overview.

7.1   How to Secure the Configuration Settings (Backup)

You can save the configuration settings (including drivers and certificates) as backup copy on your local client. This allows you to get back to a stable configuration status at any time.

Afterwards, the backup file can be loaded onto a primos. The configuration settings in the file will then be taken over by the device.

<u>Saving a Backup</u>

1. Start the primos Control Center.
2. Select **MAINTENANCE – Backup**.
3. Click **Save**.
↳ The backup file is saved to your client.

<u>Loading a Backup onto a primos</u>

1. Start the primos Control Center.
2. Select **MAINTENANCE – Backup**.
3. Click **Browse**.
4. Specify the primos backup file.
5. Click **Install**.
↳ The configuration settings in the backup file will then be taken over by primos.

7.2   How to Reset primos to Its Default Settings (Reset)

You can reset primos to its default settings (factory settings). All previously configured settings will be deleted in this process.

———   **Note**   ———
If you do a reset, the IP address of primos may change and the connection to the primos Control Center may be terminated.

You must reset the configuration settings, for example, if you have changed the location of primos and thus want to use it in a different network. Before this change of location, you should reset primos to the default settings to install primos in another network.

Note

By means of the reset button of the device you can reset the configuration settings without entering the password.

What Do You Want to Do?

☐ 'Resetting the Configuration Settings via the primos Control Center' ⇨ 🖹62

☐ 'Resetting the Configuration Settings via the Reset Button' ⇨ 🖹62

Resetting the Configuration Settings via the primos Control Center

1. Start the primos Control Center.
2. Select **MAINTENANCE – Default settings**.
3. Click **Default settings**.
↳ The configuration settings are reset.

Resetting the Configuration Settings via the Reset Button

LEDs, various ports and the reset button can be found on primos. These components are described in the 'Quick Installation Guide'.

Using the reset button you can reset the primos the configuration settings to their default setting.

The reset process can be divided into two phases:

- During phase 1, primos is forced into the reset mode. During the reset mode, the configuration settings are reset.
- The second phase describes the restart of the device.

Warning

IMPORTANT: The reset mode is indicated by the status and activity LED blinking alternatingly. Afterwards, both LEDs blink synchronously. At this moment you must release the reset button, otherwise primos switches to the BIOS mode. If this happens, try the reset again.

---

1. Turn primos off (interrupt the power supply).
2. Remove the network cable (RJ-45) from primos.
3. Press and hold the reset button.
4. Turn primos on (establish the power supply).
5. Wait until the status and activity LED blink synchronously.
   The reset mode has been activated.
6. Release the reset button for 2 seconds at most.

The status and activity LED blink alternatingly.
7. Press and hold the reset button again.
   The LEDs blink synchronously.
8. After a few seconds, only the activity LED will blink. Then release the reset button.
9. Turn primos off (interrupt the power supply).
10. Connect the network cable (RJ-45) to primos.
11. Turn primos on (establish the power supply).
↳ The configuration settings are reset.

7.3   How to Perform an Update

You can carry out software and firmware updates on primos in order to benefit from currently developed features.

What Happens during an Update?

In the course of an update, the old firmware/software will be overwritten and replaced by the new firmware/software. The original configuration settings (including drivers and certificates) of the device remain unchanged.

When Is an Update Recommended?

An update should be undertaken if functions do not work properly and if a new software or firmware version with new functions, printer driver updates or bug fixes has been released by SEH Computertechnik GmbH.

Check the installed software and firmware version in primos. You will find the version number in the primos Control Center or in the list of the SEH primos App.

Where Do I Find the Update Files?

Current firmware and software files can be downloaded from the homepage of SEH Computertechnik GmbH:

<div align="center">

http://www.seh-technology.com/services/downloads/
download-mobility-solutions/primos.html

</div>

---------- **Note** ----------

Every update file has its own 'readme' file. Take note of the information contained in the 'readme' file.

---

1. Start the primos Control Center.

2.   Select **MAINTENANCE – Update**.
3.   Click **Browse**.
4.   Select the update file.
5.   Click **Install**.
↳ The update is executed. This may take a few minutes. Afterwards primos will restart.

7.4   How to Restart primos

primos will restart automatically after an update. If primos is in an undefined state it can also be rebooted manually.

1.   Start the primos Control Center.
2.   Select **MAINTENANCE – Restart**.
3.   Click **Restart**.
↳ primos is restarted.

7.5   How to Shut Down primos

You can shut down primos, e.g. over the weekend. Shut down primos before you interrupt the power supply. In doing so undefined states and data loss are avoided.

1.   Start the primos Control Center.
2.   Select **MAINTENANCE – Shutdown**.
3.   Click **Shutdown**.
↳ primos is shut down.

7.6   How to Use the Service Function

primos offer service functions These functions help the SEH support during troubleshooting. Contact details can be found in the chapter 'Support And Service' ⇨🖹5.

Service file   The service file is a compressed file which contains diagnostic information. In case of error, save this file to you local client and send it to the SEH Support together with your request (e.g. via email).

Logging   Per default only some information is stored in the service file. If logging is enabled, much more detailed information will be logged. The SEH support can perform a more detailed error analysis with this information.

SSH Access   The Secure Shell (SSH) network protocol can be used to access primos remotely for support purposes. If the remote access is required, you will be asked by the SEH support to activate this function. The SEH support will guide you through all measures necessary. After all support action has been taken, deactivate the SSH access.

☐ 'Enable Logging' ⇨🖹65

☐ 'Saving a Service File' ⇨🖹65

☐ 'Configuring the SSH Access' ⇨🖹65

Enable Logging

―――――― **Note** ――――――
Only activate this option after consultation with the SEH support team.

1. Start the primos Control Center.
2. Select MAINTENANCE – Service.
3. In the Logging area, click Enable logging.
↳ Logging is enabled.

Saving a Service File

1. Start the primos Control Center.
2. Select **MAINTENANCE – Service**.
3. In the **Service file** area, click **Save**.
↳ The service file is saved to your client.
   Send the service file to the SEH support.

✓ Configuring the SSH Access

―――――― **Note** ――――――
The SSH connection may only be established and used after consultation with the SEH support. Using SSH for purposes other than that (remote maintenance etc.) is forbidden.

1. Start the primos Control Center.
2. Select **MAINTENANCE – Service**.
3. Tick/clear **SSH access**.
4. Click **Save** to confirm.
↳ The setting will be saved.

8   Appendix

> The appendix contains a glossary, trouble shooting information and the index of this document.

8.1   Glossary

This glossary contains information about manufacturer-specific software solutions and terms from the world of network technology.

What Information Do You Need?

Default Name   The primos default name is made up of the two letters 'IC' and the device number. The device number consists of the last six numbers of its hardware address.

Example: IC0001ff

The default name can be found in the primos Control Center.

Gateway   Using a gateway, you can address IP addresses from other networks. If you want to use a gateway, you can configure the relevant parameter via the primos Control Center (⇨🖹13).

Hardware Address

primos is addressable by means of its world-wide unique hardware address. This address is commonly referred to as the MAC or Ethernet address. The manufacturer has defined this address in the hardware of the device. The address consists of 12 hexadecimal numbers. The first six numbers represent the manufacturer, while the last six numbers identify the individual device.

The hardware address can be found on the housing or in the SEH primos App.

The use of separators within the hardware address depends on the platform. Note the following conventions when entering the hardware address:

Operating system	Representation	Example
Windows	Hyphen	00-c0-eb-00-01-ff
UNIX	Colon or dot	00:c0:eb:00:01:ff respectively 00.c0.eb.00.01.ff

Host name

The host name is an alias for an IP address. The host name uniquely identifies primos in the network and makes it easier to remember.

IP Address

The IP address is a unique address for every node in your network, i.e., an IP address may appear only once in your local network. The IP address must be saved in primos to make sure that it can be addressed within the network.

Subnet Mask

With the help of the subnet mask, large networks can be split up into subnetworks. In this case, the user IDs of the IP addresses are assigned to the various subnetworks.

By default, primos is configured for the use without subnetworks. If you want to use a subnetwork, you can configure the relevant parameter via the primos Control Center (⇨ 13).

primos Control Center

primos can be configured and monitored via the primos Control Center. The TPG Control Center is stored in the TPG and can be displayed by means of a browser software (Internet Explorer, Mozilla Firefox, Safari).

SEH primos App

The SEH primos App has been developed by SEH Computertechnik GmbH for finding primos devices within a predefined network. Furthermore, the SEH primos App can be used to execute simple administrative tasks.

8.2   Troubleshooting

This chapter describes some problems and their solutions.

Problem

- 'primos is in the BIOS mode.' ⇨▨68
- 'A connection to the primos Control Center cannot be established' ⇨▨69
- 'The password is no longer available' ⇨▨69
- 'The printer does not print.' ⇨▨70
- 'The print out is flawed' ⇨▨70
- 'I cannot find a suitable printer driver' ⇨▨70
- 'primos cannot be embedded into a directory service.' ⇨▨70
- 'Wide-Area AirPrint™ does not work' ⇨▨71

Solution

primos is in the BIOS mode.

primos switches to the BIOS mode if the firmware functions well but the software is faulty. This may happen in the case of an incorrect software update, for example. primos signalizes the BIOS mode if the activity LED blinks regularly.

——— **Warning** ———
primos is not operational in the BIOS mode.

If a primos is in the BIOS mode, the device will be marked accordingly in the SEH primos App with an indicator.

To switch primos from BIOS to normal mode you have to first assign a temporary IP address to primos and then load software onto it. After the software update primos switches to normal mode and will be assigned a new, permanent IP address.

1. Start the SEH primos App.
2. Mark primos in the list.
3. Select **Actions– Define IP address** from the menu bar.
   The **Set IP Address dialog** appears.
4. Define the **IP address**, **subnet mask** and **gateway**.
5. Click **OK** to confirm.
   primos has a temporary IP address.
6. Download the current software file from the SEH Computertechnik GmbH website:

> http://www.seh-technology.com/services/downloads/
> download-mobility-solutions/primos.html

7. Select **Actions – Load software** software from the menu bar.
    The dialog **Load software** appears.
8. Specify the primos software file.
9. Click **Load**.
    The software update is executed. This may take a few minutes.
10. Confirm the success notification by clicking **OK**.
↳ primos assigns itself a new IP address automatically and is displayed in the SEH pri-
    mos App under this address. primos assigns itself a new IP address automatically and
    is displayed in the SEH primos App under this address. If necessary, refresh the SEH
    primos App list.

A connection to the primos Control Center cannot be established
Eliminate possible error sources. First of all, check:

- the cabling connections,
- the primos IP address (⇨🖹7) and
- the proxy settings of your browser.

If you still cannot establish any connection, the following safety mechanisms might be
the cause:

☐ The access is protected via SSL/TLS (HTTPS) ⇨🖹44.

☐ The TCP port access control is enabled ⇨🖹47.

☐ The cipher suites of the encryption level are not supported by the browser ⇨🖹43.

☐ primos is in the BIOS mode ⇨🖹68.

The password is no longer available
The access to the primos is controlled by means of user accounts. You will need a user
name and a password to get access (⇨🖹44).

If the password is no longer available, you can reset the primos configuration settings to
their default settings in order to get access to the primos Control Center ⇨🖹61. Previous
settings will be deleted.

The printer does not print.

In order to print from iOS devices via primos, you have to create a print queue for the respective printer in primos. For each queue you then define numerous settings (driver, print protocol, access control and much more). Check

☐ all queue settings ⇨🖹27.
    (Pay special attention to the printer driver chosen.)

☐ all print settings ⇨🖹33.

☐ the printer for errors (paper empty, toner empty, paper jam etc.)

☐ if the certificates exist and if they are valid
    (Only if the print data transmission is encrypted ⇨🖹49.)

The print out is flawed

Check

☐ the printer driver chosen ⇨🖹27.

☐ the connection to the printer chosen ⇨🖹27.

☐ the paper size chosen ⇨🖹27.

☐ all print settings ⇨🖹33.

☐ the printer for errors (toner empty, etc.)

I cannot find a suitable printer driver

A big number of printer drivers for the most common printer models is alread installed in primos. In case that the driver required for your printer is not available, you can upload and manage drivers ⇨🖹31.

The following options are available:

☐ You can ask your printer manufacturer for a PPD suitable for your printer.

☐ You can use a similar driver
    - from a preceding or later model of your printer.
    - for a printer from a different manufacturer that is similar to your printer model.
      Example: The HP LaserJet4 driver can be used for common laser printers that support PCL 4 oder PostScript Level 2.

primos cannot be embedded into a directory service.

☐ In all of the directory service, a synchronized time must be set. The primos device time must not differ from that of the directory service. We recommend to use the same time server (SNTP server) for primos and the directory service. Check the primos time server configuration ⇨🖹19.

☐ Make sure that a DNS server is configured in primos and that primos can access it ⇨🗎16.

<u>Wide-Area AirPrint™ does not work</u>
Check if

☐ the desired printer is being published via wide-Area AirPrint™ ⇨🗎37.

☐ the primos subdomain is configured as search domain on the iOS devices:
- 'Configuring the primos Subdomain as Search Domain on iOS Devices Automatically' ⇨🗎39.
- 'Configuring the primos Subdomain as Search Domain on iOS Devices Manually' ⇨🗎40.

☐ the conditional forwarder has been implemented correctly on the DNS server. Requests which contain the primos subdomain must be forwarded to primos ⇨🗎38.

8.3   Index