primos

Print. Mobile. Secure.

by SEH

# Benutzerhandbuch

## Hersteller & Kontakt

SEH Computertechnik GmbH
Südring 11
33647 Bielefeld
Deutschland

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

## Dokument

Typ: Benutzerhandbuch
Titel: primos
Version: 2.0

## Rechtliche Hinweise

# Inhalt

# 1 Allgemeine Information

In diesem Kapitel erhalten Sie Informationen zu Gerät und Dokumentation sowie Hinweise zu Ihrer Sicherheit.
Sie erfahren, wie Sie primos optimal einsetzen und eine schnelle Funktionsbereitschaft herstellen.

**Welche Information benötigen Sie?**

## 1.1 primos

**Verwendungszweck**

primos ist eine mobile Drucklösung mit der Inhalte wie Dokumente und Bilder von iOS-Geräten (iPhone®, iPad® usw.) gedruckt werden können. Die über primos abgewickelten Druckaufträge verbleiben im Netzwerk des Unternehmens, werden nur lokal verarbeitet und nicht via Internet oder Cloud-Lösungen übertragen. primos macht bis zu 10 Drucker für iOS-Geräte verfügbar. Dies sind drahtgebundene oder drahtlose AirPrint®-fähige Netzwerkdrucker, Dabei erweitert primos die AirPrint-Funktionalität mit verschiedenen Features (Wide-Area AirPrint, Unterstützung von Directory-Services u. v. m.).

primos wurde vornehmlich für den professionellen Einsatz in Unternehmen (Enterprise-Umfeld) konzipiert.

**Funktionsweise**

primos wird kabelgebunden an Ihr Netzwerk angeschlossen. Mit diesem Netzwerk sind die iOS-Geräte via WLAN verbunden. Druckaufträge werden aus iOS-Apps mit AirPrint-Unterstützung über Ihr Netzwerk an primos gesendet. primos leitet die Druckaufträge zur Ausgabe an die Netzwerkdrucker weiter.

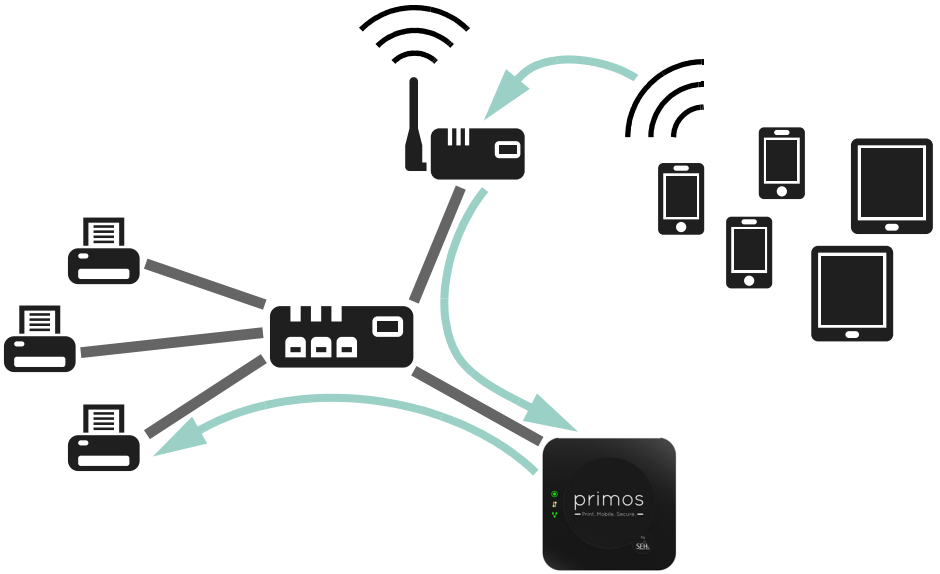


Abbildung 1: Topologie

**Voraussetzungen**

Netzwerk

Drahtgebundenes TCP/IP-Netzwerk (LAN) mit Wireless Access Point (WLAN).

Unterstützte iOS-Geräte

primos unterstützt alle iOS-Geräte mit AirPrint-Unterstützung. AirPrint ist in allen iOS-Geräten ab iOS 4.2 verfügbar. Die iOS-Geräte sind via WLAN mit dem drahtgebundenen Netzwerk verbunden.

Unterstützte Drucker

Netzwerkdrucker mit AirPrint-Funktionalität.

## 1.2 Dokumentation

Informationen zum Leistungsumfang Ihres Produktes entnehmen Sie dem primos Datenblatt.

**Aufbau der Dokumentation**

Die primos Dokumentation besteht aus den folgenden Dokumenten:

| | | |
|---|---|---|
| Benutzerhandbuch | PDF | Detaillierte Beschreibung der Konfiguration und Administration von primos. |
| Quick Installation Guide | Print<br>PDF | Informationen zur Hardware-Installation sowie zur Inbetriebnahme. |
| Wichtige Produktinformationen | Print<br>PDF | Informationen zu Sicherheit, Konformitäts-Erklärungen und zur Entsorgung. |
| Online Hilfe<br>(primos Control Center) | HTML | Die Online Hilfe enthält detaillierte Informationen zur Bedienung des 'primos Control Center'. |

**Merkmale dieses Dokumentes**

Diese Dokumentation ist als elektronisches Dokument für die Betrachtung am Bildschirm konzipiert. Viele Anzeigeprogramme (z.B. Adobe® Reader®) verfügen über eine Lesezeichen-Funktion, in deren Fenster die gesamte inhaltliche Struktur des Dokumentes dargestellt wird.

Dieses Dokument enthält Verknüpfungen (Hyperlinks), über die Sie mit einem Mausklick zusammenhängende Informationseinheiten anzeigen lassen können. Zum Ausdrucken dieser Dokumentation empfehlen wir die Druckereinstellung 'Duplex' oder 'Heft bzw. Buch'.

**Fachbegriffe in diesem Dokument**

In diesem Dokument sind Erläuterungen von Fachbegriffen in einem Glossar zusammengefasst. Das Glossar bietet einen schnellen Überblick über technische Zusammenhänge und Hintergrundinformationen ⇨🗎70.

**Symbole und Auszeichnungen**

Innerhalb dieses Dokumentes finden Sie verschiedene Symbole und Auszeichnungen. Entnehmen Sie deren Bedeutung der Tabelle:

| | |
|---|---|
| **Warnung**<br>**Warnung** | Ein Warnhinweis enthält wichtige Informationen, die Sie unbedingt beachten müssen. Nichtbeachtung kann zu Fehlfunktionen führen. |

| | |
|---|---|
| **Hinweis**<br>Hinweis | Ein Hinweis enthält Informationen, die Sie beachten sollten. |
| 1. Markieren Sie... | Eine Nummerierung führt Sie durch eine Handlungsanweisung. |
| ↳ Bestätigung | Der Pfeil bestätigt die Auswirkung einer ausgeführten Handlung. |
| ✓ Voraussetzung | Ein Haken kennzeichnet Bedingungen, die erfüllt sein müssen, bevor Sie mit einer Handlung beginnen. |
| ☐ Option | Ein Quadrat weist Sie auf unterschiedliche Verfahren und Varianten hin, die Sie durchführen können. |
| • | Blickfangpunkte kennzeichnen Aufzählungen. |
|  | Das Zeichen signalisiert die inhaltliche Zusammenfassung eines Kapitel. |
| ⇨ | Der Pfeil symbolisiert einen Verweis auf eine Seite innerhalb dieses Dokuments. Im PDF-Dokument kann durch einen einfachen Mausklick auf das Symbol die Seite angesprochen werden. |
|  | Die Glühbirne signalisiert einen Tipp. |
| **Fett** | Feststehende Bezeichnungen (z.B. von Schaltflächen oder Menüpunkten) sind fett ausgezeichnet. |
| Courier | Kommandozeilen sind im Schrifttyp Courier dargestellt. |
| 'Eigennamen' | Eigennamen sind in Anführungszeichen gesetzt |

## 1.3 Support und Service

**Kontakt**

SEH Computertechnik GmbH bietet einen umfassenden Support. Falls Sie Fragen haben, kontaktieren Sie unsere Hotline.

Montag–Donnerstag 8:00–16:45 Uhr
Freitag 8:00–15:15 Uhr

+49 (0)521 94226-44

support@seh.de

http://www.seh.de/

**Downloads**

Downloads finden Sie auf der Homepage von SEH Computertechnik GmbH:
http://www.seh.de/services/downloads/download-mobility-loesungen/primos.html

Für primos finden Sie dort:

- aktuelle Firmware/Software
- aktuelle Tools
- aktuelle Dokumentationen
- aktuelle Produktinformationen
- Produktdatenblätter
- u.v.m.

## 1.4 Ihre Sicherheit

Lesen und beachten Sie alle in der Dokumentation, auf dem Gerät oder auf der Verpackung dargestellten Sicherheits- und Warnhinweise. Das Beachten der Hinweise vermeidet potentiellen Fehlgebrauch und schützt Personen vor Gefahren und das Gerät vor Schäden.

Bei Nichtbeachtung der dargebotenen Sicherheits- und Warnhinweise übernimmt die SEH Computertechnik GmbH keine Haftung bei Sach- und Personen- oder Folgeschäden. Zudem entfällt in diesem Fall jeglicher Garantieanspruch.

**Bestimmungsgemäße Verwendung**

primos wird in TCP/IP-Netzwerken eingesetzt und ist konzipiert für den Einsatz in Büroumgebungen. primos leitet Druckaufträge von iOS-Geräten an Netzwerkdrucker mit AirPrint-Funktionalität weiter. Dabei erweitert primos die AirPrint-Funktionalität mit verschiedenen Features (Wide-Area AirPrint, Unterstützung von Directory-Services u. v. m.).

**Bestimmungswidrige Verwendung**

Alle Verwendungen des Gerätes, die den in der primos Dokumentation beschriebenen Funktionalitäten nicht entsprechen, sind bestimmungswidrig. Eigenmächtige konstruktive Veränderungen an Hardware oder Software sowie Reparaturversuche am Gerät sind verboten.

**Sicherheitshinweise**

Lesen und beachten Sie vor der Inbetriebnahme von primos die Sicherheitshinweise im Dokument 'Wichtige Produktinformationen'. Dieses Dokument liegt in gedruckter Form dem Lieferumfang bei.

**Warnhinweise**

Lesen und beachten Sie alle in diesem Dokument dargestellten Warnhinweise. Die Hinweise sind gefahrenträchtigen Handlungsanleitungen vorangestellt. Sie werden wie folgt dargestellt:

**Warnung**

**Dies ist ein Warnhinweis!**

## 1.5 Erste Schritte

In diesem Abschnitt erhalten Sie alle notwendigen Informationen, um eine schnelle Funktionsbereitschaft herzustellen.

1. Lesen und beachten Sie die Sicherheitsinformationen, um Schaden an Personen und Gerät zu vermeiden ⇨🗎6.
2. Führen Sie die Hardware-Installation aus. Die Hardware-Installation beinhaltet das Anschließen von primos an Netzwerk und Stromnetz; siehe: 'Quick Installation Guide'.
3. Ermitteln Sie die IP-Adresse von primos; siehe: ⇨🗎7.
4. Konfigurieren Sie Queues (Druckerwarteschlangen) auf primos ⇨🗎25.

↳ primos ist funktionsbereit. Sie können von iOS-Geräten drucken ⇨🗎38.

## 1.6 IP-Adresse von primos ermitteln

**Wozu eine IP-Adresse?**

Eine IP-Adresse dient zur Adressierung von Netzwerkgeräten in einem IP-Netzwerk. Im Rahmen des TCP/IP-Netzwerkprotokolls ist es erforderlich, eine IP-Adresse im primos zu speichern, damit das Gerät im Netzwerk angesprochen werden kann.

**Wie erhält primos eine IP-Adresse?**

primos wird ohne IP-Adresse ausgeliefert. Nachdem primos an das Netzwerk angeschlossen ist, erhält primos eine IP-Adresse über DHCP. Ist das nicht der Fall, sucht sich primos eine ZeroConf-IP-Adresse aus dem ZeroConf-Adressbereich (169.254.0.0/16).

Die Einstellungen für die IP-Adresse können Sie nachträglich ändern:

- 'Wie konfiguriere ich IPv4-Parameter?' ⇨🗎13
- 'Wie konfiguriere ich IPv6-Parameter?' ⇨🗎14

**Wie finde ich die IP-Adresse?**

Die primos IP-Adresse kann über die SEH primos App ermittelt werden.

<u>Systemvoraussetzungen der SEH primos App:</u>

- Windows 7, Windows 8, Windows 10;
  Mac OS X 10.7.x, OS X 10.8.x–10.11.x, macOS10.12.x und höher
- Die Installation kann ausschließlich durch Benutzer mit administrativen Rechten durchgeführt werden.

**Voraussetzung**

✓ primos ist an ihr Netzwerk angeschlossen; siehe: 'Quick Installation Guide'.

1. Notieren Sie sich die Hardware-Adresse Ihres primos. Die Hardware-Adresse finden Sie im Typenschild auf der Unterseite von primos.

2. Laden Sie die SEH primos App für Ihr Betriebssystem von der SEH Computertechnik GmbH-Homepage.
   http://www.seh.de/services/downloads/download-mobility-loesungen/primos.html

3. Installieren Sie die SEH primos App auf Ihrem Client.
4. Starten Sie die SEH primos App.
   Alle im Netzwerk gefundenen primos Geräte werden angezeigt.
5. Finden Sie mithilfe der Hardware-Adresse Ihren primos.

**Hinweis**

Die IP-Adresse kann ebenfalls über Bonjour ermittelt werden. primos ist unter dem Namen 'primos@ICxxxxxx' zu finden (wobei ICxxxxxx der Default- Name ⇨🗎70 ist). Alle Geräte mit iOS und Mac OS X/OS X/macOS unterstützen Bonjour nativ. Auf Geräten mit anderen Betriebssystemen, z.B. Windows, müssen Bonjour-Dienste nachträglich installiert werden.

# 2 Administrationsmethoden

Sie können primos auf unterschiedliche Weise administrieren und konfigurieren. In diesem Kapitel erhalten Sie eine Übersicht über die verschiedenen Administrationsmöglichkeiten.

Sie erfahren, unter welchen Voraussetzungen die Methoden verwendet werden können und welche Funktionalitäten die jeweilige Methode unterstützt.

**Welche Information benötigen Sie?**

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

## 2.1 Administration via primos Control Center

**Was ist das primos Control Center?**

Über das primos Control Center kann primos konfiguriert und überwacht werden. Das primos Control Center ist in Ihrem primos gespeichert und kann mit einer Browsersoftware (Microsoft Edge, Safari, Mozilla Firefox) dargestellt werden.

**Sicherheit**

Der Zugang zum primos Control Center ist geschützt (⇨🗎48). Das voreingestellte Benutzerprofil ist:
Benutzername: admin
Passwort: admin

**Hinweis**

Ändern Sie das voreingestellte Passwort sobald wie möglich (⇨🗎48)!

Für weitere Informationen zu Benutzerprofilen siehe ⇨🗎48.

**primos Control Center starten**

Sie können das primos Control Center direkt im Browser öffnen oder es über die SEH primos App aufrufen:

- 'primos Control Center im Browser öffnen' ⇨🗎10
- 'primos Control Center über SEH primos App aufrufen' ⇨🗎10

**Hinweis**

Falls das primos Control Center nicht angezeigt wird, überprüfen Sie die Proxy-Einstellungen Ihres Browsers.

## primos Control Center im Browser öffnen

**Voraussetzung**

- ✓ primos ist an Netzwerk und Netzspannung angeschlossen.
- ✓ primos hat eine gültige IP-Adresse.

1. Öffnen Sie Ihren Browser.
2. Geben Sie als URL die IP-Adresse von primos ein.

↳ Das primos Control Center wird im Browser dargestellt.

## primos Control Center über SEH primos App aufrufen

**Voraussetzung**

- ✓ primos ist an Netzwerk und Netzspannung angeschlossen.
- ✓ primos hat eine gültige IP-Adresse.
- ✓ Ihr primos wird in der SEH primos App angezeigt (⇨🗎12).

1. Doppelklicken Sie in der Liste auf Ihren primos.

↳ Ihr Standard-Browser wird geöffnet und das primos Control Center dargestellt.

**Aufbau des primos Control Centers**

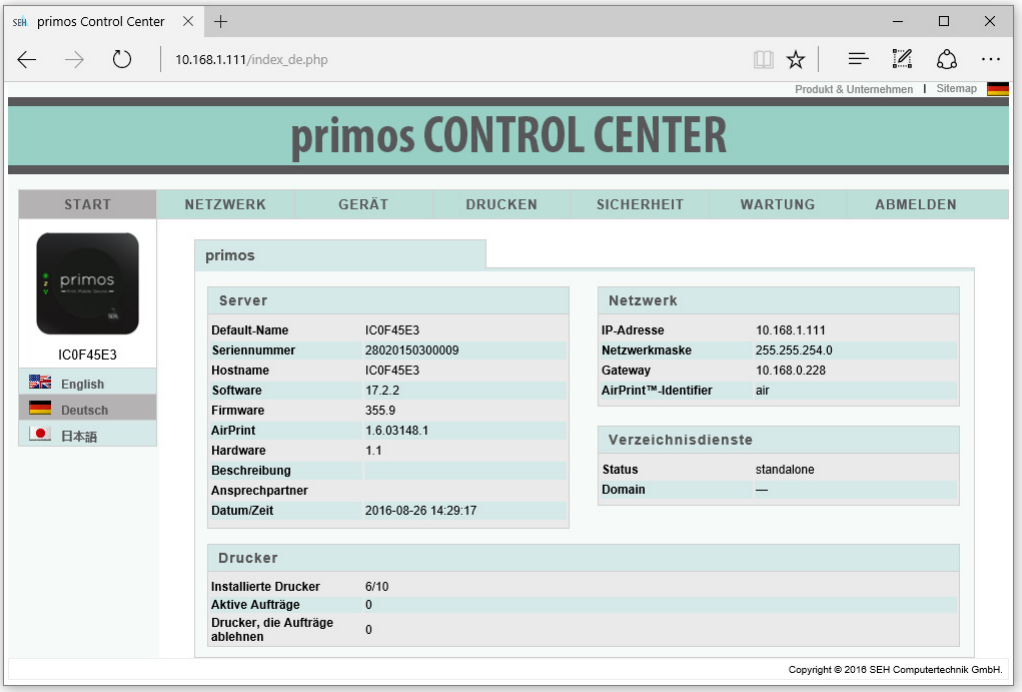


Abbildung 2: primos Control Center

Die Sprache können Sie über die Anwahl des entsprechenden Flaggensymbols einstellen.

In der Navigationsleiste (oben) befinden sich die verfügbaren Menüpunkte. Nach dem Anwählen eines Menüpunkts (einfacher Mausklick) werden auf der linken Seite die verfügbaren Untermenüpunkte angezeigt. Nach dem Anwählen eines Untermenüs wird die entsprechende Seite mit den Menüinhalten dargestellt (rechts).

Über den Punkt **Produkt & Unternehmen** werden die Kontaktdaten des Herstellers sowie weiterführende Informationen zum Produkt angezeigt. Über den Punkt **Sitemap** erhalten Sie eine Übersicht und direkten Zugriff auf alle Seiten des primos Control Centers.

Alle anderen Menüpunkte beziehen sich auf die Konfiguration von primos. Die Menüpunkte sind in der Online Hilfe des primos Control Centers beschrieben. Um die Online Hilfe zu starten, wählen Sie das ⓘ-Symbol an.

### Logout

Aus Sicherheitsgründen sollten Sie sich am primos Control Center abmelden nachdem Sie Ihre Einstellungen vorgenommen haben.

1. Wählen Sie die Schaltfläche **Abmelden** an.

↳ Die Login-Seite wird dargestellt. Sie haben sich erfolgreich abgemeldet.

## 2.2 Administration via SEH primos App

Die SEH primos App eine von der SEH Computertechnik GmbH entwickelte Software zur Administration von primos Geräten.

**Funktionsweise**

Nach dem Start scannt die SEH primos App das Netzwerk nach angeschlossenen primos Geräten. Der zu scannende Netzwerkbereich ist frei definierbar. Nach dem Scannen werden alle gefundenen primos Geräte in einer Liste angezeigt. Die gefundenen Geräte können markiert und administriert werden.

**Installation**

Um mit der SEH primos App zu arbeiten, muss das Programm auf einem Rechner mit einem Windows- oder Mac OS X/OS X/macOS-Betriebssystem installiert werden. Je nach Betriebssystem sind verschiedene Installationsdateien verfügbar.

**Systemvoraus-setzungen**

- Windows 7, Windows 8, Windows 10;
  Mac OS X 10.7.x, OS X 10.8.x–10.11.x, macOS10.12.x und höher
- Die Installation kann ausschließlich durch Benutzer mit administrativen Rechten durchgeführt werden.

1. Laden Sie die SEH primos App für Ihr Betriebssystem von der SEH Computertechnik GmbH-Homepage.
   http://www.seh.de/services/downloads/download-mobility-loesungen/primos.html

2. Installieren Sie die SEH primos App auf Ihrem Client.

↳ Die SEH primos App ist auf Ihre Client installiert.

**Starten**

Sie erkennen die SEH primos App an ihrem Icon:  . Die SEH primos App wird wie auf Ihrem Betriebssystem üblich gestartet.

# 3 Netzwerkeinstellungen

Zur optimalen Integration von primos in ein Netzwerk können verschiedene Einstellungen definiert werden.
In diesem Kapitel erfahren Sie, welche Netzwerkeinstellungen primos unterstützt.

**Welche Information benötigen Sie?**

- 'Wie konfiguriere ich IPv4-Parameter?' ⇨🗎13
- 'Wie konfiguriere ich IPv6-Parameter?' ⇨🗎14
- 'Wie konfiguriere ich den DNS?' ⇨🗎15
- 'Wie konfiguriere ich Bonjour?' ⇨🗎16
- 'Wie konfiguriere ich Verzeichnisdienste?' ⇨🗎17

## 3.1 Wie konfiguriere ich IPv4-Parameter?

Zur optimalen Integration von primos in ein TCP/IP-Netzwerk können Sie verschiedene IPv4-Parameter definieren. Standardmäßig erfolgt die IP-Adresszuweisung am primos dynamisch über DHCP. Sie können primos aber auch manuell eine statische IP-Adresse zuweisen.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK - IPv4** an.
3. Konfigurieren Sie die IPv4-Parameter; Tabelle 1 ⇨🗎13.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

Tabelle 1: IPv4-Parameter

| Parameter | Beschreibung |
|---|---|
| DHCP | De-/aktiviert das Protokoll DHCP.<br>*Über DHCP können primos automatisch TCP/IP-Parameter zugewiesen werden.* |
| Statisch | De-/aktiviert die manuelle Vergabe von festen TCP/IP-Parametern für primos.<br>*Definieren Sie IP-Adresse, Netzwerkmaske und Gateway.* |
| IP-Adresse | Definiert eine manuell vergebene IPv4-Adresse für primos. |
| Netzwerkmaske | Definiert eine manuell vergebene Netzwerkmaske für primos. |
| Gateway | Definiert eine manuell vergebene Gateway-Adresse für primos. |

## 3.2 Wie konfiguriere ich IPv6-Parameter?

Sie können primos in ein IPv6-Netzwerk einzubinden.

**Welche Vorteile bietet IPv6?**

IPv6 (Internet Protocol Version 6) ist der Nachfolger des gegenwärtig überwiegend verwendeten Internet-Protokolls in der Version 4. Beide Protokolle sind Standards für die Netzwerkschicht des OSI-Modells und regeln die Adressierung und das Routing von Datenpaketen durch ein Netzwerk. Die Einführung von IPv6 bietet viele Vorteile:

- Vergrößerung des Adressraums von $2^{32}$ (IPv4) auf $2^{128}$ (IPv6) IP-Adressen
- Autokonfiguration und Renumbering
- Effizienzsteigerung beim Routing durch reduzierte Header-Informationen
- Standardmäßig integrierte Dienste wie IPSec, QoS, Multicast
- Mobile IP

**Wie wird eine IPv6-Adresse dargestellt?**

IPv6-Adressen sind 128 Bit lang und werden als 8 x 16 Bit hexadezimal dargestellt.

Die acht Blöcke sind durch einen Doppelpunkt zu trennen. Beispiel:

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

Führende Nullen können zur Vereinfachung vernachlässigt werden. Beispiel:

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

Ein Block aus zusammenhängenden Nullen kann mit zwei aufeinander folgenden Doppelpunkten zusammengefasst werden. Damit die Adresse eindeutig bleibt, darf diese Regel nur einmal angewandt werden. Beispiel:

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

In einer URL wird eine IPv6-Adresse in eckigen Klammern eingeschlossen. Diese Notation verhindert eine falsche Interpretation von Portnummern als Teil der IPv6-Adresse. Beispiel:

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

**Hinweis**

Die URL wird ausschließlich von IPv6-fähigen Browsern akzeptiert.

**Welche IPv6-Adresstypen gibt es?**

IPv6-Adressen lassen sich in verschiedene Typen einteilen. Anhand der Präfixe in den IPv6-Adressen lassen sich IPv6-Adressentypen ableiten.

- Unicast-Adressen sind routbare weltweit einzigartige und damit eindeutige Adressen. Ein Paket, das an eine Unicast-Adresse gesendet wird, kommt nur an der Schnittstelle an, die dieser Adresse zugeordnet ist. Unicast-Adressen haben die Präfixe '2' oder '3'.
- Anycast-Adressen können mehrere Teilnehmer gleichzeitig erhalten. Ein Datenpaket

das an diese Adresse gesendet wird kommt also an mehreren Geräten an. Anycast-Adressen unterscheiden sich in ihrer Syntax nicht von Unicast-Adressen, sie wählen allerdings aus mehreren Schnittstellen eine Schnittstelle aus.

- Ein für eine Anycast-Adresse bestimmtes Paket kommt an der nächstgelegenen (entsprechend der Router-Metrik) Schnittstelle an. Anycast-Adressen werden nur von Routern verwendet.
- Mit der Multicast-Adresse kann man Datenpakete an mehrere Schnittstellen gleichzeitig versenden, ohne dass die Bandbreite proportional zu den Teilnehmern steigt. Eine Multicast-Adresse erkennt man an dem Präfix 'ff'.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK - IPv6** an.
3. Konfigurieren Sie die IPv6-Parameter; Tabelle 2 ⇨🗎15.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

Tabelle 2: IPv6-Parameter

| Parameter | Beschreibung |
|---|---|
| IPv6 | De-/aktiviert die IPv6-Funktionalität von primos. |
| Automatische Konfiguration | De-/aktiviert die automatische Vergabe der IPv6-Adressen für primos. |
| IPv6-Adresse | Definiert eine manuell vergebene IPv6-Unicast-Adresse im Format n:n:n:n:n:n:n:n für primos.<br>*Jedes 'n' stellt den hexadezimalen Wert von einem der acht 16-Bit-Elemente der Adresse dar.* |
| Router | Definiert die IPv6-Unicast-Adresse des Routers, an den primos seine 'Router Solicitations' (RS) sendet. |
| Präfixlänge | Definiert die Länge des Subnetz-Präfixes für die IPv6-Adresse. Der Wert 64 ist voreingestellt.<br>*Adressbereiche werden durch Präfixe angegeben. Dazu wird die Präfixlänge (Anzahl der verwendeten Bits) als Dezimalzahl mit vorangehendem '/' an die IPv6-Adresse angehängt dargestellt.* |

## 3.3 Wie konfiguriere ich den DNS?

DNS (Domain Name Service) erlaubt die gegenseitige Zuordnung von Namen und Adressen.

Mithilfe des DNS lassen sich einige Einstellungen im primos mit dem DNS einfacher vornehmen (Eingabe von Hostnamen anstelle von IP-Adressen bei Server-Definitionen).

**Hinweis**

Ist Ihr Netzwerk entsprechend konfiguriert, erhält primos die DNS-Einstellungen automatisch über DHCP.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK - DNS** an.
3. Konfigurieren Sie die DNS-Parameter; Tabelle 3 ⇨🗎16.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

Tabelle 3: DNS-Parameter

| Parameter | Beschreibung |
|---|---|
| Erster DNS-Server | Definiert die IP-Adresse des ersten DNS-Servers. |
| Zweiter DNS-Server | Definiert die IP-Adresse des zweiten DNS-Servers.<br>*Der zweite DNS-Server wird verwendet, wenn der erste DNS-Server nicht verfügbar ist.* |
| Domain-Name (Suffix) | Definiert den Domain-Namen eines vorhandenen DNS-Servers. |

## 3.4 Wie konfiguriere ich Bonjour?

Bonjour ermöglicht die automatische Erkennung von Computern, Geräten und Netzwerkdiensten in TCP/IP-basierten Netzwerken.

primos nutzt Bonjour zu folgenden Zwecken:

- Zur Suche von Druckern im Netzwerk (⇨🗎25).
- Überprüfung der über ZeroConf (⇨🗎7) zugewiesenen IP-Adresse.
- Bekanntgabe seiner Bonjour-Dienste.

Bonjour ist im primos immer aktiv. Konfiguriert werden kann der Name, unter dem primos seine Bonjour-Dienste bekannt gibt. Standardmäßig wird der Name 'primos@ICxxxxxx' verwendet (wobei ICxxxxxx der Default- Name ⇨🗎70 ist).

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK - Bonjour** an.
3. Konfigurieren Sie den Bonjour-Namen.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellung wird gespeichert.

## 3.5 Wie konfiguriere ich Verzeichnisdienste?

Sie können primos in einen Verzeichnisdienst einbinden. Über den Verzeichnisdienst werden Benutzerdaten zentral verwaltet und primos zur Verfügung gestellt. Verzeichnisdienstbenutzer können Sie nutzen

- um zu kontrollieren, wer drucken darf ⇨🗎36
- zur Benutzeranmeldung am primos Control Center ⇨🗎48

primos unterstützt folgende Verzeichnisdienste:

- Active Directory
- LDAP (z.B. OpenLDAP oder Apple® Open Directory)

**Was möchten Sie tun?**

☐ 'primos in ein Active Directory einbinden' ⇨🗎17
☐ 'primos in ein LDAP-Verzeichnis einbinden' ⇨🗎18

<u>primos in ein Active Directory einbinden</u>

primos wird in ein Active Directory eingebunden, indem es Mitglied einer Domain wird.

**Voraussetzung**

✓ Im primos ist ein DNS-Server konfiguriert ⇨🗎15.
✓ primos ist mit einem Resource Record vom Typ A (IPv4-Adresse des Hosts) auf dem verwendeten DNS-Server eingetragen.
✓ Im primos ist ein Time-Server konfiguriert ⇨🗎20.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK - Verzeichnisdienste** an.
3. Konfigurieren Sie die Active Directory-Parameter; Tabelle 4 ⇨🗎17.
4. Bestätigen Sie mit **Speichern**.

↳ primos ist Mitglied einer Domain und damit in das Active Directory eingebunden.

Tabelle 4: Active Directory-Parameter

| Parameter | Beschreibung |
|---|---|
| Active Directory | De-/aktiviert das Einbinden von primos in ein vorhandenes Active Directory. |
| Active Directory-Name | Definiert den Namen des Active Directorys in das primos eingebunden wird.<br>*Geben Sie den vollständigen Name der Domain (Fully Qualified Domain Name – FQDN) ein.* |
| Arbeitsgruppe | Definiert den Namen der Arbeitsgruppe.<br>*Geben Sie den NetBIOS-Domain-Namen ein.* |

| Parameter | Beschreibung |
|---|---|
| Passwort-Server | Definiert den Passwort-Server des Active Directorys über die IP-Adresse oder den Hostnamen. (Optional)<br>*Ein Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde.* |
| WINS-Server | Definiert den WINS-Server des Active Directorys über die IP-Adresse oder den Hostnamen.<br>*Ein WINS-Server sollte angegeben werden, um eine Kommunikation zwischen Teilnehmern in unterschiedlichen Netzwerksegmenten zu ermöglichen.*<br>*Ein Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde.* |
| Administratorkonto | Definiert den Namen des Administrator-Accounts mit dem primos auf dem Domain Controller des Active Directorys angelegt ist. |
| Passwort | Passwort des Administrator-Accounts mit dem primos auf dem Domain Controller des Active Directorys angelegt ist. |

## primos in ein LDAP-Verzeichnis einbinden

**Voraussetzung**

- ✓ Im primos ist ein DNS-Server konfiguriert ⇨🗎15.
- ✓ primos ist mit einem Resource Record vom Typ A (IPv4-Adresse des Hosts) auf dem verwendeten DNS-Server eingetragen.
- ✓ Im primos ist ein Time-Server konfiguriert ⇨🗎20.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK - Verzeichnisdienste** an.
3. Konfigurieren Sie die LDAP-Parameter; Tabelle 5 ⇨🗎18.
4. Bestätigen Sie mit **Speichern**.

↳ primos ist in das LDAP-Verzeichnis eingebunden.

Tabelle 5: LDAP-Parameter

| Parameter | Beschreibung |
|---|---|
| LDAP | De-/aktiviert das Einbinden von primos in einen vorhandenen LDAP-Verzeichnisdienst. |
| LDAP-Server | Definiert den LDAP-Server über die IP-Adresse oder den Hostnamen.<br>*Ein Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde.* |
| Basis-DN | Definiert den Basis-DN (Distinguished Name). Der Basis-DN definiert, von welchem Verzeichnisort abwärts die Suche nach Benutzern gestartet wird.<br>*Domainkomponenten sind durch Komma zu trennen (Beispiel: dc=MeineDomäne,dc=com).* |
| Sicheres LDAP | Verschlüsselt die LDAP-Verbindung (LDAP over SSL/TLS – LDAPS).<br>*Für die Verschlüsselung wird ein CA-Zertifikat benötigt.* |

| Parameter | Beschreibung |
|---|---|
| LDAP-CA-Zertifikat | Wählen Sie das Wurzel-CA-Zertifikat der Zertifizierungsstelle, die das Zertifikat für den Domain Controller (DC) ausgegeben hat.<br>*Das CA-Zertifikat muss zuvor auf dem Gerät installiert worden sein* ⇨ 58. |

# 4 Geräteeinstellungen

Im primos können Beschreibungen und die Geräte-Zeit konfiguriert werden. Dieses Kapitel informiert Sie über diese Geräteeinstellungen.

**Welche Information benötigen Sie?**

- 'Wie lege ich eine Beschreibung fest?' ⇨🗎20
- 'Wie konfiguriere ich die Gerätezeit?' ⇨🗎20
- 'Wie konfiguriere ich lokale Benutzer?' ⇨🗎21
- 'Wie konfiguriere ich lokale Gruppen?' ⇨🗎22

## 4.1 Wie lege ich eine Beschreibung fest?

Sie können primos freidefinierbare Beschreibungen zuzuweisen. Auf diese Weise erhalten Sie einen besseren Überblick über die in Ihrem Netzwerk vorhandenen Geräte.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **GERÄT** - **Beschreibung** an.
3. Geben Sie in die Felder **Hostname**, **Beschreibung** und **Ansprechpartner** freidefinierbare Bezeichnungen ein.
4. Bestätigen Sie mit **Speichern**.

↳ Die Beschreibungen werden gespeichert.

## 4.2 Wie konfiguriere ich die Gerätezeit?

Die Gerätezeit im primos kann über einen Time-Server (SNTP-Server) im Netzwerk gesteuert werden. Ein Time-Server synchronisiert die Zeit mehrerer Geräte innerhalb eines Netzwerkes.

**Nutzen und Zweck**

Im primos wird die Gerätezeit u.a. benötigt, um Verzeichnisdienste (⇨🗎17) zu nutzen und Einträge in der Job History (⇨🗎32) mit einem Zeitstempel zu versehen.

**UTC**

Als Basis verwendet primos 'UTC' (Universal Time Coordinated). UTC ist eine Referenzzeit, die als globaler Standard benutzt wird.

**Zeitzone**

Die über den Time-Server empfangene Zeit entspricht also nicht automatisch Ihrer lokalen Zeitzone. Abweichungen zu Ihrem Standort und der damit verbundenen Zeitverschiebung, inklusive länderspezifischer Eigenheiten wie z.B. Sommerzeit, können über den Parameter 'Zeitzone' ausgeglichen werden.

**Hinweis**

Time-Server können automatisch über DHCP eingetragen werden. Ein Time-Server der über DHCP eingetragen wird, hat gegenüber einem manuell definierten Time-Server immer Vorrang.

**Voraussetzung**

✓ Im Netzwerk ist ein Time-Server integriert.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **NETZWERK - Datum/Zeit** an.
3. Aktivieren Sie die Option **Datum/Zeit**.
4. Geben Sie im Feld **Time-Server** die IP-Adresse oder den Hostnamen des Time-Servers ein.
   **(Ein Hostname kann nur verwendet werden, wenn zuvor ein DNS-Server konfiguriert wurde.)**
5. Wählen Sie aus der Liste **Zeitzone** das Kürzel für Ihre lokale Zeitzone.
6. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

## 4.3 Wie konfiguriere ich lokale Benutzer?

Bei der Benutzerauthentifizierung legen Sie über Benutzer fest, wer drucken darf ⇨🗎36. Dabei können Sie Benutzer aus einem Verzeichnisdienst (⇨🗎17) oder lokale Benutzer verwenden.

Die lokalen Benutzer legen Sie auf primos an. Für jeden Benutzer muss ein Name und Passwort definiert werden. Zudem kann ein Benutzer einer oder mehreren Benutzergruppen zugeordnet werden (⇨🗎22), um bei der Benutzerauthentifizierung die Eingabe mehrerer Benutzer zu vereinfachen.

**Was möchten Sie tun?**

- ☐ 'Lokalen Benutzer anlegen' ⇨🗎21
- ☐ 'Passwort ändern' ⇨🗎22
- ☐ 'Gruppenzugehörigkeit ändern' ⇨🗎22
- ☐ 'Lokalen Benutzer löschen' ⇨🗎22

<u>Lokalen Benutzer anlegen</u>

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **GERÄT - Benutzer** an.
3. Geben Sie im Feld **Name** einen freidefinierbaren Benutzernamen ein.
   **(a–z, A–Z und 0–9 können eingegeben werden.)**
4. Geben Sie im Feld **Passwort** ein Kennwort ein.
5. Wiederholen Sie die Kennworteingabe.

6. Wählen Sie im Bereich **Gruppen** die Benutzergruppen aus.
7. Bestätigen Sie mit **Speichern**.

↳ Der lokale Benutzer wird angelegt.

Passwort ändern

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **GERÄT - Benutzer** an.
3. Wählen Sie den zu bearbeitenden Benutzer über das Symbol aus.
4. Geben Sie im Feld **Passwort** ein Kennwort ein.
5. Wiederholen Sie die Kennworteingabe.
6. Bestätigen Sie mit **Speichern**.

↳ Das Passwort wird geändert.

Gruppenzugehörigkeit ändern

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **GERÄT - Benutzer** an.
3. Wählen Sie den zu bearbeitenden Benutzer über das Symbol aus.
4. Wählen Sie im Bereich **Gruppen** die gewünschten Benutzergruppen aus.
5. Bestätigen Sie mit **Speichern**.

↳ Die Gruppenzugehörigkeit wird geändert.

Lokalen Benutzer löschen

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **GERÄT - Benutzer** an.
3. Wählen Sie für den zu löschenden Benutzer das Symbol an.
4. Bestätigen Sie die Sicherheitsabfrage.

↳ Der Benutzer wird gelöscht.

## 4.4 Wie konfiguriere ich lokale Gruppen?

Bei der Benutzerauthentifizierung legen Sie über Benutzer fest, wer drucken darf ⇨36. Dabei können Sie Benutzer aus einem Verzeichnisdienst (⇨17) oder lokale Benutzer (⇨21) verwenden.

Um bei der Benutzerauthentifizierung die Eingabe von vielen lokalen Benutzern zu vereinfachen, können sie in lokalen Gruppen zusammengefasst werden. Anschließend werden die Gruppen anstelle der einzelnen Benutzer eingetragen.

Die lokalen Gruppen legen Sie auf primos an. Sie können entweder direkt im

Gruppenmenü Benutzer zu der Gruppe zuordnen oder im Benutzermenü die Gruppen für den jeweiligen Benutzer auswählen.

**Was möchten Sie tun?**

- ☐ 'Lokale Gruppe anlegen' ⇨🗎23
- ☐ 'Zugeordnete Benutzer ändern' ⇨🗎23
- ☐ 'Lokale Gruppe löschen' ⇨🗎23

Lokale Gruppe anlegen

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **GERÄT - Gruppen** an.
3. Geben Sie im Feld **Name** einen freidefinierbaren Gruppenamen ein.
   **(a–z, A–Z und 0–9 können eingegeben werden.)**
4. Wählen Sie im Bereich **Benutzer** die Benutzer aus.
5. Bestätigen Sie mit **Speichern**.

↳ Die lokale Gruppe ist angelegt.

Zugeordnete Benutzer ändern

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **GERÄT - Benutzer** an.
3. Wählen Sie die zu bearbeitende Gruppe über das Symbol ✎ aus.
4. Wählen Sie im Bereich **Benutzer** die Benutzer aus.
5. Bestätigen Sie mit **Speichern**.

↳ Die zugeordneten Benutzer sind geändert.

Lokale Gruppe löschen

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **GERÄT - Gruppe** an.
3. Wählen Sie für den zu löschenden Gruppe das Symbol ✖ an.
4. Bestätigen Sie die Sicherheitsabfrage.

↳ Die Gruppe wird gelöscht.

# 5 Drucken

Wie Sie primos für das Drucken einrichten und weitere Einstellungen für das Drucken konfigurieren erfahren Sie in diesem Kapitel.

Damit von iOS-Geräten über primos gedruckt werden kann, muss im primos für den jeweiligen Drucker eine Queue (Druckerwarteschlange) angelegt werden. Für jede Queue können Sie anschließend zahlreiche Einstellungen (Zugriffskontrolle usw.) konfigurieren. Zudem können Sie allgemeine Einstellungen für das Drucken vornehmen.

**Welche Information benötigen Sie?**


- 'Wie konfiguriere ich Drucker auf primos? (Queues anlegen)' ⇨🗎25
- 'Wie verwalte ich Queues?' ⇨🗎30
- 'Wie sehe ich die Job History ein?' ⇨🗎32
- 'Wie definiere ich die Anzeige von Druckernamen auf dem iOS-Gerät?' ⇨🗎34
- 'Wie warte oder teste ich einen Drucker via primos?' ⇨🗎35
- 'Wie verschlüssele ich die Druckdatenübertragung?' ⇨🗎35
- 'Wie kontrolliere ich, wer drucken darf?' ⇨🗎36
- 'Wie drucke ich von einem iOS-Gerät?' ⇨🗎38
- 'Wie drucke ich über Subnetze hinweg? (Wide-Area AirPrint)' ⇨🗎39

## 5.1 Wie konfiguriere ich Drucker auf primos? (Queues anlegen)

Damit von iOS-Geräten über primos gedruckt werden kann, muss in primos für den jeweiligen Drucker eine Druckerwarteschlange, eine sogenannte Queue, angelegt werden.

**Was ist eine Queue?**

Über Queues werden Drucker angesprochen und Druckaufträge übermittelt. Die Druckaufträge werden in der Queue gesammelt und nacheinander abgearbeitet. Dadurch können mehrere Personen einen Drucker teilen ohne sich gegenseitig zu behindern.

**Hinweis**

Maximal 10 Queues können im primos erstellt werden.

**Wie lege ich eine Queue an?**

In primos können Queues auf 3 Arten angelegt werden:

- **Smart Printer Setup**: Startet eine Suche nach Netzwerkdruckern. Anschließend werden bis zu 10 Queues automatisch angelegt.
- **Expert Printer Setup**: Startet eine Suche nach Netzwerkdruckern. Anschließend erhalten Sie eine Übersicht der gefundenen Drucker mit Queue-Vorschlägen. Diese können Sie bearbeiten und bis zu 10 Queues anlegen.
  (Erfordert Kenntnisse über Druckereinstellungen)
- Queue **manuell anlegen**: Beim manuellen Anlegen einer Queue legen Sie alle Einstellungen für eine einzelne Queue fest. Dabei findet eine Suche nach Netzwerkdruckern statt. Entweder wählen Sie den Drucker, für den Sie die Queue erstellen möchten, aus der Liste der Suchergebnisse oder Sie definieren manuell eine Druckerverbindung.
  (Diese Art eine Queue anzulegen eignet sich besonders, wenn Sie nur für einen einzelnen oder einen spezifischen Drucker eine Queue anlegen möchten.)

**Hinweis**

Das Smart Printer Setup steht nur zur Verfügung, wenn keine Queue auf primos angelegt ist.

**Was möchten Sie tun?**

- ☐ 'Smart Printer Setup nutzen' ⇨📄26
- ☐ 'Expert Printer Setup nutzen' ⇨📄27
- ☐ 'Queue manuell erstellen' ⇨📄28

Smart Printer Setup nutzen

Rufen Sie die START-Seite des primos Control Centers auf und es ist keine Queue auf primos angelegt, z.B. bei der Inbetriebnahme, erscheint automatisch eine Pop-Up-Abfrage mit der Sie das Smart Printer Setup starten können. Alternativ können Sie das Smart Printer Setup manuell starten.

**Welche Queues werden angelegt?**

Es werden bis zu 10 Queues für Drucker auf primos automatisch angelegt.

✓ Es ist keine Queue auf primos angelegt.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **DRUCKEN - Printer Setup** an.
3. Definieren Sie im **Bereich Standardeinstellungen für Suchergebnisse** die Standardeinstellungen für das Erstellen von Queues mit den Suchergebnissen.
4. Wählen Sie die Schaltfläche **Smart Printer Setup** an.

↳ Das Smart Printer Setup startet. primos sucht Netzwerkdrucker und legt für bis zu 10 gefundene Drucker Queues automatisch an. Abschließend wird eine Übersicht der angelegten Queues angezeigt.

**Hinweis**

Abhängig von der Größe Ihres Netzwerks kann das Durchlaufen des Smart Printer Setups mehrere Minuten dauern.

Expert Printer Setup nutzen

✓ Es sind maximal 9 Queues auf primos angelegt.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **DRUCKEN - Druckersuche** an.
3. Definieren Sie im **Bereich Standardeinstellungen für Suchergebnisse** die Standardeinstellungen für das Erstellen von Queues mit den Suchergebnissen.
   **(Sie können Queues später beim Bearbeiten der Suchergebnisse einzeln ändern.)**
4. Wählen Sie die Schaltfläche **Expert Printer Setup** an.
   Die Druckersuche startet. Nach Abschluss des Suchvorgangs wird eine Übersicht der gefundenen Netzwerkdrucker angezeigt.

**Hinweis**

Abhängig von der Größe Ihres Netzwerks kann die Druckersuche mehrere Minuten dauern.

5. Definieren Sie die Queue-Einstellungen für die gewünschten Drucker; Tabelle 6 ⇨🗎28.
   - Über das Häkchen vor dem Drucker können Sie einen oder mehrere Drucker auswählen, für die eine Queue erstellt werden soll.
   - Sie können die Suchergebnisse nach Art des Suchergebnisses (nur neu gefundene Drucker / alle Drucker) und nach dem Typ der Druckerverbindung (IPP/IPPS) filtern.

**Hinweis**

Filtern Sie nicht die Suchergebnisse, wenn Sie bereits Konfigurationseinstellungen vorgenommen haben. Ausgeblendete Queues werden automatisch auf die Ausgangswerte zurückgesetzt.

6. Wählen Sie die Schaltfläche **Alle speichern** oder **Auswahl speichern** an.

↳ Die Queues werden im primos erstellt.

**Hinweis**

Erweiterte Queue-Einstellungen können Sie erst nach Erstellen der Queue definieren. Siehe 'Queue bearbeiten' ⇨🗎30.

Tabelle 6: Queue-Parameter

| Parameter | Beschreibung |
|---|---|
| Adressierung | Definiert wie Drucker im Netzwerk angesprochen werden:<br>- via Bonjour<br>- via Hostname oder IP-Adresse (routbar)<br>*Wählen Sie Hostname/IP-Adresse falls Sie primos oder Drucker nach dem Setup in ein anderes Netzwerksegment integrieren.* |
| Name | Freidefinierbarer Name der Queue. Der Queue-Name bildet zusammen mit dem AirPrint-Identifier den Druckernamen, der im Druckdialog auf dem iOS-Gerät angezeigt wird.<br>*Maximal 50 ASCII-Zeichen (außer runde Klammern, Leerzeichen, Schrägstriche, Anführungszeichen und Doppelkreuz) können eingegeben werden. Unterstriche werden im angezeigten Druckernamen (⇨ 34) als Leerzeichen angezeigt.*<br>*Der Queue-Name kann im Nachhinein nicht geändert werden!* |
| Standort | Freidefinierbare Beschreibung (des Gerätestandorts).<br>*Maximal 80 Zeichen können eingegeben werden.* |
| Geographischer Standort | Gerätestandort in geografischen Koordinaten.<br>*Geben Sie Koordinaten für Breitengrad (-90 bis 90) und Längengrad (-180 bis 180) als Dezimalwerte und durch Komma getrennt ein.*<br>*Beispiel: 51.982898,8.493206* |

## Queue manuell erstellen

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **DRUCKEN - Queue erstellen** an.
3. Konfigurieren Sie die Queue-Parameter; Tabelle 7 ⇨ 28.
4. Wählen Sie die Schaltfläche **Queue erstellen** an.

↳ Die Queue wird im primos erstellt.

Tabelle 7: Queue erstellen – Parameter

| Parameter | Beschreibung |
|---|---|
| Name | Freidefinierbarer Name der Queue. Der Queue-Name bildet zusammen mit dem AirPrint-Identifier (⇨ 34) den Druckernamen, der im Druckdialog auf dem iOS-Gerät angezeigt wird.<br>*Maximal 50 ASCII-Zeichen (außer runde Klammern, Leerzeichen, Schrägstriche, Anführungszeichen und Doppelkreuz) können eingegeben werden. Unterstriche werden im angezeigten Druckernamen (⇨ 34) als Leerzeichen angezeigt.*<br>*Der Queue-Name kann im Nachhinein nicht geändert werden!* |

| Parameter | Beschreibung |
|---|---|
| Standort | Freidefinierbare Beschreibung (des Gerätestandorts).<br>*Maximal 80 Zeichen können eingegeben werden.* |
| Geographischer Standort | Gerätestandort in geografischen Koordinaten.<br>*Geben Sie Koordinaten für Breitengrad (-90 bis 90) und Längengrad (-180 bis 180) als Dezimalwerte und durch Komma getrennt ein.*<br>*Beispiel: 51.982898,8.493206* |
| Drucker auswählen | Definiert den Drucker.<br>*Automatisch im Netzwerk gefundene Drucker werden in der Liste angezeigt. Alternativ können Sie manuell eine Druckerverbindung spezifizieren ('Verbindung').* |
| Verbindungstyp | Definiert das Druckprotokoll (IPP/IPPS) für den aus der Liste gewählten Drucker.<br>*Es können nur Druckprotokolle ausgewählt werden, die der jeweilige Drucker unterstützt.* |
| Verbindung | Definiert die Verbindung zu einem Drucker über einen Geräte-URI (Uniform Resource Identifier).<br>*IPP/IPPS: Beim Internet Printing Protocol werden die Druckdaten via HTTP an den Drucker gesendet. Via SSL/TLS kann die Verbindung zwischen primos und Drucker verschlüsselt werden (IPPS). Standard-Port IPP: 631. Standard-Port IPPS: 443.*<br>`ipp://<IP-Adresse, Bonjour-Name oder Hostname des Druckers>:<Portnummer>/ipp/print`<br>`ipp://<IP-Adresse, Bonjour-Name oder Hostname des Druckers>/ipp/print`<br>`ipps://<IP-Adresse, Bonjour-Name oder Hostname des Druckers>:<Portnummer>/ipp/print`<br>`ipps://<IP-Adresse, Bonjour-Name oder Hostname des Druckers>/ipp/print`<br>*Alternativ können Sie einen automatisch im Netzwerk gefundenen Drucker aus der Liste und einen Verbindungstyp wählen.* |

## 5.2 Wie verwalte ich Queues?

Nachdem Sie Queues für Ihre Netzwerkdrucker im primos erstellt haben, können Sie diese nachträglich bearbeiten oder löschen.

**Was möchten Sie tun?**

- ☐ 'Queue bearbeiten' ⇨🗎30
- ☐ 'Queue löschen' ⇨🗎31

Queue bearbeiten

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **DRUCKEN - Queues** an.
3. Wählen Sie die zu bearbeitende Queue über das Symbol ✎ aus.
4. Konfigurieren Sie die Queue-Parameter; Tabelle 8 ⇨🗎30.
5. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

Tabelle 8: Queue bearbeiten – Parameter

| Parameter | Beschreibung |
|---|---|
| Standort | Freidefinierbare Beschreibung (des Gerätestandorts).<br>*Maximal 80 Zeichen können eingegeben werden.* |
| Geographischer Standort | Gerätestandort in geografischen Koordinaten.<br>*Geben Sie Koordinaten für Breitengrad (-90 bis 90) und Längengrad (-180 bis 180) als Dezimalwerte und durch Komma getrennt ein.*<br>*Beispiel: 51.982898,8.493206* |
| Verbindung | Definiert die Verbindung zu einem Drucker über einen Geräte-URI (Uniform Resource Identifier).<br>*IPP/IPPS: Beim Internet Printing Protocol werden die Druckdaten via HTTP an den Drucker gesendet. Via SSL/TLS kann die Verbindung zwischen primos und Drucker verschlüsselt werden (IPPS). Standard-Port IPP: 631. Standard-Port IPPS: 443.*<br>`ipp://<IP-Adresse, Bonjour-Name oder Hostname des Druckers>:<Portnummer>/ipp/print`<br>`ipp://<IP-Adresse, Bonjour-Name oder Hostname des Druckers>/ipp/print`<br>`ipps://<IP-Adresse, Bonjour-Name oder Hostname des Druckers>:<Portnummer>/ipp/print`<br>`ipps://<IP-Adresse, Bonjour-Name oder Hostname des Druckers>/ipp/print` |
| Aktion | Siehe 'Wie warte oder teste ich einen Drucker via primos?' ⇨🗎35. |
| Multicast-Veröffentlichung | Siehe 'Manuell erstellte Queue kann nicht veröffentlicht werden' ⇨🗎75. |
| Sicheres AirPrint | Siehe 'Wie verschlüssele ich die Druckdatenübertragung?' ⇨🗎35. |

| Parameter | Beschreibung |
|---|---|
| Benutzerauthentifizierung | Siehe 'Wie kontrolliere ich, wer drucken darf?' ⇨ 36. |
| Zugriff | Siehe 'Wie kontrolliere ich, wer drucken darf?' ⇨ 36. |

Queue löschen

**Hinweis**

Gelöschte Queues werden unter Umständen nach dem Löschen noch eine Zeit lang auf den iOS-Geräten angezeigt. Die Anzeige im iOS-Gerät aktualisiert sich mit der Zeit, so dass die gelöschten Queues nicht mehr angezeigt werden.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **DRUCKEN - Queues** an.
3. Wählen Sie für die zu löschende Queue das Symbol ✖ an.
4. Bestätigen Sie die Sicherheitsabfrage.

↳ Die Queue wird gelöscht.

## 5.3 Wie sehe ich die Job History ein?

In der 'Job History' können Sie Informationen über die Druckaufträge, die über primos abgewickelt wurden, einsehen.

Maximal 100 Druckaufträge werden angezeigt. Ab dem 101. Druckauftrag gilt das FIFO-Prinzip (First In – First Out). Durch einen Reset von primos werden die gespeicherten Aufträge gelöscht.

**Hinweis**

Damit Datum und Uhrzeit korrekt angezeigt werden, muss ein Time-Server (⇨🗎20) im primos konfiguriert sein. Ist kein Time-Server konfiguriert, entspricht der Zeitstempel der Defaultzeit.

**Filter**

Die angezeigten Druckaufträge können gefiltert werden:

- alle Aufträge
- abgeschlossene Aufträge
- aktive Aufträge

**Aktionen**

Aktive Druckaufträge können gelöscht werden:

- Auftrag löschen
- Alle aktiven Aufträge löschen

Wenn im Fehlerfall ein anstehender Druckauftrag nicht ausgeführt wird, können nachfolgende Aufträge nicht ausgeführt werden. In diesem Fall löschen Sie die „blockierenden“ Druckaufträge sodass die nachfolgenden abgearbeitet werden.

**Was möchten Sie tun?**

- ☐ 'Job History einsehen' ⇨🗎32
- ☐ 'Einträge in der Job History filtern' ⇨🗎32
- ☐ 'Druckaufträge löschen' ⇨🗎33

Job History einsehen

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **DRUCKEN - Job History** an.

↳ Die Job History wird angezeigt.

Einträge in der Job History filtern

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **DRUCKEN - Job History** an.
   Die Job History wird angezeigt.

3. Wählen Sie die Filter-Schaltfläche an.

↳ Die Einträge in der Job History werden gefiltert angezeigt.

Druckaufträge löschen

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **DRUCKEN - Job History** an.
   Die Job History wird angezeigt.
3. Wählen Sie die Schaltfläche **Aktive Aufträge** an.
   Alle aktiven Druckaufträge werden angezeigt.
4. Löschen Sie einen oder alle aktiven Druckaufträge.
   - 1 Druckauftrag löschen: Wählen Sie die Schaltfläche **Auftrag löschen** an.
   - Alle Druckaufträge löschen: Wählen Sie die Schaltfläche **Alle aktiven Aufträge löschen** an.

↳ Die gewählten Druckaufträge werden gelöscht.

## 5.4 Wie definiere ich die Anzeige von Druckernamen auf dem iOS-Gerät?

Im Druckdialog auf dem iOS-Gerät wird der Druckername mit folgendem Schema angezeigt: '<AirPrint-Identifier> <Queue-Name>'. Beide Elemente können Sie frei definieren.

**Queue-Name**

Der Queue-Name wird für jede Queue individuell beim Erstellen definiert (⇨25) und kann im Nachhinein nicht mehr geändert werden.

**AirPrint-Identifier**

Der AirPrint-Identifier ist ein Präfix, das über primos verfügbar gemachte Drucker auf iOS-Geräten kennzeichnet. Der AirPrint-Identifier gilt für alle Queues. Er kann jederzeit geändert werden. Voreingestellt ist 'air '.

Wählen Sie einen kurzen Identifier, dessen Anfangsbuchstabe vorne im Alphabet steht. Damit stellen Sie sicher, dass die über primos verfügbar gemachten Drucker auf iOS-Geräten im Druckdialog an vorderer Stelle angezeigt werden und leicht erkennbar sind.

Beispiel: Sie nutzen den Standard-AirPrint-Identifier 'air ' und als Queue-Namen den Druckernamen:


Abbildung 3: Druckername im Druckdialog auf dem iOS-Gerät

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **DRUCKEN - Einstellungen** an.
3. Geben Sie im Feld **AirPrint-Identifier** ein freidefinierbares Kürzel ein.
   **Unterstriche können nicht verwendet werden.**
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellung wird gespeichert.

## 5.5 Wie warte oder teste ich einen Drucker via primos?

Über primos können Sie für eine Queue, d.h. einen Drucker, bestimmte Aktionen auslösen:

- Testseite drucken
- Drucker anhalten oder wieder starten
- alle Druckaufträge ablehnen oder wieder annehmen
- alle Druckaufträge löschen

**Nutzen und Zweck**

Die Aktionen vereinfachen Tests und Wartungsarbeiten am Drucker. Beispiele:

- Drucken Sie eine Testseite um die Verbindung zum Drucker zu testen.
- Halten Sie den Drucker an, wenn kurze Wartungsarbeiten (Toner wechseln, Papier nachfüllen) am Drucker durchgeführt werden.
- Ist ein länger andauernder Ausfall des Druckers abzusehen, z.B. bei Reparaturen, sollten alle Druckaufträge abgelehnt werden.

**Voraussetzung**

✓ Es ist eine Queue im primos erstellt ⇨🗎25.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **DRUCKEN - Queues** an.
3. Wählen Sie die gewünschte Queue über das Symbol ✎ aus.
4. Wählen Sie im Bereich **Gerät** aus der Liste **Aktion** eine Druckeraktion aus.
5. Bestätigen Sie mit **Speichern**.

↳ Die Drucker-Aktion wird ausgelöst.

## 5.6 Wie verschlüssele ich die Druckdatenübertragung?

Die Druckdaten werden vom iOS-Gerät über primos zu den Druckern gesendet. Der Druckdatenstrom lässt sich in zwei Wege aufteilen:

- Druckdaten werden vom iOS-Gerät zu primos gesendet
  (Standardmäßig werden die Daten unverschlüsselt übertragen. Die Übertragung kann mit der Funktion Sicheres AirPrint verschlüsselt werden. Siehe unten.)
- Druckdaten werden von primos zum Drucker gesendet
  (Der für die Queue definierte Verbindungstyp definiert das Protokoll mit dem die Druckdaten von primos zum Drucker gesendet werden. Vom Protokoll ist abhängig, ob die Druckdaten verschlüsselt übertragen werden. Siehe ⇨🗎25.)

**Sicheres AirPrint**

Sie können die Druckdatenübertragung zwischen iOS-Gerät und primos verschlüsseln durch den Einsatz einer SSL-/TLS-Verschlüsselung. Die Verschlüsselungsstärke wird über Protokoll und Verschlüsselungsstufe definiert ⇨🗎45. Die Verschlüsselung wird für jede

Queue einzeln definiert.

**Voraussetzung**

- ✓ Es ist eine Queue im primos erstellt ⇨🗎25.
- ✓ Es ist ein Zertifikat auf primos installiert ⇨🗎52.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **DRUCKEN - Queues** an.
3. Wählen Sie die gewünschte Queue über das Symbol aus.
4. De-/aktivieren Sie die Option **Sicheres AirPrint**.
5. Bestätigen Sie mit **Speichern**.

↳ Die Einstellung wird gespeichert.

**Hinweis**

Um die Druckdatenübertragung vollständig zu verschlüsseln, empfehlen wir den Übertragungsweg zwischen primos und Drucker über eine IPPS-Verbindung zu sichern ⇨🗎25.

## 5.7 Wie kontrolliere ich, wer drucken darf?

Sie können den Zugriff auf Queues und damit das Drucken über den zugehörigen Drucker einschränken. Dafür wird eine Benutzerauthentifizierung verwendet, d.h. vor dem Drucken muss auf dem iOS-Gerät ein Benutzername und das zugehörige Passwort eingeben werden. Ohne Benutzername und Passwort kann folglich nicht von iOS-Geräten gedruckt werden.

**Hinweis**

Queues mit eingeschränkten Druckberechtigungen sind auf iOS-Geräten durch das Symbol gekennzeichnet.

**Hinweis**

iOS-Geräte speichern Benutzername und Passwort automatisch; die Abfrage erfolgt nur, wenn zum ersten mal über die Queue gedruckt wird.

**Funktionsweise**

Die Benutzerauthentifizierung wird für jede Queue einzeln eingerichtet. Die Benutzer können auf zwei Arten eingetragen werden:

- als lokale Benutzer (⇨🗎21) oder
- über einen Verzeichnisdienst (Active Directory oder LDAP) ⇨🗎17

Um die Eingabe von vielen Benutzern zu vereinfachen, können sie in Gruppen (lokal ⇨🗎22 oder im Verzeichnisdienst) zusammengefasst werden. Anschließend werden die Gruppen anstelle der einzelnen Benutzer eingetragen.

Die Benutzer-Einschränkung kann ebenfalls auf zwei Arten eingerichtet werden:

- Zugriff für alle Benutzer: Alle lokalen Benutzer/Gruppen bzw. Benutzer/Gruppen aus dem eingebundenen Verzeichnisdienst dürfen drucken.
- Eingeschränkter Zugriff: Druckberechtigte Benutzer/Gruppen werden über Listen definiert.
  - Liste 'Zulassen': Nur Benutzer/Gruppen in der Liste dürfen drucken.
  - Liste 'Verweigern': Benutzer/Gruppen aus der Liste dürfen nicht drucken. Alle anderen Benutzer/Gruppen dürfen drucken.

**Voraussetzung**

✓ Es ist eine Queue im primos erstellt ⇨🗎25.

✓ primos ist in einen Verzeichnisdienst eingebunden (⇨🗎17) wo Benutzer und/oder Gruppen eingerichtet sind.
Oder:
Lokale Benutzer sind eingerichtet (⇨🗎21) und ggf. in Gruppen zusammengefasst (⇨🗎22).

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **DRUCKEN - Queues** an.
3. Wählen Sie die gewünschte Queue über das Symbol aus.
4. Aktivieren Sie die Option **Benutzerauthentifizierung**.
5. Wählen Sie die Art der Einschränkung:
   - Zugriff für alle Benutzer: Alle lokalen Benutzer/Gruppen bzw. Benutzer/Gruppen aus dem eingebundenen Verzeichnisdienst dürfen drucken.
   - Eingeschränkter Zugriff: Druckberechtigte Benutzer/Gruppen werden über Listen definiert.
6. Sofern Sie den eingeschränkten Zugriff definiert haben, wählen Sie den **Listentyp**.
   - 'Zulassen': Nur Benutzer/Gruppen in der Liste dürfen drucken.
   - 'Verweigern': Benutzer/Gruppen aus der Liste dürfen nicht drucken. Alle anderen Benutzer/Gruppen dürfen drucken.

   Tragen Sie anschließend im Feld **Benutzer/Gruppe der Liste hinzufügen** die gewünschten Benutzer und Gruppen ein und bestätigen Sie mit **Hinzufügen**. Hinweise zur Eingabe:
   - Mehrere Benutzer und/oder Gruppen sind durch Komma getrennt einzugeben.
   - Benutzereingabe: lokalerBenutzername bzw. Domänenname\Benutzername
   - Gruppeneingabe: @lokalerGruppenname bzw. @Domänenname\Gruppenname
7. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

## 5.8 Wie drucke ich von einem iOS-Gerät?

Drucken Sie Inhalte wie Dokumente und Bilder von iOS-Geräten (iPhone, iPad usw.) einfach und flexibel. Druckaufträge werden dazu aus iOS-Apps mit AirPrint-Unterstützung über Ihr Netzwerk an primos gesendet. primos leitet den Druckauftrag zur Ausgabe an den Drucker weiter.

**Hinweis**

Sind die Druckberechtigungen eingeschränkt (⇨🗎36), werden vor dem Drucken Benutzername und Passwort auf dem iOS-Gerät abgefragt. iOS-Geräte speichere diese Informationen automatisch; die Abfrage erfolgt nur, wenn zum ersten mal über die Queue gedruckt wird.

**Voraussetzung**

- ✓ Für den Drucker ist im primos eine Queue angelegt ⇨🗎25.
- ✓ Ihr iOS-Gerät ist über WLAN mit dem Netzwerk verbunden.
- ✓ Ihr iOS-Gerät unterstützt AirPrint.
- ✓ Die gewählte App unterstützt AirPrint.

1. Öffnen Sie auf Ihrem iOS-Gerät die App, aus der Sie drucken möchten.
2. Wählen Sie den Inhalt aus, den Sie drucken möchten.
3. Öffnen Sie das Druckmenü.
4. Tippen Sie **Drucker** an.
   Alle verfügbaren Drucker werden angezeigt. Über primos verfügbar gemachte Drucker sind standardmäßig gekennzeichnet durch den AirPrint-Identifier ⇨🗎34.
5. Wählen Sie aus der Liste den gewünschten Drucker aus.
6. Definieren Sie die Druckeinstellungen, z.B. die Anzahl der Kopien.
7. Tippen Sie **Drucken** an.

↳ Der Inhalt wird gedruckt.

Während des Druckvorgangs können Sie auf Ihrem iOS-Gerät in der Druckzentrale den Status einsehen. Um die Druckzentrale aufzurufen, klicken Sie zweimal auf die Home-Taste und tippen auf **Druckzentrale**.

## 5.9 Wie drucke ich über Subnetze hinweg? (Wide-Area AirPrint)

AirPrint nutzt das Bonjour-Protokoll (⇨16), um Drucker im Netzwerk zu finden und verfügbar zu machen.

Bonjour ist jedoch beschränkt auf lokale Netzwerksegmente. Sie müssen primos so konfigurieren, dass das Suchen und Finden von Druckern über Netzwerksegmente hinweg möglich ist. Dann können Sie im gesamten Netzwerk drucken. Befolgen Sie die unten aufgeführten Punkte in der angegebenen Reihenfolge.

**Vorgehensweise**

- Aktivieren Sie auf primos Wide-Area AirPrint: 'Wide-Area AirPrint auf primos konfigurieren' ⇨40.
- Definieren Sie eine Unterdomäne für primos, z.B. primos.mydomain.com. Tragen Sie diese Unterdomäne auf dem primos ein: 'Wide-Area AirPrint auf primos konfigurieren' ⇨40.

**Warnung**

**Die primos Unterdomäne darf nicht mit '.local' enden. Diese Domain ist reserviert für Multicast-Bonjour (mDNS).**

- Definieren Sie auf primos die Drucker, die über Wide-Area AirPrint genutzt werden sollen: 'Wide-Area AirPrint auf primos konfigurieren' ⇨40.
- Optional können Sie den Standardmechanismus zum Veröffentlichen von Queues, die Multicast-Veröffentlichung, im Netzwerk deaktivieren. Drucker werden dann ausschließlich über Wide-Area AirPrint veröffentlicht. Siehe 'Wide-Area AirPrint auf primos konfigurieren' ⇨40.
- Konfigurieren Sie auf Ihrem DNS-Server eine bedingte Weiterleitung. Anfragen welche die primos Unterdomäne enthalten müssen an primos weitergeleitet werden: ⇨40.
- Weisen Sie die iOS-Geräte, die Wide-Area AirPrint nutzen sollen an, Drucker in der primos Unterdomäne zu suchen und zu finden. Dazu muss die primos Unterdomäne als Suchdomäne auf den iOS-Geräten eingetragen werden. Dies kann manuell auf jedem iOS-Gerät einzeln oder automatisch auf allen iOS-Geräten in der Domäne erfolgen:
  - 'primos Unterdomäne als Suchdomäne automatisch auf iOS-Geräten konfigurieren' ⇨41
  - 'primos Unterdomäne als Suchdomäne manuell auf iOS-Geräten konfigurieren' ⇨43

Wide-Area AirPrint auf primos konfigurieren

**Voraussetzung**

- ✓ In Ihrem Netzwerk wird ein DNS-Server betrieben.
- ✓ Im primos ist ein DNS konfiguriert ⇨🗎15.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **DRUCKEN - Einstellungen** an.
3. Konfigurieren Sie die Wide-Area AirPrint-Parameter; Tabelle 9 ⇨🗎40.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

Tabelle 9: Wide-Area AirPrint-Parameter

| Parameter | Beschreibung |
|---|---|
| Wide-Area AirPrint | De-/aktiviert Wide-Area AirPrint. |
| primos Unterdomäne | Wide-Area AirPrint Domänenname, für den auf dem DNS-Server eine bedingte Weiterleitung zum primos konfiguriert ist. |
| Drucker, die über Wide-Area AirPrint veröffentlicht werden | Definiert die Drucker, die via Wide-Area AirPrint genutzt werden können. |
| Multicast-Veröffentlichung | De-/aktiviert die Standard-Veröffentlichung von Queues im Netzwerk (via Multicast).<br>*Deaktivieren Sie die Option, werden Drucker ausschließlich über Wide-Area AirPrint verfügbar gemacht.* |

Bedingte Weiterleitung auf DNS-Server konfigurieren

Die Konfiguration wird beispielhaft für Windows Server 2012 beschrieben.

**Voraussetzung**

- ✓ Auf primos ist Wide-Area AirPrint konfiguriert ⇨🗎40.
- ✓ In Ihrem Netzwerk wird ein DNS-Server betrieben.
- ✓ Sie sind als Administrator auf dem Windows Server 2012 angemeldet.

1. Starten Sie den **DNS Manager**.
2. Rechtsklicken Sie auf **Bedingte Weiterleitung** und wählen Sie im Kontextmenü **Neue bedingte Weiterleitung**.
   Der Dialog **Neue bedingte Weiterleitung** erscheint.
3. Geben Sie im Feld **DNS-Domäne** die primos Unterdomäne ein.
4. Geben Sie im Bereich **IP-Adressen der Masterserver** im Feld **IP-Adresse** die IPv4-Adresse von primos ein.
   Windows Server 2012 überprüft Ihre Eingaben. Nach erfolgreicher Prüfung erscheint ein grünes Häkchen und die Schaltfläche 'OK' kann angewählt werden.
5. Bestätigen Sie mit **OK**.

↳ Die bedingte Weiterleitung wird gespeichert.

primos Unterdomäne als Suchdomäne automatisch auf iOS-Geräten konfigurieren

Die primos Unterdomäne kann mit Hilfe Ihres DHCP-Servers automatisch als Suchdomäne auf allen iOS-Geräten eingetragen werden. Dazu wird die primos Unterdomäne auf dem DHCP-Server mit der Option 119 eingetragen. Sobald ein iOS-Gerät eine Anfrage an den DHCP-Server stellt, wird ihm automatisch die primos Unterdomäne als Suchdomäne mitgeteilt. Das iOS-Gerät speichert diese Information automatisch.

**Vorbereitung**

Die Konfiguration wird am Beispiel von Windows Server 2012 beschrieben. Auf dem DHCP-Server von Windows 2012 müssen Unterdomänen für die Option 119 in codierter Form (gemäß RFC 3397) eingetragen werden. Da diese Codierung komplex ist, steht im primos Control Center ein Tool zur Umwandlung zur Verfügung. Geben Sie Ihren IPv4-DHCP-Bereich und Ihre primos Unterdomäne dort ein, erhalten Sie einen Kommandozeilen-Befehl, der Ihre primos Unterdomäne in codierter Form und Ihren IPv4-DHCP-Bereich enthält:

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **WARTUNG - SERVICE** an.
3. Geben Sie im Bereich **DHCP-Option 119** im Feld **DHCP-Bereich** Ihren IPv4-DHCP-Bereich ein.
4. Geben Sie im Bereich **DHCP-Option 119** im Feld **primos Unterdomäne** Ihre primos Unterdomäne ein.

↳ Im Feld **Befehl** werden die Kommandozeilen-Befehle angezeigt. Sichern Sie die Kommandozeilen-Befehle (z.B. in einem Textdokument oder in der Zwischenablage).

**Konfiguration**

Die grafischen Benutzeroberflächen von Windows-Servern bieten keine benutzerfreundliche Konfigurationsmöglichkeit für die DHCP-Option 119. Nachfolgend wird die Konfiguration auf Windows Server 2012 daher via Kommandozeile beschrieben.

**Beispiel**

Um die Konfiguration zu verdeutlichen, verwenden wir folgendes Beispiel.

Ihre primos Unterdomäne heißt: primos.mydomain.com

Ihr IPv4-DHCP-Bereich ist: 10.168.0.0

Kommandozeilenbefehle:

```
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
```

**Hinweis**

Die ersten beiden Zeilen dienen nur der Information und sind daher mit 'REM' als Kommentar gekennzeichnet und von der Verarbeitung ausgeschlossen.

**Voraussetzung**

- ✓ Auf primos ist Wide-Area AirPrint konfiguriert ⇨🗎40.
- ✓ In Ihrem Netzwerk wird ein DNS-Server betrieben.
- ✓ Auf Ihren DNS-Server ist eine bedingte Weiterleitung zur primos Unterdomäne konfiguriert ⇨🗎40.
- ✓ In Ihrem Netzwerk wird ein DHCP-Server betrieben.
- ✓ Sie sind als Administrator auf dem Windows Server 2012 angemeldet.
- ✓ *Sie verfügen über den Kommandozeilen-Befehl; siehe: 'Vorbereitung'* ⇨🗎41.

1. Starten Sie die Eingabeaufforderung.
   Das Fenster **Administrator: Eingabeauffoderung** erscheint.
2. Führen Sie nacheinander die in der Vorbereitung erstellten Kommandozeilenbefehle aus.
   Beispiel:
   ```
   netsh dhcp server V4 delete optiondef 119
   ```
   (Löscht eine eventuell bereits konfigurierte Option 119.)
   ```
   netsh dhcp server V4 add optiondef 119 "DNS Search Path" BYTE 1
   ```
   (Aktiviert 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
   ```
   (Konfiguriert Option 119.)
   Nach jeder Eingabe wird das erfolgreiche Ausführen des jeweiligen Befehls bestätigt.

↳ Die primos Unterdomäne ist als Suchdomäne auf dem DHCP-Server mit der Option 119 eingetragen. Der DHCP-Server trägt die primos Unterdomäne automatisch als Suchdomäne auf allen iOS-Geräten ein.

Prüfen Sie, dass der Eintrag auf dem DHCP-Server erscheint. Starten Sie dafür den DHCP-Server und prüfen Sie, ob der Eintrag unter **<Ihre Domain>** - **IPv4** - **<Bereich>** - **Bereichsoptionen** erscheint. Aktualisieren Sie gegebenenfalls die Anzeige.

primos Unterdomäne als Suchdomäne manuell auf iOS-Geräten konfigurieren

Sie können die primos Unterdomäne als Suchdomäne direkt auf Ihrem iOS-Gerät eintragen.

**Voraussetzung**

- ✓ Auf primos ist Wide-Area AirPrint konfiguriert ⇨🗎40.
- ✓ In Ihrem Netzwerk wird ein DNS-Server betrieben.
- ✓ Auf Ihren DNS-Server ist eine bedingte Weiterleitung zur primos Unterdomäne konfiguriert ⇨🗎40.

1. Öffnen Sie auf Ihrem iOS-Gerät das Menü **Einstellungen**.
2. Wählen Sie den Menüpunkt **WLAN** an.
   Das WLAN-Menü wird angezeigt.
3. Wählen Sie Ihr WLAN aus der Liste aus.
   Die WLAN-Einstellungen werden angezeigt.
4. Wählen Sie die Option **Such-Domains** an.
   Die Eingabe-Tastatur erscheint.
5. Fügen Sie die primos Unterdomäne hinzu.
   **(Mehrere Such-Domains sind durch Komma zu separieren.)**
6. Blenden Sie die Tastatur aus.

↳ Die primos Unterdomäne ist als Suchdomäne auf dem iOS-Gerät konfiguriert. Das iOS-Gerät sucht und findet Drucker in der primos Unterdomäne.

# 6 Sicherheit

Um beim Einsatz von primos eine hohe Sicherheit gewährleisten zu können, stehen primos verschiedene Schutzmechanismen zur Verfügung. In diesem Kapitel erfahren Sie, wie die Schutzmechanismen sinnvoll eingesetzt und realisiert werden.

**Welche Information benötigen Sie?**

## 6.1 Wie definiere ich die Verschlüsselungsstärke für SSL-/TLS-Verbindungen?

Sie können folgende Verbindungen am primos via SSL/TLS verschlüsseln:

- Webzugang zum primos Control Center: HTTPS (⇨47)
- Druckdatenübertragung: IPPS und Sicheres AirPrint (⇨35)

**Verschlüsselungsstärke**

Die Stärke der Verschlüsselung und damit die Sicherheit der Verbindung wird über das Verschlüsselungsprotokoll und die Verschlüsselungsstufe definiert.

**Protokoll**

Zur Verschlüsselung der Verbindung werden die Verschlüsselungsprotokolle SSL (Secure Sockets Layer) und dessen Nachfolger TLS (Transport Layer Security) verwendet.

**Verschlüsselungsstufe**

Jede Verschlüsselungsstufe stellt eine Sammlung sog. Cipher Suites dar. Eine Cipher Suite ist eine standardisierte Folge aus vier kryptografischen Algorithmen, die zum Aufbau einer sicheren Verbindung verwendet werden. Cipher Suites werden gemäß ihrer Verschlüsselungsstärke zu einer Verschlüsselungsstufe zusammengefasst. Welche Cipher Suites von primos unterstützt werden, also Teil einer Verschlüsselungsstufe sind, hängt vom verwendeten SSL-/TLS-Protokoll ab.Folgende Verschlüsselungsstufen sind wählbar:

- **Beliebig**: Die Verschlüsselung wird zwischen beiden Parteien automatisch ausgehandelt. Dabei wird immer die stärkste Verschlüsselung gewählt, die beide Parteien unterstützen.
- **Normal**
- **Hoch**: Es werden nur Cipher Suites mit einer starken Verschlüsselung verwendet. (Langsame Übertragung)

**Verbindungsaufbau**

Beim Aufbau einer sicheren Verbindung wird das zu verwendende Protokoll sowie eine Liste von unterstützten Cipher Suites an den Kommunikationspartner gesendet. Es wird eine Cipher Suite ausgehandelt, die im Weiteren verwendet wird. Standardmäßig handelt es sich um die stärkste von beiden Parteien unterstützte Cipher Suite. Unterstützt der Kommunikationspartner das gewählte Protokoll nicht und/oder gibt es keine von beiden Seiten unterstützte Cipher Suite, wird keine SSL-/TLS-Verbindung aufgebaut.

**Warnung**

**Die Kommunikationspartner von primos (z.B. Browser) müssen das Verschlüsselungsprotokoll und die Cipher Suites der gewählten Verschlüsselungsstufe für einen erfolgreichen Verbindungsaufbau unterstützen. Bei Problemen wählen Sie andere Einstellungen oder setzen die Parameter von primos zurück; siehe: ⇨65.**

Wählen Sie für das Verschlüsselungsprotokoll und die Verschlüsselungsstufe die Option 'Beliebig', werden beide Einstellungen zwischen primos und dem Kommunikationspartner automatisch ausgehandelt. Mit diesen Einstellungen sind die Chancen für einen erfolgreichen Verbindungsaufbau am größten.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT - SSL-Verbindungen** an.
3. Wählen Sie im Bereich **Verschlüsselungsprotokoll** das gewünschte Protokoll.

**Warnung**

**Verwenden Sie nicht das Verschlüsselungsprotokoll 'SSL', wenn Sie aktuelle Browser-Software nutzen und für den Webzugang zum primos Control Center ausschließlich HTTPS als erlaubter Verbindungstyp definiert ist. Aktuelle Browser unterstützen SSL nicht, somit kann keine Verbindung aufgebaut werden.**

4. Wählen Sie im Bereich **Verschlüsselungsstufe** die gewünschte Verschlüsselungsstufe.

**Warnung**

**Verwenden Sie nicht die Verschlüsselungsstufe 'Niedrig', wenn Sie aktuelle Browser-Software nutzen und für den Webzugang zum primos Control Center ausschließlich HTTPS als erlaubter Verbindungstyp definiert ist. Aktuelle Browser unterstützen Cipher Suites der Stufe 'Niedrig' nicht, somit kann keine Verbindung aufgebaut werden.**

5. Bestätigen Sie mit **Speichern**.

↳ Die Einstellung wird gespeichert.

## 6.2 Wie verschlüssele ich die Verbindung zum primos Control Center?

Der Webzugang zum primos Control Center kann durch die Wahl der erlaubten Verbindungstypen (HTTP/HTTPS) geschützt werden.

Wird ausschließlich HTTPS als Verbindungstyp gewählt, ist der administrative Webzugang zum primos Control Center via SSL/TLS geschützt. Die Verschlüsselungsstärke wird über Protokoll und Verschlüsselungsstufe definiert ⇨🗎45.

**Hinweis**

Beim Anmelden am primos Control Center (⇨🗎48) wird das Passwort im Klartext übertragen. Wir empfehlen, als Verbindungstyp nur HTTPS zu verwenden.

Bei SSL/TLS wird ein Zertifikat benötigt, um die Identität von primos zu überprüfen. Bei einem so genannten 'Handshake' fragt der Client via Browser nach einem Zertifikat. Dieses Zertifikat muss vom Browser akzeptiert werden; lesen Sie hierzu die Dokumentation Ihrer Browsersoftware. URLs, die eine SSL-/TLS-Verbindung erfordern, beginnen mit 'https'.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT - Gerätezugriff** an.
3. Aktivieren Sie im Bereich **Verbindung** die Option **HTTP/HTTPS** bzw. **Nur HTTPS**.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellung wird gespeichert.

## 6.3 Wie verwalte ich Benutzerprofile? (Zugriffskontrolle)

Der Zugriff auf das primos Control Center wird über Benutzerprofile reglementiert. Der Zugang erfolgt über einen Benutzernamen in Kombination mit einem Passwort.

**Hinweis**

Beim Anmelden wird das Passwort im Klartext übertragen. Wir empfehlen, die Verbindung zum primos Control Center zu verschlüsseln (HTTPS ⇨🗎47).

**Lokaler Administrator**

Der Zugang zum primos Control Center ist jederzeit über ein lokales Administrator-Benutzerprofil möglich. Dieser lokale Administrator kann nicht gelöscht und der Benutzername nicht geändert werden.

Benutzername: admin

Passwort: admin

Das Kennwort für das Administrator-Benutzerprofil kann geändert werden.

**Hinweis**

Ändern Sie das voreingestellte Passwort sobald wie möglich!

**Verzeichnis-dienst**

Sie können primos in einen Verzeichnisdienst (Active Directory oder LDAP) einbinden ⇨🗎17. Dort angelegte Benutzer können zum Anmelden am primos Control Center genutzt werden. Dazu müssen Sie auf primos eingetragen werden. Die eingetragenen Verzeichnisdienst-Benutzer können sich dann mit ihrem Verzeichnis-Benutzernamen und -Passwort am primos Control Center authentisieren.

**Hinweis**

Nur System-Administratoren sollten Zugriff auf das primos Control Center haben, weil dort sicherheitsrelevante Einstellungen vorgenommen werden.

**Sitzungs-Timeout**

Über ein Sitzungs-Timeout können Sie definieren, dass die Verbindung zum primos Control Center aus Sicherheitsgründen beendet wird, wenn innerhalb eines definierten Zeitraums keine Benutzeraktivität stattfindet. Ein angemeldeter Benutzer wird ausgeloggt und muss sich am primos neu anmelden.

**Logout**

Aus Sicherheitsgründen sollten Sie sich am primos Control Center abmelden nachdem Sie Ihre Einstellungen vorgenommen haben ⇨🗎9.

**Was möchten Sie tun?**

- ☐ 'Passwort des lokalen Administrators ändern' ⇨🗎49
- ☐ 'Verzeichnisdienst-Benutzer-Anmeldung konfigurieren' ⇨🗎49
- ☐ 'Sitzungs-Timeout konfigurieren' ⇨🗎49

Passwort des lokalen Administrators ändern

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT - Gerätezugriff** an.
3. Geben Sie im Feld **Passwort** ein Kennwort ein.
4. Wiederholen Sie die Kennworteingabe.
5. Bestätigen Sie mit **Speichern**.

↳ Die Einstellung wird gespeichert.

Verzeichnisdienst-Benutzer-Anmeldung konfigurieren

**Voraussetzung**

✓ primos ist in einen Verzeichnisdienst eingebunden ⇨🗎17.
✓ Im Verzeichnisdienst sind Benutzer angelegt.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT - Gerätezugriff** an.
3. Geben Sie im Feld **Benutzer, die auf dieses Gerät zugreifen können** die Verzeichnisdienst-Benutzer ein, die sich am primos Control Center anmelden können.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

Sitzungs-Timeout konfigurieren

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT - Gerätezugriff** an.
3. Aktivieren Sie die Option **Sitzungs-Timeout**.
4. Geben Sie im Feld **Sitzungsdauer** den Zeitraum in Minuten ein, nach dem das Timeout wirksam werden soll.

↳ Die Einstellung wird gespeichert.

## 6.4 Wie schütze ich primos vor Cross-Site-Scripting-Angriffen?

**Was ist Cross-Site-Scripting?**

Cross-Site-Scripting (XSS) ist eine Form des Angriffs, bei dem eine Sicherheitslücke in Webseiten ausgenutzt wird: Standardmäßig werden Benutzereingaben auf einer Webseite ohne eine Überprüfung an den Browser übermittelt. Ein Angreifer kann dies ausnutzen, um Schadcode (z.B. Skripte) zu übermitteln. Ziel ist zum Beispiel, Benutzerdaten wie etwa Benutzerprofile zu ermitteln.

Um Cross-Site-Scripting-Angriffe zu verhindern, können Werte die im primos Control Center eingegeben werden geprüft und nur vertrauenswürdige Werte angenommen werden.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT - Gerätezugriff** an.
3. De/-aktivieren Sie im Bereich **Cross-Site-Scripting (XSS)** die Option **Werte prüfen**.

↳ Die Einstellung wird gespeichert.

## 6.5 Wie kontrolliere ich den Zugriff auf primos? (TCP-Portzugriffskontrolle)

**TCP-Portzugriffs-kontrolle**

Sie haben die Möglichkeit, den Zugriff auf primos zu kontrollieren. Hierzu können alle TCP-Ports am primos gesperrt werden. Zugriffsberechtigte Netzwerkelemente können als Ausnahme definiert und von der Sperrung ausgenommen werden. primos akzeptiert dann nur Datenpakete von den als Ausnahme definierten Netzwerkelementen. Beachten Sie: Dies gilt auch für iOS-Geräte. Ist die TCP-Portzugriffskontrolle aktiv, kann nur von iOS-Geräten gedruckt werden, die als Ausnahme definiert sind.

**Ausnahmen**

Um Netzwerkelemente (z.B. iOS-Geräte, Clients, DNS-Server, SNTP-Server) von einer Portsperrung auszuschließen, müssen diese als Ausnahme definiert werden. Hierzu werden im Bereich 'Ausnahmen' die IP-Adressen oder MAC-Adressen (Hardware-Adressen) der zugriffsberechtigten Netzwerkelemente eingegeben. Beachten Sie:

- MAC-Adressen werden nicht über Router weitergeleitet!
- Adressbereiche können mit der CIDR-Notation definiert werden.

Drucker für die eine Queue im primos angelegt ist, sind automatisch von der Portsperrung ausgenommen.

**Testmodus**

Der 'Testmodus' bietet die Möglichkeit, den eingestellten Zugriffsschutz zu überprüfen. Bei aktiviertem Testmodus bleibt der Zugriffsschutz bis zum Neustart von primos aktiv. Nach dem Neustart ist der Schutz nicht mehr wirksam.

Die Option 'Testmodus' ist voreingestellt aktiv. Nach einem erfolgreichen Test müssen Sie den Testmodus deaktivieren, damit der Zugriffsschutz dauerhaft aktiv bleibt.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT - TCP-Portzugriff** an.
3. Aktivieren Sie die Option **Portzugriff kontrollieren**.
4. Definieren Sie im Bereich **Ausnahmen** die Netzwerkelemente, die von der Portsperrung ausgeschlossen sind. Geben Sie hierzu die IP- oder MAC-Adressen ein und aktivieren Sie die Optionen.
5. Stellen Sie sicher, dass der Testmodus aktiviert ist.
6. Bestätigen Sie mit **Speichern**.
   Die Einstellungen werden gespeichert.
   Die Portzugriffskontrolle ist bis zum Geräte-Neustart aktiv.
7. Überprüfen Sie den Portzugriff und die Konfigurationsfähigkeit von primos.

**Hinweis**

Kann primos über das primos Control Center nicht mehr erreicht werden, initiieren Sie einen Geräte-Neustart (⇨🗎67).

8. Deaktivieren Sie den **Testmodus**.
9. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert. Die Portzugriffskontrolle ist aktiv. Der Zugriff auf die Ports ist geschützt.

## 6.6 Wie setze ich Zertifikate korrekt ein?

primos verfügt über eine eigene Zertifikatsverwaltung. Dieser Abschnitt informiert Sie über die Anwendung von Zertifikaten und Sie erfahren, in welchen Situationen ein Einsatz sinnvoll ist.

**Was sind Zertifikate?**

Zertifikate können in TCP/IP-basierten Netzwerken verwendet werden, um Daten zu verschlüsseln und Kommunikationspartner zu authentifizieren. Zertifikate sind elektronische Nachrichten, die einen Schlüssel (Public Key) sowie eine Signatur enthalten.

**Nutzen und Zweck**

Mit dem Einsatz von Zertifikaten werden mehrere Sicherheitsmechanismen realisiert. Verwenden Sie Zertifikate im primos,

- um die Identität von primos im Netzwerk überprüfen zu lassen (⇨ 59).
- um den Client zu authentifizieren, wenn Verbindung zum primos Control Centers via HTTPS (SSL/TLS) geschützt ist (⇨ 47).
- um Druckdaten zu verschlüsseln (IPPS und Sicheres AirPrint ⇨ 35).

**Welche Zertifikate gibt es?**

Im primos können sowohl selbstsignierte Zertifikate als auch fremdsignierte Zertifikate verwendet werden. Es werden die folgenden Zertifikate unterschieden:

- Bei Auslieferung ist im primos ein Zertifikat gespeichert, das sog. **Default-Zertifikat**. Sie sollten das Default-Zertifikat zeitnah durch ein selbstsigniertes oder ein angefordertes Zertifikat ersetzen.
- **Selbstsignierte Zertifikate** tragen eine digitale Unterschrift, die vom primos erstellt wurde.
- Ein **angefordertes Zertifikat** wird auf Basis einer Zertifikatsanforderung von einer Zertifizierungsstelle (Certification Authority - CA) für primos erstellt.
- **CA-Zertifikate** sind Zertifikate, die für eine Zertifizierungsstelle (Certification Authority - CA) ausgestellt wurden. Mit ihnen werden Zertifikate überprüft, die von der jeweiligen Zertifizierungsstelle ausgegeben wurden.

Im primos können folgende Zertifikate zeitgleich installiert sein:

- 1 Selbstsigniertes Zertifikat
- 1 Client-Zertifikat, d.h. 1 angefordertes Zertifikat ODER 1 PKCS#12-Zertifikat
- 1 bis 32 CA-Zertifikate

Alle Zertifikate können separat gelöscht werden.

**Was möchten Sie tun?**

- ☐ 'Zertifikat anzeigen' ⇨🗎53
- ☐ 'Selbstsigniertes Zertifikat erstellen' ⇨🗎53
- ☐ 'Zertifikatsanforderung für ein angefordertes Zertifikat erstellen' ⇨🗎54
- ☐ 'Angefordertes Zertifikat im primos speichern' ⇨🗎55
- ☐ 'PKCS#12-Zertifikat im primos speichern' ⇨🗎55
- ☐ 'CA-Zertifikat im primos speichern' ⇨🗎56
- ☐ 'Zertifikat löschen' ⇨🗎57

Zertifikat anzeigen

Im primos installierte Zertifikate oder Zertifikatsanforderungen können dargestellt und eingesehen werden.

**Voraussetzung**

✓ Im primos ist ein Zertifikat installiert.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT - Zertifikate** an.
3. Wählen Sie das Zertifikat über das Symbol 🔍 aus.

↳ Das Zertifikat wird angezeigt.

Selbstsigniertes Zertifikat erstellen

**Hinweis**

Ist bereits ein selbstsigniertes Zertifikat im primos erstellt worden, muss dieses zunächst gelöscht werden (⇨🗎57).

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT - Zertifikate** an.
3. Wählen Sie die Schaltfläche **Selbstsigniertes Zertifikat** an.
4. Geben Sie die entsprechenden Parameter ein; Tabelle 10 ⇨🗎54.
5. Wählen Sie die Schaltfläche **Erstellen/Installieren** an.

↳ Das Zertifikat wird erstellt und installiert. Dieser Vorgang kann einige Minuten dauern.

Tabelle 10: Parameter für die Erstellung von Zertifikaten

| Parameter | Beschreibung |
|---|---|
| Allgemeiner Name | Dient der eindeutigen Identifizierung des Zertifikats. Es empfiehlt sich, hier z.B. die IP-Adresse oder den Hostnamen von primos zu verwenden, um eine eindeutige Zuordnung des Zertifikats zu primos zu ermöglichen.<br>*Maximal 64 Zeichen können eingegeben werden.* |
| E-Mail-Adresse | Gibt eine E-Mail-Adresse an.<br>*Maximal 40 Zeichen können eingegeben werden.*<br>*(Optionale Eingabe)* |
| Organisation | Gibt den Namen der Firma an, die primos einsetzt.<br>*Maximal 64 Zeichen können eingegeben werden.* |
| Unternehmensbereich | Gibt die Abteilung oder eine Untergruppe der Firma an.<br>*Maximal 64 Zeichen können eingegeben werden.*<br>*(Optionale Eingabe)* |
| Ort | Gibt den Ort an, an dem die Firma ansässig ist.<br>*Maximal 64 Zeichen können eingegeben werden.* |
| Bundesland | Gibt den Namen des Bundeslandes an, in dem die Firma ansässig ist.<br>*Maximal 64 Zeichen können eingegeben werden.*<br>*(Optionale Eingabe)* |
| Domain-Komponente | Ermöglicht das Eintragen weiterer Attribute.<br>*(Optionale Eingabe)* |
| Land | Gibt das Land an, in dem die Firma ansässig ist. Geben Sie das zweistellige Länderkürzel gemäß ISO 3166 ein. Beispiele:<br>DE = Deutschland, GB = Großbritannien, US = USA |
| Endet am | Gibt das Datum an, an dem das Zertifikat ungültig wird. |
| RSA-Schlüssellänge | Definiert die Länge des verwendeten RSA-Schlüssels:<br>- 512 Bit (schnelle Ver- und Entschlüsselung)<br>- 768 Bit<br>- 1024 Bit (standardmäßige Ver- und Entschlüsselung)<br>- 2048 Bit (langsame Ver- und Entschlüsselung) |

### Zertifikatsanforderung für ein angefordertes Zertifikat erstellen

Als Vorbereitung auf das Verwenden eines Zertifikats, das von einer Zertifizierungsstelle für primos ausgestellt wird, kann im primos eine Zertifikatsanforderung erstellt werden. Die Anforderung muss an die Zertifizierungsstelle gesendet werden, welche anhand der Zertifikatsanforderung ein Zertifikat erstellt. Das Zertifikat muss im 'Base64'-Format vorliegen.

**Hinweis**

Ist bereits eine Zertifikatsanforderung erstellt, muss diese zunächst gelöscht werden (⇨🗎57).

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT - Zertifikate** an.
3. Wählen Sie die Schaltfläche **Zertifikatsanforderung** an.
4. Geben Sie die benötigten Parameter ein; Tabelle 10 ⇨🗎54.
5. Wählen Sie die Schaltfläche **Anforderung erstellen** an.
   Die Zertifikatsanforderung wird erstellt. Dieser Vorgang kann einige Minuten dauern.
6. Wählen Sie die Schaltfläche **Upload** an und speichern Sie die Anforderung in einer Textdatei.
7. Wählen Sie die Schaltfläche **OK** an.
8. Senden Sie die Textdatei als Zertifikatsanforderung an eine Zertifizierungsstelle.

Nach Erhalt muss das angeforderte Zertifikat im primos gespeichert werden ⇨🗎55.

Angefordertes Zertifikat im primos speichern

**Voraussetzung**

- ✓ Es wurde zuvor eine entsprechende Zertifikatsanforderung erstellt ⇨🗎54.
- ✓ Das Zertifikat muss im 'Base64'-Format vorliegen.

**Hinweis**

Ist bereits ein PKCS#12-Zertifikat installiert, muss dieses zunächst gelöscht werden (⇨🗎57).

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT - Zertifikate** an.
3. Wählen Sie die Schaltfläche **Angefordertes Zertifikat** an.
4. Wählen Sie die Schaltfläche **Durchsuchen** an.
5. Geben Sie das angeforderte Zertifikat an.
6. Wählen Sie die Schaltfläche **Installieren** an.

↳ Das angeforderte Zertifikat wird im primos gespeichert.

PKCS#12-Zertifikat im primos speichern

Zertifikate im PKCS#12-Format werden verwendet, um private Schlüssel mit dem zugehörigen Zertifikat passwortgeschützt zu speichern.

**Hinweis**

Ist bereits ein PKCS#12-Zertifikat oder ein angefordertes Zertifikat im primos installiert, muss dieses zunächst gelöscht werden (⇨🗎57).

**Voraussetzung**

✓ Das Zertifikat muss im 'Base64'-Format vorliegen.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT - Zertifikate** an.
3. Wählen Sie die Schaltfläche **PKCS#12-Zertifikat** an.
4. Wählen Sie die Schaltfläche **Durchsuchen** an.
5. Geben Sie das PKCS#12-Zertifikat an.
6. Geben Sie das Passwort ein.
7. Wählen Sie die Schaltfläche **Installieren** an.

↳ Das PKCS#12-Zertifikat wird im primos gespeichert.

CA-Zertifikat im primos speichern

Um in einem Netzwerk die Identität von Kommunikationspartnern von primos überprüfen zu können, ist es erforderlich, deren Zertifikate zu validieren. Hierzu werden die Wurzel-CA-Zertifikate von denjenigen Zertifizierungsstellen, die die Zertifikate der Kommunikationspartner ausgestellt haben im primos installiert.

Bis zu 32 CA-Zertifikate können installiert werden. Dadurch werden mehrstufige Public Key Infrastrukturen (PKI) unterstützt.

Beispiel: Um in einem Netzwerk die Identität von primos zu überprüfen, bietet primos mehrere Authentifizierungsverfahren an. Wenn Sie das Authentifizierungsverfahren 'EAP-TLS' (⇨🗎59) verwenden, ist es erforderlich, das Wurzel-CA-Zertifikat der Zertifizierungsstelle im primos zu installieren, die das Zertifikat für den Authentifizierungsserver (RADIUS) ausgegeben hat.

**Voraussetzung**

✓ Das Zertifikat muss im 'Base64'-Format vorliegen.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT - Zertifikate** an.
3. Wählen Sie die Schaltfläche **CA-Zertifikat** an.
4. Wählen Sie die Schaltfläche **Durchsuchen** an.
5. Geben Sie das CA-Zertifikat an.
6. Wählen Sie die Schaltfläche **Installieren** an.

↳ Das CA-Zertifikat wird im primos gespeichert.

Zertifikat löschen

**Warnung**

**Löschen Sie nicht das Zertifikat (CA/selbstsigniert/PKCS#12), wenn für die Verbindung zum primos Control Center ausschließlich HTTPS als erlaubter Verbindungstyp definiert ist. Wird das zugehörige Zertifikat gelöscht, kann das primos Control Center nicht mehr erreicht werden. Setzen Sie in diesem Fall die Konfigurationseinstellungen auf die Standardwerte zurück (⇨ 65).**

**Voraussetzung**

✓ Im primos ist ein Zertifikat installiert.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT - Zertifikate** an.
3. Wählen Sie das zu löschende Zertifikat über das Symbol 🔍 aus. Das Zertifikat wird angezeigt.
4. Wählen Sie die Schaltfläche **Löschen** an.

↳ Das Zertifikat wird gelöscht.

## 6.7 Wie verwende ich Authentifizierungsmethoden?

Durch Authentifizierung kann ein Netzwerk vor unautorisiertem Zugriff geschützt werden. primos kann an verschiedenen Authentifizierungsverfahren teilzunehmen. In diesem Abschnitt erfahren Sie, welche Verfahren unterstützt und wie diese im primos konfiguriert werden.

**Was ist IEEE 802.1X?**

Der Standard IEEE 802.1X stellt eine Grundstruktur für verschiedene Authentifizierungs- und Schlüsselverwaltungsprotokolle dar. IEEE 802.1X bietet die Möglichkeit, den Zugang zu Netzwerken zu kontrollieren. Bevor ein Benutzer über ein Netzwerkgerät Zugang zum Netzwerk erhält, muss dieser sich am Netzwerk authentisieren. Nach erfolgreicher Authentisierung wird der Zugang zum Netzwerk freigegeben.

**Was ist EAP?**

Dem Standard IEEE 802.1X liegt das EAP (Extensible Authentication Protocol) zugrunde. EAP ist ein universelles Protokoll für viele verschiedene Authentifizierungsverfahren. Das EAP ermöglicht einen standardisierten Authentifizierungsvorgang zwischen dem Netzwerkgerät und einem Authentifizierungsserver (RADIUS). Das zu verwendende Authentifizierungsverfahren TLS, PEAP, TTLS usw. muss zuvor definiert und bei allen beteiligten Netzwerkgeräten konfiguriert werden.

**Was ist RADIUS?**

RADIUS (Remote Authentication Dial-In User Service) ist ein Authentifizierungs- und Kontoverwaltungssystem, das Benutzeranmeldeinformation überprüft und Zugriff auf die gewünschten Ressourcen gewährt.

Damit primos sich an einem geschützten Netzwerk authentisieren kann, unterstützt das primos mehrere EAP-Authentifizierungsverfahren.

**Was möchten Sie tun?**

- ☐ 'EAP-MD5 konfigurieren' ⇨🗎59
- ☐ 'EAP-TLS konfigurieren' ⇨🗎59
- ☐ 'EAP-TTLS konfigurieren' ⇨🗎60
- ☐ 'PEAP konfigurieren' ⇨🗎61
- ☐ 'EAP-FAST konfigurieren' ⇨🗎62

EAP-MD5 konfigurieren

**Nutzen und Zweck**

Das EAP-MD5 überprüft die Identität von Geräten oder Benutzern, bevor diese Zugang zu Netzwerkressourcen haben. Damit primos in geschützten Netzwerken einen Zugriff erhält, können Sie primos für die EAP-MD5-Netzwerkauthentifizierung konfigurieren.

**Funktionsweise**

EAP-MD5 beschreibt eine benutzerbasierte Authentifizierung über einen RADIUS-Server. Hierzu wird primos auf dem RADIUS-Server als Benutzer (mit einem Benutzernamen und einem Passwort) angelegt. Anschließend wird das EAP-MD5-Authentifizierungsverfahren im primos aktiviert und die beiden Benutzerangaben (Benutzername und Passwort) werden eingegeben.

**Voraussetzung**

✓ Auf dem RADIUS-Server ist primos als Benutzer mit einem Benutzernamen und einem Passwort angelegt.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT - Authentifizierung** an.
3. Wählen Sie aus der Liste **Authentifizierungsmethode** den Eintrag **MD5**.
4. Geben Sie **Benutzername** und **Passwort** ein, mit denen primos auf dem RADIUS-Server eingerichtet ist.
5. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

EAP-TLS konfigurieren

**Nutzen und Zweck**

Das EAP-TLS (Transport Layer Security) überprüft die Identität von Geräten oder Benutzern, bevor diese Zugang zu Netzwerkressourcen haben. Damit primos in geschützten Netzwerken einen Zugriff erhält, können Sie primos für die EAP-TLS-Netzwerkauthentifizierung konfigurieren.

**Funktionsweise**

EAP-TLS beschreibt eine zertifikatbasierte Authentifizierung über einen RADIUS-Server. Hierzu werden zwischen dem primos und dem RADIUS-Server Zertifikate ausgetauscht. Dabei wird eine verschlüsselte TLS-Verbindung zwischen primos und RADIUS-Server aufgebaut. Sowohl RADIUS-Server als auch primos benötigen ein gültiges digitales von einer CA unterschriebenes Zertifikat, das diese gegenseitig überprüfen müssen. Ist die beidseitige Authentisierung erfolgreich, wird der Zugang freigegeben.

Da jedes Gerät ein Zertifikat benötigt, muss eine PKI (Public Key Infrastructure) vorhanden sein. Benutzerpasswörter sind nicht erforderlich.

Um eine EAP-TLS-Authentifizierung anzuwenden, stellen Sie sicher, dass die unten aufgeführten Punkte in der angegebenen Reihenfolge erfüllt werden. Wird die Vorgehensweise nicht eingehalten, kann primos im Netzwerk möglicherweise nicht

angesprochen werden. Setzen Sie in diesem Fall die Konfigurationseinstellungen auf die Standardwerte zurück (⇨🗎65).

**Vorgehensweise**

- Erstellen Sie im primos eine Zertifikatsanforderung ⇨🗎54.
- Erstellen Sie mit der Zertifikatsanforderung und mit Hilfe des Authentifizierungsservers ein Zertifikat.
- Installieren Sie das angeforderte Zertifikat im primos ⇨🗎55.
- Installieren Sie im primos das Wurzel-CA-Zertifikat der Zertifizierungsstelle, die das Zertifikat für den Authentifizierungsserver (RADIUS) ausgegeben hat ⇨🗎56.
- Aktivieren Sie das Authentifizierungsverfahren 'EAP-TLS' im primos.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT - Authentifizierung** an.
3. Wählen Sie aus der Liste **Authentifizierungsmethode** den Eintrag **TLS**.
4. Wählen Sie in der Liste **EAP-Wurzelzertifikat** das Wurzel-CA-Zertifikat aus.
5. Geben Sie das Passwort ein, mit dem primos auf dem RADIUS-Server eingerichtet ist.
6. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

EAP-TTLS konfigurieren

**Nutzen und Zweck**

Das EAP-TTLS (Tunneled Transport Layer Security) überprüft die Identität von Geräten oder Benutzern, bevor diese Zugang zu Netzwerkressourcen haben. Damit primos in geschützten Netzwerken einen Zugriff erhält, können Sie primos für die EAP-TTLS-Netzwerkauthentifizierung konfigurieren.

**Funktionsweise**

EAP-TTLS besteht aus zwei Phasen:

In der Phase 1 wird zunächst ein verschlüsselter TLS-Tunnel zwischen primos und RADIUS-Server aufgebaut. Dazu identifiziert sich nur der RADIUS-Server mit einem von einer CA unterschriebenen Zertifikat am primos. Dieser Vorgang wird auch als 'Äußere Authentifizierung' bezeichnet.

In der Phase 2 wird für die Kommunikation innerhalb des TLS-Tunnels eine weitere Authentifizierungsmethode angewandt. Dabei werden die von EAP definierten sowie ältere Methoden (CHAP, PAP, MS-CHAP und MS-CHAPv2) unterstützt. Dieser Vorgang wird auch als 'Innere Authentifizierung' bezeichnet.

Vorteil dieses Verfahrens ist, dass nur der RADIUS-Server ein Zertifikat benötigt. Es muss somit keine PKI-Struktur vorhanden sein. Zudem unterstützt TTLS die meisten Authentisierungsprotokolle.

**Voraussetzung**

✓ Auf dem RADIUS-Server ist primos als Benutzer mit einem Benutzernamen und einem Passwort angelegt.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT - Authentifizierung** an.
3. Wählen Sie aus der Liste **Authentifizierungsmethode** den Eintrag **TTLS**.
4. Wählen Sie optional aus der Liste **EAP-Wurzelzertifikat** das Wurzel-CA-Zertifikat der Zertifizierungsstelle, die das Zertifikat für den Authentifizierungsserver (RADIUS) ausgegeben hat. Das Zertifikat erhöht die Sicherheit beim Verbindungsaufbau.
   **(Das Wurzel-CA-Zertifikat muss zuvor im primos installiert worden sein ⇨ 56.)**
5. Geben Sie im Feld **Anonymer Name** den Namen für den unverschlüsselten Teil von EAP-TTLS ein.
6. Wählen Sie aus der Liste **Innere Authentifizierung** die Methode, mit der die Kommunikation im TLS-Tunnel gesichert werden soll.
7. Geben Sie **Benutzername** und **Passwort** ein, mit denen primos auf dem RADIUS-Server eingerichtet ist.
8. Installieren Sie optional ein WPA-Add-on.
9. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

PEAP konfigurieren

**Nutzen und Zweck**

Das PEAP (Protected Extensible Authentication Protocol) überprüft die Identität von Geräten oder Benutzern, bevor diese Zugang zu Netzwerkressourcen haben. Damit primos in geschützten Netzwerken einen Zugriff erhält, können Sie primos für die PEAP-Netzwerkauthentifizierung konfigurieren.

**Funktionsweise**

Beim PEAP wird (wie bei EAP-TTLS ⇨ 60) zunächst ein verschlüsselter TLS-Tunnel (Transport Layer Security) zwischen primos und RADIUS-Server aufgebaut. Dazu identifiziert sich nur der RADIUS-Server mit einem von einer CA unterschriebenen Zertifikat am primos.

Der TLS-Tunnel wird anschließend benutzt, um eine weitere Verbindung aufzubauen, wobei diese mit zusätzlichen EAP-Authentifizierungsmethoden (z.B. MSCHAPv2) geschützt werden kann.

Vorteil dieses Verfahrens ist, dass nur der RADIUS-Server ein Zertifikat benötigt. Es muss somit keine PKI-Struktur vorhanden sein. PEAP nutzt die Vorteile von TLS auf Serverebene und unterstützt verschiedene Authentifizierungsmethoden, einschließlich Benutzerkennwörtern und Einmalkennwörtern.

**Voraussetzung**

✓ Auf dem RADIUS-Server ist primos als Benutzer mit einem Benutzernamen und einem Passwort angelegt.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT - Authentifizierung** an.
3. Wählen Sie aus der Liste **Authentifizierungsmethode** den Eintrag **PEAP**.
4. Wählen Sie optional aus der Liste **EAP-Wurzelzertifikat** das Wurzel-CA-Zertifikat der Zertifizierungsstelle, die das Zertifikat für den Authentifizierungsserver (RADIUS) ausgegeben hat. Das Zertifikat erhöht die Sicherheit beim Verbindungsaufbau.
   **(Das Wurzel-CA-Zertifikat muss zuvor im primos installiert worden sein ⇨🗎56.)**
5. Geben Sie im Feld **Anonymer Name** den Namen für den unverschlüsselten Teil von PEAP ein.
6. Wählen Sie aus der Liste **Innere Authentifizierung** die Methode, mit der die Kommunikation im TLS-Tunnel gesichert werden soll.
7. Wählen Sie aus der Liste **PEAP-Version** die zu verwendende Version des PEAP-Protokolls.
8. Wählen Sie aus der Liste **PEAP-Label** die zu verwendende Version.
9. Geben Sie **Benutzername** und **Passwort** ein, mit denen primos auf dem RADIUS-Server eingerichtet ist.
10. Installieren Sie optional ein WPA-Add-on.
11. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

## EAP-FAST konfigurieren

**Nutzen und Zweck**

Das EAP-FAST (Flexible Authentication via Secure Tunneling) überprüft die Identität von Geräten oder Benutzern, bevor diese Zugang zu Netzwerkressourcen haben. Damit primos in geschützten Netzwerken einen Zugriff erhält, können Sie primos für die EAP-FAST-Netzwerkauthentifizierung konfigurieren.

**Funktionsweise**

EAP-FAST nutzt (wie EAP-TTLS ⇨🗎60) einen Tunnel zum Schutz der Datenübertragung. Der Hauptunterschied besteht darin, dass EAP-FAST keine Zertifikate zum Authentifizieren benötigt. (Die Verwendung von Zertifikaten ist optional.)

Um den Tunnel aufzubauen werden PACs (Protected Access Credentials) verwendet. PACs sind Anmeldeinformationen, die bis zu drei Komponenten umfassen können:

- Einen gemeinsamen geheimen Schlüssel, der den zwischen primos und dem RADIUS-Server geteilten Schlüssel enthält.
- Ein undurchsichtiges Element, das primos zur Verfügung steht und dem RADIUS-Server vorgelegt wird, wenn primos auf die Netzwerkressourcen zugreifen möchte.

- Zusätzliche Informationen, die für den Client nützlich sein können. (Optional)

EAP-FAST verwendet zwei Methoden, um die PACs auszugeben:

- Der manuelle Liefermechanismus kann jeder Mechanismus sein, den der Administrator für das Netzwerk als sicher erachtet und konfiguriert.
- Die automatische Bereitstellung richtet einen verschlüsselten Tunnel ein, um die Authentifizierung von primos sowie die Lieferung der PACs zu schützen.

**Voraussetzung**

✓ Auf dem RADIUS-Server ist primos als Benutzer mit einem Benutzernamen und einem Passwort angelegt.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **SICHERHEIT - Authentifizierung** an.
3. Wählen Sie aus der Liste **Authentifizierungsmethode** den Eintrag **FAST**.
4. Wählen Sie optional aus der Liste **EAP-Wurzelzertifikat** das Wurzel-CA-Zertifikat der Zertifizierungsstelle, die das Zertifikat für den Authentifizierungsserver (RADIUS) ausgegeben hat. Das Zertifikat erhöht die Sicherheit beim Verbindungsaufbau.
   **(Das Wurzel-CA-Zertifikat muss zuvor im primos installiert worden sein ⇨ 56.)**
5. Geben Sie im Feld **Anonymer Name** den Namen für den unverschlüsselten Teil von EAP-FAST ein.
6. Wählen Sie aus der Liste **Innere Authentifizierung** die Methode, mit der die Kommunikation im TLS-Tunnel gesichert werden soll.
7. Wählen Sie aus der Liste **FAST-Bereitstellung** die Bereitsstellungsmethode für PACs.
8. Geben Sie **Benutzername** und **Passwort** ein, mit denen primos auf dem RADIUS-Server eingerichtet ist.
9. Installieren Sie optional ein WPA-Add-on.
10. Bestätigen Sie mit **Speichern**.

↳ Die Einstellungen werden gespeichert.

# 7 Wartung

Am primos können verschiedene Wartungsmaßnahmen durchgeführt werden. Dieses Kapitel gibt einen Überblick.

**Welche Information benötigen Sie?**

## 7.1 Wie sichere ich die Konfigurationseinstellungen? (Backup)

Sie können die Konfigurationseinstellungen (inklusive Zertifikaten) als Sicherungskopie auf Ihren lokalen Client speichern. Auf diese Weise können Sie jederzeit auf einen festen Konfigurationsstatus zurückgreifen.

Die Backup-Datei kann anschließend auf einen primos geladen werden. Die in der Datei enthaltenen Konfigurationseinstellungen werden dann von dem Gerät übernommen.

**Was möchten Sie tun?**

- ☐ 'Backup speichern' ⇨🗎65
- ☐ 'Backup auf einen primos laden' ⇨🗎65

Backup speichern

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **WARTUNG - Backup** an.
3. Wählen Sie die Schaltfläche **Speichern** an.

↳ Die Backup-Datei wird auf Ihrem Client gespeichert.

Backup auf einen primos laden

**Hinweis**

Sie können nur Backups laden, die für dieselbe Hauptversion der primos-Software erstellt wurden. (Hauptversionen werden durch die Zahl hinter dem ersten Punkt der Versionsnummer unterschieden.)
Beispiel: Eine Backup für die primos Software 17.1.x kann nicht auf primos mit 17.2.x-Software installiert werden.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **WARTUNG - Backup** an.
3. Wählen Sie die Schaltfläche **Durchsuchen** an.
4. Geben Sie die primos Backup-Datei an.
5. Wählen Sie die Schaltfläche **Installieren** an.

↳ Die in der Backup-Datei enthaltenen Konfigurationseinstellungen werden von dem primos übernommen.

## 7.2 Wie setze ich primos auf die Standardwerte zurück? (Reset)

Sie können primos auf die Standardeinstellung (Werkseinstellung) zurückzusetzen. Dabei werden alle zuvor definierten Konfigurationseinstellungen gelöscht.

**Nutzen und Zweck**

Das Zurücksetzen der Konfigurationseinstellungen ist z.B. erforderlich, wenn primos durch einen Standortwechsel in einem anderen Netzwerk eingesetzt werden soll. Vor dem Wechsel sollten die Konfigurationseinstellungen auf die Standardeinstellung zurückgesetzt werden, um primos im anderen Netzwerk neu zu installieren.

**Per Fernwartung oder am Gerät**

Über das primos Control Center können Sie primos per Fernwartung zurücksetzen. Alternativ können Sie über den Reset-Taster am Gerät die Konfigurationseinstellungen ohne eine Passworteingabe zurücksetzen.

**Hinweis**

Durch das Zurücksetzen kann sich die IP-Adresse von primos ändern und die Verbindung zum primos Control Center abbrechen.

**Was möchten Sie tun?**

- ☐ 'Konfigurationseinstellungen via primos Control Center zurücksetzen' ⇨🗎66
- ☐ 'Konfigurationseinstellungen via Reset-Taster zurücksetzen' ⇨🗎66

Konfigurationseinstellungen via primos Control Center zurücksetzen

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **WARTUNG - Standardeinstellung** an.
3. Wählen Sie die Schaltfläche **Standardeinstellung** an.

↳ Die Konfigurationseinstellungen werden zurückgesetzt.

Konfigurationseinstellungen via Reset-Taster zurücksetzen

Am primos finden Sie LEDs, verschiedene Anschlüsse sowie den Reset-Taster. Eine Beschreibung dieser Komponenten finden Sie im 'Quick Installation Guide'.

Über den Reset-Taster können Sie die Konfigurationseinstellungen von primos auf die Standardeinstellung zurücksetzen.

1. Drücken Sie den Reset-Taster für 5 Sekunden.
   primos startet neu.

↳ Die Parameter sind zurückgesetzt.

## 7.3 Wie führe ich ein Update aus?

Sie können Soft- und Firmware-Updates auf primos ausführen, um von aktuell entwickelten Features profitieren.

**Was passiert beim Update?**

Beim Update wird die vorhandene Firmware/Software von einer neuen Version überschrieben und ersetzt. Die ursprünglichen Konfigurationseinstellungen (inkl. Zertifikate) des Gerätes bleiben erhalten.

**Hinweis**

Bei einem Update auf eine andere Software-Hauptversion wird primos auf die Standardwerte zurückgesetzt. (Hauptversionen werden durch die Zahl hinter dem ersten Punkt der Versionsnummer unterschieden.)
Beispiel: Bei einem Update von der primos Software 17.1.x auf 17.2.x wird primos auf die Standardwerte zurückgesetzt (d.h. alle Einstellungen gehen verloren).

**Wann ist ein Update sinnvoll?**

Ein Update sollte durchgeführt werden, wenn Funktionen nur eingeschränkt laufen und von der SEH Computertechnik GmbH eine neue Soft- oder Firmware-Version mit neuen Funktionen oder Fehlerbereinigungen bereitgestellt wird.

Überprüfen Sie die installierte Soft- und Firmware-Version im primos. Die Versionsnummer entnehmen Sie der Startseite des primos Control Centers oder der Liste in der SEH primos App.

**Wo finde ich Update-Dateien?**

Aktuelle Firmware- und Software-Dateien können von der SEH Computertechnik GmbH-Homepage geladen werden

http://www.seh.de/services/downloads/download-mobility-loesungen/primos.html

**Hinweis**

Jeder Update-Datei ist eine 'Readme'-Datei zugeordnet. Nehmen Sie die in der 'Readme'-Datei enthaltenen Informationen zur Kenntnis.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **WARTUNG - Update** an.
3. Wählen Sie die Schaltfläche **Durchsuchen** an.
4. Geben Sie die Update-Datei an.
5. Wählen Sie die Schaltfläche **Installieren** an.

↳ Das Update wird ausgeführt. Dieser Vorgang kann einige Minuten dauern. Anschließend startet primos neu.

## 7.4 Wie starte ich primos neu?

Nach einem Update wird primos automatisch neu gestartet. Befindet sich primos in

einem undefinierten Zustand, kann primos auch manuell neu gestartet werden.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **WARTUNG - Neustart** an.
3. Wählen Sie die Schaltfläche **Neustart** an.

↳ primos wird neu gestartet.

## 7.5 Wie fahre ich primos herunter?

Sie können primos ausschalten, z.B. über das Wochenende. Fahren Sie primos herunter bevor Sie die Stromversorgung unterbrechen. Damit werden undefinierte Zustände und Datenverlust vermieden.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **WARTUNG - Herunterfahren** an.
3. Wählen Sie die Schaltfläche **Herunterfahren** an.

↳ primos wird heruntergefahren.

## 7.6 Wie nutze ich die primos Servicefunktionen?

primos stellt Servicefunktionen zur Verfügung. Diese Funktionen unterstützen die Fehlerbehebung durch den SEH Support. Die Kontaktdaten finden Sie im Kapitel 'Support und Service' ⇨🗎5.

**Service-Datei**

Die Service-Datei ist eine komprimierte Datei mit Diagnose-Informationen. Im Fehlerfall speichern Sie diese Datei auf Ihrem lokalen Client und senden sie zusammen mit Ihrer Anfrage an den SEH Support (z.B. via E-Mail).

**Logging**

Standardmäßig werden nur einige Informationen in der Service-Datei protokolliert. Ist zusätzlich das Logging aktiviert, werden erweiterte Informationen in die Service-Datei geschrieben. Damit kann der SEH Support ein detailliertere Fehleranalyse durchführen.

**SSH-Zugriff**

Über das Secure Shell-Netzwerkprotokoll (SSH) kann der Fernzugriff auf primos zu Supportzwecken hergestellt werden. Sollte der Fernzugriff erforderlich sein, werden Sie vom SEH Support aufgefordert diese Funktion zu aktivieren. Der SEH Support leitet Sie dann an, alle nötigen Maßnahmen durchzuführen. Nachdem alle Supportmaßnahmen durchgeführt wurden, deaktivieren Sie den SSH-Zugriff wieder.

**Was möchten Sie tun?**

- ☐ 'Logging aktivieren' ⇨🗎68
- ☐ 'Service-Datei speichern' ⇨🗎69
- ☐ 'SSH-Zugriff konfigurieren' ⇨🗎69

Logging aktivieren

**Hinweis**

Aktivieren Sie die Option nur in Absprache mit dem SEH Support.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **WARTUNG - Service** an.
3. Wählen Sie im Bereich **Logging** die Schaltfläche **Logging aktivieren** an.

↳ Das Logging ist aktiviert.

Service-Datei speichern

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **WARTUNG - Service** an.
3. Wählen Sie im Bereich **Service-Datei** die Schaltfläche **Speichern** an.

↳ Die Service-Datei wird auf Ihrem Client gespeichert.
Senden Sie die Service-Datei an den SEH-Support.

SSH-Zugriff konfigurieren

**Hinweis**

Die SSH-Verbindung darf ausschließlich nach Absprache mit dem SEH Support hergestellt und genutzt werden. Die Nutzung von SSH für eigene Zwecke (Fernwartung usw.) ist nicht erlaubt.

1. Starten Sie das primos Control Center.
2. Wählen Sie den Menüpunkt **WARTUNG - Service** an.
3. De-/aktivieren Sie die Option **SSH-Zugriff**.
4. Bestätigen Sie mit **Speichern**.

↳ Die Einstellung wird gespeichert.

# 8 Anhang

Der Anhang enthält ein Glossar, eine Problembehandlung sowie den Index dieses Dokumentes.

**Welche Information benötigen Sie?**

- ☐ 'Glossar' ⇨🗎70
- ☐ 'Problembehandlung' ⇨🗎72
- ☐ 'Index' ⇨🗎76

## 8.1 Glossar

Dieses Glossar informiert Sie über herstellerspezifische Softwarelösungen sowie Begriffe aus der Netzwerktechnologie.

**Welche Information benötigen Sie?**

Herstellerspezifische Softwarelösungen

- 'primos Control Center' ⇨🗎71
- 'SEH primos App' ⇨🗎71

Netzwerktechnologie

- 'Default-Name' ⇨🗎70
- 'Gateway' ⇨🗎70
- 'Hardware-Adresse' ⇨🗎71
- 'Hostname' ⇨🗎71
- 'IP-Adresse' ⇨🗎71
- 'Netzwerkmaske' ⇨🗎71

**Default-Name**

Der Default-Name von primos setzt sich aus den zwei Buchstaben 'IC' und der Gerätenummer zusammen. Die Gerätenummer können Sie aus den sechs letzten Ziffern der Hardware-Adresse entnehmen.

Beispiel: IC0001ff

Der Default-Name kann im primos Control Center abgelesen werden.

**Gateway**

Über ein Gateway können IP-Adressen in einem anderen Netzwerk angesprochen werden. Möchten Sie ein Gateway verwenden, können Sie über das primos Control Center den entsprechenden Parameter konfigurieren (⇨🗎13).

**Hardware-Adresse**

primos ist über seine weltweit eindeutige Hardware-Adresse adressierbar. Sie wird häufig auch als MAC- oder Ethernet-Adresse bezeichnet. Diese Adresse wird vom Hersteller in der Hardware des Gerätes festgelegt. Sie besteht aus zwölf hexadezimalen Ziffern. Die ersten sechs Ziffern kennzeichnen den Hersteller, die letzten sechs Ziffern identifizieren das individuelle Gerät.

Die Hardware-Adresse kann am Gehäuse und in der SEH primos App abgelesen werden.

Die Verwendung von Trennzeichen in der Hardware-Adresse ist plattformabhängig. Beachten Sie bei Eingabe der Hardware-Adresse die folgende Konvention:

| Betriebssystem | Darstellung | Beispiel |
|---|---|---|
| Windows | Bindestrich | 00-c0-eb-00-01-ff |
| UNIX | Doppelpunkt oder Punkt | 00:c0:eb:00:01:ff bzw. 00.c0.eb.00.01.ff |

**Hostname**

Der Hostname ist ein Alias für eine IP-Adresse. Mit dem Hostnamen wird primos in seinem Netzwerk eindeutig bezeichnet und in einem von Menschen merkbaren Format angegeben.

**IP-Adresse**

Die IP-Adresse ist eine eindeutige Adresse jedes Knotens in Ihrem Netzwerk, d.h. eine IP-Adresse darf nur einmal in Ihrem lokalen Netzwerk auftreten. Sie muss im primos gespeichert werden, damit es im Netzwerk angesprochen werden kann.

**Netzwerkmaske**

Mit Hilfe der Netzwerkmaske können große Netzwerke in Subnetzwerke unterteilt werden. Dabei werden die Teilnehmerkennungen der IP-Adresse verschiedenen Subnetzwerken zugeordnet.

primos ist standardmäßig für den Einsatz ohne Subnetzwerke konfiguriert. Möchten Sie ein Subnetzwerk verwenden, können Sie über das primos Control Center den entsprechenden Parameter konfigurieren (⇨13).

**primos Control Center**

Über das primos Control Center kann primos konfiguriert und überwacht werden. Das primos Control Center ist in dem primos gespeichert und kann mit einer Browsersoftware (Microsoft Edge, Safari, Mozilla Firefox) dargestellt werden.

**SEH primos App**

Die SEH primos App ist eine von der SEH Computertechnik entwickelte Software zum Auffinden von primos Geräten innerhalb eines zuvor definierten Netzwerks. Weiterhin können mit der SEH primos App einfache administrative Arbeiten durchgeführt werden.

## 8.2 Problembehandlung

Dieses Kapitel stellt einige Problemursachen und erste Lösungshilfen dar.

**Problem**



**Lösung**

primos befindet sich im BIOS-Modus

primos fällt in den BIOS-Modus, wenn die Firmware funktioniert, jedoch die Software fehlerhaft ist. Dieses Verhalten tritt z.B. bei einem nicht korrekt durchgeführtem Softwareupdate auf. primos signalisiert den BIOS-Modus, indem die Activity-LED regelmäßig blinkt.

**Warnung**

**primos ist im BIOS-Modus nicht funktionsfähig.**

Ist ein primos im BIOS-Modus, wird das Gerät in der SEH primos App automatisch mit einem entsprechenden Hinweis angezeigt.

Damit primos vom BIOS-Modus in den Standardmodus wechselt, müssen Sie primos zunächst eine temporäre IP-Adresse zuweisen und anschließen auf primos die Software neu aufspielen. Nach dem Software-Update wechselt primos in den Standardbetrieb und sucht sich eine neue, dauerhafte IP-Adresse.

1. Starten Sie die SEH primos App.
2. Markieren Sie primos in der Liste.
3. Wählen Sie im Menü **Aktionen** den Befehl **IP-Adresse definieren**.
   Der Dialog **IP-Adresse definieren** erscheint.
4. Konfigurieren Sie **IP-Adresse**, **Netzwerkmaske** und **Gateway**.
5. Bestätigen Sie mit **OK**.
   primos hat eine temporäre IP-Adresse.
6. Laden Sie die aktuelle Software-Datei von der SEH Computertechnik-Homepage:

http://www.seh.de/services/downloads/download-mobility-loesungen/primos.html

7. Wählen Sie im Menü **Aktionen** den Befehl **Software laden**.
   Der Dialog **Software laden** erscheint.
8. Geben Sie die primos Software an.
9. Wählen Sie die Schaltfläche **Laden** an.
   Das Software-Update wird durchgeführt. Dieser Vorgang kann einige Minuten dauern.
10. Bestätigen Sie die Erfolgsmeldung mit **OK**.

↳ primos wechselt in den Standardbetrieb. primos sucht sich automatisch eine neue IP-Adresse und wird mit dieser in der SEH primos App angezeigt. Aktualisieren Sie ggf. die Anzeige in der SEH primos App.

Die Verbindung zum primos Control Center kann nicht hergestellt werden

Schließen Sie Fehlerquellen aus. Überprüfen Sie zunächst:

- die Kabelverbindungen,
- die IP-Adresse von primos (⇨🗎7) sowie
- die Proxy-Einstellungen Ihres Browsers.

Kann weiterhin keine Verbindung hergestellt werden, können folgende Sicherheitsmechanismen verantwortlich sein:

- ☐ Der Zugang ist via SSL/TLS (HTTPS) geschützt ⇨🗎47.
- ☐ Die TCP-Portzugriffskontrolle ist aktiviert ⇨🗎50.
- ☐ Die Cipher Suites der Verschlüsselungsstufe werden vom Browser nicht unterstützt ⇨🗎45.
- ☐ primos befindet sich im BIOS-Modus ⇨🗎72.

Das Passwort ist nicht mehr verfügbar

Der Zugriff auf primos wird über Benutzerprofile reglementiert. Der Zugang erfolgt über einen Benutzernamen in Kombination mit einem Passwort. Es kann das lokale Administratorkonto verwendet werden und/oder Verzeichnisdienstbenutzer (⇨🗎48).

Verwenden Sie ausschließlich das lokale Administratorkonto und das Passwort ist nicht mehr verfügbar, können sie primos auf die Standardeinstellung (Werkseinstellung) zurücksetzen ⇨🗎65. Dabei wird auch das Passwort auf den Standard zurückgesetzt, allerdings gehen beim Zurücksetzen sämtliche Einstellungen verloren.

Der Drucker druckt nicht

Damit von iOS-Geräten über primos gedruckt werden kann, muss im primos für den jeweiligen Drucker eine Queue (Druckerwarteschlange) angelegt werden. Für jede Queue können Sie anschließend zahlreiche Einstellungen (Druckprotokoll, Zugriffskontrolle usw.) konfigurieren. Überprüfen Sie

- ☐ alle Queue-Einstellungen ⇨🗎30.
- ☐ den Drucker auf Fehler (Papier leer, Toner leer, Papierstau usw.).
- ☐ die Zertifikate hinsichtlich Existenz und Gültigkeit
  (Nur bei verschlüsselter Übertragung der Druckdaten ⇨🗎35.)

Der Ausdruck ist fehlerhaft

Überprüfen Sie

- ☐ die gewählte Verbindung zum Drucker ⇨🗎30.
- ☐ den Drucker auf Fehler (Toner leer usw.).

Das Einbinden in einen Verzeichnisdienst funktioniert nicht

- ☐ Im gesamten Verzeichnisdienst muss eine synchronisierte Zeit verwendet werden. Die Gerätezeit von primos darf nicht abweichen von der des Verzeichnisdiensts. Wir empfehlen, im Verzeichnisdienst und auf primos denselben Time-Server (SNTP-Server) zu verwenden. Überprüfen Sie die Time-Server-Konfiguration auf primos ⇨🗎20.
- ☐ Stellen Sie sicher, dass in primos ein DNS-Server konfiguriert ist und primos auf den DNS-Server zugreifen kann ⇨🗎15.

Wide-Area AirPrint funktioniert nicht

Überprüfen Sie, ob

- ☐ der gewünschte Drucker für Wide-Area AirPrint freigegeben ist ⇨🗎38.
- ☐ auf den iOS-Geräten, die Wide-Area AirPrint nutzen sollen, die primos Unterdomäne

als Suchdomäne konfiguriert:

- 'primos Unterdomäne als Suchdomäne automatisch auf iOS-Geräten konfigurieren' ⇨🗎41.
- 'primos Unterdomäne als Suchdomäne manuell auf iOS-Geräten konfigurieren' ⇨🗎43.

☐ auf dem DNS-Server die bedingte Weiterleitung korrekt eingerichtet ist: Anfragen welche die primos Unterdomäne enthalten müssen an primos weitergeleitet werden ⇨🗎40.

Manuell erstellte Queue kann nicht veröffentlicht werden

Wenn beim manuellen Erstellen einer Queue (⇨🗎28) der definierte Drucker nicht erreichbar ist, kann die Queue nicht über Multicast im Netzwerk veröffentlicht werden und wird nicht verfügbar sein. Stellen Sie sicher, dass der Drucker erreichbar ist und veröffentlichen Sie die dann die Queue via Multicast ⇨🗎30.

## 8.3 Index