



primos

— Print. Mobile. Secure. —

by

SEH

ユーザーマニュアル

本社・製造元

SEH Computertechnik GmbH
Suedring 11
33647 Bielefeld
Germany

電話：+49 (0)521 94226-29
FAX：+49 (0)521 94226-99
サポート：+49 (0)521 94226-44
電子メール：info@seh.de
Web サイト：http://www.seh.de



文書

種類：User Manual
タイトル：primos
バージョン：2.0

法律上の注意事項

SEH Computertechnik GmbH はあらゆるマニュアルの記載事項が正確であるよう努めておりますが、万一誤りを見つけられた場合には、上記に記載されている住所にご連絡ください。SEH Computertechnik GmbH は、誤りまたは脱落についていかなる責任も負いません。本マニュアルの記載事項は予告なく変更されることがあります。

この製品マニュアルには、製品に関する有益な情報が記載されています。製品の使用中は、常に参照できるように保管しておいてください。

無断複写、転載を禁じます。SEH Computertechnik GmbH による事前承諾なしの複写や他の複製行為、翻訳を禁じます。

© 2017 SEH Computertechnik GmbH

iPad, iPhone, iPod, and iPod touch are trademarks of Apple Inc., registered in the U.S. and other countries. AirPrint and the AirPrint logo are trademarks of Apple Inc.

この文書に記載されている商標、登録商標及び製品名は、それぞれの会社（所有者）に帰属します。

目次

1 一般情報	1
1.1 primos.....	2
1.2 説明書.....	3
1.3 サポートとサービス.....	5
1.4 安全の確保.....	6
1.5 最初のステップ.....	7
1.6 primos の IP アドレスの検索.....	7
2 管理方法	9
2.1 primos Control Center による管理.....	9
2.2 SEH primos App による管理.....	12
3 ネットワーク設定	13
3.1 IPv4 パラメータの設定方法.....	13
3.2 IPv6 パラメータの設定方法.....	14
3.3 DNS の設定方法.....	16
3.4 Bonjour の設定方法.....	17
3.5 ディレクトリサービスを設定する方法.....	17
4 デバイス設定	20
4.1 説明の記述内容を決定する方法.....	20
4.2 デバイス時間の設定方法.....	20
4.3 ローカルユーザを設定する方法.....	21
4.4 ローカルグループを設定する方法.....	23
5 印刷	25
5.1 primos 上でプリンタを設定する方法 (キューの作成).....	26
5.2 キューを管理する方法.....	31
5.3 ジョブ履歴を表示する方法.....	33
5.4 iOS デバイス上に表示するプリンタ名を設定する方法.....	35
5.5 primos でプリンタを管理、検査する方法.....	36
5.6 データ転送を暗号化する方法.....	36
5.7 印刷するユーザを制御する方法.....	37

5.8	iOS デバイスから印刷する方法.....	39
5.9	サブネット間で印刷する方法 (Wide-Area AirPrint).....	40
6	セキュリティ.....	46
6.1	SSL/TLS 接続の暗号化強度を設定する方法.....	47
6.2	primos Control Center へのアクセスを制御する方法.....	49
6.3	ユーザプロファイルを管理する方法 (アクセス制御).....	50
6.4	クロスサイトスクリプティングから primos を保護する方法.....	52
6.5	primos へのアクセスを制御する方法 (TCP ポートアクセス制御).....	52
6.6	証明書の正しい使用方法.....	54
6.7	認証方式を使用する方法.....	60
7	メンテナンス.....	66
7.1	primos の設定の安全を確保する方法 (バックアップ).....	66
7.2	primos を 初期設定にリセットする方法 (リセット).....	67
7.3	更新 (アップグレード) の実行方法.....	68
7.4	primos を再起動する方法.....	69
7.5	primos をシャットダウンする方法.....	70
7.6	サービス機能を使用する方法.....	70
8	付録.....	72
8.1	用語集.....	73
8.2	トラブルシューティング.....	75

必要な情報

1 一般情報



この章では、デバイスおよび付属の説明書、また安全上の注意について説明します。

primos を有効に利用する方法やデバイスの正しい操作方法が確認できます。

- 「primos」⇒[2](#)
- 「説明書」⇒[3](#)
- 「サポートとサービス」⇒[5](#)
- 「安全の確保」⇒[6](#)
- 「最初のステップ」⇒[7](#)
- 「primos の IP アドレスの検索」⇒[7](#)

目的

1.1 primos

primos は、iOS デバイス (iPhone®、iPad® など) から文書や画像を印刷するためのモバイル印刷ソリューションです。primos から送られた印刷ジョブはネットワーク内にとどまります。ローカルで処理され、インターネットやクラウドのメカニズムを介して送信されることはありません。primos を使用することにより、最大で 10 台のプリンタが iOS デバイスで利用できるようになります。AirPrint® 対応のネットワークプリンタには有線と無線があります。また、primos は、AirPrint を様々な機能 (Wide-Area AirPrint、ディレクトリサービスなど) で強化します。

primos は、主に業務用 (企業環境向け) に開発されました。

動作モード

primos はケーブルでネットワークに接続します。iOS デバイスは、このネットワークに無線 LAN を経由して接続されます。印刷ジョブは、AirPrint 対応の iOS アプリからネットワークを介して primos に送信されます。primos は、印刷処理のため印刷ジョブをネットワークプリンタに転送します。

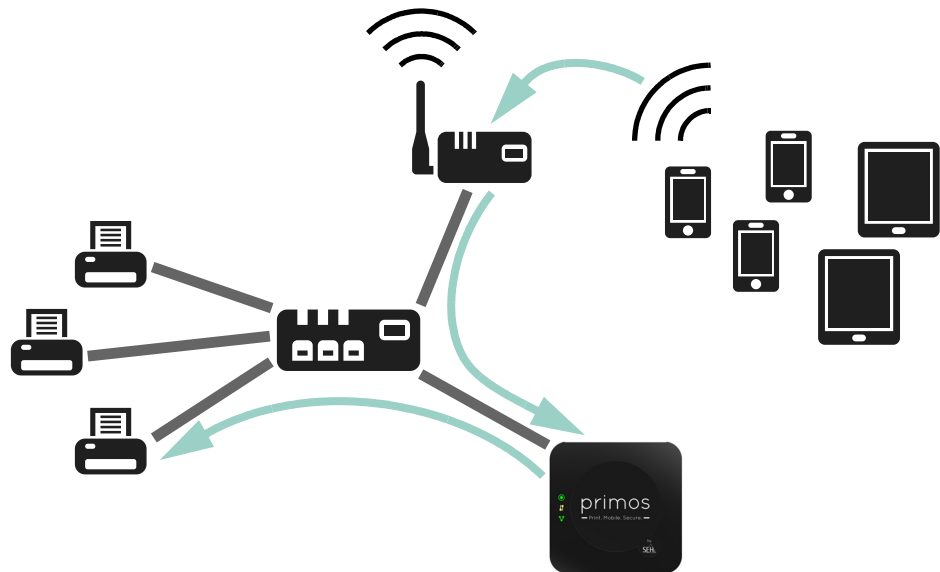


図 1: トポロジー

必要事項ネットワーク

無線アクセスポイント (無線 LAN) を備えた TCP/IP 有線ネットワーク (有線 LAN)。

対応 iOS デバイス

primos は、AirPrint 対応のすべての iOS デバイス、AirPrint 装備の iOS 4.2 以降のすべての iOS デバイスに対応しています。iOS デバイスは、無線 LAN を介して有線ネットワークに接続されていることが必要です。

対応プリンタ

AirPrint 対応のネットワークプリンタ。

1.2 説明書

使用する製品の機能に関する情報は、primos に添付のデータシートを参照してください。

説明書の構成

primos の説明書は、次のように構成されています。

ユーザーマニュアル	PDF	primos の設定および管理について詳細に説明しています。
クイック・インストールガイド	印刷済 PDF	ハードウェアのインストール、および初期操作の手順について説明しています。
重要な製品情報	印刷済 PDF	セキュリティ、法規制の遵守情報、および廃棄処理について説明しています。
オンラインヘルプ (primos Control Center)	HTML	オンラインヘルプは、「primos Control Center」の使用方法について詳しく説明しています。

説明書の特長

この説明書は、モニタで参照できる電子文書として作成されています。多くのプログラム (例: Adobe Reader) が備えているブックマークナビゲーション機能を使用して、文書構造の全体を参照できます。


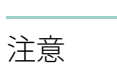


また、関連情報へのハイパーリンクも設定されています。印刷する場合は、プリンタの設定を「両面印刷」または「小冊子印刷」にしておくことをお奨めします。

この文書で使用される専門用語

この文書で使用される技術用語は、用語集で説明されています。用語集には、技術情報やバックグラウンド情報の概要が記載されています。⇒ 73

記号と表記規則

本書では、様々な記号が使用されています。次の表に、その意味を示します。

	警告	警告には、細心の注意が必要な重要な情報が含まれます。警告に従わない場合、誤動作することがあります。
	メモ	注意には、細心の注意が必要な情報が含まれます。
	注意	
1. 記号		番号は手順の順番を示します。
↳ 確認		矢印の記号は、操作結果について確認します。
✓ 必要事項		チェック記号は、操作を始める前に準備が必要な要件を示します。
□ オプション		四角の記号は、手順と選択可能なオプションを示します。
•		中点は、箇条書き表示で使用されます。
		各章の要約を示します。
⇒		矢印は、文書内で参照するページを示します。PDF ファイルでは、この記号をクリックすると該当のページにジャンプできます。
		電球は、ヒントを示します。
太字		ボタンやメニュー項目などの製品の用語は、太字で表記されます。
Courier		コマンドライン (半角英数字) は Courier フォントで表記されています。
「固有名」		固有名はかぎ括弧「」内に表記されています。

窓口

1.3 サポートとサービス

SEH Computertechnik GmbH では広範囲なサポートを提供しています。利用方法に関するご質問は、弊社のサポート窓口までご連絡ください。



午前 9 : 00 ~ 午後 6 : 00 月 ~ 金曜日 (祝日を除く)



0570-02-3666



support@seh-technology.jp



<http://www.seh-technology.jp/>

ダウンロード

ダウンロードについては、次の SEH Computertechnik GmbH のホームページを参照してください。

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



primos に関連する次のデータがダウンロードできます。

- 最新のファームウェアおよびソフトウェア
- 最新のツール
- 最新の説明書
- 最新の製品情報
- 製品データシート
- その他

1.4 安全の確保

この説明書、またデバイスとパッケージに記載された安全規定および警告は、すべて読み遵守してください。誤った使用方法を避けることで、人体への悪影響や製品の故障を防ぐことができます。

安全規定と警告を遵守しなかった結果による、人への傷害や財産の損害および間接的損害について、SEH Computertechnik GmbH は一切の責任を負いません。安全規定と警告を遵守しなかった結果による、データの損失、財産への損害、および間接的損害について、SEH Computertechnik GmbH は一切の責任を負いません。

目的用途

primos は TCP/IP ネットワークで使用し、オフィス環境向けに設計されています。primos は、印刷ジョブを iOS デバイスから AirPrint® 対応のネットワークプリンタに転送します。また、primos は、AirPrint を様々な機能 (Wide-Area AirPrint、ディレクトリサービスなど) で強化します。

不正使用

この説明書に記載されている primos の機能に適合しないデバイスの使用は、すべて不正使用とみなされます。ハードウェアおよびソフトウェアの改造やデバイスの修理は許可されていません。

安全規定

primos をはじめて操作する前に、「重要な製品情報」に記載された安全規定を読んで遵守してください。この説明書は、印刷物としてパッケージに含まれています。

警告

本書に記載されたすべての警告を読み遵守してください。警告は、危険と判断される操作説明の箇所に、次のように表記されています。

警告

警告!

1.5 最初のステップ

この節では、即座に使用するための操作に必要な準備について説明をします。

1. 人への傷害およびデバイスへの損傷を避けるため、セキュリティ規定を読み遵守ください。⇒[16](#)
2. ハードウェア設定を実行します。ハードウェア設定では、primos をネットワークや電源に接続します。「クイック・インストールガイド」を参照してください。
3. primos の IP アドレスを検索します。⇒[17](#)
4. primos で印刷キューを設定します。⇒[31](#)
↳ primos が使用できるようになります。iOS デバイスからの印刷することができません。⇒[39](#)

1.6 primos の IP アドレスの検索

IP アドレスは、IP ネットワーク内でネットワークデバイスのアドレス指定に使用します。ネットワーク内でデバイスをアドレス指定できるように、TCP/IP ネットワークプロトコルは primos 内に IP アドレスを保存することを要求します。

primos は IP アドレスが設定されない状態で出荷されます。ネットワークに接続すると、primos は DHCP から IP アドレスを受信します。DHCP が利用できない場合、primos は ZeroConf アドレス範囲 (169.254.0.0/16) から ZeroConf IP アドレスを検索します。

この IP アドレスの設定は後で変更できます。

- 「IPv4 パラメータの設定方法」⇒[13](#)
- 「IPv6 パラメータの設定方法」⇒[14](#)

primos の IP アドレスは SEH primos App で確認します。

SEH primos アプリのシステム要件：

- Windows 7、Windows 8、Windows 10;
Mac OS X 10.7.x、OS X 10.8~10.11.x、macOS 10.12.x 以降
- インストールは、管理権限のあるユーザのみが実行できます。

IP アドレスの
必要性

primos が IP ア
ドレスを取得する
方法

IP アドレスを検
索する方法

必要事項

- ✓ primos がネットワークに接続されていること。「クイック・インストールガイド」を参照してください。
- 1. 使用する primos のハードウェアアドレスをメモします。ハードウェアアドレスは、primos 底部のラベルに記載されています。
- 2. 使用するオペレーティングシステム用の SEH primos App を、SEH Computertechnik GmbH の Web サイトからダウンロードします。
<http://www.seh-technology.jp/services/downloads/download-mobility-solutions/primos.html>



- 3. SEH primos App をクライアントにインストールします。
- 4. SEH primos App を起動します。
ネットワーク上で検出された primos デバイスがすべて表示されます。
- 5. 使用する primos をハードウェアアドレスで検索します。

メモ

IP アドレスは Bonjour でも検索できます。primos は「primos@ICxxxxxx」という名でアドバタイズされます。(「ICxxxxxx」はデフォルト名 ⇨ 73) すべての iOS と Mac OS X/OS X/macOS のデバイスはデフォルトで Bonjour に対応しています。Windows などの他のオペレーティングシステムのデバイスの場合は、Bonjour サービスを手動でインストールする必要があります。

2 管理方法



primos の管理および設定には、複数の方法があります。この章では、様々な管理オプションについて概説します。

各管理オプションを使用する状況、また対応する機能について説明します。

必要な情報

- 「primos Control Center による管理」⇒119
- 「SEH primos App による管理」⇒112

primos Control Center の役割

primos は、primos Control Center から設定および管理できます。primos Control Center は primos に格納され、ブラウザソフトウェア (Microsoft Edge, Safari, Mozilla Firefox) で表示できます。

セキュリティ

primos Control Center へのアクセスは制限されています。(⇒150) 初期設定のユーザプロファイルは次のとおりです。

ユーザ名： admin

パスワード： admin

メモ

初期設定のパスワードは、できるだけ早く変更してください。(⇒150)

ユーザプロファイルの詳細は、⇒150 を参照してください。

primos Control Center の起動

primos Control Center は、ブラウザで直接起動する、または SEH primos App から起動します。

- 「primos Control Center をブラウザで起動する」⇒110
- 「primos Control Center を SEH primos App で起動する」⇒110

メモ

primos Control Center が表示されない場合は、ブラウザのプロキシ設定を確認してください。

必要事項

primos Control Center をブラウザで起動する

- ✓ primos がネットワークに接続され、電源が供給されていること。
- ✓ primos に有効な IP アドレスが設定されていること。

1. ブラウザを開きます。
2. primos の IP アドレスを URL で入力します。
 - ↳ primos Control Center がブラウザに表示されます。

primos Control Center を SEH primos App で起動する

必要事項

- ✓ primos がネットワークに接続され、電源が供給されていること。
- ✓ primos に有効な IP アドレスが設定されていること。
- ✓ 使用する primos が SEH primos App に表示されていること。(⇒12)

1. リスト上で、対象の primos をダブルクリックします。
 - ↳ 標準のブラウザが起動して、primos Control Center が表示されます。

primos Control Center の構造



図 2: primos Control Center

ログアウト

表示する言語は、対応する国旗をクリックして選択します。

利用できるメニュー項目はナビゲーションバー(上)にあります。メニュー項目を選択すると(マウスをクリック)、使用可能なサブメニューが左側に表示されます。サブメニューの項目を選択すると、対応するページとその内容が右側に表示されます。

メーカーの連絡先や製品の詳細情報は、**製品と会社情報**に表示されます。**サイトマップ**には、primos Control Center の全体図が表示され、primos Control Center のすべてのページに直接アクセスできます。

他のすべての項目は、primos の設定に関するメニューです。これらの詳細は、primos Control Center のオンラインヘルプを参照してください。オンラインヘルプを起動するには、**?** アイコンをクリックします。

セキュリティ上の理由で、primos Control Center は設定の終了後、必ずログアウトしてください。

1. **ログアウト**をクリックします。
↳ ログインページが表示されます。正常にログアウトされました。

2.2 SEH primos App による管理

SEH primos App は、SEH Computertechnik GmbH が開発した、primos デバイスを管理するソフトウェアです。

動作モード

SEH primos App を起動すると、ネットワークをスキャンして、接続された primos デバイスを検出します。スキャンするネットワークの範囲は任意に設定できます。検出したすべての primos デバイスは、「デバイスリスト」に表示されます。検出したデバイスはすべて選択し管理することができます。

インストール

SEH primos App を使用するには、Windows または Mac OS X/OS X/macOS のオペレーティングシステムで動作するコンピュータにインストールする必要があります。オペレーティングシステムにより異なるインストール用ファイルが利用できません。

システム要件

- Windows 7、Windows 8、Windows 10;
Mac OS X 10.7.x、OS X 10.8~10.11.x、macOS 10.12.x 以降
- インストールは、管理権限のあるユーザのみが実行できます。


1. 使用するオペレーティングシステム用の SEH primos App を、SEH Computertechnik GmbH の Web サイトからダウンロードします。

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



2. SEH primos App をクライアントにインストールします。
↳ SEH primos App がクライアントにインストールされます。

起動

SEH primos App は次のアイコンで識別できます：。SEH primos App は、使用するオペレーティングシステムの通常のメカニズムで起動できます。

必要な情報

3 ネットワーク設定



primos をネットワークへ適切に組み込むために、様々な設定が可能です。

この章では、対応しているネットワーク設定を説明します。

- 「IPv4 パラメータの設定方法」⇒13
- 「IPv6 パラメータの設定方法」⇒14
- 「DNS の設定方法」⇒16
- 「Bonjour の設定方法」⇒17
- 「ディレクトリサービスを設定する方法」⇒17

3.1 IPv4 パラメータの設定方法

primos を TCP/IP ネットワークへ適切に組み込むための、様々な IPv4 パラメータを設定できます。初期設定では、IP アドレスは DHCP により primos に動的に割り当てられます。しかし、静的 IP アドレスを手動で primos に割り当てることもできます。

1. primos Control Center を起動します。
 2. **ネットワーク - IPv4** を選択します。
 3. IPv4 パラメータを設定します。表 1 ⇒13
 4. **保存**をクリックして確定します。
- ↳ 設定が保存されます。

表 1: IP パラメータ

パラメータ	説明
DHCP	DHCP プロトコルを有効または無効にします。 TCP/IP パラメータは、DHCP により primos に自動的に割り当てることができます。
静的	primos への静的な TCP/IP パラメータの手動による割り当てを、有効または無効にします。 IP アドレス、サブネットマスクおよびゲートウェイを指定します。
IP アドレス	primos に手動で割り当てる IPv4 アドレスを指定します。
サブネットマスク	primos に手動で割り当てるサブネットマスクを指定します。
ゲートウェイ	primos に手動で割り当てるゲートウェイアドレスを指定します。

IPv6 の利点

3.2 IPv6 パラメータの設定方法

primos は、IPv6 ネットワークに組み込むことができます。

IPv6 (インターネットプロトコルバージョン 6) は、より一般的な IPv4 の後継バージョンです。IPv6 と IPv4 は、OSI モデルのネットワーク層の標準プロトコルで、ネットワーク経由のデータパケットのアドレス指定およびルーティングを制御します。IPv6 の導入には、多くの利点があります。

- IPv6 により、IP アドレス空間は 2^{32} (IPv4) から 2^{128} (IPv6) へと拡大します。
- 自動設定と再番号割り当て
- ヘッダ情報の縮小によるルーティングの効率化
- IPSec、QoS、マルチキャストなどの統合サービス
- モバイル IP

IPv6 アドレスの構造

IPv6 アドレスは、128 ビットで構成されます。IPv6 アドレスの標準形式は、8 フィールドです。各フィールドに、16 ビットを表す 4 つの 16 進数が含まれます。

各フィールドはコロン (:) で区切られます。例：

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

フィールド内の先頭のゼロは省略できます。例：

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

IPv6 アドレスは、連続するフィールドの内容がすべてゼロ (0) である場合、短縮バージョンを使用して入力または表示できます。この場合、2 つのコロン (::) を使用します。ただし、2 つのコロンが使用できるのは、1 つのアドレスに対し 1 回のみです。例：

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

Web ブラウザで URL として使用する場合、IPv6 アドレスは角括弧 (ブラケット) で囲う必要があります。これにより、ポート番号を IPv6 アドレスの一部と間違えることを防止できます。例：

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

メモ

IPv6 形式の URL は、IPv6 に対応するブラウザでのみ使用できます。

使用できる IPv6 アドレスのタイプ

IPv6 アドレスには、様々なタイプがあります。IPv6 アドレスのプレフィックスは、IPv6 アドレスのタイプに関する情報を提供します。

- ユニキャストアドレスは、グローバルにルーティングできます。これらのアドレスは一意です。ユニキャストアドレスに送信されるパケットを受信できるのは、このアドレスに割り当てられたインターフェイスのみです。ユニキャストアドレスのプレフィックスは「2」または「3」です。
- エニーキャストアドレスは、複数のインターフェイスに割り当てられます。つまり、このアドレスに送信されるデータパケットは様々なデバイスで受信できます。エニーキャストアドレスの構文は、ユニキャストアドレスの構文と同じです。違いは、エニーキャストアドレスが多数のインターフェイスから1つを選択するという点です。
- エニーキャストアドレス専用のパケットは、最も近いインターフェイスで(ルータのメトリックスに従って)受信されます。エニーキャストアドレスは、ルータのみで使用します。
- マルチキャストアドレスにより、帯域幅を比例的に増加させることなく、データパケットを同時に様々なインターフェイスに送信できます。マルチキャストアドレスは、プレフィックス「ff」で認識できます。

1. primos Control Center を起動します。
2. **ネットワーク - IPv6** を選択します。
3. IPv6 パラメータを設定します。表 2 ⇨ 15
4. **保存** をクリックして確定します。
↳ 設定が保存されます。

表 2: IPv6 パラメータ

パラメータ	説明
IPv6	primos の IPv6 機能を有効または無効にします。
自動設定	primos への IPv6 アドレスの自動割り当てを、有効または無効にします。
IPv6 アドレス	primos の IPv6 ユニキャストアドレスを指定します。このアドレスは、n:n:n:n:n:n:n:n の形式で手動で割り当てます。 各「n」は、アドレスの 8 つの 16 ビット要素の 1 つの 16 進値を示します。
ルータ	ルータの IPv6 ユニキャストアドレスを指定します。primos は「ルータ要請」(RS) をこのルータに送信します。

パラメータ	説明
プレフィックス長	IPv6 アドレスのサブネットプレフィックスの長さを設定します。64 の値があらかじめ設定されています。 アドレス範囲はプレフィックスによって決まります。プレフィックス長 (使用するビット数) が IPv6 アドレスに追加され、10 進値で指定されます。10 進数は「/」で区切られます。

3.3 DNS の設定方法

DNS はドメイン名を IP アドレスに変換するサービスです。DNS を使用すると、ドメイン名の IP アドレスへの割り当てや IP アドレスのドメイン名への割り当てができます。

サーバを指定するときに IP アドレスの代わりにホスト名を入力する、など DNS により、設定が容易になることがあります。

メモ

適切に設定されたネットワーク上で、primos は DNS 設定を DHCP により自動的に受信します。

1. primos Control Center を起動します。
2. **ネットワーク - DNS** を選択します。
3. DNS パラメータを設定します。表 3 ⇨ 16
4. **保存** をクリックして確定します。
↳ 設定が保存されます。

表 3: DNS パラメータ

パラメータ	説明
プライマリ DNS サーバ	プライマリ DNS サーバの IP アドレスを指定します。
セカンダリ DNS サーバ	セカンダリ DNS サーバの IP アドレスを指定します。 セカンダリ DNS サーバは、プライマリ DNS サーバが利用できない場合に使用されます。
ドメイン名 (サフィックス)	既存の DNS サーバのドメイン名を指定します。

3.4 Bonjour の設定方法

Bonjour を使用すると、TCP/IP ベースのネットワーク内のコンピュータやデバイスおよびネットワークサービスが自動的に認識されます。

primos は Bonjour を使用して、

- ネットワーク内のプリンタを検索します。(⇒126)
- ZeroConf により割り当てられた IP アドレスを確認します。(⇒17)
- Bonjour サービスをアナウンスします。

primos では Bonjour が常にアクティブです。primos が使用する名を設定して、Bonjour サービスをアナウンスすることができます。初期設定では、primos は「primos@lCxxxxxx」という名前でアドバタイズします。(「lCxxxxxx」はデフォルト名 ⇒173)

1. primos Control Center を起動します。
2. **ネットワーク - Bonjour** を選択します。
3. Bonjour 名を設定します。
4. **保存**をクリックして確定します。
↳ 設定が保存されます。

3.5 ディレクトリサービスを設定する方法

primos をディレクトリサービスに組み込むことができます。ディレクトリサービスにより、ユーザデータを集中管理して primos に提供することができます。ディレクトリサービスのユーザにより、

- 印刷することができるユーザを制御します。⇒137
- primos Control Center にログインするユーザを設定します。⇒150

primos は次のディレクトリサービスに対応しています。

- Active Directory
- LDAP (例：OpenLDAP や Apple® Open Directory)

- 「primos を Active Directory に組み込む」⇒118
- 「primos を LDAP ディレクトリに組み込む」⇒119

選択できる作業

必要事項

primos を Active Directory に組み込む

primos はドメインのメンバーに含めると Active Directory に組み込まれます。

- ✓ DNS サーバが primos 内で設定されていること。⇒[16](#)
 - ✓ primos が、DNS サーバ上にタイプ A のリソースレコード (ホストの IPv4 アドレス) で入力されていること。
 - ✓ タイムサーバが primos 内で設定されていること。⇒[20](#)
1. primos Control Center を起動します。
 2. **ネットワーク - ディレクトリサービス**を選択します。
 3. Active Directory パラメータを設定します。表 4 ⇒[18](#)
 4. **保存**をクリックして確定します。
 - ↳ primos がドメインのメンバーに含まれ、Active Directory に組み込まれます。

表 4: Active Directory パラメータ

パラメータ	説明
Active Directory	primos の既存の Active Directory への組み込みを、有効または無効にします。
Active Directory 名	primos を組み込む Active Directory の名前を指定します。 ドメインのフルネーム (FQDN: 完全修飾ドメイン名) を入力します。
ワークグループ	ワークグループの名前を指定します。 NetBIOS ドメイン名を入力します。
パスワードサーバ	Active Directory のパスワードサーバを IP アドレスまたはホスト名で指定します。(オプション) ホスト名での指定は、DNS サーバがあらかじめ設定されている場合のみ可能です。
WINS サーバ	Active Directory の WINS サーバを IP アドレスまたはホスト名で指定します。 異なるネットワークセグメントの加入者間の通信を可能にするため、WINS サーバを指定することを推奨します。 ホスト名での指定は、DNS サーバがあらかじめ設定されている場合のみ可能です。
アドミニストレータアカウント	ドメインコントローラ上で primos 用に作成された管理者アカウントの名前を指定します。
パスワード	ドメインコントローラ上で primos 用に作成された管理者アカウントのパスワードを指定します。

必要事項

primos を LDAP ディレクトリに組み込む

- ✓ DNS サーバが primos 内で設定されていること。⇒16
 - ✓ primos が、DNS サーバ上にタイプ A のリソースレコード (ホストの IPv4 アドレス) で入力されていること。
 - ✓ タイムサーバが primos 内で設定されていること。⇒20
1. primos Control Center を起動します。
 2. **ネットワーク - ディレクトリサービス**を選択します。
 3. LDAP パラメータを設定します。表 5 ⇒19
 4. **保存**をクリックして確定します。
 - ↳ primos が LDAP ディレクトリに組み込まれます。

表 5: LDAP パラメータ

パラメータ	説明
LDAP	primos の既存の LDAP ディレクトリサービスへの組み込みを、有効または無効にします。
LDAP サーバ	LDAP サーバを IP アドレスまたはホスト名で設定します。 ホスト名での指定は、DNS サーバがあらかじめ設定されている場合にのみ可能です。
ベース DN	ベース DN (識別名) を指定します。ベース DN とは、ディレクトリ内で下方向にユーザ検索するときの出発点です。 ドメイン要素の区切りにはコンマを使用します。 (例: dc=mydomain,dc=com)
セキュアな LDAP	LDAP 接続 (LDAP over SSL/TLS - LDAPS) を暗号化します。 暗号化には CA 証明書が必要です。
LDAP CA 証明書	ドメインコントローラ (DC) の証明書を発行した認証局のルート CA 証明書を選択します。 CA 証明書は、事前にデバイスにインストールされている必要があります ⇒54。

4 デバイス設定



primos に説明とデバイス時間を設定します。この章では、デバイスの設定について説明します。

必要な情報

- 「説明の記述内容を決定する方法」⇒[20](#)
- 「デバイス時間の設定方法」⇒[20](#)
- 「ローカルユーザを設定する方法」⇒[21](#)
- 「ローカルグループを設定する方法」⇒[23](#)

4.1 説明の記述内容を決定する方法

primos には、任意の説明を割り当てることができます。説明により、ネットワーク内で利用できるデバイスの概要がわかりやすくなります。

1. primos Control Center を起動します。
2. **デバイス - 説明**を選択します。
3. **ホスト名、説明および担当者**の任意の名前を入力します。
4. **保存**をクリックして確定します。
↳ 説明が保存されます。

4.2 デバイス時間の設定方法

primos のデバイス時間は、ネットワーク内のタイムサーバ (SNTP サーバ) により管理できます。タイムサーバは、ネットワーク内のデバイスの時間を同期します。

利点と目的

primos がディレクトリサービス (⇒[17](#)) に参加して、ジョブ履歴内 (⇒[33](#)) の印刷ジョブにタイムスタンプを設定する際に、デバイス時間が必要です。

UTC

primos は、「UTC」(協定世界時) を基準として使用します。UTC は時間の標準として使用される基準時です。

タイムゾーン

タイムサーバから受信する時間は、必ずしもローカルタイムゾーンに対応していないことがあります。地域や時間差 (夏時間のように国独自の制度を含む) による差

異は、「タイムゾーン」パラメータを使用して対処できます。

メモ

タイムサーバは、DHCP により自動的に割り当てることができます。DHCP により割り当てられたタイムサーバは、手動で設定されたタイムサーバより常に優先されます。

必要事項

- ✓ タイムサーバがネットワークに接続されていること。
- 1. primos Control Center を起動します。
- 2. **デバイス - 日付 / 時間** を選択します。
- 3. **日付 / 時間** にチェックマークを付けます。
- 4. **タイムサーバ** 欄に、タイムサーバの IP アドレスまたはホスト名を入力します。
ホスト名での指定は、DNS サーバがあらかじめ設定されている場合にのみ可能です。
- 5. **タイムゾーン** リストからローカルタイムゾーンのコードを選択します。
- 6. **保存** をクリックして確定します。
↳ 設定が保存されます。

4.3 ローカルユーザを設定する方法

ユーザ認証を使用すると、印刷できるユーザを制御することができます。⇒ 37 制御するには、ディレクトリサービスのユーザ (⇒ 17) またはローカルユーザのいずれかを使用することができます。

primos にローカルユーザをセットアップします。各ユーザには名前とパスワードが必要です。また、各ユーザは 1 つ以上のユーザグループ (⇒ 37) に割り当てることができるため、ユーザ認証を使用する際に、より簡単に複数のユーザを登録することができます。

選択できる作業


- 「ローカルユーザの作成」⇒ 21
- 「パスワードの変更」⇒ 22
- 「グループのメンバシップの変更」⇒ 22
- 「ローカルユーザの削除」⇒ 22

ローカルユーザの作成


1. primos Control Center を起動します。

2. **デバイス - ユーザ**を選択します。
3. **名前欄**に任意のユーザ名を入力します。
(A～z、A～Z、0～9が使用できます。)
4. **パスワード欄**に、パスワードを入力します。
5. パスワードを再度入力します。
6. **グループ**領域でユーザグループを選択します。
7. 確定するには、**保存**をクリックします。
↳ ローカルユーザが作成されます。


パスワードの変更

1. primos Control Center を起動します。
2. **デバイス - ユーザ**を選択します。
3.  アイコンをクリックし、編集するユーザを選択します。
4. **パスワード欄**に、パスワードを入力します。
5. **パスワード**を再度入力します。
6. 確定するには、**保存**をクリックします。
↳ パスワードが変更されます。

グループのメンバシップの変更

1. primos Control Center を起動します。
2. **デバイス - ユーザ**を選択します。
3.  アイコンをクリックして、編集するユーザを選択します。
4. **グループ**領域でユーザグループを選択します。
5. 確定するには、**保存**をクリックします。
↳ グループのメンバシップが変更されます。

ローカルユーザの削除

1. primos Control Center を起動します。
2. **デバイス - ユーザ**を選択します。
3.  アイコンをクリックして、削除するユーザを選択します。
4. セキュリティクエリを確認します。
↳ ユーザが削除されます。

4.4 ローカルグループを設定する方法

ユーザ認証を使用すると、印刷できるユーザを制御することができます。⇒[137](#) 制御するには、ディレクトリサービスのユーザ (⇒[17](#)) またはローカルユーザ (⇒[21](#)) のいずれかを使用することができます。

複数のローカルユーザをより簡単に登録するには、ユーザをローカルグループでグループ化し、ユーザを個別に入力する代わりにグループとして一括で登録することができます。

primos にローカルグループをセットアップします。グループメニューで、ユーザをグループに割り当てることができます。または、ユーザメニューで各ユーザに対してグループを選択できます。


選択できる作業

- 「ローカルグループの作成」⇒[23](#)
- 「ユーザのメンバシップの変更」⇒[23](#)
- 「ローカルグループの削除」⇒[24](#)

ローカルグループの作成

1. primos Control Center を起動します。
2. **デバイス - グループ**を選択します。
3. **名前欄**に任意のグループ名を入力します。
(A～z、A～Z、0～9が使用できます。)
4. **ユーザ領域**でユーザを選択します。
5. 確定するには、**保存**をクリックします。
↳ ローカルグループが作成されます。

ユーザのメンバシップの変更

1. primos Control Center を起動します。
2. **デバイス - グループ**を選択します。
3.  アイコンをクリックして、編集するグループを選択します。
4. **ユーザ領域**でユーザを選択します。
5. 確定するには、**保存**をクリックします。
↳ ユーザのメンバシップが変更されます。

ローカルグループの削除

1. primos Control Center を起動します。
2. **デバイス - グループ**を選択します。
3. **✕** アイコンをクリックして、削除するグループを選択します。
4. セキュリティクエリを確認します。
↳ グループが削除されます。

5 印刷



この章では、primos の印刷設定をする方法と印刷の拡張設定をする方法について説明します。

iOS デバイスから primos を使用して印刷するには、primos の各プリンタに対して印刷キューを作成する必要があります。次に、各キューに対して、アクセス制御などを設定します。また、一般的な印刷オプションも設定できます。

必要な情報

- 「primos 上でプリンタを設定する方法 (キューの作成)」⇒[26](#)
- 「キューを管理する方法」⇒[31](#)
- 「ジョブ履歴を表示する方法」⇒[33](#)
- 「iOS デバイス上に表示するプリンタ名を設定する方法」⇒[35](#)
- 「primos でプリンタを管理、検査する方法」⇒[36](#)
- 「primos でプリンタを管理、検査する方法」⇒[36](#)
- 「データ転送を暗号化する方法」⇒[36](#)
- 「印刷するユーザを制御する方法」⇒[37](#)
- 「iOS デバイスから印刷する方法」⇒[39](#)
- 「サブネット間で印刷する方法 (Wide-Area AirPrint)」⇒[40](#)

5.1 primos 上でプリンタを設定する方法 (キューの作成)

iOS デバイスから primos を介して印刷するには、primos 上に各プリンタの簡単な印刷キューを作成する必要があります。

キューとは

キューは、プリンタとの通信や印刷ジョブの送信に使用されます。キューに収集された印刷ジョブは、順番に処理されます。これにより、一台のプリンタを競合せずに、複数で共有することができます。

メモ

primos 内に最大 10 個のキューが作成できます。

キューを作成する
方法

primos 上のキューは、次の 3 つの場合に作成される可能性があります。

- **スマートプリンタセットアップ**：ネットワークプリンタの検索を開始します。最大で 10 個のキューが自動的に作成されます。
- **エキスパートプリンタセットアップ**：ネットワークプリンタの検索を開始します。次に、検出されたプリンタが一覧表示され、プリンタに対し提案されたキューも表示されます。提案されたキューを編集することで最大 10 個のキューが作成できます。
(プリンタ設定の知識が必要です。)
- **手動でキューを作成します**：キューを手動で作成する場合は、単一のキューですべてを設定する必要があります。手動で作成している場合は、ネットワークのプリンタが検索されます。キューを作成するプリンタを検索結果リストから選択する、またはプリンタ接続を手動で設定します。
(このキューの作成方法は、キューを 1 つのみ作成する場合、または特定のプリンタにキューを作成する場合に適しています。)

メモ

スマートプリンタセットアップは、primos 上でキューが作成されていない場合のみ利用できます。

選択できる作業

- 「スマートプリンタセットアップの使用」⇒ 27
- 「エキスパートプリンタセットアップの使用」⇒ 27
- 「手動によるキューの作成」⇒ 29

どのキューが作成されるか

スマートプリンタセットアップの使用

primos を初めてインストールした場合など、起動した primos Control Center のホームページに primos 上の作成されたキューがない場合は、スマートプリンタセットアップを起動することができるポップアップ画面が自動的に表示されます。または、スマートプリンタセットアップは手動でも起動できます。

primos 上では、最大 10 個のキューが自動的に作成されます。

- ✓ primos 上に作成されたキューはありません。
- 1. primos Control Center を起動します。
- 2. **プリンティング - プリンターの設定**を選択します。
- 3. **検出結果の初期設定 領域**に検出結果に基づきキューを作成する初期設定を指定します。
- 4. **スマートプリンタセットアップ**をクリックします。
 - ↳ スマートプリンタセットアップが起動します。primos によりネットワークプリンタが検索され、検出された最大 10 台のプリンタのキューが自動的に作成されます。次に、作成されたキューの概要が表示されます。

メモ

ネットワークの規模によっては、スマートプリンタセットアップの実行に数分かかる場合があります。

エキスパートプリンタセットアップの使用

- ✓ primos 上では、最大 9 個のキューが作成されます。
- 1. primos Control Center を起動します。
- 2. **プリンティング - プリンターの設定**を選択します。
- 3. **検出結果の初期設定領域**に検出結果に基づきキューを作成する初期設定を指定します。
(検出結果の編集では、キューを個別に変更できます。)
- 4. **エキスパートプリンタセットアップ**をクリックします。
プリンタの検出が開始されます。プリンタの検出が終了すると、検出されたプリンタのリストが表示されます。

メモ

ネットワークの規模によっては、プリンタの検出に数分かかる場合があります。

5. 任意のプリンタのキューを設定します。表 6 ⇨ 28。
 - キューを作成するプリンタを複数選択するには、プリンタの前にあるチェックボックスを使用します。
 - 検索結果は、結果の種類 (新たに検出されたプリンタのみ、またはすべてのプリンタ) およびプリンタ接続 (IPP/IPPS) に従って、絞り込むことができます。

メモ

すでに設定された検出結果の場合は、絞り込みを実行しないでください。非表示のキューは、自動的に初期設定値にリセットされます。

6. **すべてを保存**または**選択対象の保存**をクリックします。
↳ primos 内にキューが作成されます。

メモ

キューを作成すると、キューに対する拡張設定を行うことができます。参照: 「キューの編集」⇨ 31。

表 6: キューのパラメータ

パラメータ	説明
アドレス指定	プリンタをネットワーク上でアドレス指定する方法を設定します。 - Bonjour を使用 - ホスト名または IP アドレス (ルーティング可能) を使用 セットアップ後に primos またはプリンタを別のネットワークに移動する場合は、ホスト名または IP アドレスを選択します。
名前	キュー名を任意で設定します。iOS デバイスのプリンタ用ダイアログで表示されるプリンタ名は、キュー名と AirPrint 識別子の組合せで構成されます。 最大で 50 ASCII 文字 (括弧、スペース、スラッシュ、クォーテーション記号、ポンド記号を除く) が使用できます。表示されたプリンタ名 (⇨ 35) では、下線はスペースとして表示されます。 キュー名は後からは変更できません。
設置場所	デバイスの場所の説明を任意に設定します。(半角 80 文字以内)
地理的場所	プリンタの場所を地理座標で指定します。 緯度 (-90 ~ 90) と経度 (-180 ~ 180) の座標を小数点表記、コンマ区切りで入力します。例: 51.982898,8.493206

手動によるキューの作成

1. primos Control Center を起動します。
2. **プリンティング - キューの作成** を選択します
3. キューのパラメータを設定します。表 7 ⇨ 29。
4. **キューの作成** をクリックします。
↳ primos 内にキューが作成されます。

表 7:

パラメータ	説明
名前	<p>キュー名を任意で設定します。iOS デバイスのプリンタ用ダイアログで表示されるプリンタ名は、キュー名と AirPrint 識別子 (⇨ 35) の組合せで構成されます。</p> <p>最大で 50 ASCII 文字 (括弧、スペース、スラッシュ、クォーテーション記号、ポンド記号を除く) が使用できます。表示されたプリンタ名 (⇨ 35) では、下線はスペースとして表示されます。</p> <p>キュー名は後からは変更できません。</p>
設置場所	<p>デバイスの場所の説明を任意に設定します。(半角 80 文字以内)</p>
地理的場所	<p>プリンタの場所を地理座標で指定します。</p> <p>緯度 (-90 ~ 90) と経度 (-180 ~ 180) の座標を小数点表記、コンマ区切りで入力します。例: 51.982898,8.493206</p>
プリンタの選択	<p>プリンタを指定します。</p> <p>このリストは、ネットワーク上で自動的に検出されたプリンタを表示します。手動でプリンタ接続を指定することもできます。(「接続」)</p>
接続の種類	<p>リストから選択したプリンタの印刷プロトコル (IPP/IPPS) を設定します。</p> <p>選択できる印刷プロトコルは、選択したプリンタに対応するプロトコルのみです。</p>

パラメータ	説明
接続	<p>デバイス URI (統一資源識別子) の形式で、プリンタへの接続を指定します。</p> <p>IPP / IPPS: IPP (インターネット印刷プロトコル) では、印刷データは HTTP によりプリンタに送信されます。primos とプリンタ間の接続は、SSL/TLS (IPPS) により暗号化できます。標準ポート IPP: 631。標準ポート IPPS: 443。</p> <p><code>ipp://<プリントの IP アドレス、Bonjour 名、またはホスト名>:<ポート番号>/ipp/print</code></p> <p><code>ipp://<プリントの IP アドレス、Bonjour 名、またはホスト名>/ipp/print</code></p> <p><code>ipps://<プリントの IP アドレス、Bonjour 名、またはホスト名>:<ポート番号>/ipp/print</code></p> <p><code>ipps://<プリントの IP アドレス、Bonjour 名、またはホスト名>/ipp/print</code></p> <p>または、ネットワーク上で自動的に検出されたプリンタをリストから選択し、接続タイプを選択します。</p>

選択できる作業

5.2 キューを管理する方法

primos 内のネットワークプリンタ用に作成したキューは、編集または削除できます。

- 「キューの編集」⇒ 31
- 「キューの削除」⇒ 32

キューの編集


1. primos Control Center を起動します。
2. **プリンティング - キュー**を選択します。
3.  アイコンをクリックして、編集するキューを選択します。
4. キューのパラメータを設定します。表 8 ⇒ 31
5. **保存**をクリックして確定します。
 - ↳ 設定が保存されます。

表 8: キューの編集 - パラメータ

パラメータ	説明
設置場所	デバイスの場所の説明を任意に設定します。(半角 80 文字以内)
地理的場所	プリンタの場所を地理座標で指定します。 緯度 (-90 ~ 90) と経度 (-180 ~ 180) の座標を小数点表記、コンマ区切りで入力します。例: 51.982898,8.493206
接続	デバイス URI (統一資源識別子) の形式で、プリンタへの接続を指定します。 IPP/IPPS : IPP (インターネット印刷プロトコル) では、印刷データは HTTP によりプリンタに送信されます。primos とプリンタ間の接続は、SSL/TLS (IPPS) により暗号化できます。標準ポート IPP : 631 標準ポート IPPS : 443 ipp://< プリントの IP アドレス、Bonjour 名、またはホスト名 > : <ポート番号 > /ipp/print ipp://< プリントの IP アドレス、Bonjour 名、またはホスト名 > /ipp/print ipps://< プリントの IP アドレス、Bonjour 名、またはホスト名 > : <ポート番号 > /ipp/print ipps://< プリントの IP アドレス、Bonjour 名、またはホスト名 > /ipp/print
アクション	参照: 「primos でプリンタを管理、検査する方法」⇒ 36。

パラメータ	説明
マルチキャストパブリッシング	参照：「手動で作成されたキューは公開されません。」⇨図78。
セキュアな AirPrint	参照：「データ転送を暗号化する方法」⇨図36。
ユーザ認証	参照：「印刷するユーザを制御する方法」⇨図37。
アクセス	参照：「印刷するユーザを制御する方法」⇨図37。

キューの削除

メモ

削除したキューがしばらくの間、iOS デバイス上に表示されている場合があります。iOS デバイスは、時間の経過に伴って自らの情報を更新するため、しばらくすると削除したキューは表示されなくなります。

1. primos Control Center を起動します。
2. **プリンティング - キュー** を選択します。
3. 削除するファイルの **✕** 記号をクリックします。
4. セキュリティクエリを確認します。
↳ キューが削除されます。

5.3 ジョブ履歴を表示する方法

「ジョブ履歴」には、primos が処理した印刷ジョブの情報が表示されます。

最大 100 個の印刷ジョブが表示されます。101 個目からは FIFO (先入れ先出し) 方式が適用されます。記録された印刷ジョブは、primos をリセットすると削除されます。

メモ

日付と時間が正確に表示されるよう、タイムサーバ (⇒ 20) を primos 内で設定する必要があります。タイムサーバが設定されていない場合、タイムスタンプは初期設定時間と一致します。

フィルタ

表示された印刷ジョブは、次の条件で絞り込むことができます。

- すべてのジョブ
- 完了したジョブ
- アクティブなジョブ

アクション

アクティブな印刷ジョブを削除できます。

- ジョブのキャンセル
- すべてのアクティブなジョブのキャンセル

1 つの印刷ジョブがエラーで処理できない場合、次のジョブもすべて処理できません。この場合、「ブロックしている」印刷ジョブを削除すると次の印刷ジョブが処理できるようになります。

選択できる作業

- 「ジョブ履歴を表示する」⇒ 33
- 「ジョブ履歴を絞り込む」⇒ 34
- 「印刷ジョブの削除」⇒ 34

ジョブ履歴を表示する

1. primos Control Center を起動します。
2. **プリンティング - ジョブ履歴** を選択します。
↳ ジョブ履歴が表示されます。

ジョブ履歴を絞り込む

1. primos Control Center を起動します。
2. **プリンティング - ジョブ履歴** を選択します。
ジョブ履歴が表示されます。
3. フィルタ (絞り込み) ボタンをクリックします。
↳ フィルタに従いジョブ履歴の内容が表示されます。

印刷ジョブの削除

1. primos Control Center を起動します。
2. **プリンティング - ジョブ履歴** を選択します。
ジョブ履歴が表示されます。
3. **アクティブなジョブ** をクリックします。
アクティブなジョブがすべて表示されます。
4. 1 つまたはすべての印刷ジョブを削除します。
 - 1 つの印刷ジョブの削除：**ジョブのキャンセル** をクリックします。
 - すべての印刷ジョブの削除：**すべてのアクティブなジョブのキャンセル** をクリックします。↳ 選択したジョブが削除されます。

キュー名

AirPrint 識別子

5.4 iOS デバイス上に表示するプリンタ名を設定する方法

iOS デバイス上の印刷ダイアログでは、プリンタ名は次の構成に従い表示されます：「<AirPrint 識別子 >< キュー名 >」両方の要素はともに任意名を付けることができます。

キュー名は、キューの作成時に個別に指定します (⇒ 26)。後から変更することはできません。

AirPrint 識別子は、iOS デバイス上で primos を使用して利用できるプリンタを表すプレフィックスです。AirPrint 識別子はすべてのキューに適用されます。この識別子はいつでも変更できます。既定値は「air」です。



最初のアルファベット文字から始まる識別子を選択します。そうすることで、primos により利用できるプリンタを、iOS デバイス上の印刷ダイアログの上位に表示することができます。

例：AirPrint 識別子の「air」とプリンタ名が使用されています。

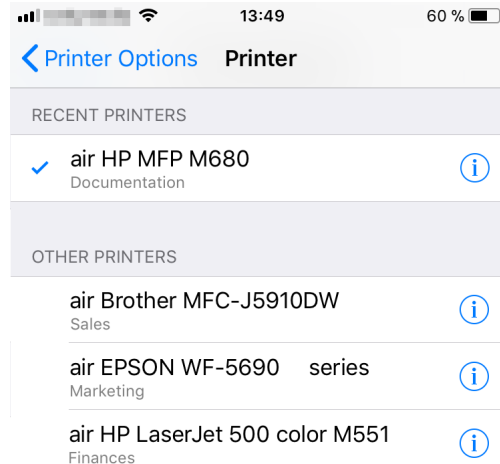


図 3: iOS デバイス上の印刷ダイアログのプリンタ名

1. primos Control Center を起動します。
2. **プリンティング - 設定**を選択します。
3. **AirPrint 識別子**欄に任意の ID を入力します。

下線は使用できません。

4. **保存**をクリックして確定します。

↳ 設定が保存されます。

5.5 primos でプリンタを管理、検査する方法

キュー、すなわちプリンタに対し、次のような動作をトリガできます。

- テストページの印刷
- プリンタの停止または再起動
(プリンタが停止すると、印刷ジョブは取り込まれるだけで印刷されません。取り込まれたすべての印刷ジョブは、プリンタの起動と同時に印刷されます。)
- すべての印刷ジョブの拒否または再受入れ
- 印刷ジョブの削除


利点と目的

この操作は、プリンタのテストやメンテナンスに役立ちます。例：

- プリンタの接続を確認するために、テストページを印刷します。
- トナーの交換、用紙の追加などプリンタの簡単なメンテナンス作業をする場合は、対象のプリンタを停止します。
- 修理などでプリンタの長時間にわたるダウンタイムが予想される場合は、すべての印刷ジョブを拒否することを推奨します。

必要事項

✓ primos にキューが作成されていること。⇒ 26

1. primos Control Center を起動します。
2. **プリンティング - キュー**を選択します。
3.  アイコンをクリックして、任意のキューを選択します。
4. **デバイス**領域で、**アクション**リストから任意のプリンタ動作を選択します。
5. **保存**をクリックして確定します。
↳ プリンタ動作がトリガされます。

5.6 データ転送を暗号化する方法

印刷データは、iOS デバイスから primos を介してプリンタに送信されます。印刷データの流れは、次の2つに分けることができます。

- 印刷データを iOS デバイスから primos に送信
(初期設定では、印刷データは暗号化されずに送信されます。セキュアな AirPrint により送信を暗号化できます。次を参照してください。)
- 印刷データを primos からプリンタに送信
(キューに指定した接続タイプは、印刷データを primos からプリンタに送信す

セキュアな AirPrint


るためのプロトコルを設定します。選択したプロトコルに従い、印刷データは暗号化あり、または暗号化なしで送信されます。(⇒[26](#) を参照してください。)

iOS デバイスから primos への印刷データの送信は、SSL/TLS 暗号化方式により暗号化できます。暗号化はプロトコル及び暗号化レベルで定義されています (⇒[47](#))。暗号化は、各キューに設定してください。

メモ

暗号化により印刷データの送信が遅くなることがあります。

必要事項

- ✓ primos にキューが作成されていること。(⇒[26](#))
 - ✓ primos に証明書がインストールされていること。(⇒[54](#))
1. primos Control Center を起動します。
 2. **プリンティング - キュー** を選択します。
 3.  アイコンをクリックして、任意のキューを選択します。
 4. **セキュアな AirPrint** にチェックマークを付ける、またはチェックマークを外します。
 5. **保存** をクリックして確定します。
↳ 設定が保存されます。

メモ

印刷データの送信を完全に暗号化するには、IPPS 接続で primos からプリンタへの送信を暗号化することを推奨します。(⇒[26](#))

5.7 印刷するユーザを制御する方法

キューへのアクセスを制限することで、対応するプリンタの印刷を制限できます。そのためには、ユーザ認証を使用しますが、印刷時にユーザ名と対応するパスワードを iOS デバイスに入力する必要があります。したがって、ユーザ名とパスワードがない場合、どのようなユーザも iOS デバイスから印刷することができません。

メモ

制限付きアクセスは、iOS デバイス上で  アイコンが付きます。

メモ

iOS デバイスは、この情報を自動的に保存します。このキューにより、最初の印刷

動作モード

時のみ認証する必要があります。

ユーザ認証は、各キューに対して個別にセットアップします。ユーザは次の2つの方法で設定できます。

- ローカルユーザとして (⇒ 21)、または
- ディレクトリサービス (Active Directory または LDAP) を使用 (⇒ 17)




複数のユーザをより簡単に登録するには、ユーザをローカルグループ (⇒ 23) またはディレクトリサービスグループにグループ化し、ユーザを個別に入力する代わりにグループとして一括で登録することができます。

さらにユーザ制限も次の2つの方法でセットアップできます。

- すべてのユーザがアクセス：すべてのローカルユーザ / グループと、設定されたディレクトリサービスのユーザ / グループは印刷することができます。
- アクセス制限：印刷を許可するユーザ / グループをリストでセットアップします。
 - 許可リスト：リストに記載されたユーザ / グループのみが印刷を実行することができます。
 - 拒否リスト：リストに記載されたユーザ / グループは印刷することができません。それ以外のすべてのユーザ / グループは印刷が実行できます。

必要事項

- ✓ primos にキューが作成されていること。 (⇒ 26)
 - ✓ ユーザやグループがセットアップされたディレクトリサービス (⇒ 17) に primos が組み込まれていること。
または
ローカルユーザをセットアップし (⇒ 21)、必要に応じてグループ化されていること (⇒ 21)。
1. primos Control Center を起動します。
 2. プリンティング - キューを選択します。
 3.  アイコンをクリックして、任意のキューを選択します。
 4. ユーザ認証にチェックマークを付けます。
 5. 制限を選択します。
 - すべてのユーザがアクセス：すべてのローカルユーザ / グループと、設定されたディレクトリサービスのユーザ / グループが印刷を実行することができます。

- アクセス制限：印刷を許可するユーザ/グループをリストでセットアップします。
- 6. アクセス制限を選択した場合は、リストの種類を選択します。
 - 許可リスト：リストに記載されたユーザ/グループのみが印刷を実行することができます。
 - 拒否リスト：リストに記載されたユーザ/グループは印刷を実行することができません。それ以外のすべてのユーザ/グループは印刷が実行できます。
- 7. 次に、**リストへのユーザ/グループの追加**欄に任意のユーザ/グループを入力し、**追加**で確定します。入力に関する注意：
 - 複数のユーザやグループは、コンマで区切ります。
 - ユーザの入力。ローカルユーザー名 と ドメイン名 \ ユーザ名
 - グループの入力：@ ローカルグループ名 と @ ドメイン名 \ ユーザ名
- 8. 確定するには、**保存**をクリックします。
 - ↳ 設定が保存されます。

5.8 iOS デバイスから印刷する方法

文書や画像のような内容を iOS デバイス (iPhone、iPad など) から簡単かつ自由に印刷します。この場合、印刷ジョブはネットワークを介して AirPrint 対応の iOS アプリから primos に送信されます。primos は、印刷ジョブを印刷処理のためにプリンタに転送します。

メモ

印刷許可が制限されている場合 (⇒ 5.37)、印刷する前に iOS デバイスはユーザ名とパスワードを問い合わせます。iOS デバイスはこの情報を自動的に保存し、このキューで最初に印刷するときのみ認証する必要があります。

必要事項

- ✓ primos 上でプリンタ用のキューが作成されていること。⇒ 5.26
 - ✓ 対象の iOS デバイスは、無線 LAN を介してネットワークに接続されていること。
 - ✓ 対象の iOS デバイスが AirPrint に対応していること。
 - ✓ 選択しているアプリが AirPrint に対応していること。
1. 使用している iOS デバイス上で、印刷元のアプリを起動します。
 2. 印刷する内容を選択します。
 3. 印刷メニューを開きます。
 4. **プリンタ**をタップします。
使用できるプリンタがすべて表示されます。primos で使用できるプリンタに

は、初期設定で AirPrint 識別子のタグが付いています。⇒[図35](#)

5. リストから目的のプリンタを選択します。
 6. 印刷部数などの印刷オプションを設定します。
 7. **印刷**をタップします。
- ↳ 選択した内容が印刷されます。



印刷中に、iOS デバイスの Print Center で印刷状況を確認できます。Print Center を起動するには、ホームボタンをダブルクリックして **Print Center** をタップします。

5.9 サブネット間で印刷する方法 (Wide-Area AirPrint)

AirPrint は、Bonjour プロトコル (⇒[図17](#)) によりプリンタを検出してネットワーク上で使用できるようにします。

ただし、Bonjour はローカルのネットワークセグメントに制限されています。複数のネットワークセグメントにわたるプリンタの検索と検出ができるように、primos を設定する必要があります。その設定によりネットワーク全体での印刷が可能になります。次の手順に従い操作してください。

手順

- primos 上の Wide-Area AirPrint を有効にします。「primos 上で Wide-Area AirPrint を設定する」⇒[図41](#)
- primos のサブドメインを指定します。(例：primos.mydomain.com) primos 上でこのサブドメインを設定します。「primos 上で Wide-Area AirPrint を設定する」⇒[図41](#)

警告

primos のサブドメインの末尾は「.local」でないことが必要です。このドメイン名はマルチキャスト Bonjour (mDNS) に予約されています。

- primos 上で、Wide-Area AirPrint で使用するプリンタを指定します。「primos 上で Wide-Area AirPrint を設定する」⇒[図41](#)
- 任意で、プリンタをネットワーク上に公開するための標準的な仕組み (マルチキャスト) を無効にすることができます。無効にすると、プリンタは Wide-Area AirPrint を介してのみの利用となります。(「primos 上で Wide-Area AirPrint を設定する」⇒[図41](#) を参照してください。)

必要事項

- DNS サーバ上で条件付きフォワーダを設定します。primos のサブドメインを含むリクエストを primos に転送する必要があります。⇒[42](#)
- Wide-Area AirPrint を使用する iOS デバイスに対して、primos のサブドメイン内にあるプリンタを検索し検出する方法を指示します。検索をするには、primos のサブドメインが iOS デバイス上で検索ドメインとして設定されている必要があります。この設定は、ドメイン内のすべての iOS デバイス上で、手動または自動で行うことができます。
 - 「iOS デバイス上で primos のサブドメインを検索ドメインとして自動的に設定する」⇒[42](#)
 - 「iOS デバイス上で primos のサブドメインを検索ドメインとして手動で設定する」⇒[44](#)

primos 上で Wide-Area AirPrint を設定する

- ✓ DNS サーバがネットワーク内で動作していること。
 - ✓ DNS サーバが primos 内で設定されていること。⇒[16](#)
1. primos Control Center を起動します。
 2. **プリンティング - 設定**を選択します。
 3. Wide-Area AirPrint パラメータを設定します。表 9 ⇒[41](#)
 4. **保存**をクリックして確定します。
 - ↳ 設定が保存されます。

表 9: Wide-Area AirPrint パラメータ

パラメータ	説明
Wide-Area AirPrint	Wide-Area AirPrint を有効、または無効にします。
primos のサブドメイン	primos の条件付きフォワーダが、DNS サーバ上で設定されている Wide-area AirPrint ドメイン名。
Wide-Area AirPrint により公開するプリンタ	Wide-Area AirPrint により使用できるプリンタを指定します。
マルチキャストパブリッシング	ネットワーク上で (マルチキャストにより) 公開するキューの標準的な仕組みを、有効または無効にします。 このオプションを無効にした場合、プリンタは Wide-Area AirPrint を介してのみ利用できます。

必要事項

DNS サーバ上で条件付きフォワーダを設定する

例として、Windows Server 2012 での設定手順を説明します。

- ✓ primos 内で、Wide-Area AirPrint が設定されていること。⇒ 41
 - ✓ DNS サーバがネットワーク内で動作していること。
 - ✓ Windows Server 2012 に管理者としてログオンしていること。
1. **DNS マネージャ** を起動します。
 2. **条件付フォワーダ** を右クリックして、ショートカットメニューから **新規条件付フォワーダ** を選択します。
新規条件付フォワーダ ダイアログが表示されます。
 3. **DNS ドメイン** 欄に、primos のサブドメインを入力します。
 4. **マスタ サーバの IP アドレス** 領域の IP アドレスに、primos の **IPv4 アドレス** を入力します。
Windows Server 2012 により入力内容が検証されます。問題なく検証が完了すると、緑色のチェック記号が表示されます。「OK」をクリックします。
 5. **OK** をクリックして確定します。
↳ 条件付きフォワーダが保存されます。

iOS デバイス上で primos のサブドメインを検索ドメインとして自動的に設定する
primos のサブドメインは、検索ドメインとして、DHCP サーバによりすべての iOS デバイスに自動的に設定することができます。そのために、DHCP サーバに primos のサブドメインをオプション 119 として入力します。iOS が DHCP サーバにリクエストを送信すると直ぐに応答があり、primos のサブドメインを検索ドメインとして自動的に受信します。iOS デバイスは、この情報を自動的に保存します。

準備

例として、Windows Server 2012 での設定手順を説明します。Windows 2012 の DHCP サーバ上では、サブドメインをコード化した形式で入力する必要があります。(RFC 3397 で規定。) このコード化は難しいため、primos Control Center にはコード化ツールが用意されています。IPv4 DHCP 範囲と primos のサブドメインを入力すると、コード化された primos のサブドメインと IPv4 DHCP 範囲を含むコマンドラインコマンドが提供されます。

1. primos Control Center を起動します。
2. **メンテナンス - サービス** を選択します。
3. **DHCP オプション 119** の領域で、IPv4 DHCP 範囲を **DHCP 範囲** 欄に入力してく

ださい。

4. **DHCP オプション 119** の領域で、**primos のサブドメイン**を primos サブドメイン欄に入力してください。

↳ **コマンド欄**は、**コマンドラインコマンド**を表示します。コマンドラインコマンドを、テキストファイルやクリップボードなどに保存します。

設定

Windows Server のグラフィカルインターフェイスでは、DHCP オプション 119 用の使い勝手の良い設定インターフェイスは提供されていません。そのため、Windows Server 2012 上での設定は、次のようにコマンドラインを使用します。

例

次の例を使用し、設定を詳しく説明します。

primos のサブドメイン： primos.mydomain.com

IPv4 DHCP 範囲： 10.168.0.0

コマンドラインコマンド：

```
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
```

メモ

最初の 2 行は情報を表示します。したがって、この行は「REM」でコメントアウトされ、実行されません。

必要事項

- ✓ primos 内で、Wide-Area AirPrint が設定されていること。⇒[41](#)
- ✓ DNS サーバがネットワーク内で動作していること。
- ✓ DNS サーバ上で、primos のサブドメインの条件付きフォワーダが設定されていること。⇒[42](#)
- ✓ DHCP サーバがネットワーク内で動作していること。
- ✓ Windows Server 2012 に管理者としてログオンしていること。
- ✓ コマンドラインコマンドが利用できます。「準備」⇒[42](#)

1. コマンドプロンプトを起動します。
管理者：コマンドプロンプト欄が表示されます。
2. 先に作成したコマンドラインコマンドを実行します。

例：

```
netsh dhcp server V4 delete optiondef 119
```

(必要な場合は、設定済みのオプション 119 を削除します。)

```
netsh dhcp server V4 add optiondef 119 "DNS Search Path"  
BYTE 1
```

(オプション 119 を有効にします。)

```
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
```

(オプション 119 を設定します。)

各コマンドの実行後、正常に実行されたことを確認します。

- ↳ primos のサブドメインが、DHCP サーバ上にオプション 119 として作成されます。DHCP サーバは、すべての iOS デバイス上に、primos のサブドメインを検索ドメインとして自動的に設定します。



この項目が DHCP サーバ上に表示されていることを確認します。そのために、DHCP サーバを起動し、**<所属するドメイン> - IPv4 - <範囲> - スコアオプション**を確認します。必要に応じて、表示を更新します。

iOS デバイス上で primos のサブドメインを検索ドメインとして手動で設定する
primos のサブドメインを、検索ドメインとして直接 iOS デバイスに入力できます。

必要事項

- ✓ primos 内で、Wide-Area AirPrint が設定されていること。⇒ 41
 - ✓ DNS サーバがネットワーク内で動作していること。
 - ✓ DNS サーバ上で、primos のサブドメインの条件付きフォワーダが設定されていること。⇒ 42
1. 使用している iOS デバイスで、**設定メニュー**を起動します。
 2. **Wi-Fi** を選択します。
Wi-Fi メニューが表示されます。
 3. リストから、使用している Wi-Fi を選択します。

Wi-Fi 設定が表示されます。

4. **検索ドメイン**オプションを選択します。
キーボードが表示されます。
5. primos のサブドメインを追加します。
(複数の検索ドメインは、コンマで区切ります。)
6. キーボードがフェードアウトします。
↳ iOS デバイス上で、primos のサブドメインが検索ドメインとして設定されます。
iOS デバイスが、primos のサブドメイン内のプリンタを検索して検出します。

6 セキュリティ



primos に最適なセキュリティを確保するために、多くのメカニズムが利用できます。この章では、これらのセキュリティメカニズムを活用する方法を説明します。

必要な情報

- 「SSL/TLS 接続の暗号化強度を設定する方法」⇒[47](#)
- 「primos Control Center へのアクセスを制御する方法」⇒[49](#)
- 「ユーザプロファイルを管理する方法 (アクセス制御)」⇒[50](#)
- 「クロスサイトスクリプティングから primos を保護する方法」⇒[52](#)
- 「primos へのアクセスを制御する方法 (TCP ポートアクセス制御)」⇒[52](#)
- 「証明書の正しい使用方法」⇒[54](#)
- 「認証方式を使用する方法」⇒[60](#)

6.1 SSL/TLS 接続の暗号化強度を設定する方法

primos を介した次の接続は、SSL/TLS で暗号化できます。

- primos Control Center への Web アクセス：HTTPS (⇒ 49)
- 印刷データの送信：IPPS と セキュアな AirPrint (⇒ 36)

暗号化の強度

暗号化の強度、さらに接続の安全性は暗号化プロトコルと暗号化レベルで設定します。

プロトコル

暗号化プロトコルの SSL (Secure Sockets Layer) とその後継の TLS (Transport Layer Security) は、接続の暗号化に使用されます。

暗号化レベル

各暗号化レベルは、いわゆる暗号スイートの集合です。暗号スイートとは、セキュアな接続を確立するために使用される 4 つの暗号アルゴリズムの標準シーケンスです。暗号スイートは、暗号強度に応じてグループ化され、暗号化レベルを形成します。primos が対応する暗号スイート、すなわち暗号化レベルを形成する暗号スイートは、使用する SSL/TLS プロトコルにより決定されます。

次の暗号化レベルが選択できます。

- **任意**: 暗号化プロトコルはサーバーと本デバイスの間に自動的に交渉されます。(両方が対応できる最大の暗号化レベルが設定されます。)
- **標準**
- **高レベル**: 高レベルの暗号化強度の暗号スイートのみを使用します。(低速のデータ転送)

接続の確立

セキュアな接続を確立する場合、使用するプロトコルと対応する暗号スイートのリストを通信相手に送信します。使用する暗号スイートを取り決めます。初期設定では、当事者双方で対応する暗号スイート中で最も強力なスイートが使用されます。通信相手が選択したプロトコルに対応していない場合や、当事者の双方が対応している暗号スイートがない場合、SSL/TLS 接続は確立されません。

警告

接続を正常に確立するには、primos の通信相手 (例えばブラウザ) が選択したプロトコルと選択した暗号化レベルの暗号スイートに対応する必要があります。問題が発生する場合は、別のレベルを選択するか、または primos のパラメータをリセットしてください。⇒ 67 を参照してください。

メモ

暗号化プロトコルと暗号化レベルは、「任意」を設定すると、双方の通信当事者で自動的にネゴシエートされます。この設定を使用すると、セキュアな接続が確立できる確率が最も高くなります。

1. primos Control Center を起動します。
2. **セキュリティ - SSL 接続**を選択します。
3. **暗号化プロトコル**領域から、任意の暗号化プロトコルを選択します。

警告

最新のブラウザソフトウェアが使用され、接続タイプとして Control Center への Web アクセスに HTTPS のみが許可されている場合は、「SSL」の暗号化プロトコルは使用しないください。最新のブラウザは SSL に対応していないため、接続が確立できません。

4. **暗号化レベル**領域から、任意の暗号化レベルを選択します。

警告

最新のブラウザソフトウェアが使用され、接続タイプとして primos Control Center への Web アクセスに HTTPS のみが許可されている場合は、「低レベル」の暗号化プロトコルは使用しないください。最新のブラウザは「低レベル」の暗号スイートに対応していないため、接続が確立できません。

5. **保存**をクリックして確定します。
↳ 設定が保存されます。

メモ

個別の SSL/TLS 接続状態に関する詳細情報（暗号スイートなど）は、**SSL 接続の状態 - 詳細から詳細**ページを参照してください。

6.2 primos Control Center へのアクセスを制御する方法

primos Control Center への Web アクセスは、許可する接続の種類 (HTTP/HTTPS) を選択することで安全を確保できます。

HTTPS による接続のみを許可する場合、primos Control Center コントロールセンターへの管理者レベルの Web アクセスは SSL/TLS によって保護されます。暗号化はプロトコル及び暗号化レベルで定義されています ⇒ 47。

メモ

primos Control Center にログインするときは (⇒ 50)、パスワードがプレーンテキストで送信されます。HTTPS 接続のみを使用することを推奨します。

SSL/TLS は、primos の識別情報を確認する証明書を要求します。いわゆる「ハンドシェイク」中に、クライアントはブラウザを介して証明書を要求します。この証明書は、ブラウザ側での受諾が必要です。ご使用のブラウザソフトウェアの説明書を参照してください。SSL/TLS 接続に必要な URL は「https」で始まります。

1. primos Control Center を起動します。
2. **セキュリティ - デバイスへのアクセス**を選択します。
3. **接続領域の HTTP/HTTPS または HTTPS のみ**にチェックマークを付けます。
4. **保存**をクリックして確定します。
↳ 設定が保存されます。

6.3 ユーザプロフィールを管理する方法 (アクセス制御)

primos Control Center へのアクセスは、ユーザアカウントにより制御されます。このプログラムにアクセスするにはユーザ名とパスワードが必要になります。

メモ

ログインするときは、パスワードがプレーンテキストで送信されます。primos Control Center への接続を暗号化することを推奨します。(HTTPS ⇨ 49)

ローカル管理者

ローカル管理者アカウントを使用すると、いつでも primos Control Center にアクセスできます。ローカル管理者は削除することができません。またユーザ名の変更もできません。

ユーザ名： admin

パスワード： admin

管理者アカウントのパスワードは変更できます。

メモ

初期設定のパスワードは、速やかに変更してください。

ディレクトリサービス

ディレクトリサービス (Active Directory または LDAP) に primos を参加させることができます。⇨ 17 primos Control Center には、ディレクトリユーザもログインすることができます。そのためには、対象のユーザを primos に設定する必要があります。設定されたユーザは、ディレクトリサービスのユーザ名とパスワードを使用して自らを認証し、primos Control Center にアクセスできるようになります。

メモ

セキュリティ関連の設定ができる primos Control Center には、システム管理者のみがアクセスできるようにします。

セッションタイムアウト

設定した時間内に何も操作しなかった場合に、セキュリティ上の理由でセッションタイムアウトにより、primos Control Center への接続を切断する設定ができます。ログイン中のユーザはログアウトされるため、再度ログインする必要があります。

ログアウト

セキュリティ上の理由で、primos Control Center は設定の終了後、必ずログアウトしてください。⇨ 9

選択できる作業

- 「ローカル管理者のパスワードを変更する」⇒■51
- 「ディレクトリサービスユーザのログインを設定する」⇒■51
- 「セッションタイムアウトを設定する」⇒■51

ローカル管理者のパスワードを変更する

1. primos Control Center を起動します。
2. **セキュリティ - デバイスへのアクセス**を選択します。
3. **パスワード**欄に、パスワードを入力します。
4. パスワードを再度入力します。
5. 確定するには、**保存**をクリックします。
↳ 設定が保存されます。

ディレクトリサービスユーザのログインを設定する

必要事項

- ✓ primos がディレクトリサービスに組み込まれていること。⇒■17
 - ✓ ディレクトリサービスにユーザが設定されていること。
1. primos Control Center を起動します。
 2. **セキュリティ - デバイスへのアクセス**を選択します。
 3. **このデバイスにアクセスできるユーザ**欄に、primos Control Center にログインできるディレクトリサービスのユーザを入力します。
 4. 確定するには、**保存**をクリックします。
↳ 設定が保存されます。

セッションタイムアウトを設定する

1. primos Control Center を起動します。
2. **セキュリティ - デバイスへのアクセス**を選択します。
3. **セッションタイムアウト**にチェックマークを付けます。
4. **セッション時間**欄に、タイムアウトが有効になるまでの時間を分単位で入力します。
↳ 設定が保存されます。

クロスサイトスクリプティングの正体

6.4 クロスサイトスクリプティングから primos を保護する方法

クロスサイトスクリプティング (XSS) は、Web サイトのセキュリティ上の脆弱性を利用した攻撃方法です。Web サイトへのユーザの入力は、初期設定ではブラウザに提示されます。攻撃は、この設定を使用して悪質なコード (例えばスクリプト) を送信します。攻撃の目的は、ユーザプロフィールなどのユーザデータを盗み取ることです。

クロスサイトスクリプティング攻撃を防ぐために、データの値を検査して信頼できる値のみを受け入れます。

1. primos Control Center を起動します。
2. **セキュリティ - デバイスへのアクセス**を選択します。
3. **クロスサイトスクリプティング (XSS)** 領域で、**値の確認**を有効または無効にします。
↳ 設定が保存されます。

6.5 primos へのアクセスを制御する方法 (TCP ポートアクセス制御)

primos へのアクセスを制御できます。primos のすべての TCP ポートを遮断できます。primos へのアクセスが許可されたネットワーク要素は、例外に設定してロック対象から除外できます。primos は、例外として設定されたネットワーク要素から送信されるデータパケットのみを受け入れます。次の点に留意してください。上記は iOS デバイスにも適用されます。TCP ポートアクセス制御が有効な場合は、例外として設定された iOS デバイスからのみ印刷が可能です。

例外

ネットワーク要素 (iOS デバイス、クライアント、DNS サーバ、SMTP サーバなど) をポートのロックから除外するには、これらを例外として設定します。設定するには、アクセス権限のあるネットワーク要素の IP アドレスまたは MAC アドレス (ハードウェアアドレス) を「例外」領域に入力する必要があります。次の点に留意してください。

- MAC アドレスはルータを通して配信されません。
- アドレス範囲は、CIDR 表記により設定できます。

primos 上でキューを作成したプリンタについては、自動的にポートロックの対象から除外されます。

テストモード

「テストモード」により、アクセス制限の設定を確認できます。テストモードをアクティブにすると、アクセス制限は primos を再起動しない限り有効な状態です。再起動すると、アクセス制限は無効になります。

「テストモード」オプションは、初期設定でアクティブになっています。テスト後は、アクセス制限を継続するために、テストモードを無効にする必要があります。

1. primos Control Center を起動します。
2. **セキュリティ - TCP ポートアクセス**を選択します。
3. **ポートアクセス制御**にチェックマークを付けます。
4. **例外領域**で、ポートのロック対象から除外するネットワーク要素を指定します。IP アドレスまたは MAC アドレスを入力して、オプションにチェックマークを付けます。
5. テストモードが有効であることを確認します。
6. **保存**をクリックして確定します。
設定が保存されます。
デバイスを再起動するまで、ポートアクセス制御はアクティブです。
7. ポートアクセス、および primos が設定可能であることを確認してください。

メモ

primos Control Center から primos にアクセスできなくなった場合は、デバイスを再起動してください。(⇒[69](#))

8. **テストモード**のチェックマークを外します。
9. **保存**をクリックして確定します。
↳ 設定が保存されます。ポートアクセス制御がアクティブになり、ポートへのアクセスが制限されます。

6.6 証明書の正しい使用方法

primos は独自の証明書管理機能があります。この節では、証明書の使用方法と推奨する使用時期について説明します。

証明書の役割

証明書は、TCP/IP ベースのネットワークでデータの暗号化と通信先の認証に使用できます。証明書は、キー（公開キー）と署名を含む電子メッセージです。

利点と目的

証明書を使用すると、様々なセキュリティメカニズムが使用できます。primos で証明書を使用して、

- ネットワーク内で primos の識別情報を確認します。(⇒ 61)
- primos Control Center への接続が HTTPS (SSL/TLS) で制限されている場合のクライアント認証。(⇒ 49)
- 印刷データを暗号化します。(IPPS およびセキュアな AirPrint ⇒ 36)

使用できる証明書

primos では、自己署名証明書と CA 証明書の両方が使用できます。これらの証明書は次のように区別できます。

- 出荷時には、証明書（**デフォルト証明書**）が primos に保存されています。デフォルト証明書は、可能な限り迅速に自己署名証明書または要求された証明書と交換することを推奨します。
- **自己署名証明書**には、primos が作成したデジタル署名が含まれます。
- **要求された証明書**は、認証局 (CA) が認証要求にもとづき primos に対して作成します。
- **CA 証明書**は、認証局 (CA) に対して発行された証明書です。CA 証明書は、各認証局が発行した証明書を検証するために使用されます。

次の証明書を primos に同時にインストールできます。

- 自己署名証明書 x 1
- クライアント証明書 (要求された証明書または PKCS#12 証明書) x 1
- CA 証明書 x 1 ~ 32

すべての証明書は個別に削除できます。

選択できる作業

- 「証明書を表示する」⇒ 55
- 「自己署名証明書を作成する」⇒ 55
- 「要求された証明書の認証要求を作成する」⇒ 56
- 「要求された証明書を primos にインストールする」⇒ 57
- 「PKCS#12 証明書を primos にインストールする」⇒ 57
- 「CA 証明書を primos にインストールする」⇒ 58
- 「証明書を削除する」⇒ 59

証明書を表示する

primos にインストールされた証明書や認証要求は、表示し参照することができます。

必要事項

✓ primos に証明書がインストールされていること。

1. primos Control Center を起動します。
2. **セキュリティ - 証明書**を選択します。
3. 🔍 アイコンで証明書を選択します。
↳ 証明書が表示されます。

自己署名証明書を作成する

メモ

すでに自己署名証明書が primos 内に作成されている場合は、最初にその証明書を削除してください。(⇒ 59)

1. primos Control Center を起動します。
2. **セキュリティ - 証明書**を選択します。
3. **自己署名証明書**をクリックします。
4. 適切なパラメータを入力します (表 10 ⇒ 56)。
5. **作成 / インストール**をクリックします。
↳ 証明書が作成されインストールされます。完了までに数分かかることがあります。

表 10: 証明書作成用パラメータ

パラメータ	説明
共通名	証明書を明確に識別するために使用します。primos への証明書の割り当てを明確に示す、primos の IP アドレスやホスト名の使用を推奨します。 入力できる文字数は、最大 64 文字 (半角) です。
電子メールアドレス	電子メールアドレスを指定します。 入力できる文字数は、最大 40 文字 (半角) です。 (任意入力)
組織名	primos を使用する会社を指定します。 入力できる文字数は、最大 64 文字 (半角) です。
組織単位	会社の部課、係名を指定します。 入力できる文字数は、最大 64 文字 (半角) です。 (任意入力)
場所	会社が本拠を置く地域を指定します。 入力できる文字数は、最大 64 文字 (半角) です。
都道府県名	会社が本拠を置く都道府県を指定します。 入力できる文字数は、最大 64 文字 (半角) です。 (任意入力)
ドメインコンポーネント	付加属性の入力ができます。 (任意入力)
国	会社が本拠を置く国を指定します。ISO 3166 に従い 2 文字の国コードを入力します。例： DE = ドイツ、GB = 英国、US = 米国
期限切れ日時	証明書が無効となる日付を指定します。指定日に無効になります。
RSA キー長	使用する RSA キーの長さを指定します。 <ul style="list-style-type: none"> • 512 ビット (高速暗号化および複合化) • 768 ビット • 1024 ビット (標準暗号化および複合化) • 2048 ビット (低速暗号化および複合化)

要求された証明書の認証要求を作成する

認証局が primos に対して発行した証明書を使用する準備として、primos で認証要求を作成できます。認証要求は、この要求にもとづき証明書を作成する認証局へ送信する必要があります。証明書が、「Base64」形式であること。

必要事項

メモ

すでに認証要求が primos 内に作成されている場合は、最初にその認証要求を削除してください。(⇒59)

1. primos Control Center を起動します。
2. **セキュリティ - 証明書**を選択します。
3. **認証要求**をクリックします。
4. 必要なパラメータを入力します (表 10 ⇒56)。
5. **要求の作成**をクリックします。
認証要求が作成されます。完了までに数分かかることがあります。
6. **アップロード**を選択して、認証要求をテキストファイルに保存します。
7. **OK**をクリックします。
8. テキストファイルを、認証要求として認証局に送信します。

受信した証明書は、デバイスに保存する必要があります。⇒57

要求された証明書を primos にインストールする

- ✓ 認証要求が、当日より前の日付で作成されていること。(⇒56)
- ✓ 証明書が、「Base64」形式であること。

メモ

すでに PKCS#12 証明書が primos にインストールされている場合は、最初にその証明書を削除してください。(⇒59)

1. primos Control Center を起動します。
2. **セキュリティ - 証明書**を選択します。
3. **要求された認証情報**をクリックします。
4. **参照**をクリックします。
5. 要求された証明書を指定します。
6. **インストール**をクリックします。
↳ primos に要求された証明書がインストールされます。

PKCS#12 証明書を primos にインストールする

PKCS#12 証明書は、秘密キーとキーの証明書を保存し、パスワードでそれらを保護するために使用します。

メモ

すでに PKCS#12 証明書または要求された証明書が primos にインストールされている場合は、最初にその証明書を削除してください。(⇒ 59)

必要事項

- ✓ 証明書が、「Base64」形式であること。
- 1. primos Control Center を起動します。
- 2. **セキュリティ - 証明書**を選択します。
- 3. **PKCS#12 認証情報**をクリックします。
- 4. **参照**をクリックします。
- 5. PKCS#12 証明書を入力します。
- 6. パスワードを入力します。
- 7. **インストール**をクリックします。
 - ↳ primos に PKCS#12 証明書がインストールされます。

CA 証明書を primos にインストールする

primos の通信先の識別情報を確認するには、その証明書を検証することが不可欠です。その目的で、該当する通信先の証明書を発行した認証局のルート CA 証明書を、primos にインストールします。

最大 32 個の CA 証明書がインストールできます。複数のレベルの公開キーインフラストラクチャ (PKIs) に対応しています。

例：primos は、ネットワーク内の識別情報を検証する複数の認証方式を提供します。「EAP-TLS」の認証方式 (⇒ 61) を使用する場合は、認証サーバ (RADIUS) の証明書を発行した認証局のルート CA 証明書を primos にインストールしてください。

必要事項

- ✓ 証明書が、「Base64」形式であること。
- 1. primos Control Center を起動します。
- 2. **セキュリティ - 証明書**を選択します。
- 3. **CA 認証情報**をクリックします。
- 4. **参照**をクリックします。
- 5. CA 証明書を指定します。
- 6. **インストール**をクリックします。
 - ↳ primos に CA 証明書がインストールされます。

証明書を削除する

警告

primos Control Center への Web アクセスに HTTPS のみが接続の種類として設定されている場合は、証明書 (CA/ 自己署名 /PKCS#12) を削除しないでください。該当する証明書が削除されると、primos Control Center に接続できなくなります。その場合は、primos の設定値をリセットします。(⇒ 67)

必要事項

- ✓ primos に証明書がインストールされていること。
- 1. primos Control Center を起動します。
- 2. **セキュリティ - 証明書** を選択します。
- 3. 🔍 アイコンで削除する証明書を選択します。証明書が表示されます。
- 4. **削除** をクリックします。
 - ↳ 証明書が削除されます。

6.7 認証方式を使用する方法

認証により、ネットワークを不正アクセスから保護できます。primos は、様々な認証方法に対応できます。この節では、対応している認証方法と、それを primos に設定する方法を説明します。

IEEE 802.1x の役割

IEEE 802.1x 標準は、各種の認証プロトコルおよびキー管理プロトコルの基本構造を提供します。IEEE 802.1x により、ネットワークへのアクセスを制御できます。ユーザは、ネットワークデバイスからネットワークにアクセスする前に、ネットワーク内の認証を受ける必要があります。認証に成功すると、ネットワークにアクセスできるようになります。

EAP の役割

標準 IEEE 802.1x は、EAP (拡張認証プロトコル) に基づいています。EAP は、多くの認証方法の汎用プロトコルです。EAP により、ネットワークデバイスと認証サーバ (RADIUS) 間で、標準化された認証方法を使用できます。最初に使用する認証方法 (TLS、PEAP、TTLS など) を決定し、それを関連するすべてのネットワークデバイスに設定する必要があります。

RADIUS の役割

RADIUS (リモート認証ダイヤルインユーザサービス) とは、認証およびアカウントの管理システムで、ユーザのログイン情報を検証して、ユーザが求めるリソースへのアクセスを許可します。

primos は、保護されたネットワーク内で自己認証するために、様々な EAP 認証方式に対応しています。

選択できる作業

- 「EAP-MD5 を設定する」⇒[60](#)
- 「EAP-TLS を設定する」⇒[61](#)
- 「EAP-TTLS を設定する」⇒[62](#)
- 「PEAP を設定する」⇒[63](#)
- 「EAP-FAST を設定する」⇒[64](#)

EAP-MD5 を設定する

利点と目的

EAP-MD5 は、デバイスまたはユーザの識別情報を検証し、ネットワークリソースへのアクセスを許可します。EAP-MD5 ネットワーク認証を行うように、primos を設定できます。これにより、primos は保護されたネットワークに確実にアクセス

できるようになります。

動作モード

EAP-MD5 は、RADIUS サーバによるユーザベースの認証方式です。RADIUS サーバ上で primos が (ユーザ名とパスワードを持つ) ユーザとして設定されている必要があります。次に、primos で EAP-MD5 の認証方法を有効にし、ユーザ名とパスワードを入力する必要があります。

必要事項

- ✓ primos が、RADIUS サーバ上で (ユーザ名とパスワードを持つ) ユーザとして設定されていること。
- 1. primos Control Center を起動します。
- 2. **セキュリティ - 認証**を選択します。
- 3. **認証方法**リストから **MD5** を選択します。
- 4. RADIUS サーバ上で primos の設定に使用する**ユーザ名とパスワード**を入力します。
- 5. **保存**をクリックして確定します。
↳ 設定が保存されます。

EAP-TLS を設定する

利点と目的

EAP-TLS (トランスポート層セキュリティ) は、デバイスまたはユーザの識別情報を検証して、ネットワークリソースへのアクセスを許可します。EAP-TLS ネットワーク認証を行うように、primos を設定できます。これにより、primos は保護されたネットワークに確実にアクセスできるようになります。

動作モード

EAP-TLS は、RADIUS サーバによる証明書ベースの認証方式です。この目的で、証明書が primos と RADIUS サーバ間で交換されます。primos と RADIUS サーバ間の暗号化 TLS 接続は、この処理中に確立されます。RADIUS サーバと primos の両方で、CA により署名された有効なデジタル証明書が必要になります。RADIUS サーバと primos は、その証明書を検証する必要があります。相互認証に成功すると、ネットワークにアクセスできるようになります。

各デバイスで証明書が必要なため、PKI (公開キー基盤) が利用できなければなりません。ユーザパスワードは必須ではありません。

EAP-TLS 認証を使用する場合は、次の手順に従い実行してください。この手順に従わなかった場合は、primos がネットワーク上でアドレス指定できないことがあります。その場合は、primos の設定値をリセットします。(⇒ 67)

手順

- primos 内に認証要求を作成します。⇒ 56
 - 認証要求と認証サーバを使用して、証明書を作成します。
 - 要求された証明書を primos にインストールします。⇒ 57
 - 認証サーバ (RADIUS) の証明書を発行した認証局のルート CA 証明書を primos にインストールします。⇒ 58
 - primos 内で、認証方式「EAP-TLS」を有効にします。
1. primos Control Center を起動します。
 2. **セキュリティ - 認証**を選択します。
 3. **認証方法**リストから **TLS** を選択します。
 4. **EAP ルート証明書**のリストから、ルート CA 証明書を選択します。
 5. RADIUS サーバ上で primos を設定するために使用するパスワードを入力します。
 6. **保存**をクリックして確定します。
↳ 設定が保存されます。

EAP-TTLS を設定する

利点と目的

EAP-TTLS (トンネル化トランスポート層セキュリティ) は、デバイスまたはユーザの識別情報を検証し、ネットワークリソースへのアクセスを許可します。EAP-TTLS ネットワーク認証を行うように、primos を設定できます。これにより、primos は保護されたネットワークに確実にアクセスできるようになります。

動作モード

EAP-TTLS は、2つのフェーズで構成されます。

フェーズ 1 では、primos と RADIUS サーバ間の TLS 暗号化チャンネルが確立されます。RADIUS サーバのみが、CA により署名された証明書を使用して primos に対する自己認証を行います。このプロセスは、「外部認証」とも呼ばれます。

フェーズ 2 では、TLS チャンネル内の通信のために、追加の認証方式が使用されます。EAP 定義の方式や以前の方式 (CHAP、PAP、MS-CHAP および MS-CHAPv2) に対応しています。このプロセスは、「内部認証」とも呼ばれます。

この方法の利点は、RADIUS サーバのみが証明書を必要とすることです。したがって、PKI は必要ありません。さらに、TTLS はほとんどの認証プロトコルに対応しています。

必要事項

- ✓ primos が、RADIUS サーバ上で (ユーザ名とパスワードを持つ) ユーザとして設定されていること。
- 1. primos Control Center を起動します。
- 2. **セキュリティ - 認証**を選択します。
- 3. **認証方法**リストから **TTLS** を選択します。
- 4. **EAP ルート証明書**のリストから、認証サーバ (RADIUS) の証明書を発行した認証局のルート CA 証明書を選択します。(オプション) 証明書は、接続を確立するときに、セキュリティを強化します。
(ルート CA 証明書が、あらかじめ primos にインストールされている必要があります。 ⇨ 658)
- 5. **匿名の名前欄**に、EAP-TTLS 認証の暗号化されていない部分の名前を入力します。
- 6. **内部認証**リストから、TLS チャンネル内の通信の安全を確保する方法を選択します。
- 7. RADIUS サーバ上で primos の設定に使用する**ユーザ名とパスワード**を入力します。
- 8. WPA アドオンをインストールします。(オプション)
- 9. **保存**をクリックして確定します。
↳ 設定が保存されます。

PEAP を設定する**利点と目的**

PEAP (保護拡張認証プロトコル) は、デバイスまたはユーザの識別情報を検証した上で、ネットワークリソースへのアクセスを許可します。PEAP ネットワーク認証を行うように、primos を設定できます。これにより、primos は保護されたネットワークに確実にアクセスできるようになります。

動作モード

PEAP の場合、暗号化 TLS (Transport Layer Security) チャンネルが、プリントサーバと RADIUS サーバ間に確立されます。(EAP-TTLS の場合と同様。 ⇨ 62 を参照してください。)RADIUS サーバのみが、CA により署名された証明書を使用して primos に対する自己認証を行います。

TLS チャンネルは、追加の EAP 認証方式 (例 : MSCHAPv2) によって保護できる別の接続を確立するために使用されます。

この方法の利点は、RADIUS サーバのみが証明書を必要とすることです。したがって、PKI は必要ありません。PEAP では、TLS の利点を活用し、ユーザパスワードやワンタイムパスワードなど、様々な認証方式に対応しています。

必要事項

- ✓ primos が、RADIUS サーバ上で (ユーザ名とパスワードを持つ) ユーザとして設定されていること。
- 1. primos Control Center を起動します。
- 2. **セキュリティ - 認証**を選択します。
- 3. **認証方法**リストから **PEAP** を選択します。
- 4. **EAP ルート証明書**のリストから、認証サーバ (RADIUS) の証明書を発行した認証局のルート CA 証明書を選択します。(オプション) 証明書は、接続を確立するときに、セキュリティを強化します。
(ルート CA 証明書が、あらかじめ primos にインストールされている必要があります。⇒ 58)
- 5. **匿名の名前欄**に、PEAP 認証の暗号化されていない部分の名前を入力します。
- 6. **内部認証**リストから、TLS チャンネル内の通信の安全を確保する方法を選択します。
- 7. **PEAP のバージョン**リストから、使用する PEAP プロトコルのバージョンを選択します。
- 8. **PEAP ラベル**リストから、使用する PEAP ラベルのバージョンを選択します。
- 9. RADIUS サーバ上で primos の設定に使用する **ユーザ名とパスワード**を入力します。
- 10. WPA アドオンをインストールします。(オプション)
- 11. **保存**をクリックして確定します。
↳ 設定が保存されます。

EAP-FAST を設定する**利点と目的**

EAP-FAST (セキュアトンネリングを介したフレキシブル認証) は、デバイスまたはユーザの識別情報を検証し、ネットワークリソースへのアクセスを許可します。EAP-FAST ネットワーク認証を行うように、primos を設定できます。これにより、primos は保護されたネットワークに確実にアクセスできるようになります。

動作モード

EAP-FAST はデータ転送の保護にチャンネルを使用します。(EAP-TTLS の場合と同様。⇒ 62) 主な相違点は、EAP-FAST が認証のための証明書を必要としないことです (証明書の使用は任意に選択できます)。

PACs (Protected Access Credentials) は、チャンネルの設定に使用されます。PACs とは、最大で次の 3 つのコンポーネントから構成された証明書です。

- primos と RADIUS サーバ間の事前共有キーを含む共有秘密キー。

必要事項

- primos がネットワークリソースにアクセスしようとする、primos に提供され、RADIUS サーバに表示される不透明な部分。
- クライアントにとって有効な他の情報。(オプション)

EAP-FAST では、2つの方法を使用して PACs を生成します。

- 手動配信メカニズムは、管理者が構成しネットワークに安全であると見なす、すべてのメカニズムです。
- 自動配信の場合、PACs の配信のみでなく、primos の認証を保護するために暗号化チャンネルが確立されます。

- ✓ primos が、RADIUS サーバ上で(ユーザ名とパスワードを持つ)ユーザとして設定されていること。
 1. primos Control Center を起動します。
 2. **セキュリティ - 認証**を選択します。
 3. **認証方法**リストから **FAST** を選択します。
 4. **EAP ルート証明書**のリストから、認証サーバ(RADIUS)の証明書を発行した認証局のルート CA 証明書を選択します。(オプション)証明書は、接続を確立するときに、セキュリティを強化します。
(ルート CA 証明書が、あらかじめ primos にインストールされている必要があります。⇒58)
 5. **匿名の名前欄**に、EAP-FAST 認証の暗号化されていない部分の名前を入力します。
 6. **内部認証**リストから、TLS チャンネル内の通信の安全を確保する方法を選択します。
 7. **FAST プロビジョニング欄**から、PACs のプロビジョニングメカニズムを選択します。
 8. RADIUS サーバ上で primos の設定に使用する**ユーザ名とパスワード**を入力します。
 9. WPA アドオンをインストールします。(オプション)
 10. **保存**をクリックして確定します。
↳ 設定が保存されます。

7 メンテナンス



primos では、様々な種類のメンテナンスを行うことができます。この章では、その概要を説明します。

必要な情報

- 「primos の設定の安全を確保する方法 (バックアップ)」⇒[66](#)
- 「primos を 初期設定にリセットする方法 (リセット)」⇒[67](#)
- 「更新 (アップグレード) の実行方法」⇒[68](#)
- 「primos を再起動する方法」⇒[69](#)
- 「primos をシャットダウンする方法」⇒[70](#)
- 「サービス機能を使用する方法」⇒[70](#)

7.1 primos の設定の安全を確保する方法 (バックアップ)

設定値 (証明書を含む) は、ローカルクライアントにバックアップコピーとして保存することができます。バックアップにより、常に安定した設定状態が復元できます。

バックアップファイルは、後で任意の primos に読み込むことができます。ファイルに含まれる設定内容がデバイスに引き継がれます。

選択できる作業

- 「バックアップを保存する」⇒[66](#)
- 「バックアップを任意の primos に読み込む」⇒[67](#)

バックアップを保存する

1. primos Control Center を起動します。
2. **メンテナンス - バックアップ**を選択します。
3. **保存**をクリックします。
↳ バックアップファイルがクライアントに保存されます。

バックアップを任意の primos に読み込む

メモ

primos ソフトウェアの同一の主要バージョン用に作成されたバックアップのみ読み込むことができます。(ソフトウェアの主要バージョンは、バージョン番号の第2レベルで識別されます。)

例：ソフトウェアバージョン 17.1.x の primos は、ソフトウェアバージョン 17.2.x の primos にインストールできません。

1. primos Control Center を起動します。
2. **メンテナンス-バックアップ**を選択します。
3. **参照**をクリックします。
4. primos のバックアップファイルを指定します。
5. **インストール**をクリックします。
↳ バックアップファイルに含まれる設定内容が primos に引き継がれます。

7.2 primos を初期設定にリセットする方法 (リセット)

primos を初期設定 (工場出荷時設定) にリセットすることができます。リセットすると、以前の設定内容はすべて削除されます。

例えば、primos の設置場所を変更して別のネットワークで primos を使用する場合に、設定値をリセットする必要があります。別のネットワークに primos を設置する場合は、設置場所を変更する前に primos の設定値を初期設定にリセットすることを推奨します。

primos は、primos Control Center からリモートメンテナンスを使用してリセットできます。または、デバイスのリセットボタンを使用すると、パスワードを入力することなくパラメータをリセットできます。

メモ

設定をリセットすると、primos の IP アドレスが変更され primos Control Center への接続が終了する場合があります。

利点と目的

リモートメンテナンスの使用、またはデバイスからのリセット

選択できる作業

- 「primos Control Center で設定値をリセットする」⇒ 68
- 「リセットボタンで設定値をリセットする」⇒ 68

primos Control Center で設定値をリセットする

1. primos Control Center を起動します。
2. **メンテナンス - 初期設定** を選択します。
3. **初期設定** をクリックします。
↳ 設定値がリセットされます。

リセットボタンで設定値をリセットする

primos 上には LED や様々なポートおよびリセットボタンがあります。これらのコンポーネントについては、「クイック・インストールガイド」で説明しています。リセットボタンを使用すると、primos の設定値を初期設定値にリセットすることができます。

1. リセットボタンを 5 秒間押します。
primos が再起動します。
↳ 設定値がリセットされます。

7.3 更新 (アップグレード) の実行方法

最新の機能を利用するために、primos のソフトウェアやファームウェアを更新 (アップグレード) することができます。

更新中に起きること

更新の際に、古いファームウェア / ソフトウェアは上書きされ、新しいファームウェア / ソフトウェアに置き換えられます。デバイスの元の設定値 (証明書を含む) は変更されません。

メモ

primos ソフトウェアの主要バージョンに更新する場合、primos は初期設定値にリセットされます。(ソフトウェアの主要バージョンは、バージョン番号の第 2 レベルで識別されます。)

例：primos をソフトウェアバージョンの 17.1.x から 17.2.x に更新すると、初期設定値にリセット (すべての設定が消去) されます。

更新を推奨する状況

機能の一部が正常に動作しない場合、および SEH Computertechnik GmbH が新しい機能の更新またはバグ修正を含む新しいソフトウェアまたはファームウェアのバージョンをリリースした場合に、更新を実行することを推奨します。

更新ファイルの 入手方法

primos にインストールされているソフトウェアとファームウェアのバージョンを確認します。バージョン番号は、primos Control Center で、または SEH primos App のリストから確認します。

最新のファームウェアおよびソフトウェアファイルは、次の SEH Computertechnik GmbH のホームページからダウンロードできます。

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



メモ

すべての更新ファイルには、専用の「readme」ファイルが付属します。「readme」ファイルに記載された情報を確認してください。

1. primos Control Center を起動します。
2. **メンテナンス - 更新**を選択します。
3. **参照**をクリックします。
4. 更新ファイルを選択します。
5. **インストール**をクリックします。
↳ 更新が実行されます。完了までに数分かかることがあります。その後、primos が再起動します。

7.4 primos を再起動する方法

更新後、primos は自動的に再起動します。primos が反応しない場合は、手動で再起動することもできます。

1. primos Control Center を起動します。
2. **メンテナンス - 再起動**を選択します。
3. **再起動**をクリックします。
↳ primos が再起動します。

7.5 primos をシャットダウンする方法

例えば週末の間、primos をシャットダウンしておくことができます。primos をシャットダウンしてから、電源を遮断してください。この手順に従い、不安定状態やデータ損失を避けます。

1. primos Control Center を起動します。
2. **メンテナンス - シャットダウン**を選択します。
3. **シャットダウン**をクリックします。
↳ primos がシャットダウンします。

7.6 サービス機能を使用する方法

primos はサービス機能を提供します。この機能は、SEH のサポート部門によるトラブルシューティングに役立ちます。問い合わせ窓口については、「サポートとサービス」⇒7.5 の章を参照してください。

サービスファイル

サービスファイルは、診断情報を記述した圧縮ファイルです。異常が発生した場合、このファイルをローカルクライアントに保存して、(電子メールなどによる)リクエストと一緒に SEH のサポート部門に送付してください。

ログイン

初期設定のサービスファイルには多くの情報が保存されていません。ログ記録を有効にすると、より多くの詳細情報が記録されます。SEH のサポートは、この情報からより詳細なエラー解析を行うことができます。

SSH アクセス

サポートの目的で primos にリモートアクセスする場合は、Secure Shell (SSH) ネットワークプロトコルが使用できます。リモートアクセスが必要な場合、SEH のサポート部門は、この機能をアクティブにするよう依頼します。SEH のサポートは、すべての必要な対策を講じることができるよう案内します。すべての対策を講じた後で、SSH アクセスを無効にしてください。

選択できる作業

- 「ログ記録を有効にします」⇒7.1
- 「サービスファイルを保存する」⇒7.1
- 「SSH アクセスを設定する」⇒7.1

ログ記録を有効にします

メモ

このオプションを有効にするには、必ず SEH のサポートチームに相談してください。

1. primos Control Center を起動します。
2. **メンテナンス - サービス**を選択します。
3. **ログイン**領域で、**ログを有効する**をクリックします。
↳ ログ記録は有効化されています。

サービスファイルを保存する

1. primos Control Center を起動します。
2. **メンテナンス - サービス**を選択します。
3. **サービスファイル**領域で、**保存**をクリックします。
↳ サービスファイルがクライアントに保存されます。
保存されたサービスファイルを SEH のサポート部門に送信します。

SSH アクセスを設定する

メモ

SSH 接続は、SEH のサポート部門と相談した上で、確立して使用することができます。SSH をそれ以外の目的 (リモートメンテナンスなど) に使用することは禁止されています。

1. primos Control Center を起動します。
2. **メンテナンス - サービス**を選択します。
3. **SSH アクセス**にチェックマークを付ける、またはチェックマークを外します。
4. **保存**をクリックして確定します。
↳ 設定が保存されます。

8 付録



付録には、用語集やトラブルシューティングが含まれています。

必要な情報

- 「用語集」⇒73
- 「トラブルシューティング」⇒75

8.1 用語集

この用語集には、メーカー固有のソフトウェアソリューションに関する情報およびネットワークテクノロジーで使用される専門用語が含まれています。

必要な情報

メーカー固有のソフトウェアソリューション

- 「primos Control Center」⇒ 74
- 「SEH primos App」⇒ 74

ネットワークテクノロジー

- 「デフォルト名」⇒ 73
- 「ゲートウェイ」⇒ 73
- 「ハードウェアアドレス」⇒ 73
- 「ホスト名」⇒ 74
- 「IP アドレス」⇒ 74
- 「サブネットマスク」⇒ 74

デフォルト名

primos のデフォルト名は、2 つの文字「IC」とデバイス番号で構成されます。デバイス番号は、ハードウェアアドレスの後半の 6 桁で構成されています。

例：IC0001ff

デフォルト名は、primos Control Center で確認できます。

ゲートウェイ

ゲートウェイにより、外部ネットワークから IP アドレスを指定できます。ゲートウェイを使用する場合は、primos Control Center から関連するパラメータを設定できます。(⇒ 9)

ハードウェアアドレス

primos は、世界でただ 1 つのハードウェアアドレスを使用してアドレス指定できます。通常、このアドレスは MAC アドレスまたはイーサネットアドレスと呼ばれます。メーカーが、デバイスのハードウェアにこのアドレスを設定しています。アドレスは 12 個の 16 進数で構成されます。最初の 6 つの数字はメーカーを表し、後の 6 つの数字で各デバイスを識別します。

ハードウェアアドレスは、筐体上や SEH primos App で確認できます。

ハードウェアアドレスの区切り文字は、プラットフォームにより異なります。ハー

ドウェアアドレスを入力するときは、次の表記規則に注意してください。

オペレーティングシステム	表記	例
Windows	ハイフン	00-c0-eb-00-01-ff
UNIX	コロンまたはドット	00:c0:eb:00:01:ff、または 00.c0.eb.00.01.ff

ホスト名

ホスト名は IP アドレスの別名です。ホスト名は、primos をネットワーク内で一意に識別し、覚えやすくします。

IP アドレス

IP アドレスとは、ネットワーク内の各ノードに割り当てられる固有アドレスです。各 IP アドレスは、ローカルなネットワーク内で 1 つしか存在しません。このアドレスは、primos に保存して、ネットワーク内部で確実にアドレス指定できるようにする必要があります。

サブネットマスク

サブネットマスクを使用すると、大規模ネットワークをサブネットワークに分割できます。この場合、IP アドレスのユーザ ID は様々なサブネットワークに割り当てられます。

既定値では、primos はサブネットワークを使用しないように設定されています。サブネットワークを使用する場合は、primos Control Center から、関連するパラメータを設定できます。(⇒ 9)

primos Control Center

primos は、primos Control Center から設定および管理できます。primos Control Center は primos に格納され、ブラウザソフトウェア (Microsoft Edge, Safari, Mozilla Firefox) で表示できます。

SEH primos App

SEH primos App は、SEH Computertechnik GmbH が開発した、所定のネットワーク上で primos デバイスを検出するソフトウェアです。SEH primos App を使用して、簡単な管理タスクを実行できます。

8.2 トラブルシューティング

この章では、問題例とその解決策について説明します。

問題

- 「primos が BIOS モードです。」⇒ 75
- 「primos Control Center との接続が確立できない」⇒ 76
- 「パスワードが利用できない」⇒ 77
- 「プリンタが印刷しません。」⇒ 77
- 「印刷出力に不具合がある」⇒ 77
- 「primos をディレクトリサービスに組み込むことができません。」⇒ 77
- 「Wide-Area AirPrint が機能しない」⇒ 78

解決策

primos が BIOS モードです。

ファームウェアが正常に機能していてもソフトウェアに問題がある場合、primos は BIOS モードに切り替わります。BIOS モードへの切り替えは、例えば、ソフトウェアの更新が不適切であった場合に発生します。Activity LED が一定間隔で点滅している場合、primos は BIOS モードにあります。

警告

BIOS モード時、primos は使用できません。

BIOS モード中の primos には、BIOS モードを示す標識が SEH primos App 上で表示されるようになります。

BIOS モードにある primos を通常モードに切り替えるには、仮の IP アドレスを primos に割り当て、ソフトウェアを読み込みます。ソフトウェアを更新すると、primos は通常モードに切り替わり、正式な IP アドレスが新しく割り当てられます。

1. SEH primos App を起動します。
2. リスト中の primos にマークを付けます。
3. メニューバーから、**アクション - IP アドレスの指定**を選択します。
IP アドレスの設定ダイアログが表示されます。
4. **IP アドレス、サブネットマスクおよびゲートウェイ**を指定します。
5. **OK** をクリックして確定します。
primos に仮の IP アドレスが設定されます。

6. SEH Computertechnik GmbH の Web サイトから、最新のソフトウェアをダウンロードします。

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



7. メニューバーから、**アクション-ソフトウェアの読み込み**を選択します。**ソフトウェアの読み込み**ダイアログが表示されます。
8. primos のソフトウェアファイルを指定します。
9. **ロード**をクリックします。
ファームウェアの更新が実行されます。完了までに数分かかることがあります。
10. **OK** をクリックして、正常に完了したことを確認します。
↳ primos には新しい IP アドレスが自動的に割り当てられて、そのアドレスで SEH primos App 上に表示されます。必要に応じて、SEH primos App のリストを更新してください。

primos Control Center との接続が確立できない

考えられるエラー原因を取り除いてください。最初に、次の点を確認します。

- ケーブルの接続
- primos の IP アドレス (⇒ 7)
- ブラウザのプロキシ設定

上記の点に問題がないにもかかわらず接続が確立できない場合は、次の保護メカニズムが原因になっている可能性があります。

- アクセスが SSL (HTTPS) で制限されている。⇒ 49
- TCP ポートアクセス制御が有効になっている。⇒ 52
- 暗号化レベルの暗号スイートにブラウザが対応していない。⇒ 47
- primos が BIOS モードになっている。⇒ 75

パスワードが利用できない

primos Control Center へのアクセスは、ユーザアカウントにより制御されます。アクセスするにはユーザ名とパスワードが必要です。ローカル管理者のアカウントまたはディレクトリサービスのユーザを使用することができます。(⇒[150](#))
ローカル管理者のアカウントのみが使用され、パスワードを忘れた場合は、primos を初期設定値 (工場出荷時設定) にリセットできます。⇒[167](#) この処理では、パスワード以外の他の設定も工場出荷時の設定にリセットされます。

プリンタが印刷しません。

iOS デバイスから primos を使用して印刷するには、primos の各プリンタに対して印刷キューを作成する必要があります。次に、各キューに対して、印刷プロトコル、アクセス制御などを設定します。次の点を確認してください。

- すべてのキュー設定 ⇒[31](#)
- プリンタの異常 (用紙切れ、トナー切れ、紙づまりなど)
- 証明書が存在し、それが有効であるか
(印刷データ送信が暗号化されている場合のみ ⇒[36](#))

印刷出力に不具合がある

次の点を確認してください。

- 選択したプリンタへの接続 ⇒[31](#)
- すべてのプリンタ設定 ⇒[36](#)
- プリンタの異常 (トナー切れなど)

primos をディレクトリサービスに組み込むことができません。

- すべてのディレクトリサービスでは、同期化された時間を設定する必要があります。primos のデバイス時間は、ディレクトリサービスの時間と同じでなければなりません。primos とディレクトリサービスには同じタイムサーバ (SNTP サーバ) を使用することを推奨します。primos タイムサーバの設定を確認してください。⇒[20](#)
- primos で DNS サーバが設定され、primos からアクセスできることを確認してください。⇒[16](#)

Wide-Area AirPrint が機能しない

次の点を確認してください。

- 対象のプリンタが、wide-Area AirPrint により公開されている。⇒[■39](#)
- iOS デバイス上で、primos のサブドメインが検索ドメインとして設定されている。
 - 「iOS デバイス上で primos のサブドメインを検索ドメインとして自動的に設定する」⇒[■42](#)
 - 「iOS デバイス上で primos のサブドメインを検索ドメインとして手動で設定する」⇒[■44](#)
- 条件付きフォワーダが、DNS サーバ上に適切に実装されている。primos のサブドメインを含むリクエストを primos に転送する必要があります。⇒[■41](#)

手動で作成されたキューは公開されません。

手動で作成されたキューがプリンタに到達できない場合 (⇒[■29](#))、対象のキューはネットワーク上にマルチキャストで公開されないため有効になりません。プリンタに到達できることを確認し、キューをマルチキャストで公開してください。⇒[■31](#)