Produktfeature

AirPrint

Zugriffsschutz & Nutzer-authentifizierung bei primos

Einfach im Umfang. Sicher. Volle Kontrolle

SEH

Zugriffsschutz & Nutzerauthentifizierung bei primos

Einfach im Umgang. Sicher. Volle Kontrolle.

primos ermöglicht unkompliziertes Drucken in Unternehmens-Netzwerken via iOS– und macOS®-basierten Devices. Für den Einsatz im Enterprise-Umfeld konzipiert, setzt der AirPrint®-Server aus dem Hause SEH neben ausgeprägter Usability besonders in den Bereichen Datensicherheit und Netzwerkschutz für AirPrint® neue Maßstäbe. Die Sicherheitsmechanismen reichen von hohem Authentifizierungs & Zugriffsschutz über eine AirPrint®-kompatible Nutzerverwaltung und einer sicheren Druckdatenverschlüsselung bis zur ausschließlich lokalen Verwaltung der Druckdaten.

Das Produkt

primos steht für modernes, mobiles Drucken gepaart mit umfangreichen Sicherheitsmechanismen, AirPrint®-fähiger Benutzerverwaltung, starkem Zugriffsschutz und Verschlüsselungs-Management.

primos bietet eine native iOS-Kompatibilität und somit Anwendern die Möglichkeit des komfortablen mobilen Druckens direkt von Ihren iOS-Endgeräten. Die Druck-Kommunikation als auch die Druckdatenverwaltung erfolgt ausschließlich über das Unternehmensnetzwerk und wird somit lokal (on premise) gehalten. Auch ein Drucken über mehrere Subnetze hinweg ist möglich (Wide-Area AirPrint®).

Hard- und Software von primos zeichnen sich durch einfaches Handling und benutzerfreundliche Oberflächenbedienung aus – wobei diese bewusst übersichtlich und transparent gestaltet ist. Die Einbindung in das bestehende Unternehmensnetzwerk ist aus administrativer wie Anwenderseite denkbar einfach – bei stetem Fokus auf Sicherheit, Datenschutz und Zugriffskontrolle. primos unterstützt gleichzeitig bis zu 10 AirPrint®-fähige Netzwerk-Drucker.

Zugriffsschutz & Nutzerverwaltung

Datenschutz und -sicherheit sind heute für Unternehmen wichtiger denn je. Gerade der Einsatz im Enterprise-Umfeld erfordert höchste Sicherheitsanforderungen. Diesen trägt primos in höchstem Maße Rechnung: die mobile Drucklösung ergänzt gebotenen Authentifizierungsschutz mit einer ausgeklügelten Nutzerverwaltung. Darüber hinaus bietet primos die Besonderheit der AirPrint®-kompatiblen Nutzerverwaltung – ein Feature, durch welches sich primos eindeutig gegenüber den Meisten der nativen AirPrint®-Lösungen bzw. AirPrint®-Druckern hervorhebt. Das gesamte Handling mit primos gestaltet sich dabei denkbar einfach: über das nutzerfreundliche und bewusst schlicht gehaltene primos Control Center erfolgt die gesamte Konfiguration und Administration.

Authentifizierungsschutz

primos ermöglicht es, AirPrint® mit einer Anwender-Authentifizierung des Anwenders zu verknüpfen. Die Authentifizierung erfolgt über Verzeichnisdienste; unterstützt werden Microsoft®, Active Directory® oder openLDAP®.

Wird nun ein Druckprozess von einem definierten Nutzer über ein iOS-Endgerät initiiert, authentifiziert primos den Druckauftrag gegenüber dem Verzeichnisdienst; es erfolgt eine Abfrage der Nutzerdatenbank für den User und sein korrektes Passwort – auf primos selbst werden aber keine Passwörter gespeichert. Erst danach wird der Druckauftrag zum entsprechenden Drucker geleitet.

primos speichert keine Passwörter.

Für jeden Drucker gibt es eine Nutzerverwaltung; dort lässt sich präzise definieren, wer berechtigt ist zu drucken. Die Konfiguration der Nutzer erfolgt durch die Auswahl entsprechender Mitglieder aus einem Verzeichnisdienst, wie z. B. Microsoft®, Active Directory®. primos bietet die Möglichkeit an, die Authentifizierung bedarfsbezogen auszugestalten. Es gibt drei Varianten der Aussteuerung: Im einfachsten Fall kann definiert werden, dass jeder User drucken darf (sofern er in der Domäne erkannt wurde). Darüber hinaus sind Zugangsbeschränkungen, etwa über Allow oder Deny-Listen möglich. Es ist somit einfach, Nutzer oder auch Gruppen mit unterschiedlichen Rechten auf die einzelnen Drucker auszustatten und beispielsweise auch die Einrichtung von Guest-Printing zu erlauben.

Ferner bietet primos über einen ähnlichen Mechanismus eine Nutzerverwaltung an, um den Zugang zum primos Control Center zu definieren. Im Gegensatz zu vielen anderen Geräten gibt es bei primos nicht zwangsläufig nur einen User, den Admin. Der Zugriff auf die Administrationsseiten von primos kann nach entsprechender Konfiguration nur Administratoren aus der Domäne gewährt werden. Dies ist besonders in großen Enterprise-Netzwerken sinnvoll – dort erhalten in aller Regel nur eindeutig definierte Nutzer den Zugriff auf die Konfiguration von sensiblen Netzwerkgeräten.

Starke Sicherheitsmechanismen

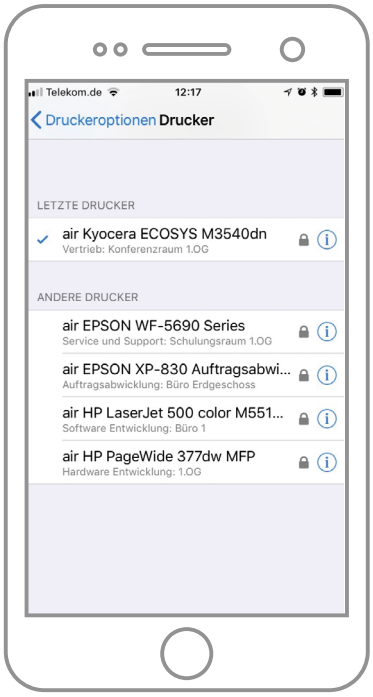
Um Sicherheit zu garantieren ist es besonders wichtig, sich der Risiken klarzuwerden. Um diese zu eliminieren bzw. so gering wie möglich zu halten, bietet primos in all seinen wichtigen Funktionsteilen zeitgemäße Sicherheitsmechanismen an, wie z. B.:

Verschlüsselte Druckdatenübertragung

primos unterstützt natürlich zeitgemäße Druckprotokolle wie das IPP Secure. In Kombination mit Verschlüsselungstechnologien, wie z. B. dem Verschlüsselungsprotokoll TLSv1.2, kann damit das Drucken während der gesamten Übertragung verschlüsselt und somit ein Mitlesen unterbunden werden.

Zertifikatsmanagement

Die in primos implementierten Sicherheitsmechanismen bedingen unter Umständen den Einsatz von Zertifikaten. Zertifikate werden unter anderem dafür verwendet, damit sich zur Identitätsprüfung miteinander kommunizierende Gegenstellen rückversichern können, dass, vereinfacht ausgedrückt, der andere auch wirklich derjenige ist, für den er sich ausgibt. Hierzu bietet primos ein Zertifikats-Management auf Enterprise-Level. Mehrere CA-Zertifikate, Zertifikats-Ketten etc.: alles kein Problem. Als mobile Drucklösung ist primos stets darauf ausgelegt, Prozesse nicht unnötig zu verkomplizieren; so liegt auch beim Umgang mit Zertifikaten der Fokus auf Nutzerfreundlichkeit.



primos schützt Ihre Daten

Authentifizierung in Rechnernetzen

Besonders Unternehmen mit Enterprise-Netzwerken stellen hohe Anforderungen an Produkte, denen der Zugriff auf das eigene Netzwerk gewährt werden soll. Die Sicherheit des eigenen Netzwerkes hat höchste Priorität. primos unterstützt den Standard IEEE 802.1X und kann sich somit selbst gegenüber einer Authentifizierungsstelle, wie z. B. einem RADIUS-Server, authentifizieren.

NO-Cloud!

primos verarbeitet Druckdaten ausschließlich lokal. Sämtliche Informationen verbleiben somit vollständig im Netzwerk des Anwenders und werden nicht in der Cloud verarbeitet oder mit Hilfe anderer externer Dienste verknüpft bzw. geteilt. Sie sind der Herr ihrer Daten und müssen nicht befürchten, sensible Informationen oder Druckdaten aus Ihrer Obhut zu entlassen.

Weitere Informationen finden Sie im **primos-Benutzerhandbuch.**

⟶ Zum Dokument

Made in Germany

Zugriffsschutz, Authentifizierung und Sicherheit bei primos

- Schnittstellen und Netzwerkanschlüsse
  - 1 × RJ-45 (IEEE 802.3; 10BaseT, 100BaseTX, 1000BaseT)
  - 1 × USB 2.0 (Typ A Anschluss), For future use/ Service
- Unterstützte Verzeichnisdienste:
  Microsoft® Active Directory®, OpenLDAP®
- Sicherheit
  - Verschlüsselung: SSL 3.0–TLS 1.2, HTTPS, IPP Secure, Secure AirPrint®, etc.
  - Authentifizierung: 802.1X (EAP-MD5, EAP-TLS, EAP-FAST, EAP-TTLS, PEAP)
  - Geräte- & Port-Zugriffskontrolle
  - Zertifikat-Management: Selbstsigniertes Zertifikat, Zertifikatsanforderung, CA-Zertifikat, PKCS#12-Zertifikat
  - Passwortschutz
- Für iOS-Geräte ab iOS 4.2
- Alle Mac® -Geräte ab OS X® 10.7.x

SEH Computertechnik GmbH

Wir, die SEH Computertechnik GmbH, sind auf die Herstellung von professionellen Netzwerklösungen spezialisiert. Die Kernbereiche unserer Arbeit sind der Netzwerkdruck und die Nutzung von USB-Geräten via Netzwerk. Unsere mehr als 30-jährige Erfahrung steht für ein innovatives und vielfältiges Produktportfolio und garantiert maßgeschneiderte Lösungen für individuelle Anforderungen.

Entwicklung und Produktion finden an unserem Hauptsitz im ostwestfälischen Bielefeld statt. Die weltweite Vermarktung erfolgt über eigene Tochtergesellschaften in den USA und Großbritannien sowie über ein umfangreiches Partner- und Distributoren-Netz.

Zu unserem Kundenstamm gehören Unternehmen, Konzerne, Behörden und Institutionen aus den verschiedensten Sektoren.

SEH Computertechnik GmbH
Südring 11
33647 Bielefeld
Telefon: +49 (0)521 94 22 6 - 0
Fax: +49 (0)521 94 22 6 - 99
Internet: www.seh.de
E-Mail: info@seh.de