PicApport Benutzerverwaltung

Seit Version 5 verfügt PicApport über eine Benutzerverwaltung

Allgemeines

Benutzer

Um Kompatibilität mit vorherigen Versionen zu erreichen ist PicApport per Default so konfiguriert, dass ein automatischer Logon über das Benutzerkonto PicApport erfolgt.
Wird das Kennwort dieses Kontos geändert, das Konto gelöscht oder deaktiviert muss sich jeder Benutzer am Server mit User-ID und Passwort anmelden.

Die Daten der Benutzerkonten werden standardmäßig im Verzeichnis ***./picapport/users*** abgelegt. Existiert dieses Verzeichnis nicht, werden beim Start von PicApport automatisch folgende Konten generiert:

User-ID	Name	Password	Mitglied in Gruppe	Anmerkungen
admin	Systemadministrator	admin	Systemadministratoren	⚠ Wir empfehlen dringend, das Admin-Passwort nach der ersten Installation zu ändern. Bei Auslieferung ist nur der Benutzer Admin berechtigt weitere Benutzer zuzulassen. Um sich als Administrator anzumelden, wählen Sie auf der Startseite von PicApport oben links im "Hamburger-Menü" den Befehl "Abmelden". Jetzt kann man sich mit dem Admin-Konto anmelden und Passwörter sowie Berechtigungen einstellen
picapport	PicApport	picapport	Familie	Bis zur Version 5 gab es in PicApport keine Benutzerverwaltung. Für private Netzwerke ist dies einfach bequemer. Damit dies auch für neue Versionen möglich ist, liefern wir ab sofort PicApport mit einem Standard-Benutzer ***picapport*** aus. Wird nun über einen Browser auf PicApport zugegriffen, wird automatisch der Benutzer PicApport (nebst den konfigurierten Rechten) angemeldet wenn folgendes zutrifft: • Ein Benutzerkonto ***picapport*** mit Kennwort ***picapport*** existiert und ist aktiv
gast	Gast	gast	Gäste	Dies ist unser Vorschlag für ein Gast-Konto mit eingeschränkten Rechten

Gruppen

Alle Rechte die ein Benutzer in PicApport hat, bekommt dieser über seine Gruppenzugehörigkeit. Folgende Regeln gelten hierbei:

- Ein Benutzer ist immer mindestens einer Gruppe zugeordnet
- Ein Benutzer kann mehreren Gruppen zugeordnet werden. Er erhält dann die Summe aller Rechte der Gruppen (Vereinigungsmenge)

Die Daten der Gruppenkonten werden standardmäßig im Verzeichnis ***./picapport/users*** abgelegt. Existiert dieses Verzeichnis nicht, werden beim Start von PicApport automatisch folgende Konten generiert:

Gruppen-ID	Name	Anmerkungen

admins	Systemadministratoren	Im Auslieferungszustand haben Mitglieder dieser Gruppe folgende Rechte:
		• Alle Rechte außer:
		  • Berechtigung Fotos zu entfernen (muss explizit aktiviert werden)
		  • Berechtigung zur Serveradministration über die Web-Gui

family	Familie	Im Auslieferungszustand haben Mitglieder dieser Gruppe folgende Rechte:
		• Alle Rechte außer:
		  • Berechtigung zum anlegen, ändern oder löschen von Benutzern
		  • Berechtigung weitere Benutzer für die eigene Gruppe(n) zulassen
		  • Berechtigung zum anlegen, ändern oder löschen von Benutzergruppen
		  • Berechtigung Geokoordinaten zu setzen (Geotagging).
		  • Berechtigung Metadaten des Fotos zu bearbeiten. (Titel, Aufnahmedatum, usw.)
		  • Berechtigung Fotos zu entfernen

guests	Gäste	Im Auslieferungszustand haben Mitglieder dieser Gruppe folgende Rechte: • Berechtigung Volltextsuchen durchzuführen (Sichtbarkeit: des globalen Suchfeldes) • Berechtigung Suchoptionen einzustellen (Sichtbarkeit: der Suchoptionen) • Berechtigung 'dynamische Sammlungen' anzuzeigen (Sichtbarkeit: 'dynamische Sammlung)

Anmelden am Server (Benutzer Sitzung / Session)

Wenn die PicApport-Weboberfläche im Browser gestartet wird, gilt folgene Reihenfolge zum Ermitteln des Benutzerkontos für die aktuelle Sitzung:

1. Prüfen auf *shared link*: Wenn eine gültige ***sid*** im Requestparameter enthalten ist, dann wird der aktuelle Tab als *shared link* angemeldet.
2. Prüfen auf AccessToken: Wenn ein gültiges ***atu*** im Requestparameter enthalten ist, dann wird das Konto des Benutzers mit diesem AccessToken angemeldet (siehe auch Die PicApport URL's).
   (Das *AccessToken* wird über die Web-GUI der Benutzerverwaltung über das Kontext Menü des Benutzers erzeugt)
3. Prüfen auf IP-Adresse: Ist für die aktuelle IP-Adresse ein Benutzerkonto verknüpft, dann wird dieses Benutzerkonto angemeldet.
4. Prüfen auf PicApport Konto: Gibt es ein Benutzerkonto ***PicApport*** mit Kennwort ***picapport*** dann wird dieses Konto angemeldet.
5. Konnte beim Abarbeiten der oben genannten Punkte kein gültiger Benutzer ermittelt werden, wird die Seite für den Logon angezeigt.

Die Rechte im einzelnen

ID der Berechtigung	Seit	Beschreibung
Berechtigungsgruppe Verwaltung		
pap:admin:user		Berechtigung zum anlegen, ändern oder löschen von Benutzern
pap:admin:user:local		Berechtigung weitere Benutzer für die eigene Gruppe(n) zulassen
pap:admin:group		Berechtigung zum anlegen, ändern oder löschen von Benutzergruppen
pap:admin:changeownpassword		Berechtigung das eigene Kennwort zu ändern
pap:admin:assignipadress		Berechtigung eine IP-Adresse mit dem eigenen Account zu verknüpfen
pap:admin:shares	6.2	Berechtigung Links für geteilte Fotos zu verwalten
pap:admin:useroptions	6.2	Berechtigung Programmoptionen über Eingaben im globalen Suchfeld zu setzen. siehe hierzu auch: Benutzerspezifische Programmoptionen (User-Options)
pap:admin:server	7.6	Berechtigung zur Serveradministration über die Web-Gui.
pap:admin:addon:config	9.0	Berechtigung Konfigurationsparameter von Add-ons einzustellen. Letztlich obliegt es dem jeweiligen Add-on, ob und wie diese Berechtigung genutzt wird.
Berechtigungsgruppe Zugriff auf Fotos		
pap:access:uploads		Berechtigung Dateien hochzuladen
pap:access:ownuploadsvisible		Uploads eines Benutzers sind für diesen immer sichtbar unabhängig von den Filtereinstellungen.
pap:access:downloads		Berechtigung Originaldateien (Fotos in Originalgröße) herunterzuladen / anzuzeigen
pap:access:metadata		Berechtigung Metadaten der Fotos anzuschauen
pap:access:share	6.2	Berechtigung Fotos zu teilen (Link erzeugen)
pap:access:removephotos	7.6	Berechtigung Fotos zu entfernen.
Berechtigungsgruppe Programmfunktionen		
pap:feature:search		Berechtigung Volltextsuchen durchzuführen (Sichtbarkeit: des globalen Suchfeldes)
pap:feature:options		Berechtigung Suchoptionen einzustellen (Sichtbarkeit: der Suchoptionen)
pap:feature:timeline	8.1	Berechtigung die Timeline zu benutzen. (Sichtbarkeit: Timeline)
pap:feature:dyncol		Berechtigung 'dynamische Sammlungen' anzuzeigen (Sichtbarkeit: 'dynamische Sammlung)

pap:feature:dyncol:edit:glob		Speichern, ändern und löschen von globalen 'dynamischen Sammlungen'
pap:feature:dyncol:edit:group		Speichern, ändern und löschen von 'dynamischen Sammlungen' innerhalb der eigenen Gruppe(n)
pap:feature:dyncol:edit:user		Speichern, ändern und löschen von 'dynamischen Sammlungen' für das eigene Benutzerkonto
pap:feature:offcol		Berechtigung 'Lokale Sammlungen' anzulegen
pap:feature:dirbrowser		Berechtigung den Verzeichnisbrowser zu benutzen. (Sichtbarkeit: Verzeichnisse)
pap:feature:msg:newfotos		Wenn gesetzt bekommt der Benutzer auf der Startseite eine Info wenn neue Fotos vorhanden sind.
pap:feature:msg:queryresult		Wenn gesetzt, wird in der Thumbnailanzeige im Titel die Abfrage sowie die Anzahl gefundenen Fotos angezeigt.
pap:feature:map	5.3	Berechtigung das integrierte Kartenmodul zu benutzen.
pap:feature:mapedit	7.6	Berechtigung Mapmarker zu bearbeiten.
pap:feature:designs:select	6.0.3	Berechtigung Designs auszuwählen
pap:feature:designs:changedefault	6.0.3	Berechtigung das Standartdesign zu setzen.
pap:feature:thumbs:canselect	6.0.3	Berechtigung Fotos in der Thumbnailansicht auszuwählen.
pap:feature:sharescreen:send	7.2.0	Berechtigung eigenen Bildschirm zu teilen.
pap:feature:sharescreen:receive	7.2.0	Berechtigung fremden Bildschirm anzuzeigen.
pap:feature:sharescreen:autorecieve	7.2.0	Berechtigung fremden Bildschirm automatisch anzuzeigen wenn Slideshow läuft (z.B. für Bilderrahmen).
Berechtigungsgruppe Metadaten bearbeiten		
pap:editmeta:mytags:like	7.0	Berechtigung ein Foto zu 'liken'.
pap:editmeta:mytags:tags	7.0	Berechtigung eigene Tags zu verwalten (Meine Tags).
pap:editmeta:geo:location	7.0	Berechtigung Geokoordinaten zu setzen (Geotagging).
pap:editmeta:photo	7.0	Berechtigung Metadaten des Fotos zu bearbeiten. (Titel, Aufnahmedatum, usw.)

Properties

Key	Default	Typ	Seit Version	Beschreibung
user.encryption.iterations	1701	int	V5.0.0	SHA-512-Iterationen zum verschlüsseln der Passwörter
user.password.min	1	int	V5.0.0	Mindest Passwortlänge
user.password.max	75	int	V5.0.0	Maximale Passwortlänge
user.log.access	false	boolean	V5.0.0	Erweitertes Serverlogging für Zugriffe einschalten

Technisches

XML-Persistenz

Benutzer-XML

XML-Path	Attribute	Beispielwert	Beschreibung
userdefinition:user	id	testuser@test.net	Eindeutige ID eines Users

	name	Max Mustermann	Benutzer- Anzeigename
	description	the quick brown fox jumps over the lazy dog	Kurzbeschreibung
	active	true	Flag ob der Benutzer aktiv ist.
	created	149370075385	Erstellungsdatum des Benutzers als *long*
	lastupdate	149370825561	Letzte Aktualisierung des Benutzers als *long*
	lastlogin	149370325561	Letzte Anmeldung des Benutzets als *long*
userdefinition:user:security: password	hashed-value	x3ASj9ahC93 ... 8IH23XgcP+Dh8	Gehashtes Passwort
	unhashed-value	klartextpasswort	Password als Klartext. Dient nur zur manueller Erzeugung eines Benutzers. Beim initialisieren wird dieser Eintrag automatisch zu einem *hashed-value*.
userdefiniton:user:ip-addresses:ip-address	value	10.66.77.1	IP-Adresse
userdefinition:user:attributes:attribute	name	street	Attributname
	value	Brückenstr. 2	Attributwert

Rollen-XML

XML-Path	Attribute	Beispielwert	Beschreibung
roledefinition:role	id	guests	Eindeutige ID einer Rolle
	name	Gäste	Rollen- Anzeigename
	description	the quick brown fox jumps over the lazy dog	Kurzbeschreibung
	active	true	Flag ob die Rolle aktiv ist.
roledefinition:role:members:member	id	testuser@test.net	Benutzer die zu dieser Rolle gehören
roledefinition:role: permissions: permission	value	pap:access:downloads	Alle Rechte der Rolle
roledefiniton:role:attributes:attribute	name	street	Attributname
	value	Brückenstr. 2	Attributwert

Verschlüsselung

Es werden zwei verschiedene Verschlüsselungsverfahren verwendet. Die interne Verschlüsselung zum Passwortschutz ist ein Hashverfahren (SHA-512).

Zudem wird ein Asymmetrisches Kryptosystem (RSA) zur Kommunikation zwischen Client und Server verwendet.

Verschlüsselung intern

Die Anzahl der Iterationen und die Salt-größe können über eine Properties-Datei konfiguriert werden.

Algorithmus	Salt-größe	Iterationen	Verwendung
SHA-512	17 Bytes	konfigurierbar	Speicherung von Passwörtern & Gegenprüfung auf Korrektheit

Verschlüsselung Client-Server-Kommunikation

Algorithmus	PublicKey größe	Verwendung
RSA	1024 bit	Erzeugung von Publickeys zur clientseitigen Verschlüsselung von Passwörtern und zur Entschlüsselung dieser auf Serverseite.