- Aktuell seit 6.2

Admin-Client, Authentifizierung, Keycloak, SAML

Achtung:
Störungen oder Ausfälle durch unsachgemäße Einstellungen. Lassen Sie die beschriebenen Komponenten nur von erfahrenem Fachpersonal einrichten. Sichern Sie vorab einen Snapshot der Anlage. Kontaktieren Sie im Zweifelsfall den UCware Support.

SSO-Integration mit Keycloak-IdP

Der UCware Server lässt sich mittels SimleSAMLphp in eine bestehende SSO-Infrastruktur integrieren. In diesem Fall *kann* der Login am UCC- oder einem anderen Client entfallen, wenn der jeweilige Benutzer bereits für eine andere teilnehmende Anwendung authentifiziert wurde.

Innerhalb einer SSO-Infrastruktur stehen sich normalerweise ein Identity Provider (IdP) und mehrere Service Provider (SP) gegenüber. Service Provider sind Anwendungen, die autorisierten Benutzern zur Verfügung stehen. Wenn sich ein Benutzer einloggen möchte, leitet ihn der SP zum IdP weiter. Der IdP nimmt die Anmeldedaten des Benutzers entgegen und authentifiziert ihn gegenüber dem SP. Dazu sendet er einen *Token*, der die Information über den erfolgreichen Login, nicht aber die Anmeldedaten enthält. Diesen Token erhalten auch alle anderen SPs, die der Benutzer innerhalb einer vorgegebenen Frist aufruft. Dadurch sind in dieser Zeit keine weiteren Logins desselben Benutzers erforderlich.

SimpleSAMLphp arbeitet als SP mit allen IdPs zusammen, die SAML 2.0 zum Austausch des SSO-Tokens unterstützen. Dazu gehören u. a. Keycloak, Shibboleth und Microsoft Entra ID.

In diesem Artikel erfahren Sie, wie Sie den UCware Server in eine bestehende SSO-Infrastruktur mit *Keycloak*-IdP integrieren.

Voraussetzungen

SimpleSAMLphp wird ab Version 5.2 des UCware Servers automatisch ausgeliefert bzw. beim Update aus den Paketquellen installiert. Die Integration als SP in eine bestehende SSO-Infrastruktur erfordert den gegenseitigen Austausch von Metadaten mit dem Keycloak-IdP. Klären Sie dazu vorab einen Termin und die Form der Datenübermittlung mit dem zuständigen Administrator.

Die vorgesehenen Benutzer des UCware Servers sollten beim Keycloak-IdP bereits angelegt sein und dort über Passwörter verfügen. Die entsprechenden externen *Usernames* müssen dem Administrator des UCware Servers bekannt sein.

SimpleSAMLphp vorbereiten

Bereiten Sie für den Austausch der Metadaten zunächst den verschlüsselten Zugriff auf das lokale Webinterface von SimpleSAMLphp vor:

1. Greifen Sie per SSH auf den UCware Server zu.
2. Konfigurieren Sie den Webserver:

```
sudo ln -s /etc/nginx/locations.d/03-saml.conf /etc/nginx/https.d/
sudo ln -s /etc/nginx/locations.d/90-simplesamlphp.conf /etc/nginx/https.d/
sudo systemctl reload nginx
```

3. Stellen Sie ein CA-signiertes Zertifikat bereit:

```
sudo mkdir -p /etc/simplesamlphp/ssl/
sudo openssl req -newkey rsa:4096 -new -x509 -days 3652 -nodes -text -out
/etc/simplesamlphp/ssl/zertifikat.crt -keyout /etc/simplesamlphp/ssl/schlüssel.key
sudo chmod 640 /etc/simplesamlphp/ssl/schlüssel.key
sudo chown root:ssl-cert /etc/simplesamlphp/ssl/schlüssel.key
```

   Verwenden Sie dazu eigene Dateinamen anstelle von `zertifikat.crt` und `schlüssel.key`.

4. Geben Sie SimpleSAMLphp Zugriff auf das Zertifikat. Ergänzen Sie dazu in `/etc/simplesamlphp/config.php` die folgende Zeile:

```
'certdir' => '/etc/simplesamlphp/ssl/',
```

5. Öffnen Sie im Webbrowser die Anmeldeseite von SimpleSAMLphp:

```
https://www.example.com/simplesamlphp/module.php/admin
```

   Verwenden Sie die Domain Ihres UCware Servers anstelle des Beispiels.

6. Melden Sie sich mit dem Adminpasswort aus `/var/lib/simplesamlphp/secrets.inc.php` an.

Metadaten austauschen

IdP-Daten exportieren

Die folgenden Schritte muss der Administrator des Keycloak-IdP durchführen:

1. Melden Sie sich bei Ihrem Keycloak-IDP an.
2. Kicken Sie in der Seitenleiste auf *Realm settings* und anschließend auf den Reiter *General*.
3. Zeigen Sie die IdP-Metadaten an, indem Sie auf den Link *SAML 2.0 Identity Provider Metadata* klicken.
4. Speichern Sie die Metadaten im XML-Format.
5. Übergeben Sie die entsprechende Datei an den Administrator des UCware Servers.

IdP-Daten importieren

Die folgenden Schritte muss der Administrator des UCware Servers durchführen, nachdem er die IdP-Metadaten im XML-Format erhalten hat:

1. Öffnen Sie im Webbrowser den *Metadatenparser* von SimpleSAMLphp:

   ```
   https://www.example.com/simplesamlphp/module.php/admin/federation/metadata-converter
   ```

   Verwenden Sie dazu die Domain Ihres UCware Servers anstelle des Beispiels.

2. Laden Sie die Datei mit den IdP-Metadaten hoch und klicken Sie auf *Parse*.
3. Speichern Sie die Ausgabe unter *Konvertierte Metadaten* als `/etc/simplesamlphp/metadata/saml20-idp-remote.php` auf dem UCware Server.
4. Passen Sie den Inhalt der Datei wie folgt an:

```
<?php                                                   // Ergänzen Sie über den konvertierten
Metadaten das PHP-Tag.
$metadata['https://example.com/realms/example'] = [     // Die URL muss zum Realm des verwendeten
Keycloak-IdP passen.
    'entityid' => 'ucware-mus',                         // Eigene Kurzbezeichnung ohne
Leerzeichen eintragen.
    'contacts' => [],
    'metadata-set' => 'saml20-idp-remote',
    'sign.authnrequest' => true,
    'SingleSignOnService' => [
...
```

authsources.php konfigurieren

Damit SimpleSAMLphp die Rolle eines Service Providers gegenüber Keycloak einnimmt, muss der Administrator des UCware Servers die Datei `/etc/simplesamlphp/authsources.php` entsprechend anpassen.

Diese sollte mindestens die folgenden Einträge enthalten:

```
<?php
$config = [
    'admin' => ['core:AdminPassword',],
    'UCware_Musterstadt' =>  [                          // Eigenen Namen für den SP ohne
Leerzeichen eintragen.
                                                        // Dieser wird später als Hosted entity im
Webinterface von SimpleSAMLphp angezeigt.
        'saml:SP',
        'entityID' => 'ucware-mus',                     // 'entityid' aus
/etc/simplesamlphp/metadata/saml20-idp-remote.php eintragen.
                                                        // Diese wird später als Client ID im
Webinterface des Keycloak-IdP angezeigt.
        'idp' => 'https://example.com/realms/example',  // URL des Keycloak-IdP aus
/etc/simplesamlphp/metadata/saml20-idp-remote.php eintragen.
        'discoURL' => null,
        'certificate' => 'zertifikat.crt',              // Zertifikatsdatei aus
/etc/simplesamlphp/ssl/ eintragen.
        'privatekey' => 'schlüssel.key',                // Schlüssel-Datei aus
```

```
/etc/simplesamlphp/ssl/ eintragen.
                                ],
];
```

SP-Daten exportieren

Die folgenden Schritte muss der Administrator des UCware Servers durchführen:

1. Öffnen Sie im Webbrowser den Bereich *Föderation* von SimpleSAMLphp:

   ```
   https://www.example.com/simplesamlphp/module.php/admin/federation/
   ```

   Verwenden Sie dazu die Domain Ihres UCware Servers anstelle des Beispiels.

2. Klappen Sie die SP-Metadaten der *Hosted entity* aus und speichern Sie diese im XML-Format.
3. Übergeben Sie die entsprechende Datei an den Administrator des Keycloak-IdP.

SP-Daten importieren

Die folgenden Schritte muss der Administrator des Keycloak-IdP durchführen, nachdem er die SP-Metadaten im XML-Format erhalten hat:

1. Melden Sie sich bei Ihrem Keycloak-IdP an.
2. Klicken Sie in der Seitenleiste auf *Clients* und anschließend auf den Reiter *Clients list*.
3. Klicken Sie auf den Link *Import client*.
4. Laden Sie anschließend die Datei mit den SP-Metadaten hoch und klicken Sie auf *Save*.
5. Klicken Sie auf den Reiter *Client scopes* und anschließend auf den gewünschten *dedicated*-Eintrag.

   Dieser entspricht der `entityID` aus der `authsources.php` des UCware Servers.

6. Klicken Sie auf *Configure a new mapper* und anschließend im Pop-up auf *User Attribute*.
7. Speichern Sie unter *Add mapper* die folgenden Werte:

Feld	Wert
Name	`username`
User Attribute	`username`
SAML Attribute Name	`username`

SimpleSAMLphp konfigurieren

optional

Bei Bedarf kann der Administrator des UCware Servers die Konfiguration von SimpleSAMLphp unter `/etc/simplesamlphp/config.php` anpassen. Erläuterungen zu den einzelnen Optionen finden Sie direkt in der Datei.

Um beispielsweise die Gültigkeitsdauer der Benutzeranmeldung global zu ändern, bearbeiten Sie den Wert für die Option `session.duration`:

```
'session.duration' => 8 * (60 * 60),
```

Der Wert entspricht der Gültigkeit pro Anmeldung in Sekunden. Im Beispiel sind dies 28800 Sekunden bzw. 8 Stunden.

Hinweis:
Stellen Sie sicher, dass der Wert für `session.duration` kleiner ist als für die Option `session.cookie.lifetime`. Letztere bestimmt die Gültigkeitsdauer des Sitzungs-Cookies im Browser bzw. im nativen UCC-Client.

SimpleSAMLphp testen

Nach dem erfolgreichen Austausch der Metadaten kann der Administrator des UCware Servers SimpleSAMLphp wie folgt testen:

1. Öffnen Sie im Webbrowser den Bereich *Test Authentication Sources* von SimpleSAMLphp:

   ```
   https://www.example.com/simplesamlphp/module.php/admin/test
   ```

   Verwenden Sie dazu die Domain Ihres UCware Servers anstelle des Beispiels.

2. Klicken Sie auf die gewünschte *Hosted entity*.

   Diese entspricht dem Namen des SPs aus der `authsources.php` des UCware Servers.

3. Melden Sie sich mit Name und Passwort eines beim Keycloak-IdP bereits angelegten Benutzers an.

Nach erfolgreicher Anmeldung erhalten Sie die *Statusseite* von SimpleSAMLphp. Das Attribut zur Authentifizierung von Benutzern wird hier unter *Ihre Attribute* angezeigt. Übernehmen Sie das Attribut *exakt* in der angezeigten Form bei der folgenden Erstellung eines SAML-Backends im Admin-Client.

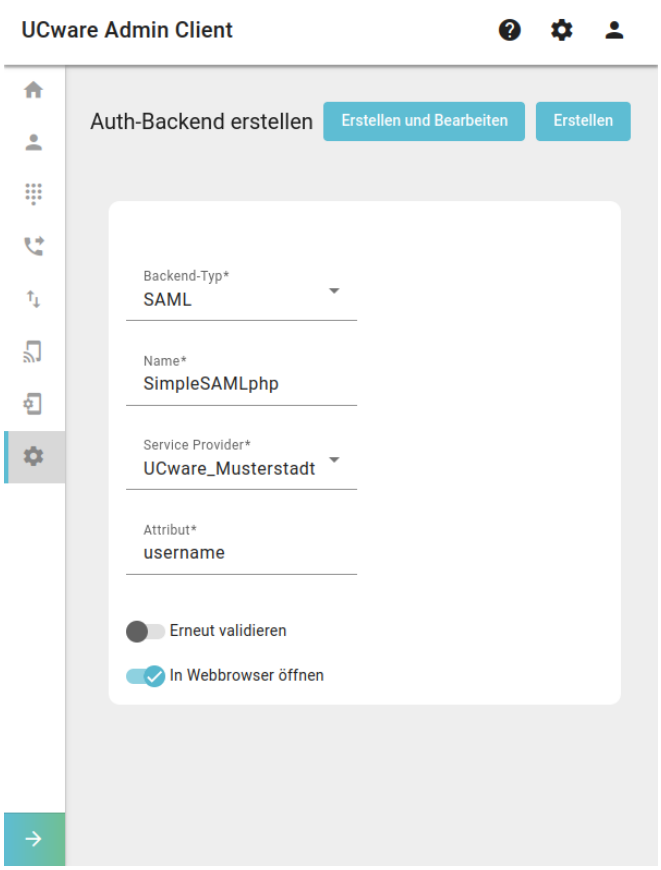
SAML-Authentifizierung für UCware Clients einrichten

Hinweis:
Sobald Sie ein Authentifizierungs-Backend vom Typ *SAML* erstellt haben, wird die Eingabemaske für lokale Anmeldungen an den UCware Clients standardmäßig ausgeblendet. Dies gilt auch für Benutzer, die ihre lokalen Zugangsdaten behalten. In diesem Fall lässt sich die Eingabemaske über die URL des jeweiligen Clients mit angehängtem `#local` aufrufen.

Auth-Backend erstellen

Damit der UCware Server die Logins an seinen Clients über SimpleSAMLphp abwickelt, müssen Sie ein entsprechendes Backend erstellen.

Gehen Sie wie folgt vor:



1. Rufen Sie im Admin-Client die Seite  *System* > *Authentifizierungs-Backend* auf und klicken Sie hier auf  .

2. Wählen Sie als *Backend-Typ* den Eintrag *SAML*.

3. Geben Sie einen *Namen* für die Anzeige des Backends im Admin-Client ein.

4. Wählen Sie den gewünschten *Service Provider* aus.

   Dieser entspricht dem Namen des SPs aus der `authsources.php` des UCware Servers.

5. Geben Sie den Namen des SAML-Attributs ein, mit dem der Keycloak-IdP die Externen IDs der Benutzers abgleichen soll.

   Zur korrekten Form des Attributs beachten Sie den Abschnitt SimpleSAMLphp testen.

6. Belassen Sie die Option *Erneut validieren* standardmäßig auf  .

   Andernfalls werden Name und Passwort bei *jeder* Anmeldung an SimpleSAMLphp weitergereicht und geprüft – auch wenn der Benutzer bereits angemeldet ist.

7. Setzen Sie die Option *Im Webbrowser öffnen* bei Bedarf auf  .

   Dadurch wird die Anmeldeseite von Keycloak auch für Benutzer des *nativen* UCC-Clients im Webbrowser geöffnet.

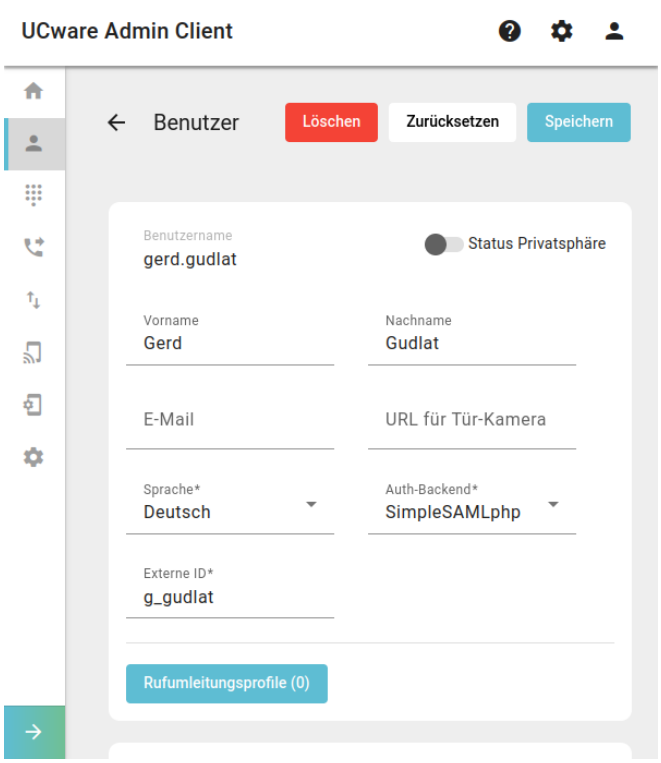
8. Übernehmen Sie die Einstellungen mit Erstellen.

Auth-Backend zuweisen

Sie können SimpleSAMLphp nun als Authentifizierungs-Backend für neue und bereits angelegte Benutzer des UCware Servers zuweisen. Dabei handelt es sich um eine individuelle Einstellung, sodass Anmeldungen mit lokalen Zugangsdaten bei Bedarf weiterhin möglich sind – beispielsweise für Administratoren. In diesem Fall gelangen die betroffenen Benutzer zur lokalen Anmeldemaske, indem sie `#local` an die URL ihres Clients anhängen.

Benutzer des SimpleSAMLphp-Backends müssen im Keycloak-IdP bereits angelegt sein. Ihr lokales Benutzerpasswort wird aus der Datenbank des UCware Servers gelöscht. Eine Anmeldung ist somit nur noch mit den beim Keycloak-IdP gespeicherten Daten möglich.

Gehen Sie wie folgt vor:



1. Rufen Sie im Admin-Client die Seite *Benutzer & Gruppen > Benutzer* auf.
2. Erstellen oder bearbeiten Sie einen Benutzer.
3. Wählen Sie dabei das gewünschte SimpleSAMLphp-*Backend* aus.
4. Geben Sie als *Externe ID* den beim Keycloak-IdP hinterlegten *Username* des Benutzers ein.

   Dieser weicht ggf. vom lokalen *Benutzernamen* auf dem UCware Server ab.
5. Übernehmen Sie die Einstellungen mit Erstellen bzw. Speichern.