

White-Paper: Single Sign-On mit Active Directory

Inhalt

- Über dieses White-Paper.....3**
 - Zusammenfassung.....3
 - Gilt für.....3
 - Status.....3

- Theorie.....4**
 - Einführung.....4
 - Hintergrund.....4

- Umsetzung.....5**
 - Voraussetzungen.....5
 - Konfiguration.....5
 - Anwendung.....7

- Weitere Informationen.....8**

- Rechtliche Hinweise.....9**

Über dieses White-Paper

Änderungsstand: 2023.0.1-SNAPSHOT

Autor: Markus KARG (karg@quipsy.de)

Zusammenfassung

Die Einrichtung der **Active Directory Federation Services** (ADFS) als **OpenID Connect Identity Provider** (OIDC IdP) ermöglicht die Anmeldung an QUIPSY[®] mit **Active-Directory[®]-Benutzerkonten**.

Gilt für

- QUIPSY[®] 2023.0.1-SNAPSHOT

Status

Dies ist ein offizielles Whitepaper für QUIPSY[®] 2023.0.1-SNAPSHOT.

Theorie

Einführung

Unternehmen bieten ihren Mitarbeitern eine Vielzahl an Anwendungen, um die betrieblichen Aufgaben zu erfüllen. Bestimmte Anwendungen, beispielsweise QUIPSY[®], müssen die *Identität* des Anwenders kennen, beispielsweise um den Zugang zu Anwendungen oder bestimmten Funktionen zu beschränken. In der Folge müssen sich Nutzer an *mehreren* Anwendungen anmelden, d. h. ihre Identität *immer wieder* belegen, beispielsweise mittels der Kenntnis eines Passwortes.

Um diese vielen Anmeldevorgänge zu reduzieren, aber auch um modernere bzw. sicherere Identitätsnachweise nutzen zu können, setzen Unternehmen SSO (Single Sign-On) ein. Hierbei erfolgt eine Trennung in ein zentrales, *identifizierendes* System, den sogenannten *Identitätsprovider* (IdP), und die Anwendungen, welche keine eigenständige Identitätsfeststellung mehr vornehmen, sondern eine vom IdP geprüfte und bestätigte Identität *nutzen*.

Viele Unternehmen setzen zur zentralen Identitätsverwaltung *Active Directory* ein, einen Teil des Betriebssystems *Windows[®] Server*.

Dieses White-Paper beschreibt, wie sich *Active Directory* als SSO-Lösung mit QUIPSY[®] einrichten und nutzen lässt.

Hintergrund

- **SSO** (Single Sign-On) bezeichnet Verfahren und Technologien zur einmaligen, zentralen Anmeldung eines Benutzers mit dem Ziel, *alle* Anwendungen zu verwenden, ohne sich an *jeder* Anwendung getrennt anmelden zu müssen.
- **OIDC** (OpenID Connect) ist ein internationaler Industriestandard für Single Sign-On, der eine weltweit einheitliche Schnittstelle zu Identitäts Providern (IdP) normiert. Dieser wird von vielen IdP, wie beispielsweise ADFS, implementiert und von vielen Anwendungen, wie beispielsweise QUIPSY[®], unterstützt.
- **ADFS** (Active Directory Federation Services) ist ein OIDC-konformer IdP der Fa. Microsoft, der als Teil des Betriebssystems *Windows[®] Server* seine Benutzerkonten aus *Active Directory* bezieht. ADFS ist im Lieferumfang des Betriebssystems enthalten, jedoch in der Standardinstallation nicht aktiviert. Daher muss ADFS nachträglich aktiviert und konfiguriert werden, um AD-Konten zur Anmeldung an OIDC-fähigen Anwendung wie z. B. QUIPSY[®] zu verwenden.

Umsetzung

Voraussetzungen

- QUIPSY® ist installiert und betriebsbereit konfiguriert und Sie verfügen über die notwendigen Kenntnisse und Berechtigungen, um Änderungen an QUIPSY® vorzunehmen.
- Anwender sind in QUIPSY® angelegt und diese können sich erfolgreich an QUIPSY® anmelden.
- Active Directory ist installiert und betriebsbereit eingerichtet und Sie verfügen über die notwendigen Kenntnisse und Berechtigungen, um Änderungen an der Windows®-Domäne, an Active Directory, und am Betriebssystem Windows® Server vorzunehmen.
- Anwender sind in Active Directory angelegt und diese können sich erfolgreich an Active Directory anmelden.
- Der Betriebsablauf darf unterbrochen werden. **Während der Abarbeitung dieses White-Papers ist QUIPSY® nicht nutzbar.**

Konfiguration

Die grundsätzliche Einrichtung von OIDC ist im QUIPSY®-Handbuch beschrieben. Dieses White-Paper beschreibt darüber hinausgehend die speziellen Belange von ADFS, die hierbei zu berücksichtigen sind.

Hinsichtlich der im Folgenden gezeigten Befehle wird auf die jeweiligen Produkthandbücher verwiesen.

Grundsätzliches

Die gesamte ADFS-Administration, incl. der Anmeldung von OIDC-Clients (somit also von QUIPSY®), erfolgt über *PowerShell*. Die OIDC Client ID wird in ADFS *wahlfrei* vom Administrator vergeben.

ADFS aktivieren

Die Aktivierung von ADFS ist grundsätzlich unter <https://learn.microsoft.com/en-us/windows-server/identity/ad-fs/operations/set-up-an-ad-fs-lab-environment> beschrieben.

Zusammengefasst lässt sich ADFS wie folgt aktivieren:

- **Voraussetzung:** Der Host für ADFS muss Mitglied einer Windows®-Domäne sein. Nötigenfalls kann wie folgt eine Windows®-Domäne aufgesetzt werden:

```
Install-WindowsFeature -Name AD-Domain-Services -  
IncludeManagementTools  
Import-Module ADDSDeployment  
Install-ADDSForest -DomainName "<Domain>" -InstallDNS -  
SafeModeAdministratorPassword $(ConvertTo-SecureString -  
string "<Admin-Password>" -asplaintext -Force) -Force
```

Nun rebooten.

- **Voraussetzung:** Der Host für ADFS ist im DNS registriert. Nötigenfalls kann wie folgt eine Registrierung durchgeführt werden:

```
Add-DnsServerResourceRecordCName -Name "adfs1" -  
HostNameAlias "<Alias>" -ZoneName "<Domain>"
```

- **Voraussetzung:** Der Host für ADFS verfügt über ein gültiges Zertifikat. Nötigenfalls kann wie folgt ein Zertifikat erzeugt und installiert werden:

```
Export-Certificate -Cert $(New-SelfSignedCertificate -
  DnsName "adfs1.<Domain>") -FilePath $env:TEMP\adfs1.cer
Import-Certificate -FilePath $env:Temp\adfs1.cer -
  CertStoreLocation "cert:\LocalMachine\Root"
Remove-Item $env:Temp\adfs1.cer
```

Das Zertifikat ist in analoger Weise auf allen Clients anzuwenden (z. B. per Gruppenrichtlinie zu verteilen).

- **Durchführung:** Das Windows-Feature *ADFS Federation* ist zu installieren.

```
Install-WindowsFeature "adfs-federation" -
  IncludeManagementTools
Add-KdsRootKey -EffectiveImmediately
```

In Produktivumgebungen nun 10 Stunden warten (in Testumgebungen kann alternativ `-EffectiveTime ((get-date).addhours(-10))` statt `-EffectiveImmediately` verwendet werden).

```
Install-AdfsFarm -CertificateThumbprint "<Thumbprint des
  Zertifikats>" -FederationServiceName "adfs1.<Domain>" -
  GroupServiceAccountIdentifier "<Domain>\FsGsmas"
Initialize-ADDeviceRegistration
Enable-AdfsDeviceRegistration
```

QUIPSY® als OIDC-Client in ADFS konfigurieren

```
Set-AdfsResponseHeaders -EnableCORS $true
Set-AdfsResponseHeaders -CORSTrustedOrigins "https://
  quipsy:8080", "http://quipsy:8080"
Add-AdfsClient -Name "QUIPSY®" -ClientId "<client-id>" -
  RedirectUri "https://quipsy:8080/oidc/callback", "http://
  quipsy:8080/oidc/callback"
```

WIA (optional)

WIA (Windows Integrated Authentication) ist eine im Browser enthaltene Technologie, welche die Anmeldungen an ADFS *automatisch* mit dem lokal angemeldeten Windows®-Domänenbenutzer-Konto vornimmt, *anstatt* eine explizite Identifikationsprüfung durch ADFS vorzunehmen.

Die Verwendung von WIA ist optional und nur in bestimmten Browsern verfügbar:

- **Firefox:** Informationen zur Nutzung von WIA mit *Firefox* sind unter <https://support.mozilla.org/en-US/kb/windows-sso> zu finden.
- **Edge** und **Chrome:** Diese Browser unterstützen WIA automatisch, sofern vom Administrator nicht explizit verhindert.

Grundsätzlich sind Browser mittels ihrer Agent-Kennung in ADFS für WIA freizuschalten (hier am Beispiel *Chrome*, das gleichzeitig *Edge* freischaltet):

```
$wiaStrings = Get-ADFSProperties | Select -ExpandProperty
  WIASupportedUserAgents
$wiaStrings = $wiaStrings + "=~Windows\s*NT.*Chrome"
```

```
Set-ADFSProperties -WIASupportedUserAgents $wiaStrings
```

In den Internetoptionen muss die *Lokale Intranetzone* explizit um die URL des ADFS Servers (z. B. `https://adfs1.<Domain>`) erweitert werden, selbst wenn diese Zone bereits so konfiguriert ist, dass sie *alle nicht anderweitig gelisteten* Adressen enthält.

ADFS in QUIPSY® als IdP konfigurieren

Die in QUIPSY® zu hinterlegende Kennung (*iss*) hat den folgenden Aufbau: `https://adfs1.<Domain>/adfs` und wird über diesen Befehl in QUIPSY® hinterlegt:

```
quipsy admin oidc add-client --iss <iss> --client-id  
<client-id>
```

AD-Konten zu QUIPSY®-Konten zuordnen

Jedes QUIPSY®-Konto, das sich per ADFS anmelden können soll, benötigt die Zuordnung des betreffenden AD-Kontos.

ADFS besitzt keinen Befehl und auch keine Benutzeroberfläche, um die benötigte Kennung (*sub*) zu ermitteln, diese kann jedoch über den Umweg einer OIDC-API-Anfrage im Browser herausgefunden werden. Hierzu ist der folgende URL-Aufbau anzuwenden:

```
https://adfs1.<Domain>/adfs/oauth2/authorize/?  
response_type=id_token&client_id=<client-  
id>&redirect_uri=https://quipsy:8080/oidc/  
callback&scope=openid&nonce=12345
```

Der Befehl zur Hinterlegung der Kennung (*sub*) in QUIPSY® ist:

```
quipsy admin oidc add-account --user-id <user-id> --iss  
<iss> --sub <sub>
```

Anwendung

Die Anmeldung an QUIPSY® durch den Anwender erfolgt bei Nutzung von WIA automatisch.

Gegebenenfalls flackert dabei kurz ein Popup-Fenster auf, das sofort wieder verschwindet.

Wird *kein* WIA verwendet, zeigt ADFS beim QUIPSY®-Login eine Anmeldeseite.

Diese kann sich optisch je nach Version des Betriebssystems als auch nach dessen Konfiguration unterscheiden.

Auf der Anmeldeseite sind der AD-Kontoname und das zugehörige Passwort einzutragen.

Weitere Informationen

- Weitere Informationen zu [OpenID Connect](#) sind auf der Webseite der OpenID Foundation (OIDF) zu finden.
- Weitere Informationen zu [Active Directory Federation Services](#) sind auf der Webseite der Microsoft Corporation zu finden.
- Weitere Informationen zu **QUIPSY**[®] finden Sie im Handbuch.

Rechtliche Hinweise

Alle genannten Markennamen sind durch die jeweiligen Markeninhaber geschützt und dürfen nicht ohne entsprechenden Hinweis verwendet werden.