

Bijlage 8a behorend bij de eisen

1. Authenticatie en SSO

Utrecht hanteert het Single Sign On beleid voor interne en externe applicaties aangevuld met een tweede factor. Medewerkers van de Gemeente Utrecht beschikken over één identiteit en een 2^e factor op basis van Microsoft MFA. Ten behoeve van SSO wordt er federatie toegepast op basis van Azure Federatie aangevuld met conditionele toegangs beleid.

Identiteiten worden automatisch beheerd, applicaties worden aangesloten voor authenticatie op de Utrecht identiteit. Hiervoor zijn aansluitvoorwaarden van toepassing (zie hoofdstuk 2. Authenticatie en provisioning standaarden)

2. Authenticatie en provisioning standaarden

De Gemeente maakt gebruik van moderne authenticatie op basis van Azure Federatie.

Onderstaande tabel bevat de door Utrecht ondersteunde protocollen en toepassing daarvan.

Er is een IAM loket beschikbaar welke de federatieve koppeling samen met de leverancier realiseert.

IAM@Utrecht.nl

Nr.	Protocol	Status	Middel	Interne applicaties	SaaS/Cloud-applicaties
1	OpenID Connect Oauthv2	Voorkeur	Azure Federatie (3)	Ja	Ja
2	SAML v2.0	Alternatief	Azure Federatie	Ja	Ja
3	Kerberos	Alleen intern	Active Directory	Ja	Nee
4	LDAPS	Niet toegestaan		n.v.t.	n.v.t.

Nr.	Protocol	Status	Middel	Interne applicaties	SaaS/Cloud-applicaties
1	SCIMv2	Voorkeur	Azure SCIM endpoint	Ja	Ja
2	SCIMv2	Alternatief	Interne SCIM endpoint	Ja	Ja
3	Maatwerk REST API	Indien beschikbaar	Azure SCIM	Ja	Ja
4	Maatwerk XML SOAP	Alleen bij uitzondering		Ja	Ja

5	Eigen implementatie	Alleen bij uitzondering		Ja	Ja
6	Handmatig	Afhankelijk van BIV classificatie toegestaan		Ja	Ja
7	Microsoft LDAPS	Niet toegestaan		n.v.t.	n.v.t.
8	Bestand: XML, JSON (beveiligd)	Niet toegestaan		n.v.t.	n.v.t.

Toelichting:

1. Nummering van protocollen staat in volgorde van voorkeur
2. De mate en inrichting van identity provisioning is mede afhankelijk BIV-classificatie en het gebruik van rollen.
3. Bij Container platform met Keycloak als broker
4. Alleen bij uitzondering; na afstemming met architectuur

3. Wachtwoordbeleid

Gemeente Utrecht hanteert het volgende minimale wachtwoordbeleid voor de Utrecht identiteiten.

Lengte: minimaal 12 karakters

1. **Complexiteit:** Een complex wachtwoord bestaat uit minimaal twaalf karakters waarin ten minste 3 van de 4 karakters gebruikt worden:
 - o kleine letters : a, b, c, ... z
 - o hoofdletters : A, B, C, ... Z
 - o cijfers : 0, 1, 2, ... 9
 - o speciaal tekens : ({[].,<>:;'"?/\`~!@#\$%^&*()_-=)
2. **Naam:** Het wachtwoord mag niet de voornaam of achternaam bevatten van de betreffende natuurlijk persoon behorende bij deze identiteit
3. **Verboden woorden / begrippen:** (delen van) wachtwoorden mogen geen woorden omvatten die opgeslagen zijn in een tabel van verboden woorden / begrippen ter voorkoming van makkelijke wachtwoorden (bijvoorbeeld 'Welkom123456')
4. **Vervaltermijn;** minimaal om 60 dagen vernieuwen van het wachtwoord (BIO-beleid).
5. **Wijzigingen van wachtwoord:** Het wachtwoord kan op zijn vroegst na 7 dagen weer veranderd worden. Zes (6) recente wachtwoordwijzigingen worden onthouden en mogen niet opnieuw worden gebruikt en worden accounts automatisch geblokkeerd;
 - o Na 3 foutieve inlogpogingen voor minimaal 10 minuten.
 - o Als de geldigheidstermijn van het wachtwoord is verlopen

4. Aansluiten op security monitoring

In onderstaande tabel worden de aansluitmogelijkheden voor interne (toepassingen binnen de Utrecht omgeving) en externe (SaaS en public cloud) weergegeven voor aansluiting op de Sentinel security monitoring omgeving.

Nr.	Protocol	Intern	Toelichting	Extern	Toelichting
-----	----------	--------	-------------	--------	-------------

1	Rest API	Rest API gebaseerde bron middels Logs Ingestion API in Azure monitor ontsloten	Conform specificaties Log Ingestion API . Voorheen “HTTP data collector API”	Rest API gebaseerde bron middels Logs Ingestion API in Azure monitor ontsloten	Conform specificaties Log Ingestion . Voorheen “HTTP data collector API”
2	Azure Logic app, Azure Function	Alleen indien log ingestion niet functioneert	Alternatief voor log ingestion.	Alleen indien log ingestion niet functioneert	Alternatief voor log ingestion.
3	Azure Monitoring Agent	AMA Agent op IaaS resource	AMA agent levert de log data naar Azure monitor	Geen aansluiting	n.v.t.
4	Syslog	Via syslog collector Azure Monitor	Via een Azure Monitoring Agent met “Syslog NG”	Geen aansluiting	n.v.t.
5	Netflow	Bijv. netwerkapparatuur	Alleen bij uitzondering	Geen aansluiting	