IQUALIFY 6.0.0

Regelmatig brengen we een minor update voor iQualify uit. In minor updates worden voornamelijk bugs opgelost. Daarnaast kunnen er kleine functionele wijzigingen in zitten. Dit zijn verbeteringen die het gebruik van iQualify nog eenvoudiger maken en zonder toelichting gebruikt kunnen worden. Grotere functionele wijzigingen worden in een major update beschikbaar gemaakt. Release 6.0.0 betreft een major release, niet omdat er grote functionele wijzigingen zijn doorgevoerd maar omdat er technisch veel gewijzigd is om de verhuizing naar het Microsoft Azure platform mogelijk te maken. Daarnaast zijn er ook een aantal bugs opgelost. Benieuwd naar wat er veranderd is in release 6.0.0? We hebben het voor je samengevat op deze pagina. Kijk op status.infoland.nl wanneer versie 6.0.0 gereleaset wordt.

Verhuizing naar Microsoft Azure platform

Met deze release gaan we iQualify verhuizen naar de Microsoft Azure-cloud, waarbij tegelijkertijd een modernisering plaatsvindt van onze technische software-architectuur om deze nog robuuster en nog beter schaalbaar te maken.

Het Microsoft Azure platform stelt ons in staat om te bouwen op een basisplatform wat een zeer hoge beschikbaarheid garandeert, en waarbinnen we bijna instant capaciteit kunnen toevoegen om ervoor te zorgen dat iQualify vlot blijft werken: ook op de drukste momenten van de dag; ook als het aantal gebruikers verder toeneemt.

Er zijn een paar veranderingen waar je mogelijk rekening mee dient te houden:

- Wijziging IP-adres
- Wel https:// geen http://
- TLS 1.2 of hoger

Wijziging IP-adres

Het externe IP-adres van iQualify gaat veranderen. Er zijn twee situaties waarin dat voor jouw organisatie gevolgen kan hebben.

- Gegevensuitwisseling met iQualify iSync
- IP-restrictie beveiligde toetsafname

Gegevensuitwisseling met iQualify iSync

Voor het ophalen van gebruikersgegevens, gebruikersgroepen en groepslidmaatschappen uit AD (Active Directory), of het aanmelden van een AD gebruiker kan iSync gebruikt worden. Om deze gegevensuitwisseling mogelijk te maken, dient de SaaS hosting infrastructuur toegang te krijgen tot een proxy (web applicatie) die draait op de infrastructuur van jouw organisatie. En om dit veilig te laten verlopen, wordt meestal het externe IP adres van de iQualify hosting infrastructuur toegevoegd aan de firewall configuratie.

Je kunt in het applicatiebeheer van iQualify zien of je organisatie gebruik maakt van een proxy voor gegevensuitwisseling. Je kunt zien wat de URL naar de proxy-applicatie binnen de infrastructuur van de organisatie is. Zie hiervoor: **iQualify Instellingen – iSync**

IP-restrictie beveiligde toetsafname

Mogelijk maakt jouw organisatie gebruik van de Secure Test Environment (STE) voor het afnemen van toetsen binnen een beveiligde omgeving. Hierbij wordt vaak in de firewall (van de instelling zelf) ingesteld dat pc's in toetslokalen beperkt toegang krijgen tot het internet, bijvoorbeeld alleen het IP-adres van de iQualify STE. Toegang naar andere websites wordt geblokkeerd.

Wat moet jouw organisatie doen?

Als jouw organisatie nu een IP-restrictie heeft ingesteld dan moeten de nieuwe IP-adressen voorafgaand aan de release worden toegevoegd aan de firewall configuratie. Controleer hiervoor of in de firewall configuratie op dit moment de volgende IP-adressen staan vermeld:

84.38.237.100
84.38.237.102
84.38.237.108
84.38.237.109
84.38.237.114

Als één van deze bovenstaande adressen is ingericht dan moeten deze nieuwe IP-adressen toegevoegd worden:

20.93.240.8/30 (20.93.240.8 t/m 20.93.240.8.11)
20.76.12.112/29 (20.76.12.112 t/m 20.76.12.119)

Wat zijn de gevolgen?

Als organisatie merk je niks van de verandering van de externe IP-adressen, mits de nieuwe adressen tijdig zijn toegevoegd. Nadat deze release is uitgebracht komen de oude IP-adressen direct te vervallen. Deze kunnen dan ook na de release uit de configuratie verwijderd worden. Ten tijden van de release is het raadzaam dat de oude en nieuwe IP-adressen in de firewall configuratie toegevoegd zijn.

Als na de release de configuratie niet is aangepast kunnen gebruikers in iQualify mogelijk niet meer aanmelden.

Wel https:// geen http://

Het is niet meer mogelijk om iQualify te benaderen via URL's waarbij het onbeveiligde http:// protocol gebruikt wordt. Alleen met URL's die starten met https:// kun je iQualify benaderen. Het standaard gedrag van browsers is dat deze van een url zoals infoland.iqualify.nl automatisch https://infoland.iqualify.nl maken. Dit maakt het dat gebruikers hier normaal geen last van hebben. Gebruik je directe verwijzingen naar iQualify, bijvoorbeeld voor gedeelde (LTI) toetsen dan is het aan te bevelen om te controleren of deze https:// als prefix gebruiken en zo nodig aan te passen.

Beveiligings-protocol TLS 1.2 of hoger

Met de overgang naar het Microsoft Azure platform wordt TLS 1.0 en TLS 1.1 niet meer ondersteund. Ook hiervoor geldt dat deze wijziging voor een standaard moderne browser geen belemmering geeft. Het zou wel een rol kunnen spelen voor organisaties die via een ander systeem API's van iQualify aanspreken of een oudere versie van i+Sync gebruiken.

Bugfixes:

- 60696: Na genoten Scorm training werd niet altijd de status van de training op afgehandeld gezet, tevens werd de vervolgtraining of toets niet geladen.
- 63949: Gebruikersgroepen die reeds aan een leerperiode gekoppeld waren werden nog in de lijst met beschikbare groepen getoond.
- 63809: De samenvatting van een nieuwe vraag begint niet met een hoofdletter.

- 63919: Na het activeren van een gebruiker die zich in de wachtkamer bevindt probeert iQualify de gebruiker 2 maal in te loggen waardoor de gebruiker soms juist uitgelogd raakt.

status.infoland.nl

Als er gepland onderhoud, ongepland onderhoud of een actuele verstoring is wordt dit altijd gecommuniceerd via de pagina status.infoland.nl. Op deze pagina kun je je abonneren om automatisch op de hoogte te worden gebracht over belangrijk onderhoud of verstoringen. Ook kun je hier de status van actuele verstoringen bekijken.