Whitepaper

november 2020

Hoe Okta applicaties integreert

Een overzicht van de architectuur

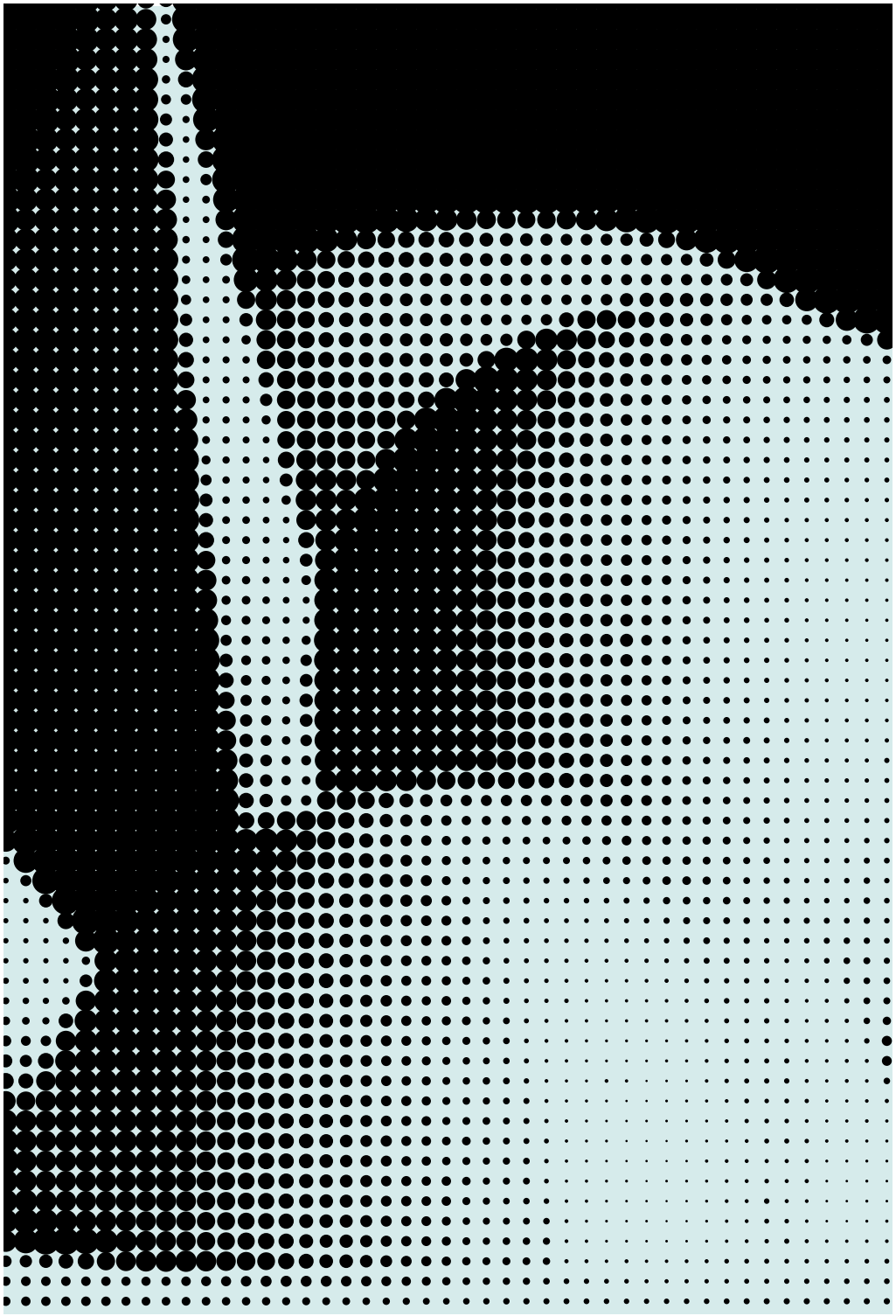
Okta Benelux

Strawinskylaan 4117,
3rd Floor

1077 ZX Amsterdam,
The Netherlands

info_benelux@okta.com

+44 (800) 3688930



okta

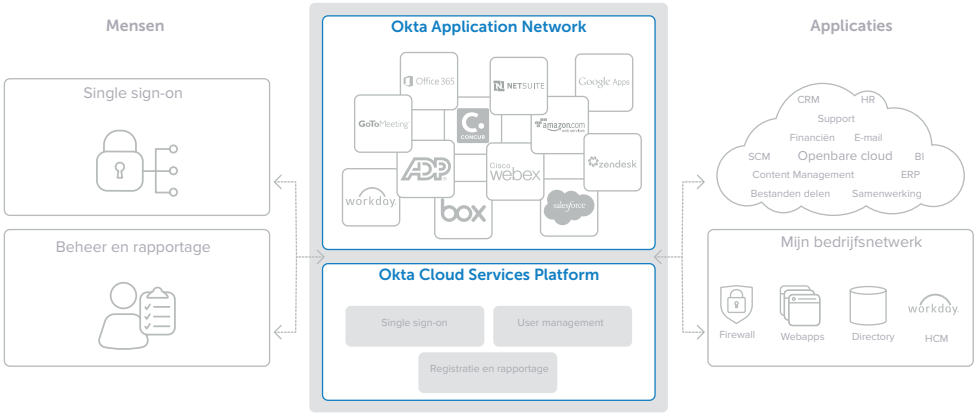
Inhoudsopgave

Okta: Enterprise-identity, kant-en-klaar

Okta is een IAM-service op enterpriseniveau, volledig gebouwd in de cloud en met een sterke focus op klantsucces. Met Okta kan de IT-afdeling de toegang voor elke applicatie, iedere persoon en elk device beheren. Of het nu gaat om medewerkers, partners of klanten, of applicaties zich nu in de cloud, on-prem of op een mobiel device bevinden, Okta zorgt voor een veiliger IT, maakt mensen productiever en helpt te voldoen aan relevante regelgeving.

Applicaties integreren met de Okta-service

Anders dan andere IAM-oplossingen is Okta niet simpelweg een toolkit waarmee u uw webapplicaties aan uw gebruikersdirectory's koppelt. Dat kost gewoon te veel tijd en resources. In plaats daarvan "integreert" Okta applicaties in zijn service. U hoeft deze vooraf geïntegreerde applicaties dan alleen nog maar waar nodig voor uw gebruikers te implementeren. U kunt die gebruikers authenticeren aan de hand van uw eigen user store (zoals Active Directory of LDAP) of u kunt Okta als user store gebruiken. Okta is uniek in het bieden van snelle, multifunctionele integraties met webgebaseerde en native mobiele apps, of die zich nu in de cloud, on-prem of op uw smartphone of tablet bevinden. Deze integraties worden geleverd als onderdeel van de Okta-service en bevatten functies voor zowel single sign-on (SSO) als user management. In dit document worden de verschillende manieren beschreven waarop Okta applicaties in zijn service integreert.



Okta: Toegang beheren voor elke applicatie, elk device of iedere persoon

Cloud-, on-prem en mobiele apps

We kunnen het beste beginnen met een onderscheid te maken tussen cloudapps, on-prem apps en mobiele apps.

Voor typische cloudapplicaties (zoals Salesforce, Google Apps, Workday, enz.) geldt dat deze integraties plaatsvinden binnen het Okta Application Network. Beheerders maken een keuze uit de Okta-lijst met duizenden ondersteunde applicaties, gebruiken een eenvoudige wizard voor het beantwoorden van standaardvragen over hun specifieke instantie van de applicaties (zoals URL en beheer-ID's) en Okta doet de rest.

Alle technische details (zoals SSO-protocollen en API-implementaties voor user management) zijn opgenomen in de service en worden door Okta namens u continu onderhouden. Deze applicaties kunnen een standaard als SAML of OpenID gebruiken, ze kunnen een zelf ontwikkelde API hebben of ze kunnen gebruikmaken van het SWA-protocol (Secure Web Authentication) van Okta.

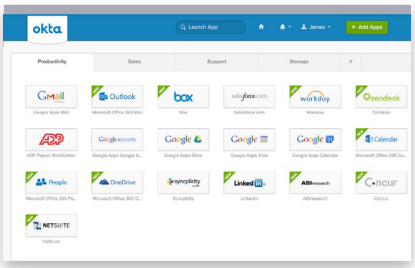
Ook zijn veel van de populairste on-prem webapplicaties (Oracle Apps, Lawson, Jira, enz.) opgenomen in het Okta Application Network. Voor zelf ontwikkelde on-prem webapplicaties biedt Okta bovendien een scala aan integratieopties. Secure Web Authentication-integratie voor SSO is eenvoudig toe te voegen. Okta heeft SAML-toolkits om uw apps geschikt te maken voor SAML en Okta ondersteunt provisioning en deprovisioning voor applicaties die user management-API's openbaar beschikbaar stellen.

Okta zorgt ook voor eenvoudige toegang tot mobiele enterprise-applicaties vanaf elk device. Of uw enterprise-apps nu voor mobiele platforms geoptimaliseerde HTML5-webapps zijn, native iOS- of Android-apps, Okta heeft altijd een oplossing. Alle webapplicaties in het Okta Application Network kunnen worden geopend met SSO vanaf elk mobiel device. Mobiele webapps kunnen gebruikmaken van de industriestandaard SAML of van de Secure Web Authentication SSO-technologie van Okta. Native applicaties zoals Box Mobile kunnen worden geïntegreerd met SAML-authenticatie voor registratie en met OAuth voor doorlopend gebruik.

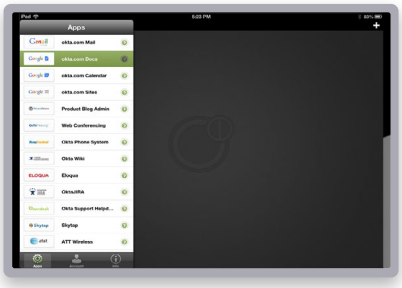
Single sign-on voor ELKE applicatie

Okta zorgt voor een naadloze user experience met behulp van single sign-on voor ALLE web- en mobiele applicaties die gebruikers nodig hebben. Gebruikers loggen eenmalig in en kunnen dan elke applicatie starten zonder opnieuw inloggegevens te moeten invoeren. Denk er wel aan dat SSO op deze manier alleen goed werkt wanneer SSO voor ALLE applicaties is ingeschakeld. Als sommige applicaties niet kunnen worden ondersteund, is er geen sprake van echte single sign-on. Daarom hanteert Okta verschillende methoden om SSO voor verschillende webapplicaties in te schakelen.

Okta brengt eerst een op veilige wijze geauthenticeerde sessie met de browser van de gebruiker tot stand. Vervolgens kan Okta de gebruiker authenticeren voor elke verbonden applicatie met behulp van een of twee SSO-integratiemethoden. De SSO-integraties van Okta zijn ofwel federatief (en ondersteunen dan een standaard zoals SAML of een ander zelf ontwikkeld federatief authenticatieprotocol) ofwel ze gebruiken Secure Web Authentication (SWA) van Okta om een beveiligd, op een formulier gebaseerd bericht naar de loginpagina van de applicatie te sturen, waardoor de gebruiker automatisch wordt aangemeld.



De landingspagina "Mijn applicaties" van Okta is een handig startpunt voor alle applicaties.



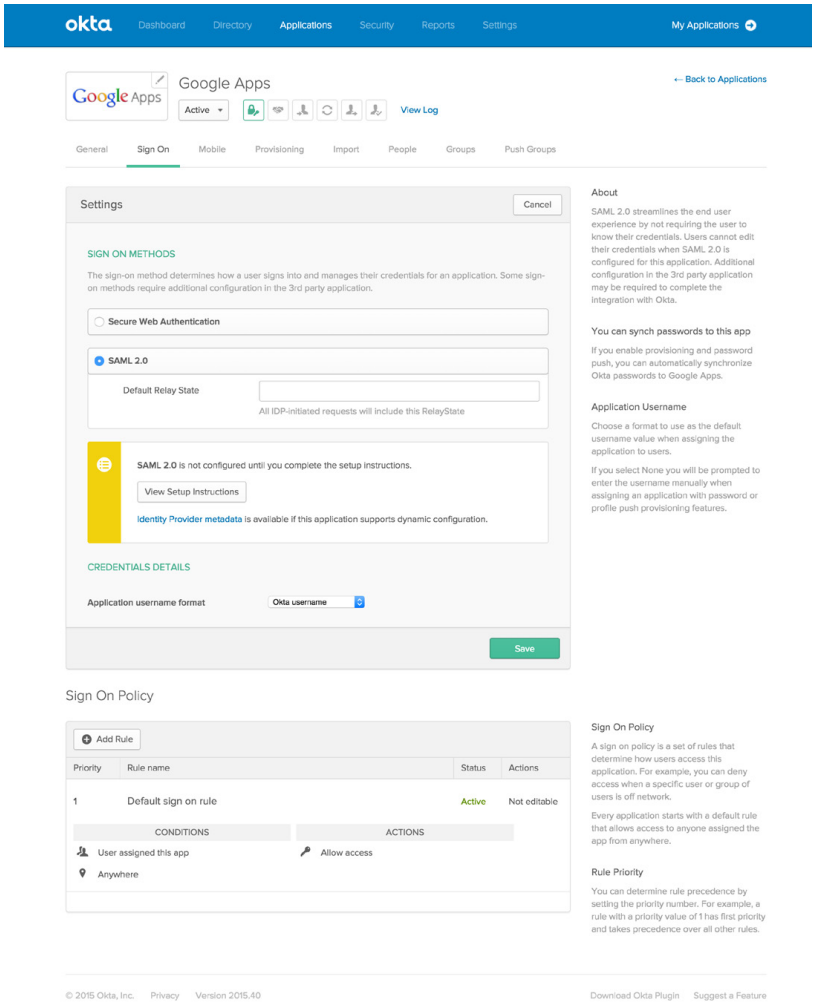
De native iOS-app van Okta is geschikt voor iPads en iPhones.

SSO gebaseerd op standaarden

Er zijn meerdere op standaarden gebaseerde manieren om SSO in te stellen. Omdat Okta een cloudservice is, kunnen we ondersteuning toevoegen voor alle mogelijke standaarden en hoeven we dus niet te kiezen tussen de ene of de andere standaard.

Okta ondersteunt een groot aantal federatieve SSO-protocollen waaronder standaarden zoals SAML (1.1 en 2.0). Sommige applicatieleveranciers ondersteunen alleen zelf ontwikkelde federatieve SSO-protocollen, maar omdat Okta die ook ondersteunt, werkt het prima. Als een applicatie authorisatieondersteuning voor OpenID nodig heeft, is het voor Okta makkelijk om ook voor die applicatie ondersteuning te bieden.

Telkens wanneer Okta een nieuwe applicatie aan zijn netwerk toevoegt, hebben al onze klanten onmiddellijk toegang tot die applicatie. Daarom kan Okta zijn engineeringresources inzetten om alle authenticatiestandaarden te ondersteunen.



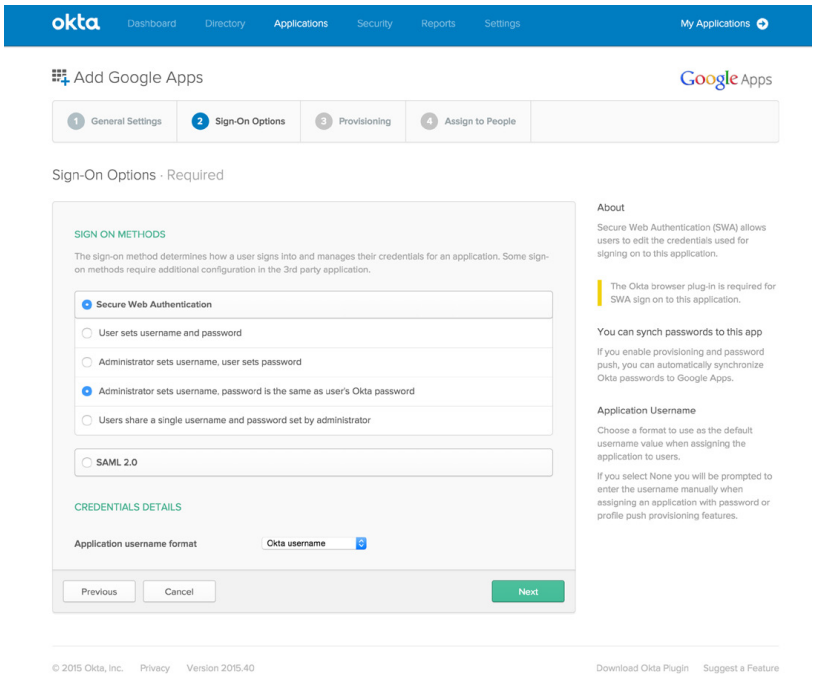
Google-apps configureren voor SAML 2.0 SSO

Secure Web Authentication (SWA) voor SSO

Voor webapplicaties die geen federatieve single sign-on ondersteunen, heeft Okta de SWA-technologie (Secure Web Authentication) ontwikkeld.

Wanneer SWA wordt ingeschakeld voor een applicatie, krijgen eindgebruikers een extra link onder het applicatiepictogram op de Okta-startpagina te zien. Via die link kunnen ze alleen voor die applicatie hun inloggegevens instellen en bijwerken in de beveiligde store. De inloggegevens worden versleuteld opgeslagen met krachtige AES-versleuteling in combinatie met een klantspecifieke privésleutel. Wanneer een gebruiker vervolgens op het applicatiepictogram klikt, stuurt Okta de gebruikersnaam en het wachtwoord via SSL veilig naar de loginpagina van de applicatie en wordt de gebruiker automatisch ingelogd.

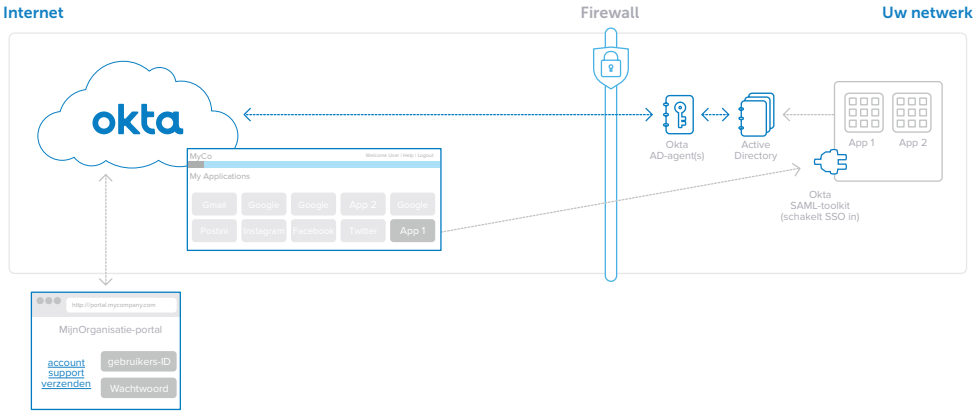
Desgewenst kan SWA voor eindgebruikers nog makkelijker worden gemaakt. Beheerders kunnen dan aangeven dat de gebruikersnaam en het wachtwoord die voor op SWA gebaseerde apps worden gebruikt, hetzelfde moeten zijn als de Okta-inloggegevens van eindgebruikers, wat betekent dat eindgebruikers één stap minder hoeven te zetten (ze hoeven niet meer het initiële wachtwoord in te voeren).



Google-apps configureren voor op SWA gebaseerde SSO

SAML-toolkits voor SSO

Ook voor aangepaste webapplicaties buiten het Okta Application Network biedt Okta integratietoolkits zodat deze applicaties SAML kunnen ondersteunen. De SAML-integratietoolkits zijn beschikbaar voor de .NET-, Java- en PHP-platforms.



Gebruik van de SAML-toolkit van Okta om SSO in te schakelen voor on-prem webapplicaties

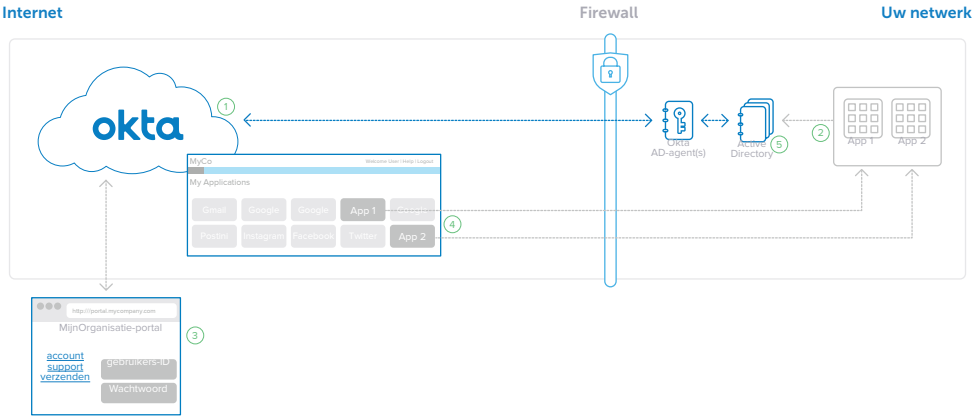
Single sign-on voor met Active Directory geauthen-ticeerde webapps

De meeste organisaties hebben on-prem webapplicaties die makkelijk te integreren zijn met de SSO-oplossing van Okta. Er zijn ook veel organisaties met on-prem webapplicaties die Active Directory-inloggegevens voor authenticatie gebruiken. Voor deze applicaties wordt geen Geïntegreerde Windows-verificatie gebruikt, maar moeten gebruikers hun AD-inloggegevens invoeren wanneer ze zich aanmelden via een browser. Wanneer Okta wordt ingesteld om authenticatie te delegeren naar Active Directory, kan ook aanmelding bij deze interne webapplicaties worden geautomatiseerd.

Dit zijn de stappen achter de schermen waarmee SSO wordt ingeschakeld voor met AD geauthenticeerde interne webapplicaties (hieronder weergegeven):

1. Okta wordt ingesteld op het delegeren van authenticatie naar AD.
2. Klant heeft on-prem apps die worden geauthenticeerd met AD.
3. Gebruiker logt in bij Okta met AD-inloggegevens.
4. Gebruiker opent App 1 en App 2 met SWA met behulp van AD-inloggegevens.
5. App 1 en App 2 authenticeren gebruiker aan de hand van AD.

Okta kan met zijn SWA-protocol gebruikers automatisch inloggen bij deze interne webapplicaties. Wanneer een interne webapplicatie is ingesteld op het delegeren van authenticatie naar AD (dezelfde bron waarnaar ook Okta authenticatie delegeert), legt Okta het AD-wachtwoord van de gebruiker bij het inloggen vast en stelt automatisch dat wachtwoord voor die gebruiker in voor elke applicatie die ook naar AD delegeert. Daardoor hoeven gebruikers alleen maar te klikken op een link voor toegang tot deze applicaties, waarna ze automatisch worden ingelogd. Okta synchroniseert het AD-wachtwoord op een veilige manier: als het wachtwoord naderhand in AD wordt gewijzigd, wordt dat vastgelegd tijdens het inloggen bij Okta en onmiddellijk bijgewerkt in de beveiligde store voor wachtwoorden voor die applicatie. Daardoor zullen alle volgende loginpogingen lukken.



Okta gebruikt SSO voor interne webapplicaties met AD-authenticatie

User management inschakelen

User management wordt gedefinieerd als provisioning van nieuwe accounts voor nieuwe gebruikers, deprovisioning van accounts voor gedeactiveerde gebruikers en waar nodig synchronisatie handhaven van gebruikersattributen tussen meerdere directory's. Met functies van Okta's user management worden gebruikersaccounts automatisch binnen applicaties beheerd, waardoor u tijd en geld bespaart en de juiste toegangsrechten altijd up-to-date zijn. Omdat user management in twee richtingen werkt, kunnen er accounts binnen de applicatie worden gemaakt en worden geïmporteerd in Okta of kan er accountinformatie worden toegevoegd aan Okta en vervolgens naar de bijbehorende applicaties worden gepusht.

Er zijn drie kerngebieden van functionaliteit voor user management die Okta te bieden heeft:

1. Bulksgewijs importeren van gebruikers (uit een scala aan bronnen)
2. Mogelijkheid om binnen Okta gebruikers aan te maken, te lezen, bij te werken en te verwijderen
3. Wachtwoordsynchronisatie / wachtwoorden pushen (tussen verschillende directory's)

Voor integraties met user management ondersteunt Okta op OAuth 2.0 gebaseerde authenticatie. Als een applicatie minder bekende standaarden zoals SCIM of SPML ondersteunt, kan Okta ook die voor user management gebruiken. Net zoals bij toegang via SSO verzorgt Okta de verbinding met deze API's – u hoeft daarvoor zelf niets te doen. U schakelt user management in door Okta te configureren met inloggegevens voor uw API-gebruiker en de gewenste functies te selecteren. Al het andere wordt afgehandeld door de Okta-service, zoals doorlopend automatisch testen en (zo nodig) het uitvoeren van updates naarmate de functionaliteit van de applicatie zich blijft doorontwikkelen.

On-prem applicaties kunnen ook in Okta worden geïntegreerd om user management mogelijk te maken. Dat kan op twee manieren: met behulp van Active Directory of door met webservices gebruikersaccounts in applicaties te beheren

- Voor organisaties die gebruikers onboarden via een HRMS zoals Workday, kan Okta user management ondersteunen voor on-prem applicaties door Active Directory als centraal punt te gebruiken. U kunt Okta configureren voor het beheren van accounts in Active Directory. Okta maakt gebruikers aan en werkt deze bij in AD op basis van gebruikersaccounts in Workday. Deze informatie kan vervolgens worden gebruikt door elke on-prem webapplicatie die Active Directory gebruikt als user store.

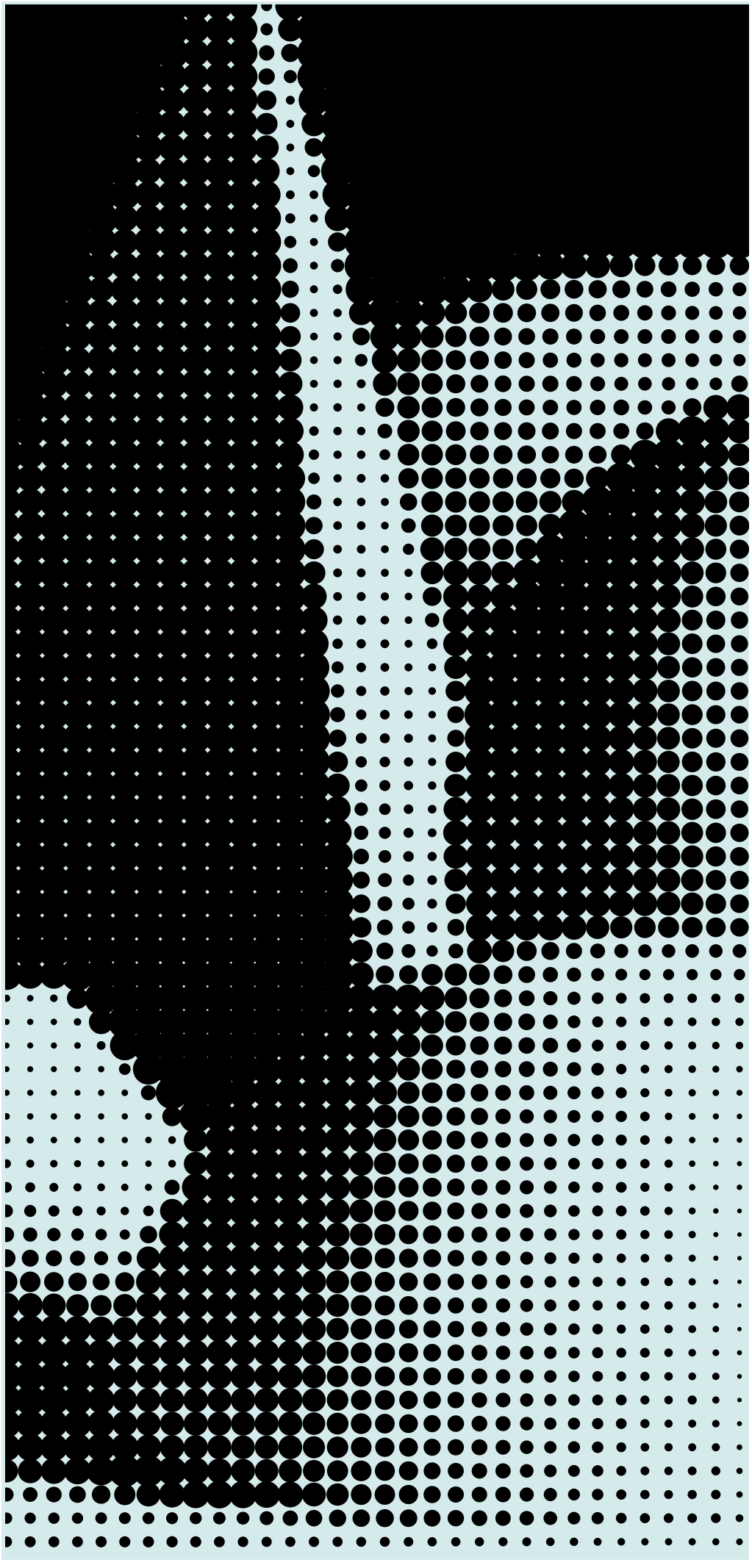
- Okta kan user management ook ondersteunen voor elke on-prem webapplicatie met een webservices-API die via een openbaar toegankelijke verbinding beschikbaar wordt gemaakt voor de Okta-service. Okta roept de webservice van die applicatie aan om waar nodig nieuwe gebruikersaccounts aan te maken, attributen bij te werken en gebruikers te deactiveren op basis van de regels voor toewijzing van gebruikers zoals geconfigureerd in de Okta-service. Okta kan bovendien gedetailleerde voorbeelden van webservice-API's geven.

Conclusie

Single sign-on en user management zijn belangrijke vereisten voor elke organisatie die gebruik gaat maken van mobiele en cloudapplicaties naast bestaande webgebaseerde on-prem applicaties. Zoals de naam al aangeeft, werkt single sign-on (SSO) alleen wanneer de functie op alle applicaties betrekking heeft. Daarom moet een geloofwaardige SSO-oplossing tal van methoden ondersteunen voor het integreren van alle mobiele en webapplicaties die u voor uw organisatie nodig hebt. Okta schakelt SSO specifiek in voor elke mobiele of webapplicatie die werkt met open standaarden, zelf ontwikkelde API's of Secure Web Authentication (SWA) en schakelt SAML in voor on-prem webapplicaties. Bovendien is user management standaard ingebouwd voor alle cloudapplicaties die deze functionaliteit ondersteunen en kunnen on-prem apps makkelijk worden geïmplementeerd via AD-integratie of door provisioning en deprovisioning rechtstreeks toe te passen op ondersteunde API's.

Over Okta

Okta is een toonaangevende, onafhankelijke identity provider voor organisaties. De Okta Identity Cloud stelt organisaties in staat om de juiste mensen op het juiste moment veilig te verbinden met de juiste technologieën. Met meer dan 6500 integraties met applicaties kunnen klanten van Okta gemakkelijk en veilig de beste technologieën gebruiken voor hun organisatie. Meer informatie kunt u vinden op **okta.com**.



okta