“Our secret SaaS to connect your workforce identities”

LinkedIn Live Webinar of January 17, 2023

An initiative of the IBM Security BeLux User Group, presented by:

Yves Debeer

Peter Volckaert

Watch the reply on below link:

https://www.linkedin.com/video/event/urn:li:ugcPost:7008798028178300928/

IBM Security

Agenda

Quick overview of Verify SaaS

Live product demos:

1. onboarding a new employee
2. granting access to an app
3. enforcing access with multi-factor authentication
4. integrating an app with Verify SaaS

Verify SaaS securely connects any identity to any resource

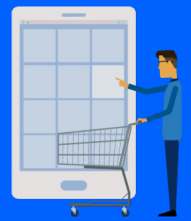
IBM Security
Verify SaaS

Workforce Identity

Drive cloud modernization, technical agility and user productivity

Continuous Access Control

- Single Sign-On and MFA
- Adaptive access
- Passwordless authentication
- Lifecycle management
- Identity analytics
- Privacy and consent management



Consumer Identity

Deliver on-demand, personalized, and trusted experiences

Hybrid Cloud Resources

Cloud Apps | On-Prem Apps | Mobile Apps | Data

VPNs | Servers | Databases | Mainframes

onboarding a new employee

Employee

IBM **Security** Verify

User Portal

Identity Agent config “winserver”

Identity Provider “winserver”

JITP

Cloud Directory

HTTPS tunnel

API (SCIM)

Internet

On-prem

Windows Server

Active Directory

Change detection

ldaps

Verify Bridge - authentication

Verify Bridge for Dir Sync - sync AD to Verify

Administrator

onboarding a new employee

So what?

What did we assume?

Your company decided to start using Verify for securely connecting their employees to their services and applications. Therefore they need to define their employees in Verify. Your company has defined most of its employee data in their corporate on-prem Active Directory, and wants to leverage that to kick off their Verify deployment.

What did we just show - *live*?

User accounts that are managed in AD are sync'ed in real-time with Verify's user registry a.k.a. Cloud Directory. Sync works for all actions on the AD account: create, modify, disable/delete. E.g modifying a user's mobile phone number is automatically pushed to the Cloud Directory.

Employees are able to sign in with their AD credentials.

Why should you care?

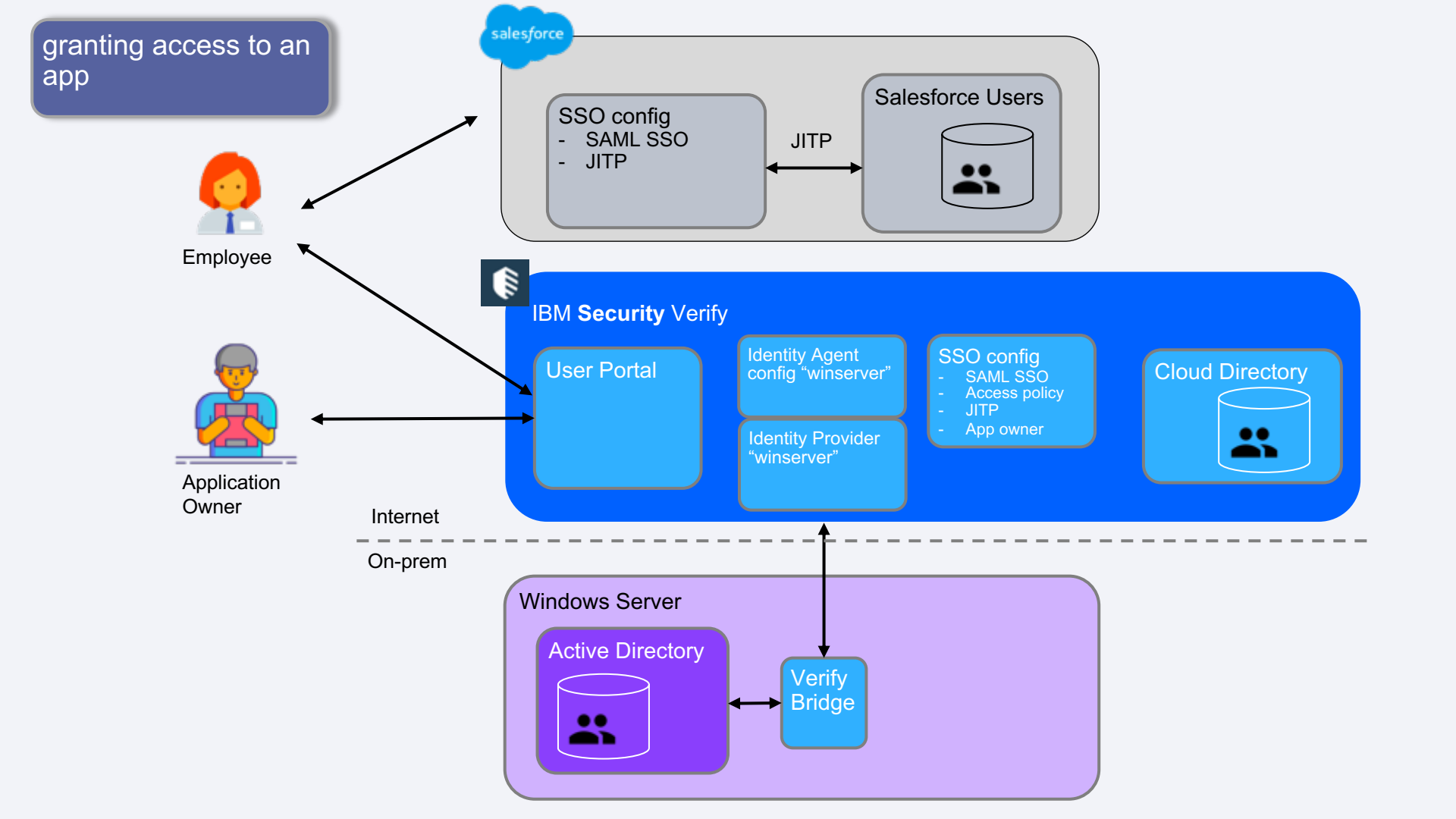
Verify's Cloud Directory can be populated using a component that comes for free with the solution: the Bridge for Directory Sync. No need to develop scripts to get the import and sync right, just configure the Bridge and done. Note that it's also possible to populate the employee in the Cloud Directory at his/her first sign-in to Verify. This can be achieved thanks to the Just-In-Time Provisioning, JITP, feature of the Bridge component.

Employees can directly start using the services of Verify (like e.g. requesting access to apps, multi-factor authentication, single sign-on, etc) and thereby simply use their known, beloved Windows password.

Error-prone, manual processes to sync employee data such as mobile phone, department, etc are replaced by an automatic and real-time process provided by the Verify solution.

You can simply keep using you Active Directory store for other integrations like e.g. a company white pages application, authentication, workstation sign-on etc. It's all transparent to the Active Directory: no schema changes, no major configuration changes, …

granting access to an app



granting access to an app

So what?

What did we assume?

Today, your employees must sign in to SalesForce using a userid & password specific to SalesForce. That's inconvenient for both the employee and the IT department; it's yet one other password to manage. Your company wants to simplify the employee's live and improve on IT security by providing single sign-on to SalesForce.

What did we just show - *live*?

The employee signs in (using his/her AD password) to Verify and requests access to SalesForce. He/she can see who needs to approve. This approver is notified of the request via email, signs in to Verify and approves the request. The employee is informed of this approval, signs in to Verify and launches the SalesForce app and is transparently signed in to SalesForce.

The SalesForce user account is automatically created, and subsequent sign-in's to SalesForce update the Salesforce user account. We've shown that changing the mobile number in AD, followed by a sign-in in to SalesForce, which is through Verify, updates the SalesForce mobile number automatically.

Why should you care?

The integration of apps like SalesForce with our connectors provides single sign-on. This (1) dramatically reduces password hassles: employees do not have to use (and remember…) yet another password (2) improves your security posture; it will allow you to centralize your access policies – like f.i. enforcing MFA, offering passwordless authentication, offering additional identity providers, etc.

It's likely that your process of requesting access to applications is far more complex than what's available out-of-the-box from Verify. It's an opportunity to replace these often manual, email-based processes by what's offered out-of-the-box with Verify.

Some applications (like e.g. SalesForce) offer Just-In-Time Provisioning (JITP) and Verify's connectors can be configured to use such JITP. At a first sign-in to the application the app's account will be automatically created, and subsequent sign-in's will update the app's account with the attributes that are provided in the single sign-on token. No more time-consuming, manual, error-prone processes to create accounts on apps that provides JITP.

enforcing access with MFA

Verify app

Employee

Administrator

salesforce

SSO config
- SAML SSO
- JITP

JITP

Salesforce Users

IBM **Security** Verify

User Portal

Admin Portal

Identity Agent config “winserver”

Identity Provider “winserver”

SSO config
- SAML SSO
- Access policy
- JITP
- App owner

Access policy config

Cloud Directory

Internet

On-prem

Windows Server

Active Directory

Verify Bridge

enforcing access with MFA

So what?

What did we assume?
Your company now wants to further use the power of Verify's centralized IAM service and decides to introduce multi-factor authentication.

What did we just show - *live*?
The Verify administrator set up an access policy for business-critical apps such as SalesForce. This policy enforces multi-factor authentication. This policy was then enforced on the Salesforce app.
The employee signs in to Verify and self-registers for the Verify mobile authenticator app.
The employee accesses Salesforce, receives a push notification on his/her smartphone, presents his/her face to authenticate, and is then signed in to Salesforce.

Why should you care?
Introducing MFA for your employees is extremely easy with Verify. Verify provides a complete set of authentication methods so that your employees and your security department can choose how to use/enforce MFA. Verify includes sending one-time password codes to your employee's mobile phone and email: no need to bother with SMS gateways or outgoing email servers: it's offered by the Verify service. The modern, smooth mobile authenticator is also included at no extra charge and you can also use the authenticator's SDK to embed in your own apps.
You're able to enforce MFA at one central point, namely Verify. Image the administrative nightmare and employee frustration when you start using multiple MFA service. Many services (like e.g. Salesforce) offer their own mobile authenticator app. You don't want your users to register and use dozens of authenticator apps…
An access policy in Verify goes beyond simple MFA: it allows for context-based access where you can define access based on date&time, IP addresses, device compliance, device location, employee attributes (e.g. manager y/n, department), and so on. One step further is to subscribe to 'Adaptive Access' which offers a sophisticated, AI-powered risk score provided by our IBM Trusteer cloud.

Demo: integrating an app with Verify SaaS

Developer

IBM **Security** Verify

Verify Developer Portal

Employee

Buy@Acme

Product-Catalog-API

Web-App

http://<auth-nodejs>:3000/login

http://<Frontend-vuejs>:8080/loginwithtoken?name=...

Get access-token & id-token

Set tokens

IBM **Security** Verify

integrating an app with Verify SaaS

So what?

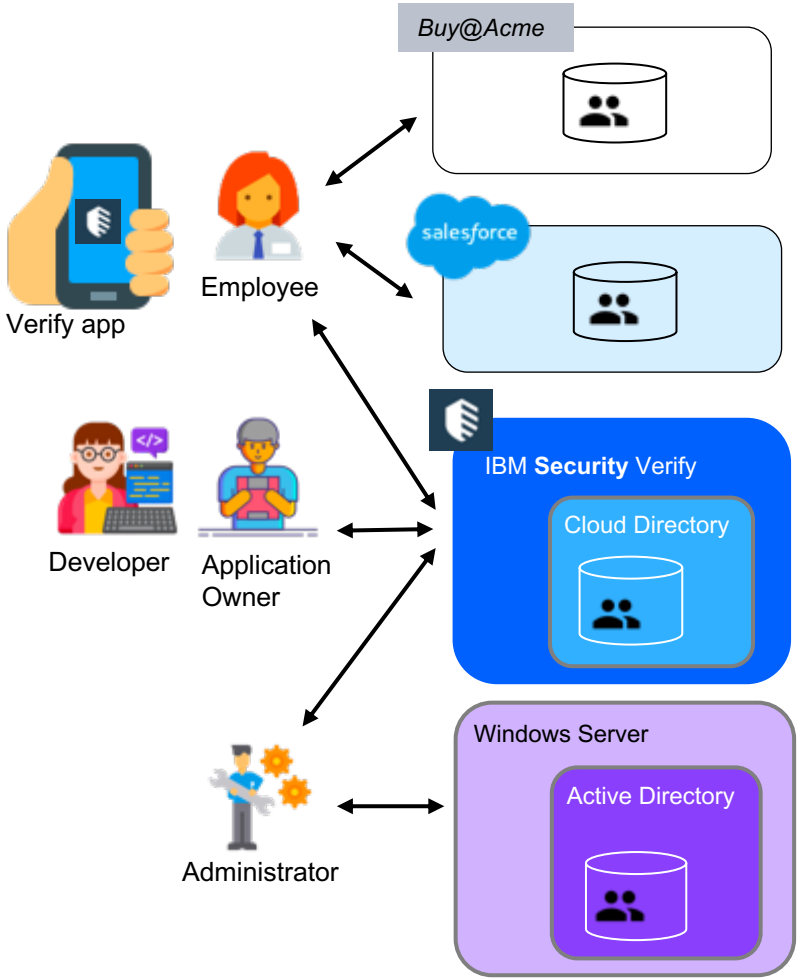
What did we assume?
Your company has decided to build a web application where employees can order hardware and software needed for their job. The development must be done in-house. The app must of course identify the employee who is ordering, and therefore Verify will be used.

What did we just show - *live*?
The developer navigated to Verify's built-in Developer Portal and registered a new app name "Buy@Acme". The OpenID Connect (OIDC) credentials were copied and used in the Buy@Acme app to configure the OIDC interaction with Verify.
After the developer finished the Buy@Acme app, the Verify administrator further configured the app and set the allowed identity sources, the entitled users and the attributes to include in the OIDC id_token.
An employee navigated to Buy@Acme, pushed the login button, was prompted for authentication at Verify and was eventually signed in to Buy@Acme. We showed that Buy@Acme received the employee's attributes through the OIDC id_token and can now further process orders.

Why should you care?
Integrating in-house apps becomes an easy task with Verify. Your developers can use standard integration techniques such a OpenID Connect (OIDC) to incorporate identity in their apps. The approach of using Verify as a central 'identity provider' offloads the developer of deciding/implementing access policies. Instead, it's your security team that will decide who and how an application can be accessed.

What did we just show - *live*?

1. onboarding a new employee
2. granting access to an app
3. enforcing access with multi-factor authentication
4. integrating an app with Verify SaaS



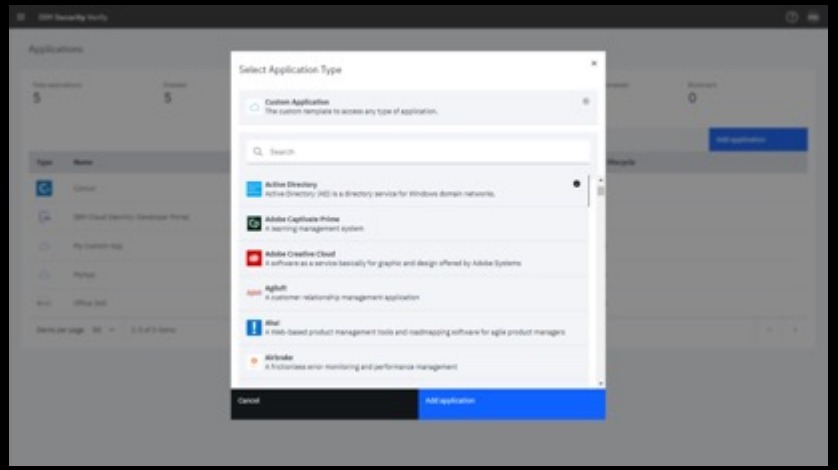
Sign up now

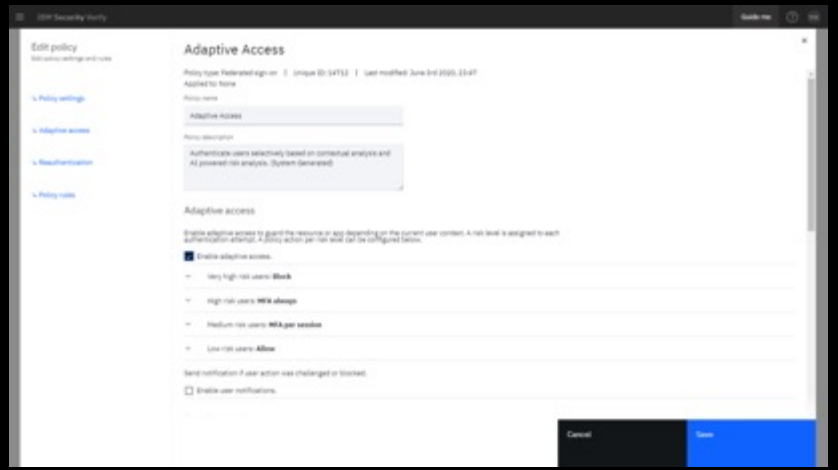
Try free edition for yourself

Explore a trial of IBM Security Verify and get started in under 10 minutes:

- Add apps to single sign-on
- Connect to a directory or add new users
- Try out MFA and adaptive access

Get started here





Verify SaaS Resources

Verify SaaS landing page
https://ibm.biz/CI-Home

Sign up for a Verify SaaS trial
https://ibm.biz/CI-Trial

Verify SaaS product documentation
https://ibm.biz/CI-KnowledgeCenter

Verify SaaS documentation hub
https://ibm.biz/CI-DocHub

Verify SaaS education on securitylearningacademy.com
https://ibm.biz/CI-Learning

Verify SaaS terms; offerings, charges, support, data handling, service level, support, etc
https://ibm.biz/CI-Terms

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity