



SAP SuccessFactors 

Create a Better User Experience and Improve Security with State-of-the-Art Authentication

Sandeep Gilotra
Sr. Director, Product Management

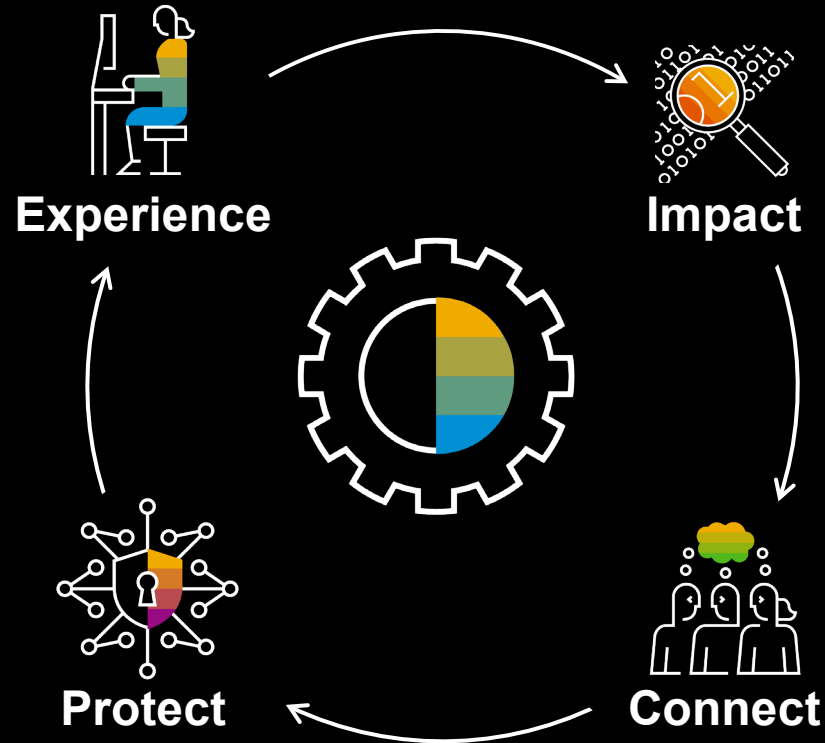
PUBLIC

SAP SuccessFactors platform

The most powerful technology and tools in the HR market

- User experience (UX)
- SAP Fiori UX adoption

- Role-based permissions
- Identity management
- Data protection and privacy



- Reporting
- Analytics
- Planning
- Admin self-service
- Instance management

- Extensions
- Integration
- API

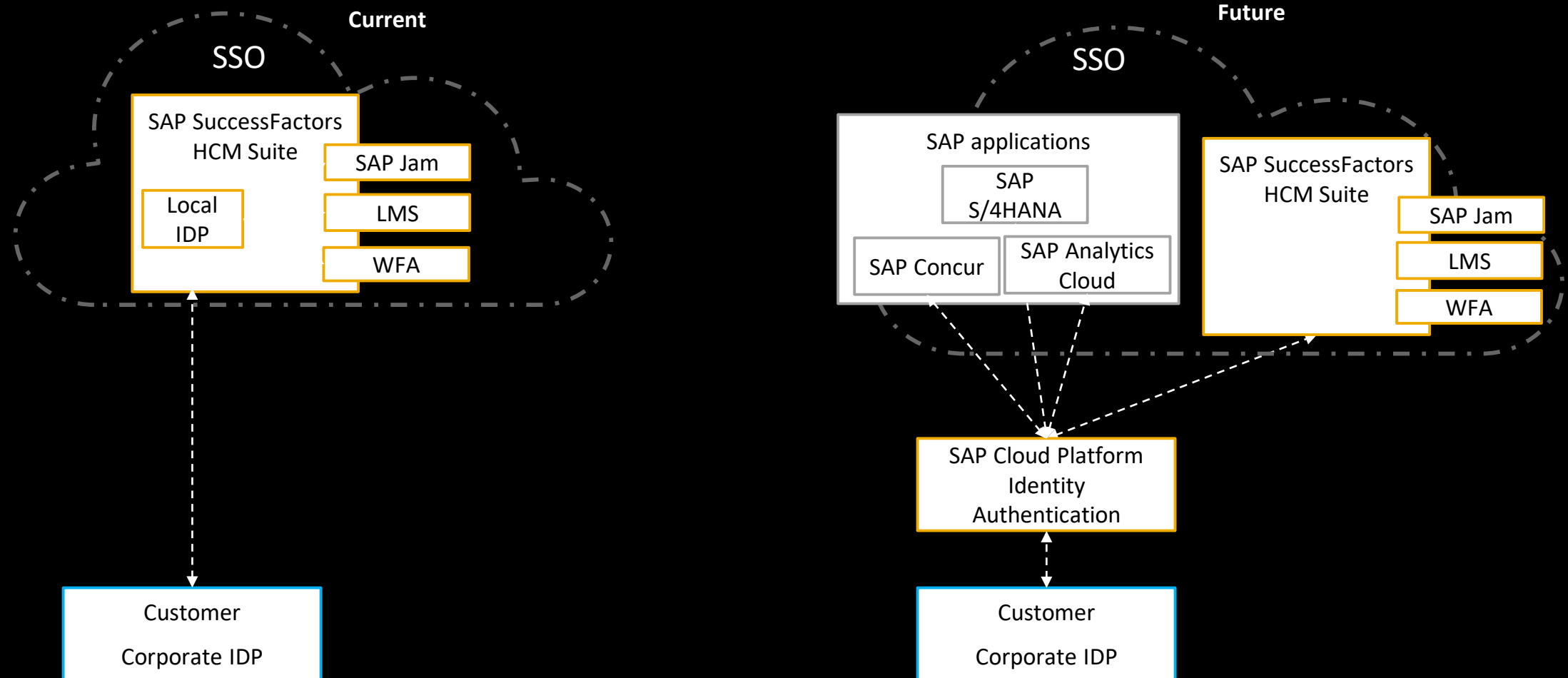
What is SAP's innovative approach to identity and access management?

- SAP Cloud Platform Identity Authentication service provides simple and secure cloud-based user access to business processes, applications, and data.
- Provides the capability to create and manage user accounts, roles, and access rights for individuals in the organization
- Simplifies the user experience through:
 - Automated user provisioning
 - State-of-the-art authentication mechanisms
 - Secure single sign-on, on-premise integration
 - Convenient self-service options

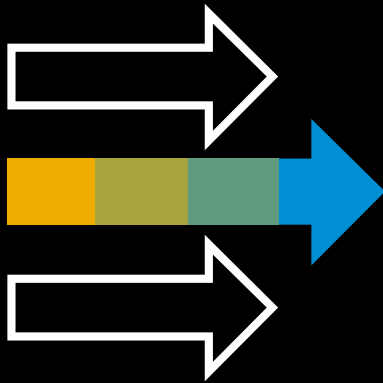
Why move to the SAP Cloud Platform Identity Authentication service?

1. Single identity service, to be used by all cloud solutions from SAP
2. Improves user experience by stopping the sprawl of different user names and passwords that came about through the incredible rise in SaaS cloud-based applications
3. More log-in options: Apart from the user name–password based log-in, it also supports 2-factor/token, social sign on, SPNEGO, and corporate user stores.
4. Central user management or reuse of existing identity infrastructure
5. Scalability and rapid provisioning for cloud-first applications
6. SAP Cloud Platform Identity Authentication as an identity provider: The service can be both used as a proxy IdP or a stand-alone IdP depending on customer's requirements.

Current SAP SuccessFactors authentication process vs. SAP Cloud Platform Identity Authentication



Availability



Available NOW (1908) for existing customers to upgrade to SAP Cloud Platform Identity Authentication



NEW customers to be set up automatically on SAP Cloud Platform Identity Authentication starting Sept. 30, 2019

How to set up SAP Cloud Platform Identity Authentication for your SAP SuccessFactors instance

Step 1: SAP SuccessFactors provisioning

- Set up SAML 2.0-based SSO in your SAP SuccessFactors instance
- This step enables customers to add identity provider-based SSO setting as well as service provider-based SSO settings.

Step 2: SAP Cloud Platform Identity Provisioning service

- Set up the source and target systems in SAP Cloud Platform Identity Provisioning for user sync.
- This would be preconfigured for the customer with necessary transformations.
- The customer can create their own transformations based on their requirements.

Step 3: SAP Cloud Platform Identity Authentication service

- Review default configurations for user management, application properties, tenant settings
- The service also enables the customer to use the existing corporate IdP and social log-in.
- Maintain reports and logs of all user activity

Configurations – SAP SuccessFactors provisioning

Delete the asserting party | Update the asserting party

SAML User Column:

SAML Asserting Party Name: This is an identifier for your SAML issuer and can be modified later.

SAML Issuer:

Company Phone:

Contact Name:

Contact Phone:

Relying Party Description:

Require Mandatory Signature:

Enable SAML Flag: ☒

Login Request Signature(SF Generated/SP/RP):

SAML Profile:

Enforce Certificate Valid Period:

SAML Verifying Certificate Valid Period:

SAML Verifying Certificate Status:

SAML Verifying Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDDDCAFAgAwIBAQIQAQVJSM1xhMA0GCSqGSIb3DQEBAQUAAQkK
EwZTQVAtU0Uxj3AkBgNVBAMTHW55c2UuYWNja3VudHM0MDAub25kZW
MDk1OFOXTDTI2MDEyNjA5MDk1OFOwRjELMAkGA1UEBhMCREUxZzAN
BgNVBAsTB1NBUC1TRTEuMCOGA1UEAxMdbn1zZS5hY2Y2NjU0c2cz
QWMC5vbmRlbWFWZC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDw
AwggEKAgIBAQIgaYw0jxIgcTEIHT0B93U7TDT1Dmb2GREaTgZDvL
sdWmt9GBNkNZJXCp07K0CFd9ir1AJUkKtoqFHz/NVesU1DB09F
rcqvHGPy3yzw1ZHF2/zpXaqXcpUwTJK6brco/CxCGamg17p8eyt
CxpajPe52qS9pnc1WBOUj21r7IqJp14Sw/9y1lG01Pd+6u1qke
VwZbu1PqekpeGNo11LkYaQD9ze261tESqStyh5Ud7g16Zubze2Mb
kXxi9HSBZzpa0w/y+b/C1Lm1fKw6a/1LwGMA/OZotliH1jwRqwb
zuFnsP8XE1c0t9N1q71w1FoEctx0T3kklw8187BAgMBAAGCAgAAMA
0GCSqGSIb3DQEBAQUAA4IBAQAgrt8FtP4nKsu n5nRke6Yl0gvdj
az9EyrwaFGBK0ZVaobPECK1qXYKngij+0mT0/zPLO17CVMZShK/
UutoK64+oTmsKyB8TrvLfyn31170AMZiWogHSFdkKxyymqgD3Wo
zMKHaiu/7O0ck6FD6Kh+AiNmG8yXXq4FLaakdqiIqob0tqYcdT2
GarwG7GV24/YFn4IR/JqPoTQxveOhgJM99iJ4MvCxpNDHrIEArM+
4n1UDhcEV4Trd0+AgUakBRQ9BN9y7bWDE5EDz1383n3oD7Q/4oa
ulvugDXn3CEFFxwYmWCqctWcoDID47g0P55i6cP0q6PoMIR7U
e1FqoQty
-----END CERTIFICATE-----
```

SAML v2 : SP-initiated login

Enable so initiated login (AuthnRequest): ☒

Default issuer: ☒

single sign on redirect service location (to be provided by idp):

Send request as Company-Wide issuer: ☒

SAML v2: SAP IAS integration

Select this checkbox if customer is using IAS as proxy IDP ☒

Common SSO Settings

Expiration of SSO Request (in seconds):

If there is no expiration, enter -1.

Maximum number of SSO Errors Logged in DB:

Please enter the token for redirecting to partner site:

Append 'target' parameter to session timeout redirect: ☐

Force Token Validation (authentication will fail if request token does not match): ☐

Use number of milliseconds since the unix epoch as the timestamp: ☐

Partial Organization SSO ☒

This feature allows defining of a per-user basis whether a user will login through SSO or through the standard username/password login page. Per-user control is managed through the standard user field loginMethod

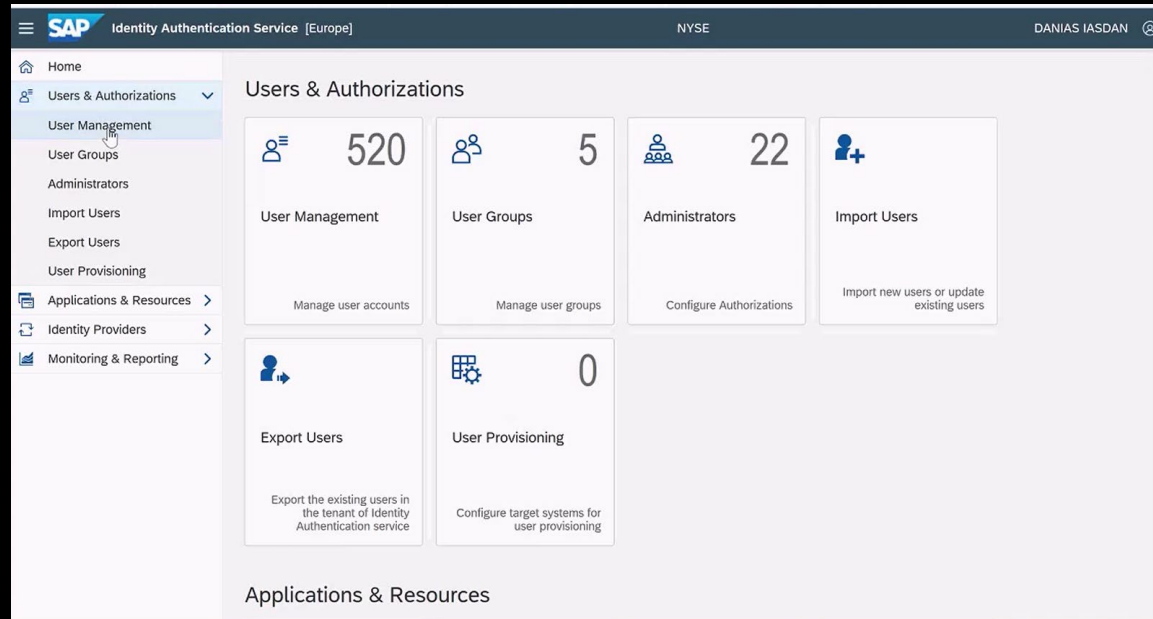
SSO URI Parameter name replacement

username	<input type="text"/>
password	<input type="text"/>
tklogin_key	<input type="text"/>
expire	<input type="text"/>
callerhash	<input type="text"/>

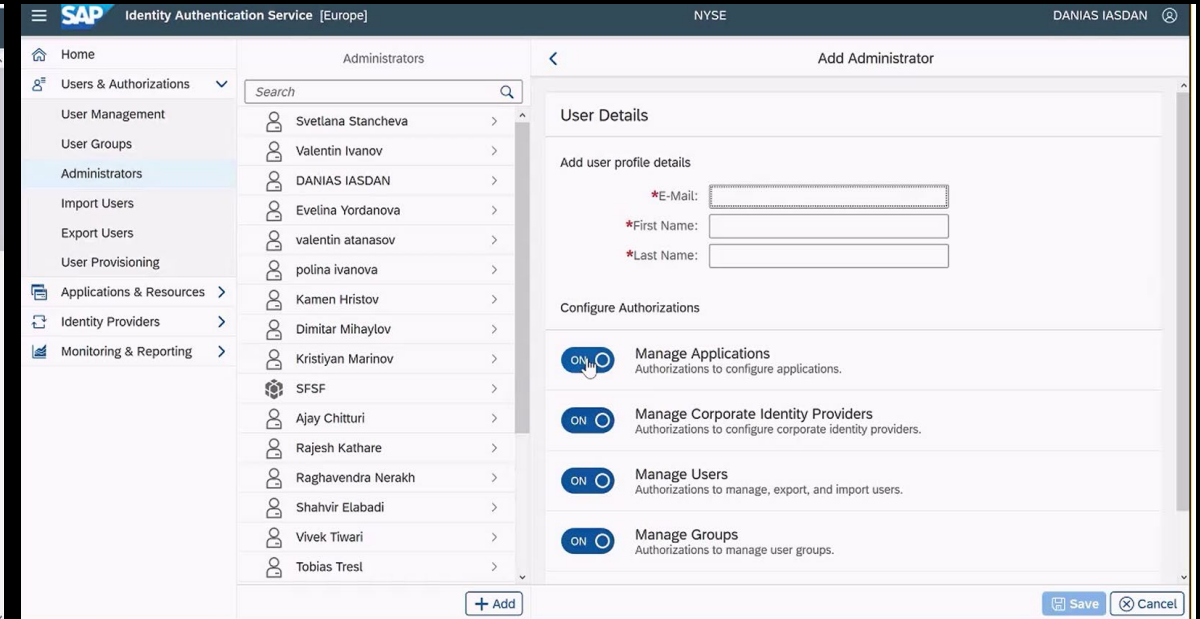
Adding an SAML 2.0-based asserting party:

- SAML flag should be enabled
- Valid certificate

Configurations – SAP Cloud Platform Identity Authentication service

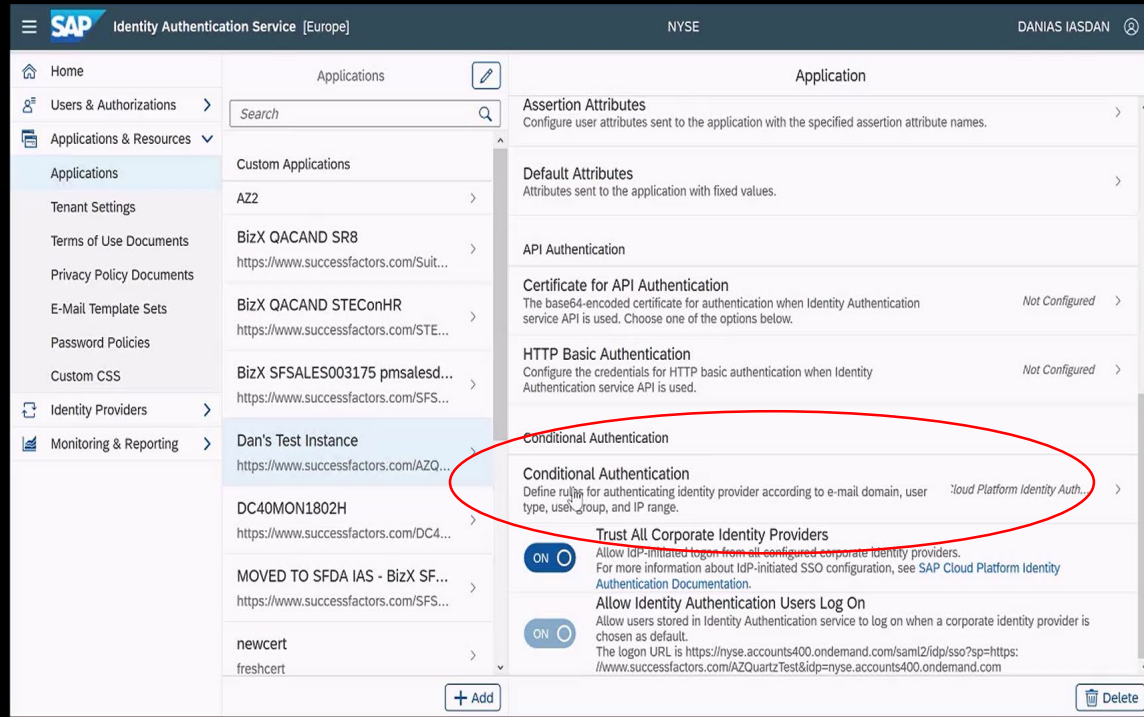


Identity authentication service console

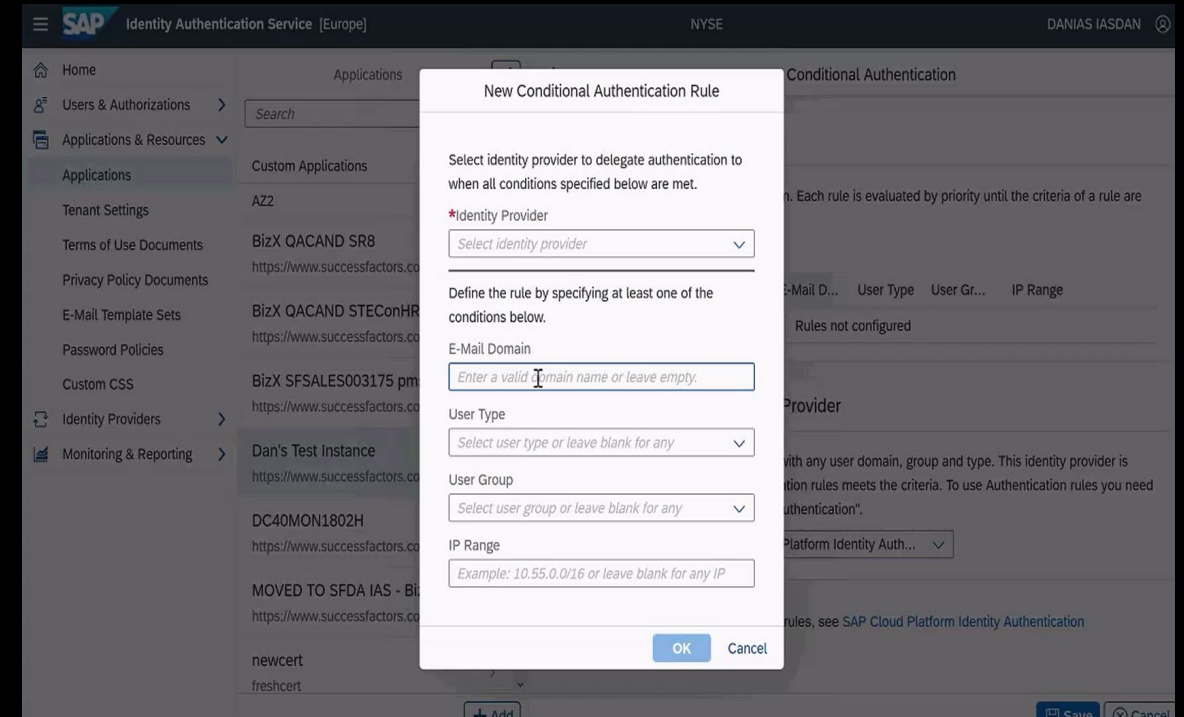


Add administrators and configure authorization

Application access: Conditional authentication

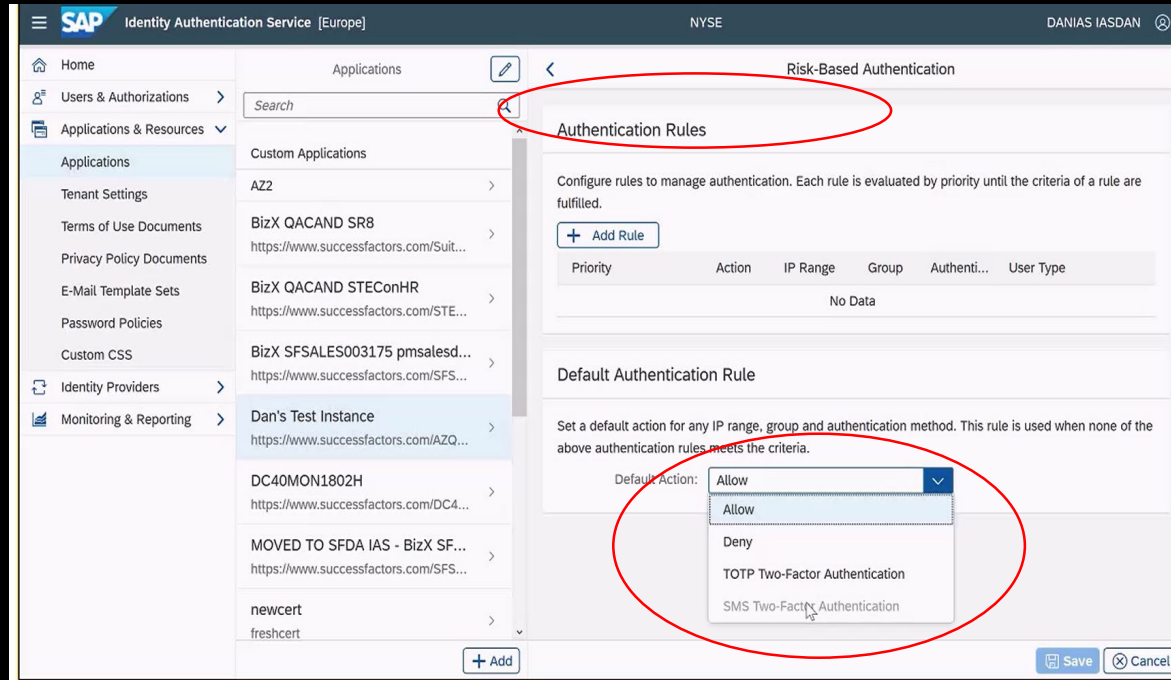


Determine authentication and access methodology

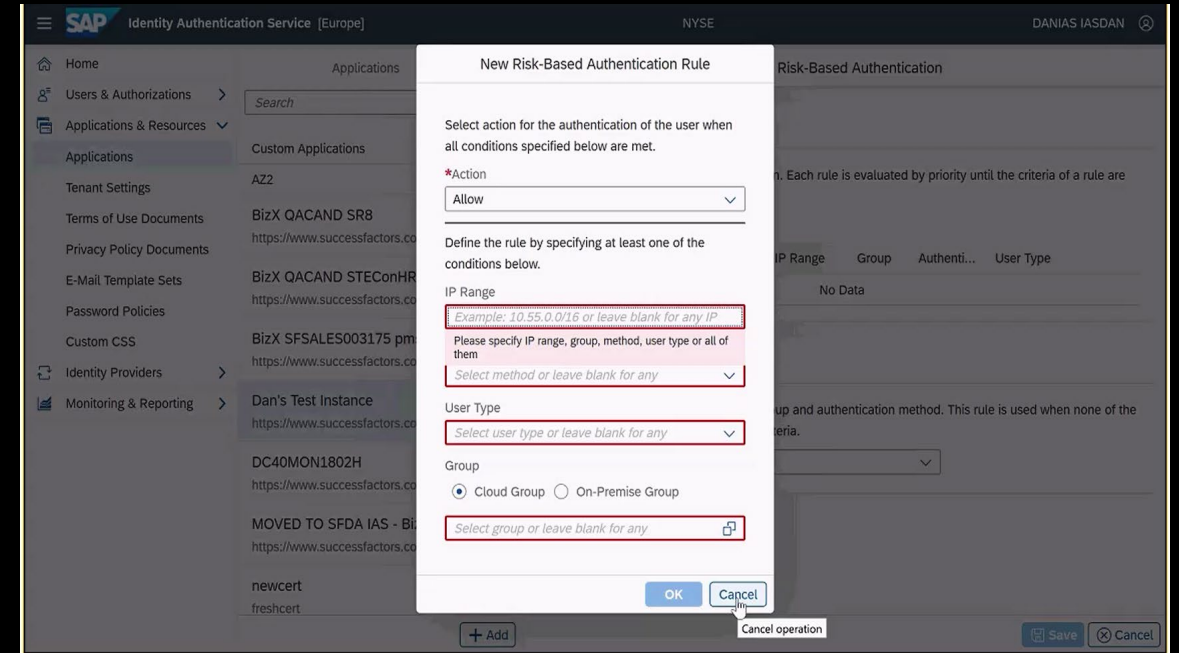


Conditional authentication – Authentication on the basis of e-mail domain, IP range, user type

Application access: Risk-based authentication



Risk-based authentication allowing/denying users based on rules



Enable 2-factor authentication (2FA) for select group of users

Thank you.

Contact information:

Sandeep Gilotra

Sr. Director, Product Management

sandeep.gilotra@sap.com

650-438-0557

Follow us



www.sap.com/contactsap

© 2019 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

See www.sap.com/copyright for additional trademark information and notices.