

The background features a complex, abstract pattern of overlapping, curved lines in various shades of blue, purple, and teal, creating a sense of depth and movement. The lines are most prominent on the right side, where they form a dense, fan-like structure that tapers towards the top right corner.

AWS re:Inforce

JULY 26 – 27, 2022 | BOSTON, MA

IAM336-R1

IAM Identity Center: Every organization can centrally manage access

Chris Mercer

Security Solutions Architect
AWS

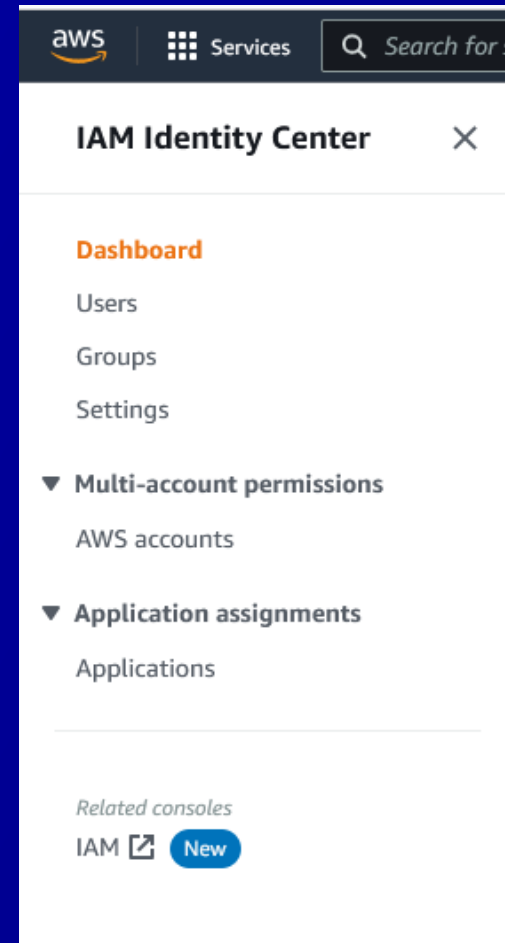
Ron Cully

Principal Product Manager
AWS



AWS SSO is now IAM Identity Center

- **One place to create or connect your workforce identities** and centrally manage secure access across AWS
- **Freedom to choose** your preferred identity source for use across AWS
- **Multi-account permissions** to manage fine-grained access at scale
- **Application assignments** to manage access to IAM Identity Center and other cloud applications



What changes

New service name

New console name

Improved console navigation

What does NOT change

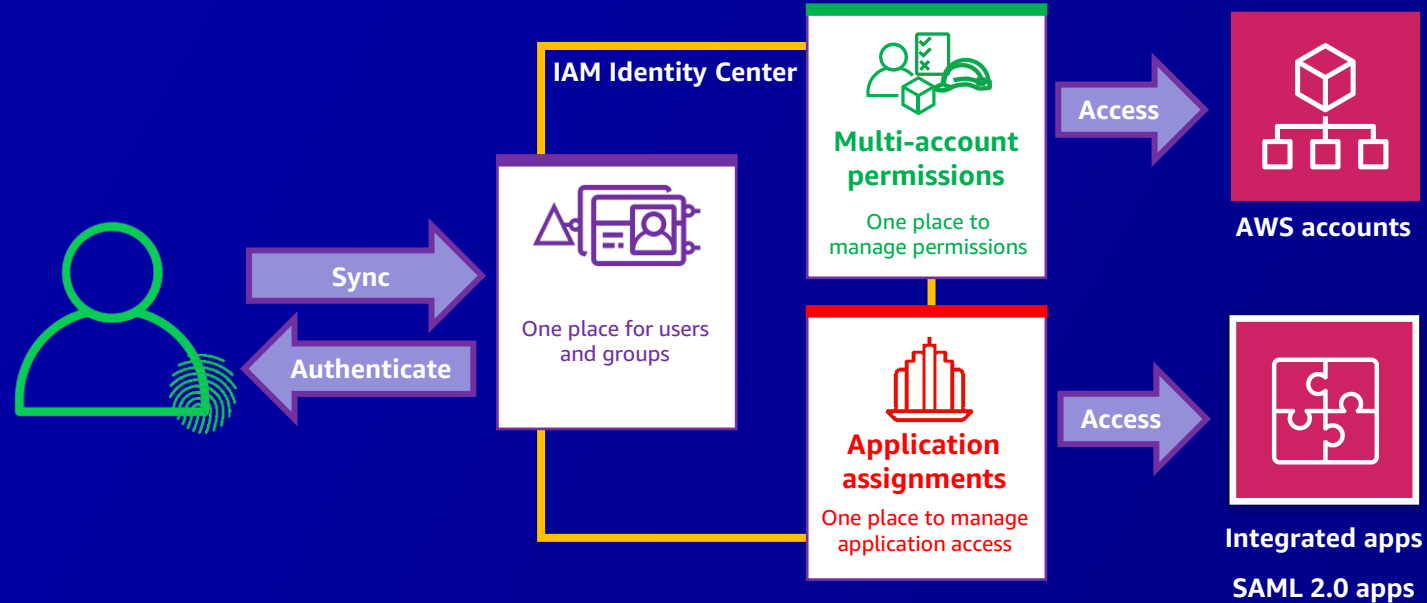
No technical changes

No API changes

IAM Identity Center (successor to AWS SSO)

Choose your identity source

- IAM Identity Center directory
- Microsoft Active Directory Domain Services
- Okta Universal Directory
- Microsoft Azure Active Directory
- Other SAML 2.0 & SCIM 2.0 compatible IdP



← One sign-in for account and application access →

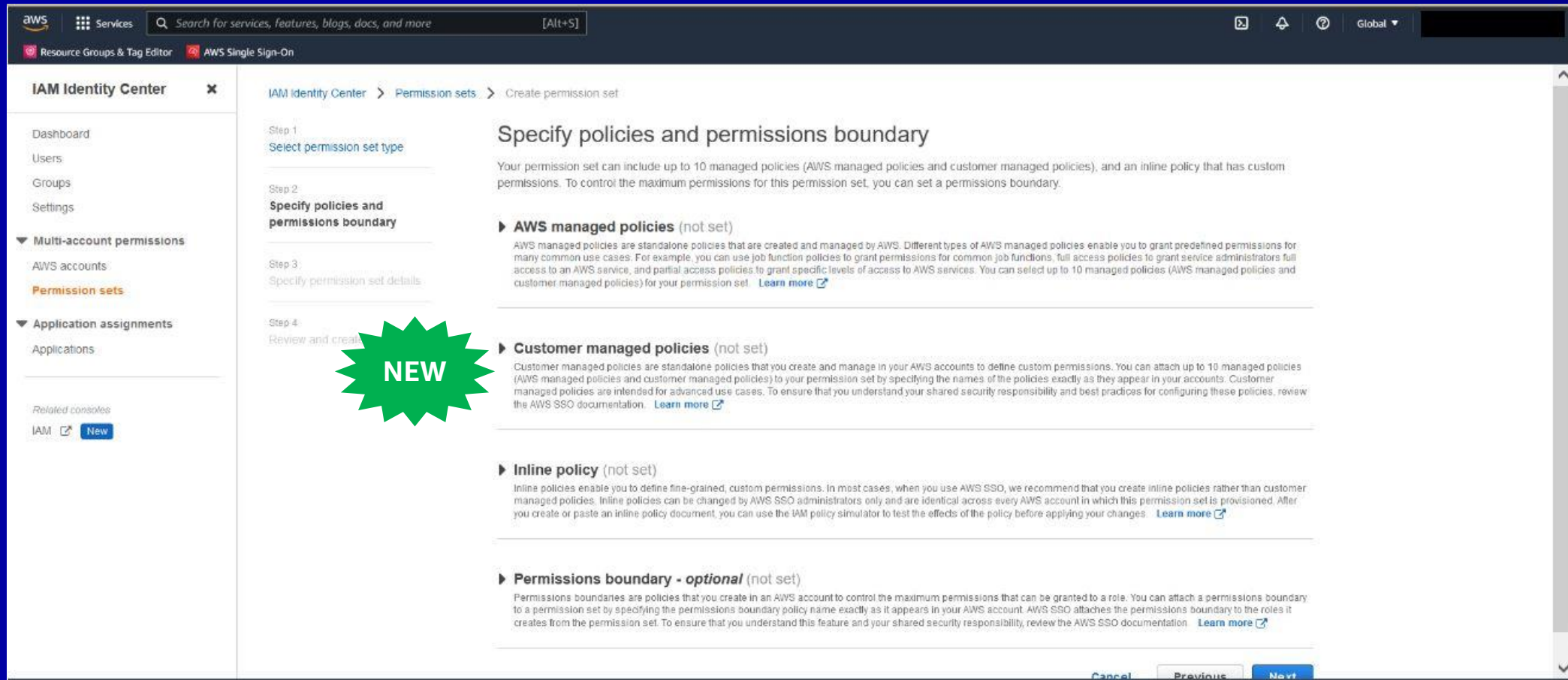
Logos for identity providers: okta, onelogin, PingIdentity, CYBERARK, jumpcloud, Microsoft Active Directory, and Azure Active Directory.

Administering IAM Identity Center from a member account

Administration task	Delegated administrator account	AWS organization management account
Add, edit, or delete users or groups	X	X
Enable or disable user access	X	X
Enable, disable, or manage incoming attributes	X	X
Change or manage identity sources	X	X
Create, edit, or delete applications	X	X
Configure MFA	X	X
Manage permission sets not provisioned in the management account	X	X
Manage permission sets provisioned in the management account		X
Enable IAM Identity Center		X
Delete IAM Identity Center configuration		X
Enable or disable user access in the management account		X
Register or deregister a member account as a delegated administrator		X



Customer managed policy support



The screenshot shows the AWS IAM Identity Center console interface. The breadcrumb navigation indicates the path: IAM Identity Center > Permission sets > Create permission set. The main content area is titled 'Specify policies and permissions boundary' and contains the following sections:

- Step 1:** Select permission set type
- Step 2:** Specify policies and permissions boundary (highlighted with a green starburst labeled 'NEW')
 - AWS managed policies (not set)**

AWS managed policies are standalone policies that are created and managed by AWS. Different types of AWS managed policies enable you to grant predefined permissions for many common use cases. For example, you can use job function policies to grant permissions for common job functions, full access policies to grant service administrators full access to an AWS service, and partial access policies to grant specific levels of access to AWS services. You can select up to 10 managed policies (AWS managed policies and customer managed policies) for your permission set. [Learn more](#)
 - Customer managed policies (not set)**

Customer managed policies are standalone policies that you create and manage in your AWS accounts to define custom permissions. You can attach up to 10 managed policies (AWS managed policies and customer managed policies) to your permission set by specifying the names of the policies exactly as they appear in your accounts. Customer managed policies are intended for advanced use cases. To ensure that you understand your shared security responsibility and best practices for configuring these policies, review the AWS SSO documentation. [Learn more](#)
 - Inline policy (not set)**

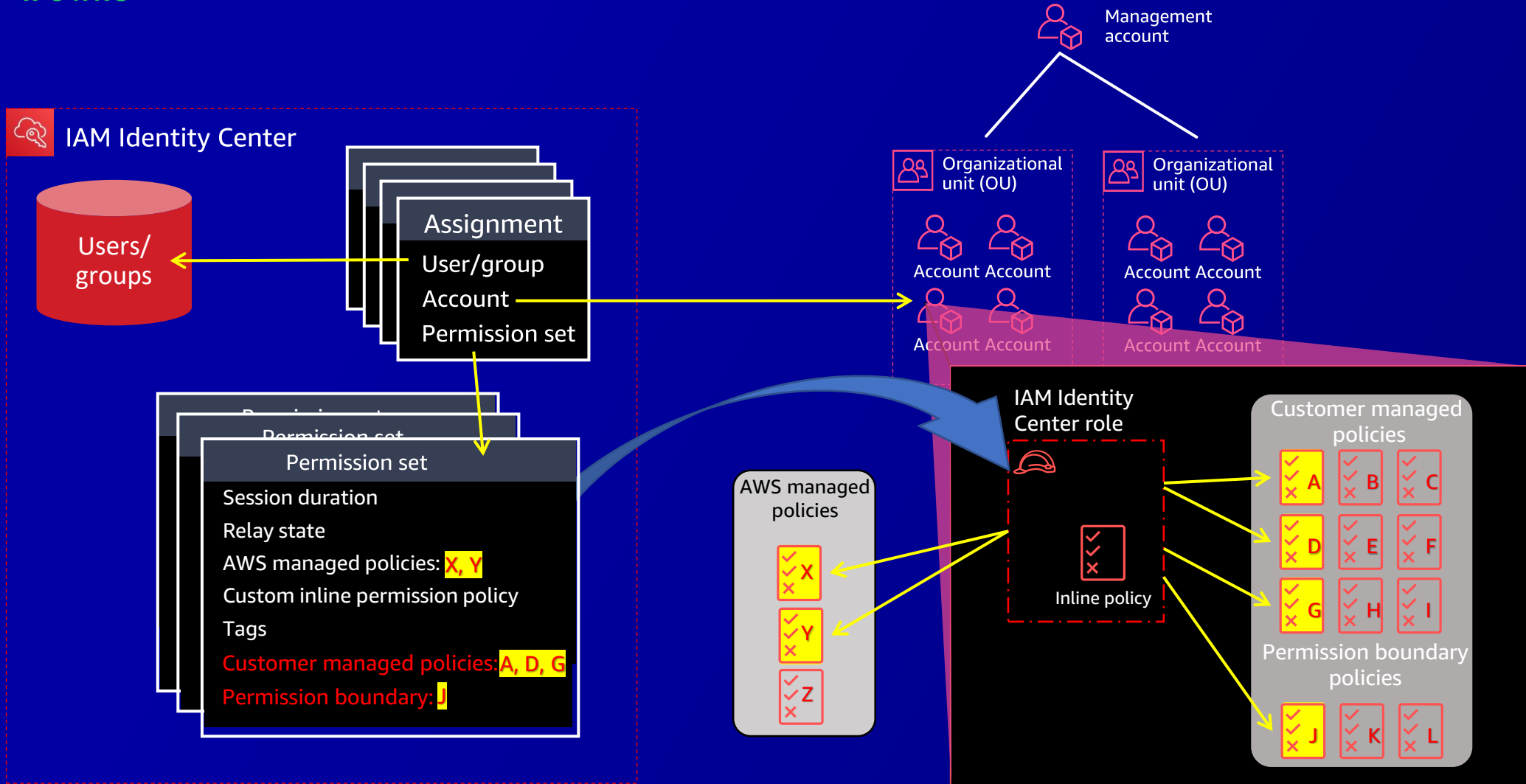
Inline policies enable you to define fine-grained, custom permissions. In most cases, when you use AWS SSO, we recommend that you create inline policies rather than customer managed policies. Inline policies can be changed by AWS SSO administrators only and are identical across every AWS account in which this permission set is provisioned. After you create or paste an inline policy document, you can use the IAM policy simulator to test the effects of the policy before applying your changes. [Learn more](#)
 - Permissions boundary - optional (not set)**

Permissions boundaries are policies that you create in an AWS account to control the maximum permissions that can be granted to a role. You can attach a permissions boundary to a permission set by specifying the permissions boundary policy name exactly as it appears in your AWS account. AWS SSO attaches the permissions boundary to the roles it creates from the permission set. To ensure that you understand this feature and your shared security responsibility, review the AWS SSO documentation. [Learn more](#)
- Step 3:** Specify permission set details
- Step 4:** Review and create

At the bottom of the page, there are buttons for 'Cancel', 'Previous', and 'Next'.

Customer managed policy support

HOW IT WORKS



Let's talk



Thank you!

