



AZURE ACTIVE DIRECTORY AND IDENTITY SECURITY

MICROSOFT IGNITE (FALL 2021)



**Microsoft Ignite Azure Recap 2021
meets Community Meetups**



THOMAS NAUNHEIM

*Cloud Security Architect
@glueckkanja-gab AG*

Koblenz, Germany



@Thomas_Live



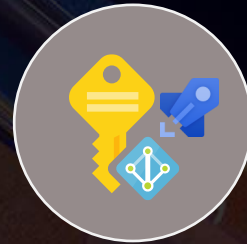
cloud-architekt.net

HIGHLIGHTS OF MICROSOFT IGNITE (FALL 2021)

AZURE IDENTITY + SECURITY



**ZERO TRUST &
CONDITIONAL ACCESS**



**SECURING NON-HUMAN
(WORKLOAD) IDENTITIES**



**IDENTITY SECURITY
AND -GOVERNANCE**



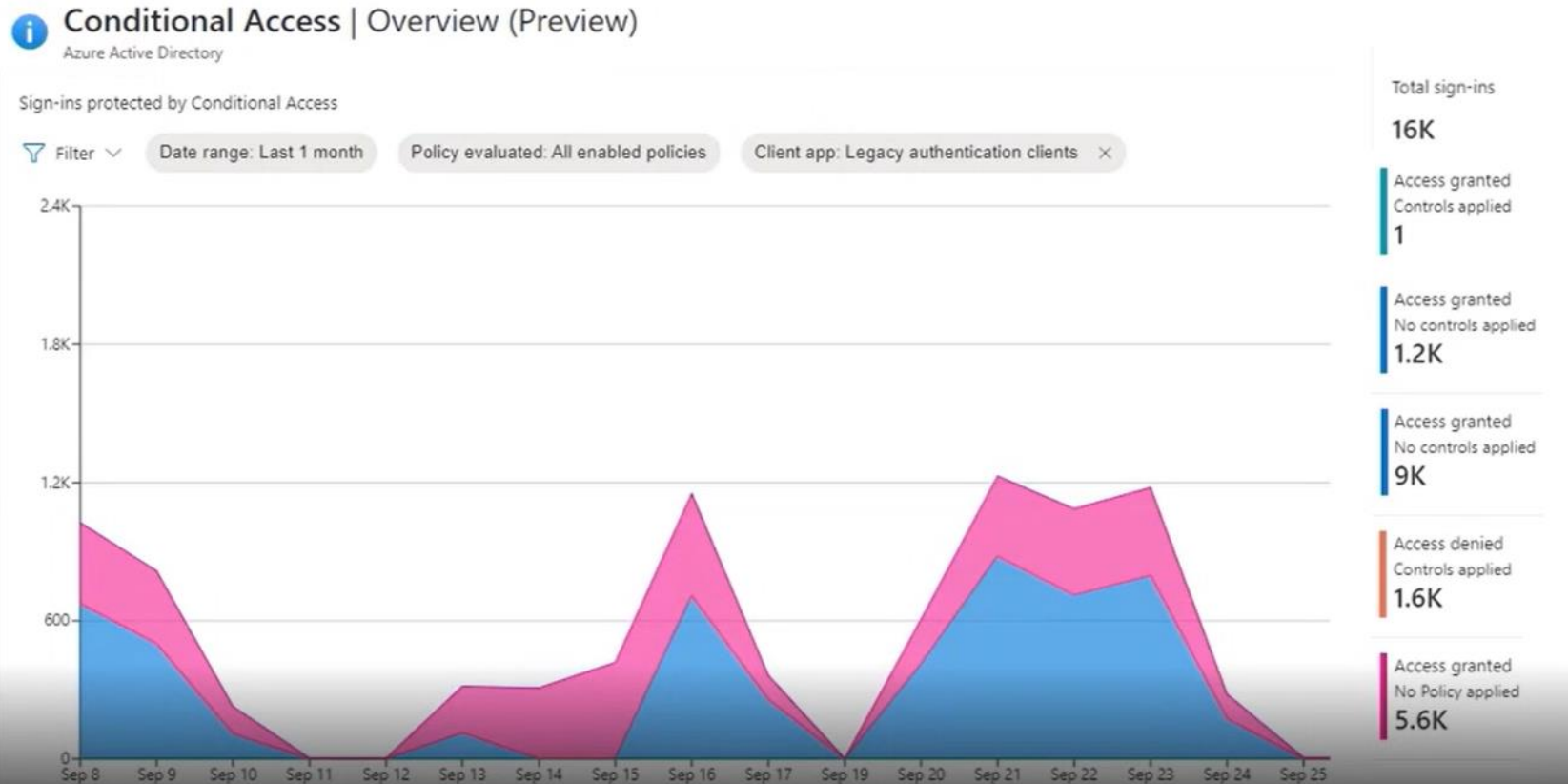
**MODERNIZING IDENTITY
& MIGRATE FROM ON-PREM**



ZERO TRUST AND CONDITIONAL ACCESS

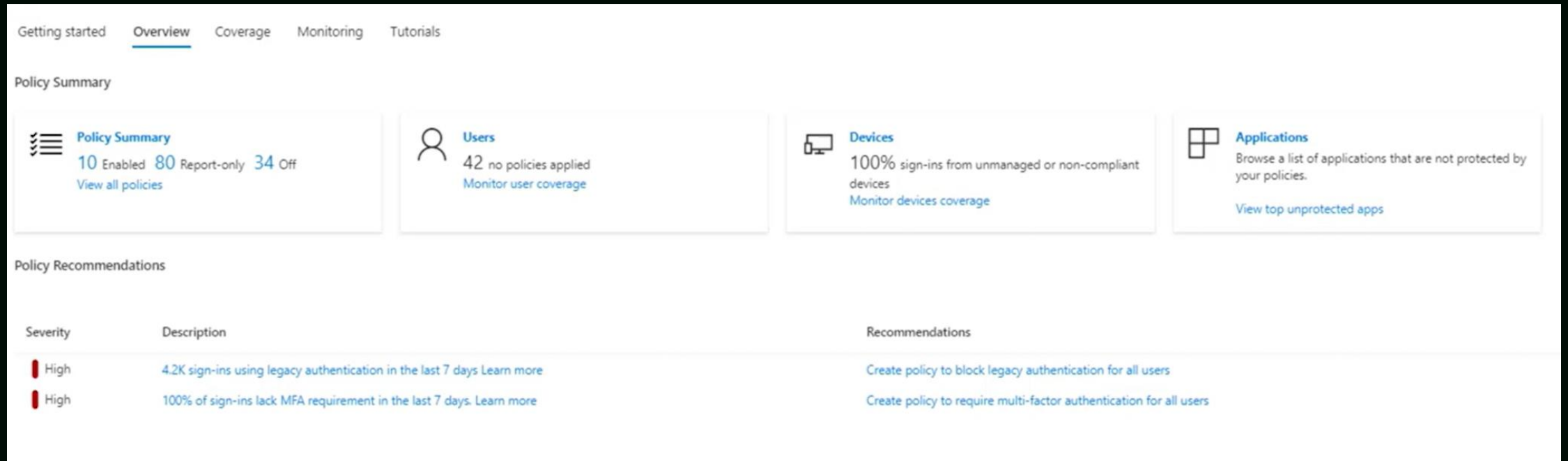
ZERO TRUST AND CONDITIONAL ACCESS

NEW DASHBOARD AND PRE-BUILT TEMPLATES



Conditional Access Overview
Dashboard with updated “Gaps Analyzer” and recommendations (incl. Policy Templates)

ZERO TRUST AND CONDITIONAL ACCESS NEW DASHBOARD AND OVERVIEW



Summary of Conditional Access Configuration and coverage incl. recommendations

ZERO TRUST AND CONDITIONAL ACCESS PRE-BUILT TEMPLATES

Optimize your build **Select template** Review + create

Recommend the following templates based on your response

<input type="radio"/> Require multi-factor authentication for admins Require multi-factor authentication for privileged administrative accounts to reduce risk of compromise. This policy will target the same roles as Security Default. View policy summary	<input type="radio"/> Securing security info registration Secure when and how users register for Azure AD Multi-Factor Authentication and self-service password. View policy summary	<input checked="" type="radio"/> Block legacy authentication Block legacy authentication endpoints that can be used to bypass multi-factor authentication. View policy summary	<input type="radio"/> Require multi-factor authentication for all users Require multi-factor authentication for all user accounts to reduce risk of compromise. View policy summary	<input type="radio"/> Require multi-factor authentication for guest access Require guest users perform multi-factor authentication when accessing your company resources. View policy summary	<input type="radio"/> Require multi-factor authentication for Azure management Require multi-factor authentication to protect privileged access to Azure resources. (Requires an Azure AD Premium 2 License) View policy summary	<input type="radio"/> Require multi-factor authentication for risky sign-in Require multi-factor authentication if the sign-in risk is detected to be medium or high. (Requires an Azure AD Premium 2 License) View policy summary
<input type="radio"/> Require password change for high-risk users Require the user to change their password if the user risk is detected to be high. (Requires an Azure AD Premium 2 License) View policy summary						

Create built-in policy templates for common use cases (right from recommendations/overview)

ZERO TRUST AND CONDITIONAL ACCESS

DYNAMIC FILTERS FOR APPS

Home > Woodgrove > Enterprise applications > IgniteNov2021-FinanceApp

IgniteNov2021-FinanceApp | Custom security attributes (preview)

Enterprise Application

Save Discard Add assignment Remove assignment Got feedback?

For this preview, if you are assigned the Attribute Definition Administrator or Attribute Definition Reader role, you can temporarily access this page, but you cannot view or manage custom security attribute assignments.

Search attribute names or values Add filters

Attribute set	Attribute name	Attribute descri...	Data type	Multi-valued	Assigned values
<input type="checkbox"/>	IgniteNov2021	datacenter	String	Yes	1 value

Overview
Deployment Plan
Manage
Properties
Owners
Roles and administrators (Preview)
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Custom security attributes (preview)
Security
Conditional Access
Permissions
Token encryption

Home > Woodgrove > Select dynamic targeting rule

New

Conditional Access policy

Control user access based on user, device, and location information. Learn more

Configure Yes No

You can use the rule builder or rule syntax text box to create or edit a dynamic targeting rule.

And/Or	Attribute	Operator	Value
	<input type="text"/>	<input type="text"/>	<Pick a property and operator first>
+ Add express	<input type="text"/>		
Rule syntax	<input type="text"/>		

Assignments
Users and groups
Specific service principals
Cloud apps or actions
No cloud apps, actions, or contexts selected
Conditions
0 conditions selected
Access controls
Grant
Enable policy
Report-only On

Project
Project name
Project manager
IgniteNov2021
businessUnit
datacenter

Dynamic Targeting Rule for Apps (Public preview by the end of the year)

ZERO TRUST AND CONDITIONAL ACCESS

DYNAMIC FILTERS FOR DEVICES

Home > Conditional Access >

120 - ALL - Privileged Access - All apps: BL...

Conditional Access policy

Delete

Name *

120 - ALL - Privileged Access - All apps: BL...

Assignments

Users and groups ⓘ

Specific users included and specific users excluded

Cloud apps or actions ⓘ

All cloud apps included and 1 app excluded

Conditions ⓘ

2 conditions selected

Access controls

Grant ⓘ

Block access

Session ⓘ

0 controls selected

Filter for devices

Configure a filter to apply policy to specific devices. [Learn more](#)

Configure ⓘ

Yes No

Devices matching the rule:

☐ Include filtered devices in policy

☒ Exclude filtered devices from policy

You can use the rule builder or rule syntax text box to create or edit the filter rule.

And/Or	Property	Operator	Value
	DeviceId	Equals	
+ Add express	Choose a property		
Rule syntax ⓘ	DeviceId		
	device.deviceId		1ac08249556"
	DisplayName		
	DeviceOwnership		
	IsCompliant		
	Manufacturer		
	MdmAppId		
	Model		

Client apps ⓘ

2 included

Device state (Preview) ⓘ

Not configured

Filter for devices ⓘ

Exclude filtered devices

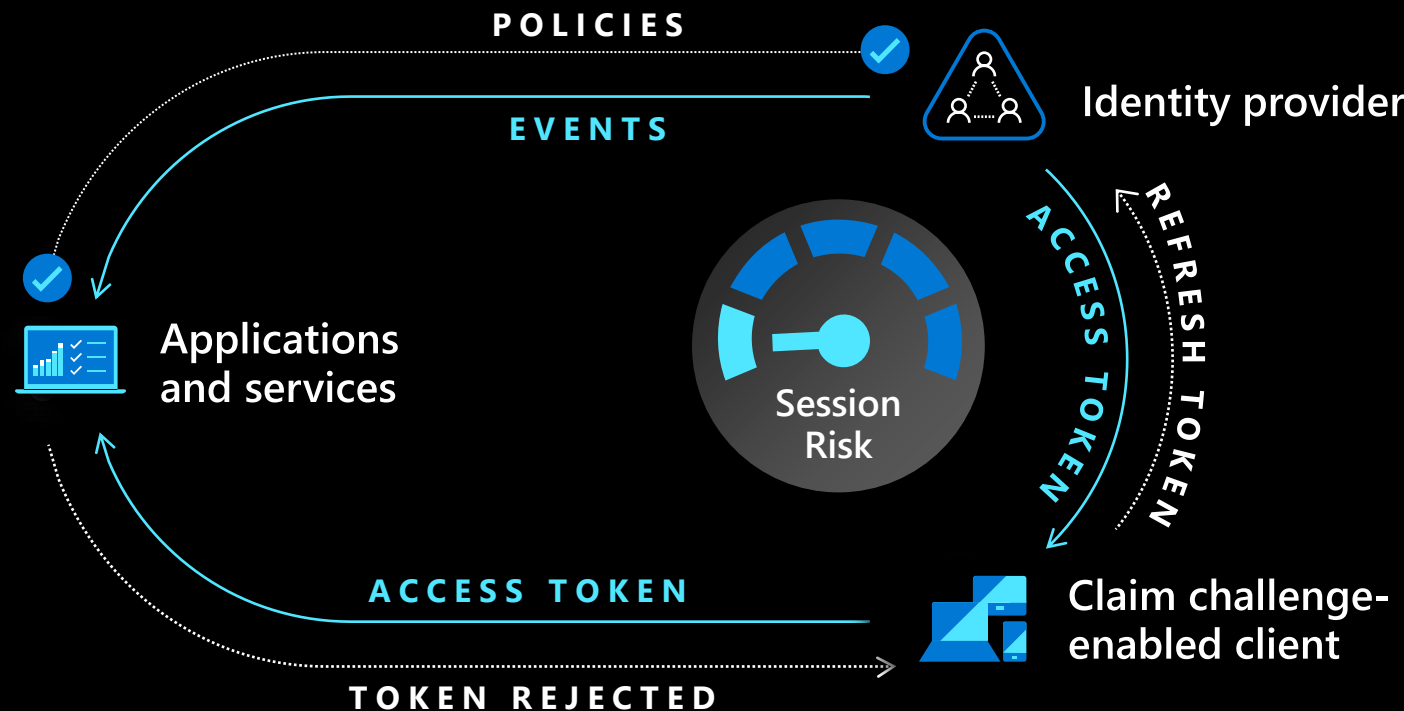
i 'Device state (Preview)' and 'Filter for devices' cannot be configured simultaneously. 'Device state (Preview)' is being deprecated. Use 'Filter for devices' instead.

[Learn more.](#)

Device Filters for granular assignment of policies (Now in GA, Device state deprecated)

ZERO TRUST AND CONDITIONAL ACCESS

CONTINUOUS ACCESS EVALUATION





Configuration and Continuous Access Evaluation (CAE) in Action

LIVE DEMO



SECURING NON-HUMAN (WORKLOAD) IDENTITIES

SECURING NON-HUMAN (WORKLOAD) IDENTITIES

SUPPORT FOR CONDITIONAL ACCESS

Home > Woodgrove > Security > Conditional Access >

New

Conditional Access policy

Control user access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

IgniteNov2021-RequireTrustedLocationF... ✓

Assignments

Users and groups ⓘ

0 users and groups selected

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Control user access based on users and groups assignment for all users, specific groups of users, directory roles, or external guest users [Learn more](#)

What does this policy apply to?

Workload identities

Include Exclude

☒ None

☐ All owned service principals

☒ Select service principals

Home > Woodgrove >

New

Conditional Access policy

Control user access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

IgniteNov2021-RequireTrustedLocationF...

Assignments

Users and groups ⓘ

Specific service principals

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

Enable policy

Report-only On

Select dynamic targeting rule

Configure ⓘ

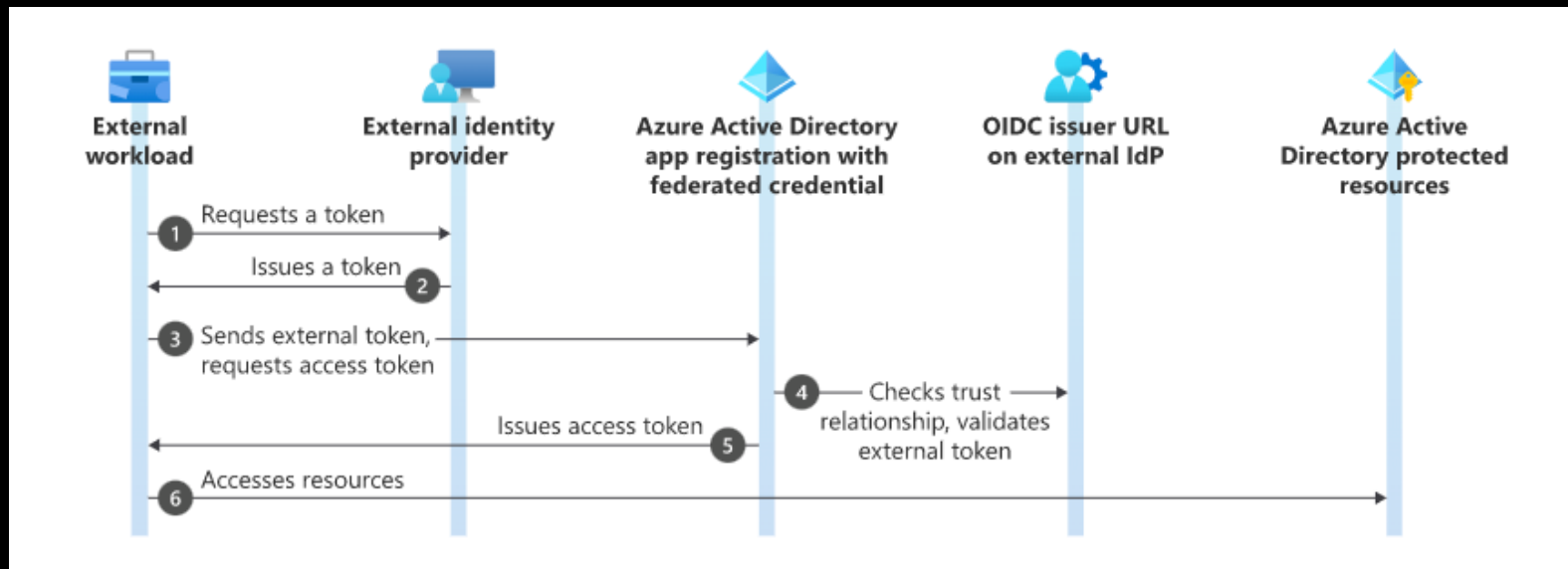
Yes No

You can use the rule builder or rule syntax text box to create or edit a dynamic targeting rule.

And/Or	Attribute	Operator	Value
			<Pick a property and operator first>
+ Add express	Choose an attribute		
Rule syntax ⓘ	Project		
	Project name		
	Project manager		
	IgniteNov2021		
	businessUnit		
	datacenter		

SECURING NON-HUMAN (WORKLOAD) IDENTITIES

- **New authentication method policies** available in Microsoft Graph
- Added Managed Identity Support for many built-in operations and connectors
- **GitHub Actions support for workload identity federation** with Azure AD
Alternative to creating and storing AAD credentials in the GitHub repo when they deploy applications to Azure:

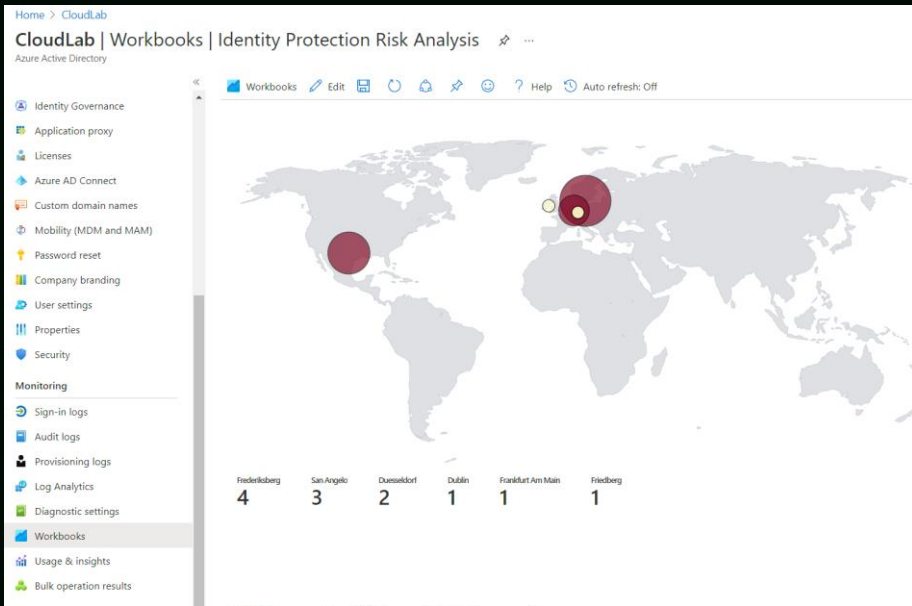




IDENTITY SECURITY AND -GOVERNANCE

IDENTITY SECURITY AND -GOVERNANCE

ENHANCED FEATURES IN IDENTITY PROTECTION



Risk analysis workbook visualizes your risk data and the effectiveness of your response

Identity Protection offers new detections:

- **detections for anomalous tokens**

Diagnostic settings to export risk data to your SIEM

Changes in Default Sign-in Failure Detections in Microsoft Defender for Cloud Apps (MCAS)

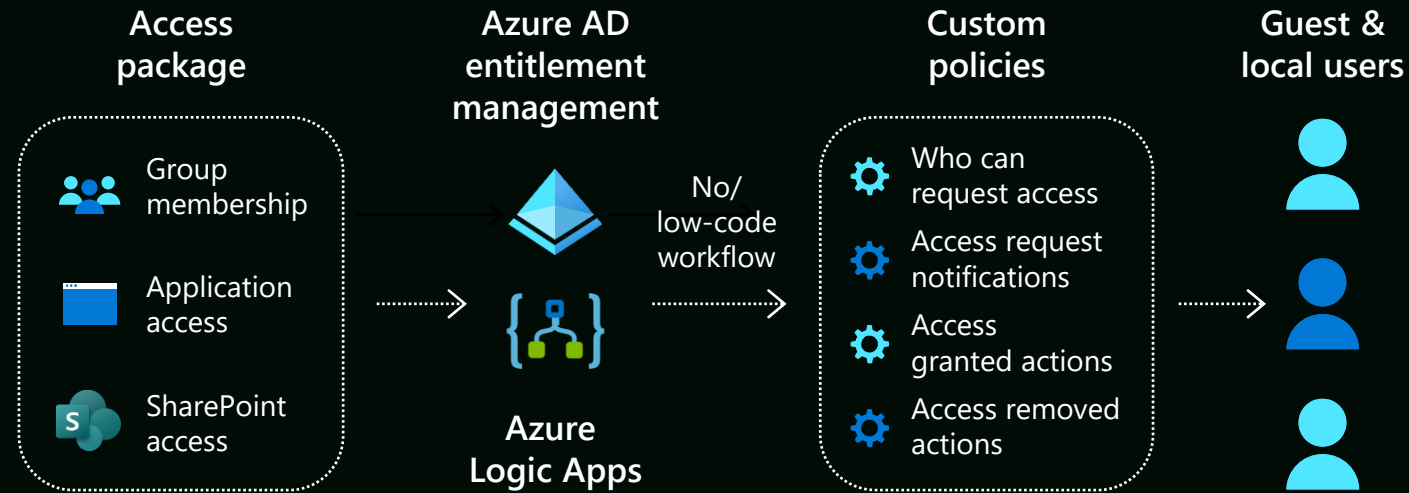


Azure AD Identity Protection Enhancements

LIVE DEMO

IDENTITY SECURITY AND -GOVERNANCE

CUSTOM APPROVAL WORKFLOWS



Trigger custom Logic Apps with Azure AD entitlement management

IDENTITY SECURITY AND -GOVERNANCE

CUSTOM APPROVAL WORKFLOWS

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Identity Governance > Tier0.M365.0.SAWEndpointHelpdesk >

Edit policy ...

* Basics * Requests Requestor information * Lifecycle Rules (Preview)

Configure a rule: If <event>, then do <flow>. A rule contains an event that/and triggers a previously defined custom flow

Stage	Custom Extension
Select stage	Select custom extension

- Request is created
- Request is approved
- Assignment is granted
- Assignment is about to expire in 14 days
- Assignment is about to expire in 1 day
- Assignment is removed

Home > Identity Governance > vikamaCustomExtension >

Create Custom Extension ...

* Basics * Details Validate + Create

Create new logic app ☒ Yes ☐ No

Select authentication resource [+ Create new Azure AD application](#)

-or-

[+ Select an existing application](#)

Selected resource application ID

Subscription *

Resource group *

Logic app name *

Create logic app

Logic App resource creation permission needed in the selected resource group.

IDENTITY SECURITY AND -GOVERNANCE

CLOUDKNOX



**Identity
Governance
& Administration**



**Privileged
Access
Management**



**Cloud Infrastructure
Entitlements
Management**

Deliver a unified multi-cloud solution that spans identity provisioning, lifecycle management, workflow automation, permissions management, and analytics

IDENTITY SECURITY AND -GOVERNANCE

CLOUDKNOX

Geeta Alapati

geeta@cloudknox.io

cloudknox.io

78

High - 86 days

4450

339

381

22

2

07 Oct 2021, 1:35PM

...

Tasks

Q Search

All Tasks

UNUSED (4114)

▶ accessapproval

!

7/7

▶ actions

!

8/8

▶ aiplatform

!

209/209

▶ androidmanagement

!

1/1

▶ apigateway

!

27/27

▶ apigee

!

194/194

▶ apigeeconnect

!

2/2

▶ apikeys

!

6/6

▶ appengine

14/25

▶ artifactregistry

!

25/25

▶ automl

!

53/53

USED (339)

▶ appengine

11/25

▶ bigquery

2/74

▶ bigtable

3/40

▶ billing

✓

1/1

▶ clientauthconfig

10/14

▶ cloudasset

1/106

▶ cloudbuild

1/11

▶ cloudfunctions

4/15

▶ cloudnotifications

✓

1/1

▶ cloudsql

13/40

▶ cloudtrace

3/10

Groups

Roles

User Groups

testgroup@cloudknox.io

engineering@cloudknox.io

Pratima Gogineni

pratima@cloudknox.io

cloudknox.io

75

High - 86 days

4449

310

381

13

1

07 Oct 2021, 1:35PM

...

Maya Neelakandhan

maya@cloudknox.io

cloudknox.io

76

High - 86 days

4460

271

381

19

1

07 Oct 2021, 1:35PM

...

IDENTITY SECURITY AND -GOVERNANCE


CLOUDKNOX

1 Details

2 Tasks

3 Statements

4 Preview



Online

Controller Enabled

Policy name:

CK_POLICY_Pratima

Authorization System:

cloudknox-development

JSON

Script

Download JSON

Download Script

Valid JSON

character count : 3306/6144

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

},

{

"Sid": "iamCreateActions",

"Effect": "Allow",

"Action": [

"iam:CreateAccessKey",

"iam:CreateLoginProfile",

"iam:CreateOpenIDConnectProvider",

"iam:CreateRole",

"iam:CreateUser"

],

"Resource": [

"*"

]

},

{

"Sid": "iamDeleteActions",

"Effect": "Allow",

"Action": [

"iam:DeleteOpenIDConnectProvider",

Back

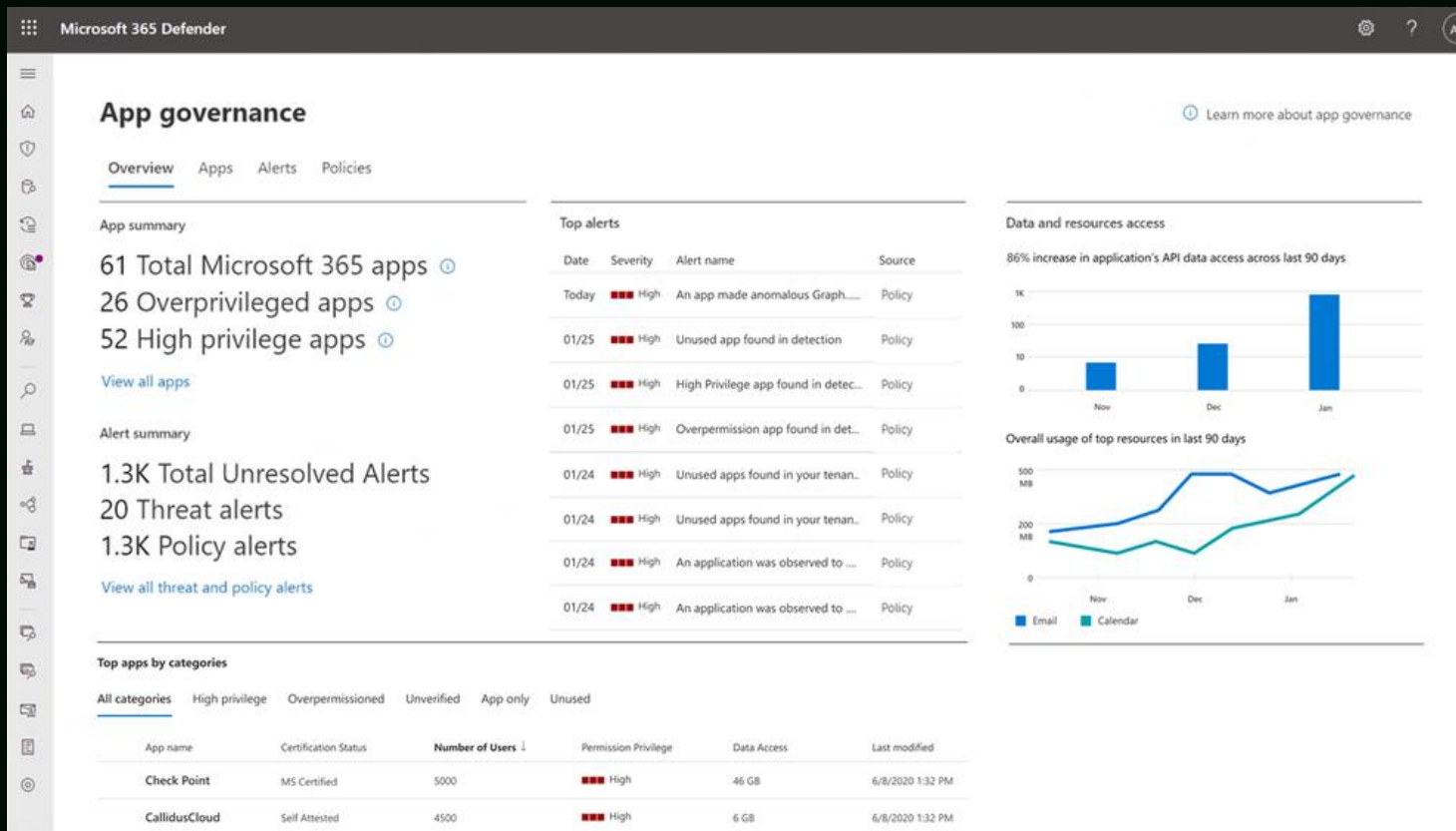
Cancel

Submit

IDENTITY SECURITY AND -GOVERNANCE

MICROSOFT DEFENDER CLOUD APPS APP GOVERNANCE

- App Governance is GA now
- Designed for OAuth-enabled apps with access to M365 data (via Graph API)

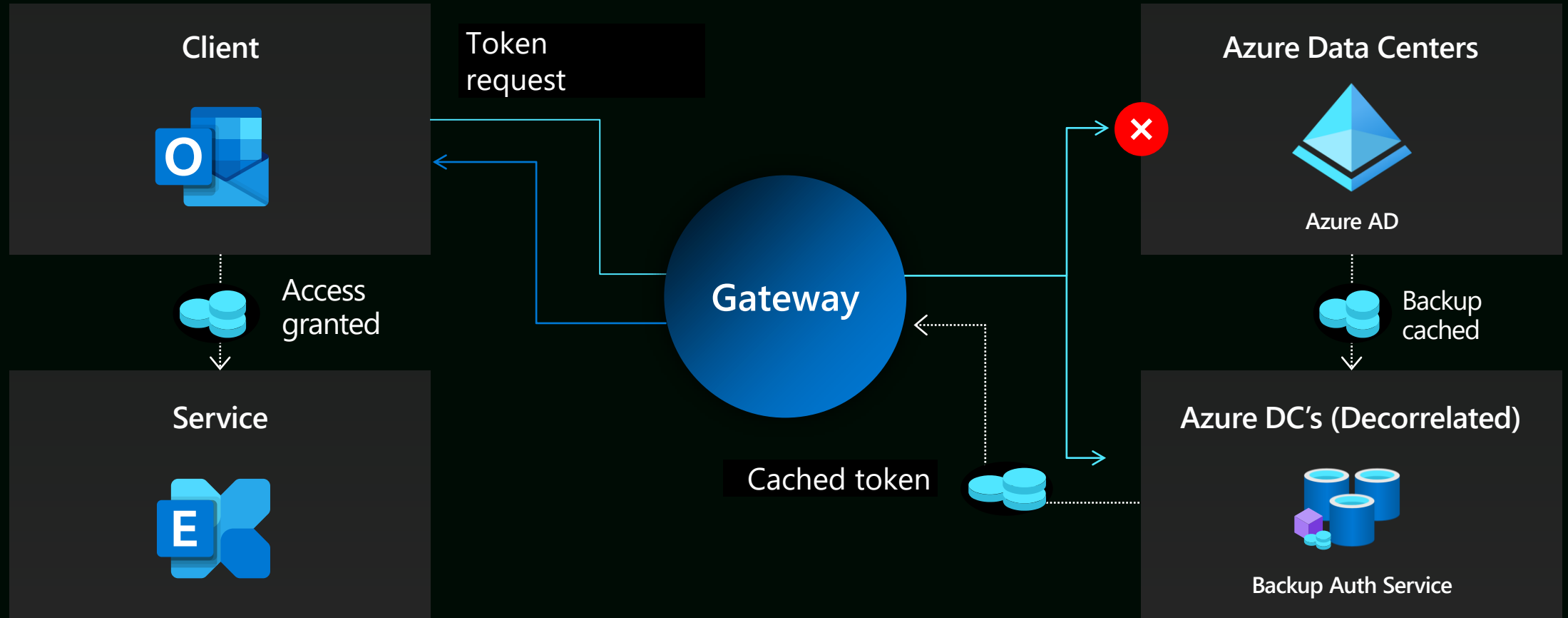




MODERNIZE IDENTITY & MIGRATE FROM ON-PREM

MODERNIZE IDENTITY & MIGRATE FROM ON-PREM

RESILIENCY IMPROVEMENTS IN PLATFORM

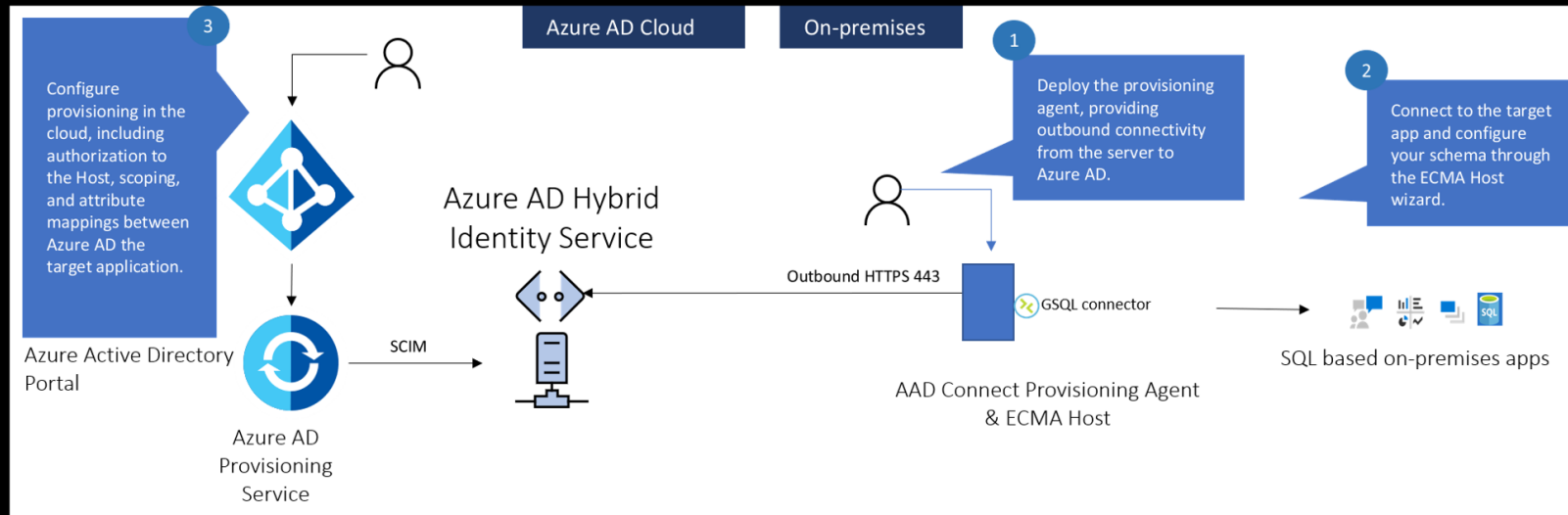


- More details on configure Resilience Defaults in Conditional Access

MODERNIZE IDENTITY & MIGRATE FROM ON-PREM

ENHANCEMENT FOR MICROSOFT HYBRID IDENTITY

- Accelerate migration from AD FS application with previews of extended claims support , token filtering, and additional SAML configuration settings
- Enable cloud sync self-service password reset writeback to an on-premises environment (preview)
- On-Premises (or private cloud) application provisioning from Azure AD



LEARN MORE ABOUT...CONDITIONAL ACCESS

The banner features a background image of a historic European town with a large church spire. Overlaid on this is a semi-transparent box containing the following elements:

- Top Left:** The Azure logo (a blue diamond shape).
- Top Right:** A portrait of Thomas Naunheim, a man with glasses wearing a blue shirt, with his name and a German flag icon below it.
- Center:** The text "Deep Dive into Azure AD Conditional Access" in a large, elegant font.
- Bottom Left:** The "Other technologies Track" logo, which includes a camera icon and the text "Other technologies Track" and "In Person in Aachen, session in German".
- Bottom Right:** A small icon of a person at a presentation board with an audience, accompanied by a German flag.

To the right of the semi-transparent box, the text "aMS Germany" and "November 16th, 2021" is displayed in a bold, sans-serif font. Next to this text is the aMS logo, which consists of a circular graphic divided into four colored segments (red, green, blue, yellow) surrounding the text "aMS".

At the bottom of the banner is a horizontal row of various Microsoft and partner logos, including the Azure logo, a checkmark, a stylized 'X', the Teams logo, the OneDrive logo, a blue arrow, a person icon, the aMS logo, a stylized 'X', a bar chart, a pencil, a diamond shape, the SharePoint logo, and the Office 365 logo.

aMS Germany → Free Registration

LEARN MORE ABOUT...WORKLOAD IDENTITIES


DECEMBER 1 - 2

VIRTUAL CONFERENCE

PROTECT YOUR
PRIVILEGED
IDENTITIES AND
DEVOPS PIPELINES IN
MICROSOFT AZURE!

▷ SPEAKER :

THOMAS NAUNHEIM
Cloud Architect, glueckkanja-gab AG



Learn More: [HIPCONF.COM](https://hipconf.com)

Hybrid Identity Protection Conference → [Free Registration](https://hipconf.com)

THANK YOU



@Thomas_Live



Thomas@Naunheim.net

www.cloud-architekt.net