



Communauté Cisco

Microsoft Azure / AD integration avec Cisco ISE

Simplicity, Visibility, Cloud-Enabled

Jean-François Pujol

TSA, Mobility & Security, Switzerland | Cisco Suisse

Polo Arroyo

Technical Consulting Engineer CCNA R&S and Security | Cisco TAC Mexique

8 mars 2021

Nouveautés et prochains événements



Événement : Ask Me Anything Global



Cisco SD-WAN : Guide rapide pour la conception, le déploiement, l'exploitation et la maintenance

Foire aux Questions
Du 8 au 19 Mars 2021
avec **Guilherme Lyra**, **Danny Blais**, **Oswaldo Salazar Tovar**
et **Thomas Matzeu**

Événement public

Suivez le lien

<https://bit.ly/AMA-08Mar21>

Ask the Cisco Community experts!

08-19 MAR
Guilherme Lyra
Thomas Matzeu
Oswaldo Salazar
Danny Blais
Public event

Ask Me Anything - Networking Global Event
Cisco SD-WAN: A Quick Guide to Design, Deploy, Operate, and Maintain.

Community Live mardi 13 Avril



Wireless : Comment réussir l'intégration Voip / Vidéo sur WiFi

Webcast en direct
le mardi 13 avril 2021
avec **Alain Faure**

Événement public

Suivez le lien

<https://bit.ly/WEB-FRapr21>

Communauté Cisco | Wireless



13 APR 2021
Alain Faure

Événement public



Community Live | Réseaux Sans-fil
Comment réussir l'intégration
VoIP / Vidéo sur WiFi

Inscrivez vous ici ! >>>

Deployment Stories Unplugged



Partagez vos propres projets !

Découvrez comment les membres de la communauté ont résolu leurs défis de manière créative grâce à la technologie Cisco.

Visitez la Galerie des Projets

Suivez le lien

[Stories Unplugged](#)

Project Stories



Share your
creative tech
project !

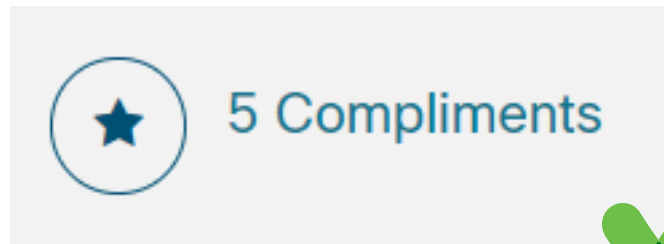


SHOW OFF

Évaluez le contenu de la Communauté Cisco

Discussions, Documents, Blogs et Vidéos

Aidez-nous à identifier les contenus de qualité et à reconnaître l'effort des membres de la Communauté Cisco en français.



Identifiez les experts

Accepter comme solution

Repérez les solutions

Apprenez à mieux utiliser la plateforme et exploiter toutes ses ressources.

Suivez le lien

<http://bit.ly/PilotVideoFR>

Reconnaissance aux Top Contributeurs


Devenez le Top Contributeur du mois de janvier !

La reconnaissance aux **Top Contributeurs** est conçue pour reconnaître et remercier ceux qui ont collaboré avec nous en fournissant des contenus techniques de qualité ainsi que les participants plus actifs qui ont permis à notre communauté de devenir un des Top sites pour les passionnés de la technologie de Cisco.

Suivez le lien

<http://bit.ly/FRCC-SpotlightAwards>



 Community Spotlight awards The Community Spotlight Awards recognizes members whose significant contributions designate leadership and commitment to their peers within their respective communities, including Cisco Community, Cisco Learning Network (CLN), and Cisco Developers Network (CDN). Spotlight awards are designed to recognize and thank individuals who help make our communities the premier online destination for Cisco enthusiasts. [FAQs](#)

2021 2020 2019 2018 2017 2016 2015 2014 2013 2012

janvier **février** mars avril mai juin juillet août septembre octobre novembre décembre

French Community Member's Choice, February 2021



Alain Faure
2021 February

Introduction

Les experts de la Communauté Cisco

Jean François Pujol

Technical Solutions Architect
Cisco Suisse

Mobility & Security



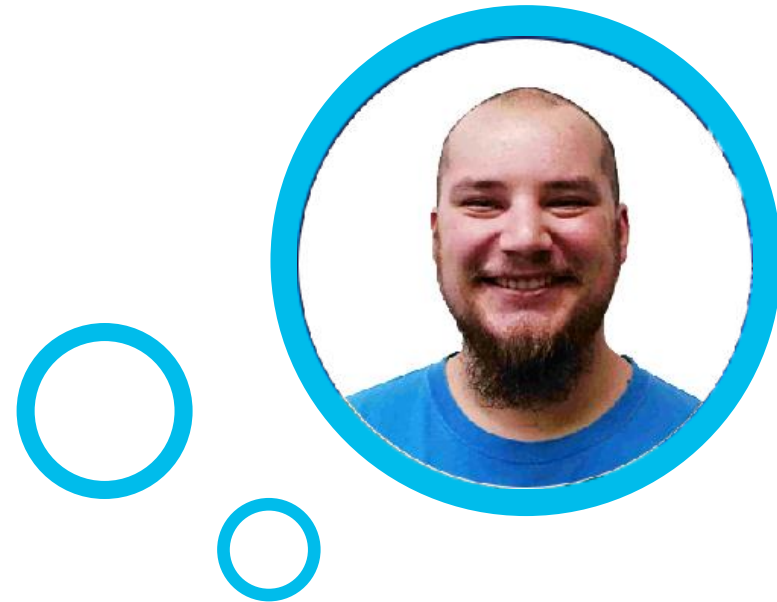
Présentateur

Les experts de la Communauté Cisco

Polo Arroyo Folange

Technical Consulting Engineer
Cisco TAC

CCNA R&S / Security



[Question Manager](#)

Merci d'être avec
nous aujourd'hui !

Téléchargez la présentation sur

<https://bit.ly/WEBsld-mar21>



Participez avec nous et posez des questions

La présentation comprendra aussi quelques questions du public.

Nous vous invitons cordialement à participer activement aux questions que vous pourrez poser pendant cette séance sur le panneau à droite « Q&R ».

Résolvez vos doutes et partagez votre opinion





Agenda

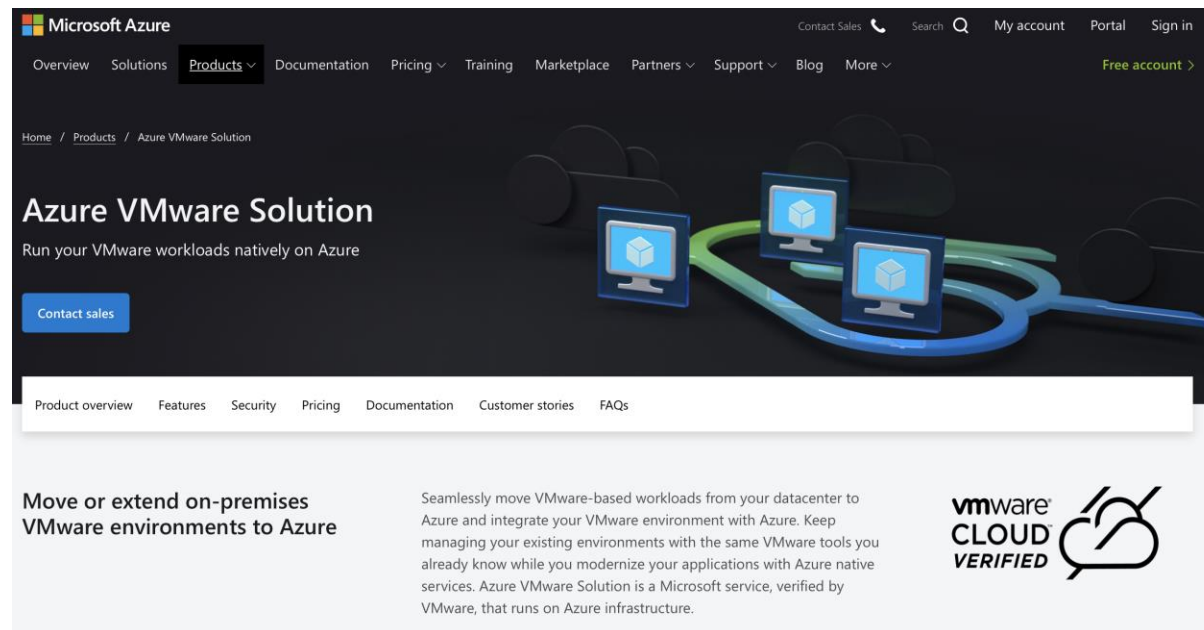
- Platform Support: VMware Cloud on Azure
- 802.1X with Azure AD using ROPC
- SAML SSO with Azure AD

ISE running in Azure AVS Cloud



ISE 3.0 Support on Azure

- Azure VMware Solution (AVS) runs VMware workloads natively on Azure, where Cisco ISE can be hosted as VMware virtual machine.
- Cisco ISE (Identity Services Engine) 3.0 is validated as virtual machine deployed on Azure VMware Solution.



- See a community post on “ISE in the Cloud” :
<https://community.cisco.com/t5/network-access-control/ise-in-the-cloud/td-p/3703425>

What is your favorite
Public Cloud platform ?

Polling Question - Sondage 1

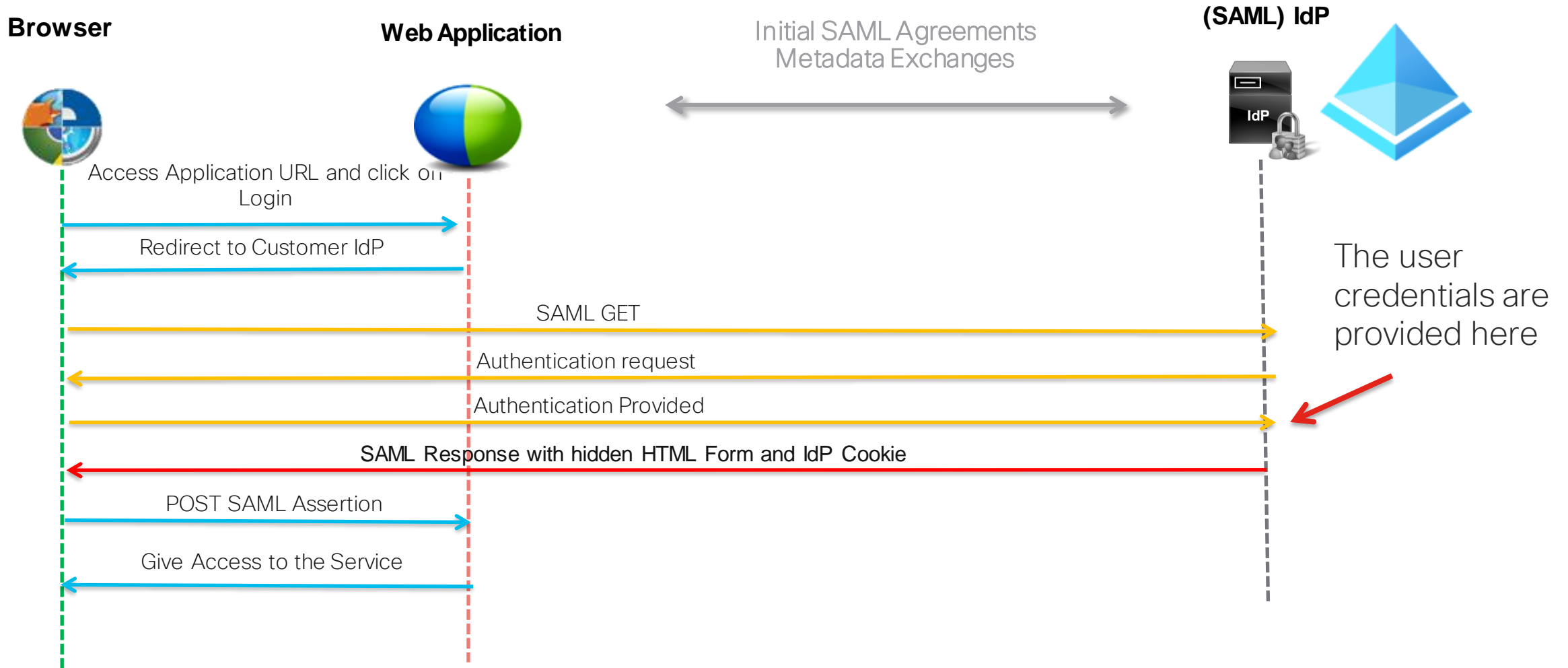
- A. Google Cloud
- B. AWS
- c. Azure



Identity Challenges with Azure IdP

- Why not Using EAP Type Protocols like usual with ISE ?

SAML SSO for Single Sign-On with an IdP



To reach a SAML compatible IdP, the client needs an IP !

- dot1X is running even before

Extensible Authentication Protocol (EAP)

- EAP provides an extensible framework for exchanging authentication information after the data link layer (L2) is established.
- EAP is a framework for multiple authentication methods, allowing the transport of various authentication methods at layer 2 to the Authenticator (NAD).
- 802.3 (Ethernet) or 802.11 (Wireless) can be used to establish the link layer.
- Examples of EAP Protocols : EAP-TLS, EAP-FAST, and PEAP(MSCHAPv2), EAP-TTLS.
- *EAP typically runs directly over data link layers such as Point-to-Point Protocol (PPP) or IEEE 802, without requiring IP.*

About EAP-TTLS

- EAP Tunneled Transport Layer Security (EAP-TTLS) is an EAP protocol that extends [TLS](#). It was co-developed by [Funk Software](#) and [Certicom](#) and is widely supported across platforms.
- [Microsoft Windows](#) started EAP-TTLS support with [Windows 8](#), support for EAP-TTLS appeared in Windows Phone [version 8.1](#).
- After the server is securely authenticated to the client via its CA certificate and optionally the client to the server, the server can then use the established secure connection ("tunnel") to authenticate the client.
- The secure tunnel provides protection from [eavesdropping](#) and [man-in-the-middle attack](#). Note that the user's name is never transmitted in unencrypted clear text, improving privacy.

Source Wikipedia : [Extensible Authentication Protocol](#)

802.1X with Azure AD using ROPC

3.0

Problem

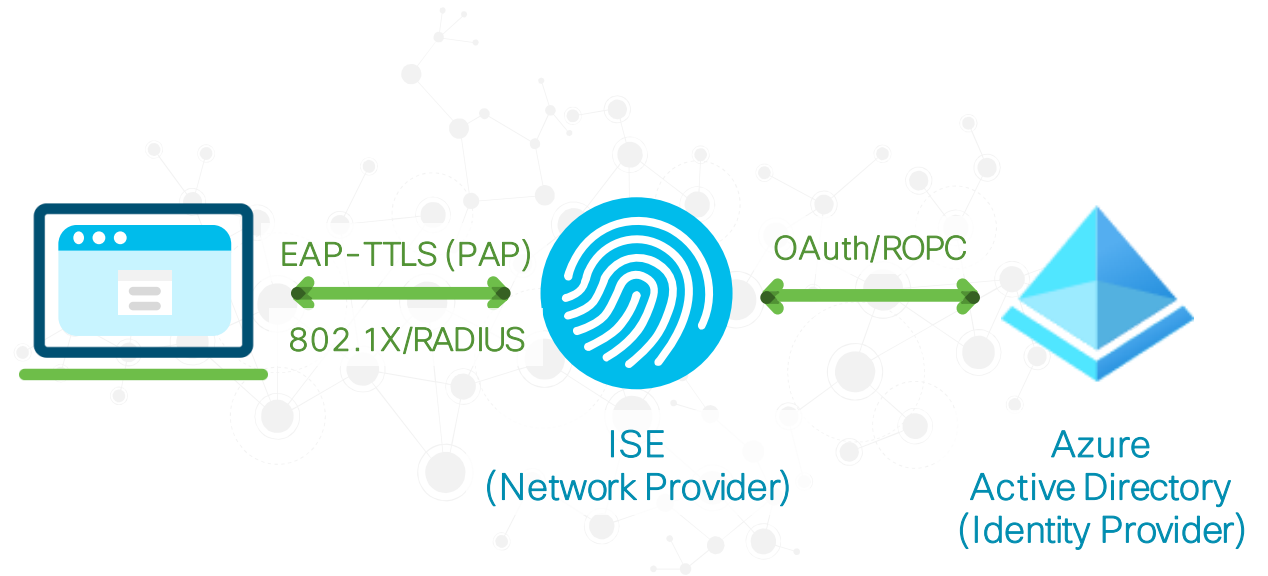
802.1X requires authentication for authorized network access but SAML/OAuth assume connectivity for brokering between user, SP and IdP.

Solution

ISE 3.0 allows you to authenticate users with 802.1X directly to Azure AD using OAuth *Resource Owner Password Credentials* (ROPC).

Caveats / Requirements

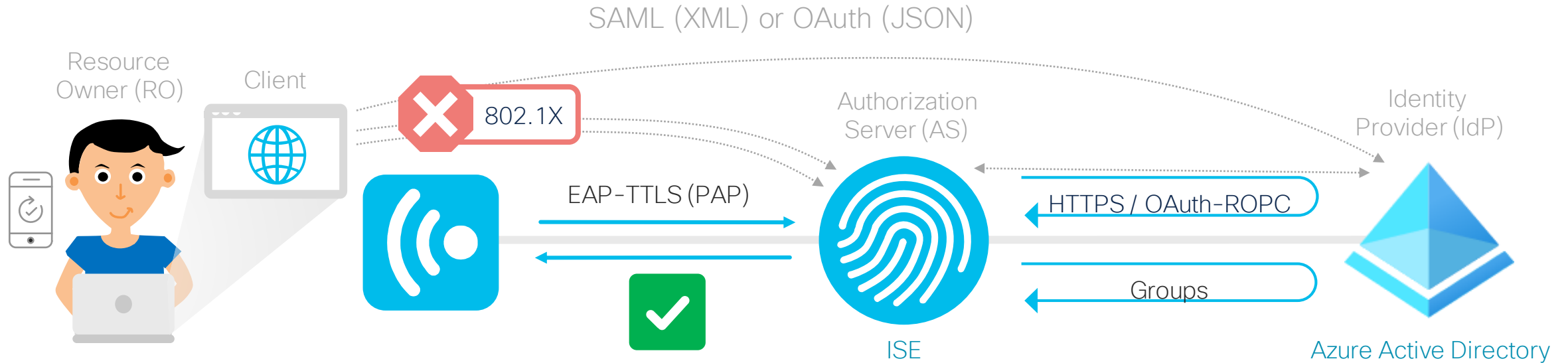
Password sent unencrypted in EAP-TTLS tunnel.



OAuth-ROPC: [RFC-6749](#)

ROPC = Resource Owner Password Credentials

802.1X with Azure AD using ROPC



Protocol Support	EAP-TTLS (PAP)	PEAP (EAP-GTC)	EAP-FAST (EAP-GTC)
Microsoft Windows 10	Manual Configuration	N/A	N/A
Apple macOS / iOS / iPadOS	MDM / MobileConfig Profile	Manual OK if preferred in ISE	CSCvg73640
Google Android	Manual Configuration	Manual Configuration	N/A

Controlled Introduction of ISE ROPC



[Cisco Community](#) > [Customer Connection](#) > [Security Customer Connection Program](#) > [ISE 802.1x with Azure AD using ROPC Trial](#)



Be aware:

- Username + Password only - No Certificates!
- No user interactions allowed for password changes, MFA, or AUPs
- No new accounts that have not yet changed the default password
- Azure AD tenants and accounts only. No invited personal accounts or federated IdPs like Microsoft, Google+, Twitter, AD-FS, Facebook
- Session Management like keep me signed-in (KMSI), is not applicable



You must install [DigiCert Global Root G2](#) CA Certificate until Patch 1 ([CSCvw80297](#))

The screenshot shows the Cisco Community website interface. At the top, there's a navigation bar with 'FIND A COMMUNITY', 'Buy or Renew', and the Cisco logo. Below that, a green banner reads 'JOIN US in congratulating September's Community Spotlight Awards Winners - Click HERE'. A search bar is present with the text 'Search Security'. A navigation menu includes 'Technology & Support', 'For Partners', 'Customer Connection', 'Webex', 'Events', and 'Members & Recognition'. The main content area is titled 'Security Customer Connection Program Early Adopter Trials' and includes a 'Sign Up for Trial' button circled in green. Below the button, there's a section for 'Cisco Identity Services Engine Early Adopter Trial' with details about the trial period (October 2020 - March 2021) and features.

Do you use Azure
Active Directory?

Polling Question - Sondage 2

Identity Stores:

- A. Active Directory (AD) only
- B. Azure AD Only
- C. AD and Azure AD
- D. We don't use AD-anything for ISE Identity Stores!





Welcome to Azure!

Don't have a subscription? Check out the following options.



Start with an Azure free trial

Get \$200 free credit toward Azure products and services, plus 12 months of popular free services.



Manage Azure Active Directory

Manage access, set smart policies, and enhance security with Azure Active Directory.



Access student benefits

Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.

802.1X with Azure AD Demo (with preliminary review of a few GUI improvements)



Create a resource



Azure Active Directory



Virtual machines



App Services



Storage accounts



SQL databases



Azure Database for PostgreSQL



Azure Cosmos DB



Kubernetes services



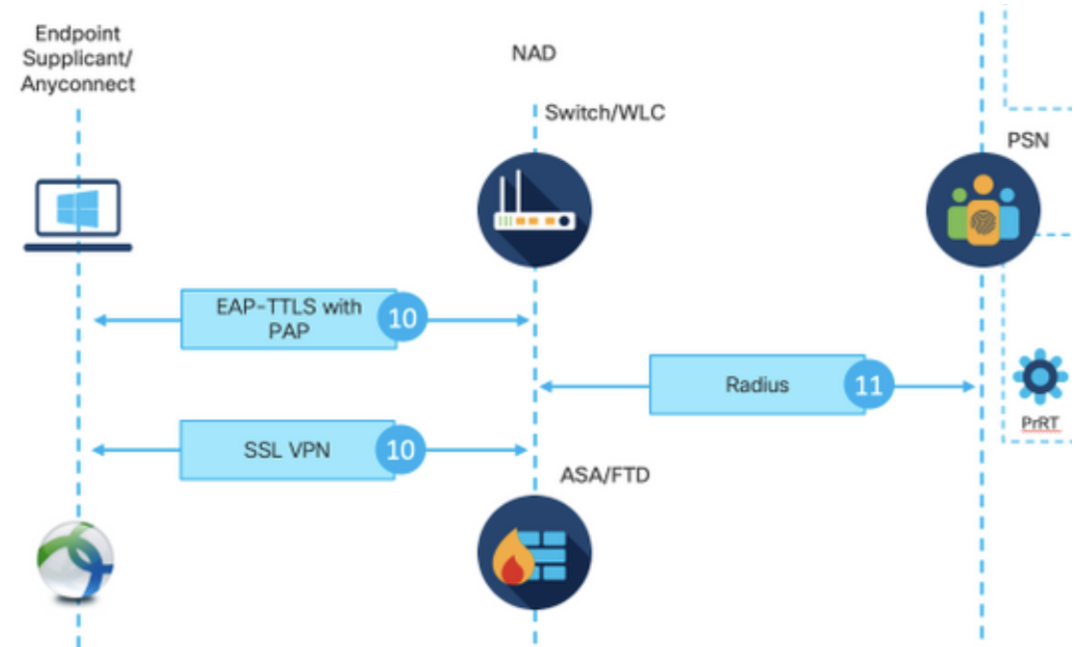
More services

More about using PAP for Authentication

As per ROPC protocol specification, user password must be provided to the Microsoft identity platform in a clear text over an encrypted HTTP connection

Due to this fact, the only available authentications options supported by ISE as of now are:

- Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) with Password Authentication Protocol (PAP) as the inner method
- AnyConnect SSL VPN authentication with PAP



Would you configure
your endpoints to use
PAP w/ Password ?

Polling Question - Sondage 3

My Security Policy :

- A. The user's password will never leave his device (laptop, smartphone, etc...)
- B. If I'm sure it is encrypted up to ISE, it could be acceptable
- C. If not available as a default configuration option in the endpoint, too complicated
- D. I don't see that requirement as an issue anyway



ISE ROPC

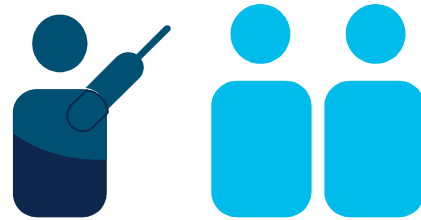
future developments

Alternative with SAML Single Sign- On and Web Portals

- Leverage WebAuth instead of dot1X

How to use natively SAML ?

- Leverage the browser on the end-point
- WebAuth based authentication instead of dot1x
- Leverage ISE capability to authenticate web portals with SAML



SAML Single Sign-On (SSO) with Azure AD MFA

3.0

Problem

Customers want to use Azure AD as a SAML 2.0 identity provider for Single Sign-On (SSO) with multi-factor authentication (MFA) for ISE portals

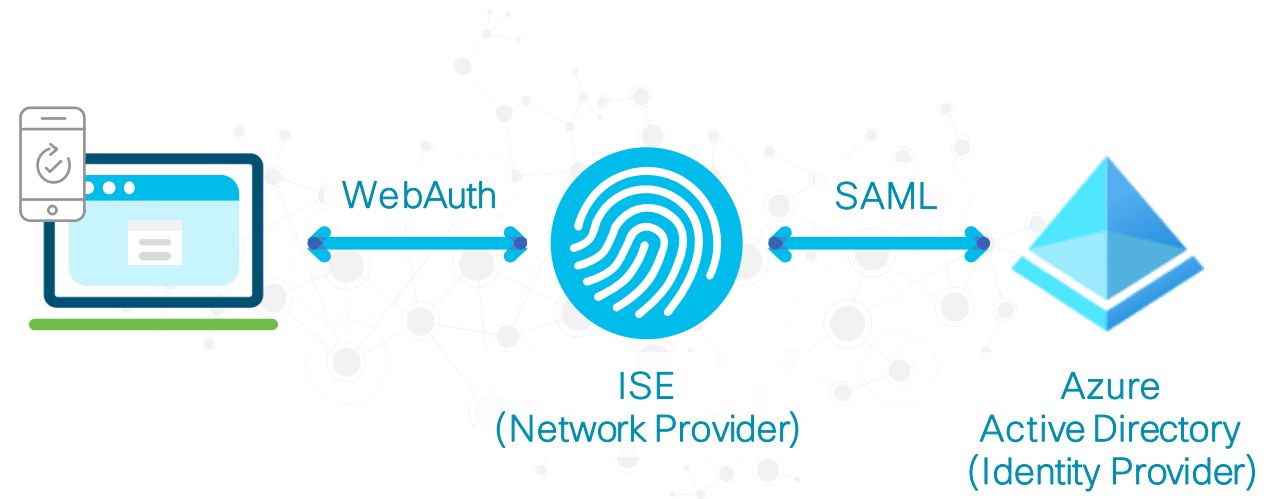
Solution

Azure AD with MFA is now possible with SAML identity providers for Single Sign-On (SSO) for Guest, BYOD and My Devices portals.

Caveats / Requirements

Only for ISE web portals.

Don't use `AuthnContextClassRef` unless you need it!



ISE 2.x

SAML SSO works but not with MFA

SAML header with Auth Context

```
<samlp:AuthnRequest xmlns:saml="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:ax="urn:oasis:names:tc:SAML:2.0:ac:classes" xmlns:ad="urn:oasis:names:tc:SAML:2.0:assertion" ID="ONELOGIN_8...>
  <saml:Issuer>http://sp.example.com/demo1/metadata.php</saml:Issuer>
  <samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress" AllowCreate="true"/>
  <samlp:RequestedAuthnContext Comparison="exact">
    <saml:AuthnContextClassRef urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml:AuthnContextClassRef>
  </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

A red 'X' icon is overlaid on the `AuthnContextClassRef` element, indicating that this configuration is problematic for MFA.

ISE 3.0

No AuthnContextClassRef : SAML SSO + MFA works!

SAML header for Azure AD

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="ONELOGIN_8...>
  <saml:Issuer>http://sp.example.com/demo1/metadata.php</saml:Issuer>
  <samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress" AllowCreate="true"/>
</samlp:AuthnRequest>
```

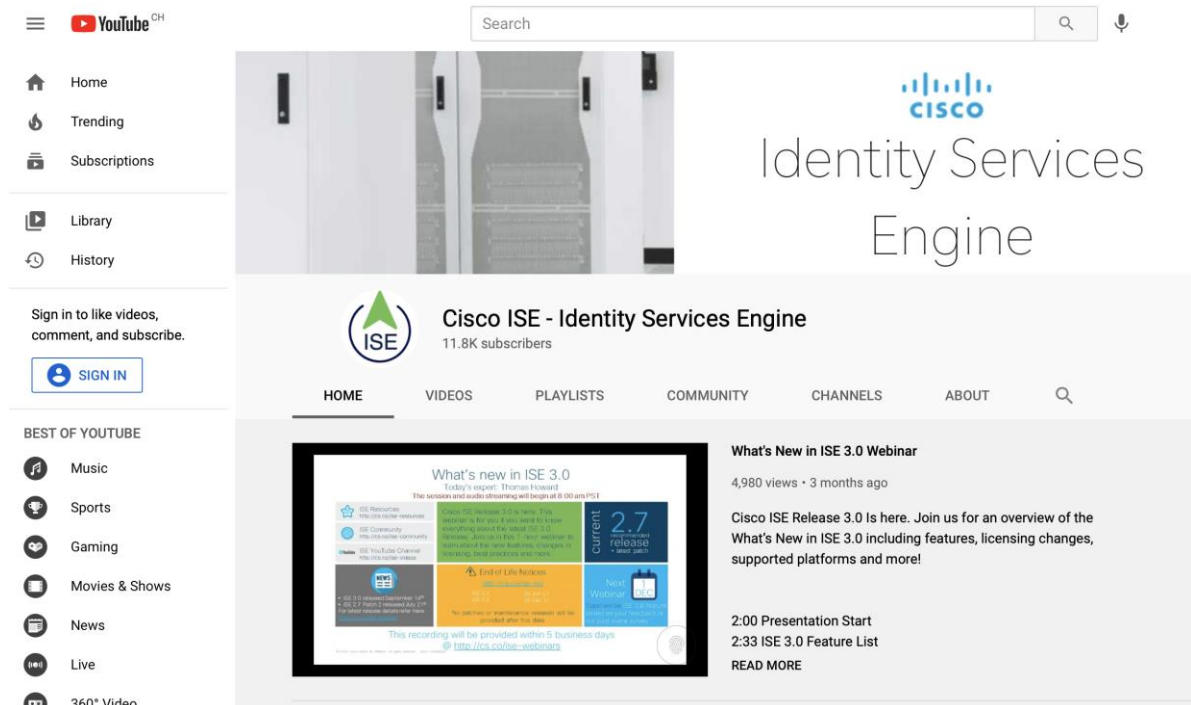

References on today's topic

- Configure ISE 3.0 REST ID with Azure Active Directory

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/216182-configure-ise-3-0-rest-id-with-azure-act.html>

- ISE Youtube channel : What's New in ISE 3.0 Webinar

https://www.youtube.com/watch?v=92ncCo3_M84

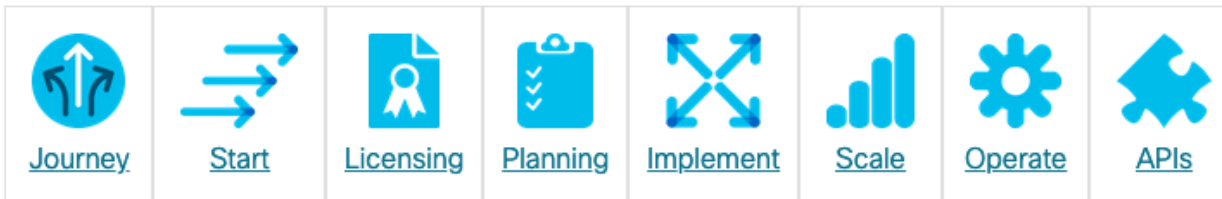


The screenshot shows the YouTube channel page for 'Cisco ISE - Identity Services Engine'. The channel has 11.8K subscribers. The main video featured is 'What's New in ISE 3.0 Webinar', which has 4,980 views and was posted 3 months ago. The video description states: 'Cisco ISE Release 3.0 Is here. Join us for an overview of the What's New in ISE 3.0 including features, licensing changes, supported platforms and more!'. The video is scheduled to start at 2:00 PM and includes a 2:33 ISE 3.0 Feature List. A 'READ MORE' link is provided. The channel navigation menu includes Home, Videos, Playlists, Community, Channels, and About. The 'BEST OF YOUTUBE' sidebar lists categories like Music, Sports, Gaming, Movies & Shows, News, Live, and 360° Video.

ISE Community Resources

 <http://cs.co/ise-resources>

 <http://cs.co/ise-community>



YouTube Channel: <http://cs.co/ise-videos>

Evaluations: <http://cs.co/ise-eval>

Integration Guides: <http://cs.co/ise-guides>

Compatibility Guides: <http://cs.co/ise-compatibility>

Licensing Guide: <http://cs.co/ise-licensing>


[ISE 3.0 License FAQ](#)

[ISE 3.0 License Migration Guide](#)

ISE & NAC Community Resources

Labels: [AAA](#) [Identity Services Engine \(...\)](#) [Policy and Access](#)
[TrustSec](#) [VPN](#)

125862 VIEWS  105 HELPFUL  0 COMMENTS

 thomas

11-13-2015 03:48 PM
Edited On: 09-21-2020 04:11 PM



- June 16: [Announcing ISE 2.7 as Recommended Release](#)
- February 27: ISE Awarded [Best NAC Solution in the SC 2020 Awards](#)
- Register for the monthly [ISE Webinars](#) to learn about ISE configuration and deployment.



Journey



Start



Licensing



Planning



Implement



Scale



Operate



APIs



Device Administration



Guest & Secure WiFi



Asset Visibility



Bring Your Own Device (BYOD)



Secure Wired Access



Segmentation



Compliance



Integrations



Threat Containment

Start

Get Started with ISE!

Cisco ISE YouTube Channel

<http://cs.co/ise-videos>

The image shows a screenshot of the Cisco ISE YouTube channel page. At the top, there is a navigation bar with the YouTube logo, a search bar, and icons for home, trending, subscriptions, and library. The main header features a large banner with the Cisco logo and the text "Identity Services Engine". Below the banner, the channel name "Cisco ISE - Identity Services Engine" is displayed, along with "10.9K subscribers" and a "SUBSCRIBED" button. The channel's navigation menu includes "HOME", "VIDEOS", "PLAYLISTS", "COMMUNITY", "CHANNELS", and "ABOUT". The "Latest Videos" section shows four video thumbnails with their titles and durations: "ISE 3.0 Agentless Posture Overview" (7:02), "ISE 3.0 Agentless Posture Demo" (9:01), "ISE 3.0 Agentless Posture Failure Scenarios" (6:33), and "Troubleshooting your Identity Services Engine..." (1:11:31). On the right side, there is a "FEATURED CHANNELS" section with links to "Cisco", "Cisco Software Define...", and "Cisco EN Programmab...".

Cisco Secure Products



<https://cisco.com/go/secure-names>

Light Background



Access



Cloud Analytics



Data Lake



Email



Endpoint



Firewall



Malware



Network Access



Network Analytics



VPN



Web



Workload

Dark Background



Access



Cloud Analytics



Data Lake



Email



Endpoint



Firewall



Malware



Network Access



Network Analytics



VPN



Web



Workload



Dissipez vos
doutes



Utilisez le panneau « Q&R » pour poser
vos questions

Cisco Community – Demandez-moi ...



Avez-vous encore des questions sur l'intégration Microsoft Azure /AD avec Cisco ISE ?

Foire aux Questions
jusqu'au vendredi 12 mars

avec Jean Francois Pujol

Événement public

Suivez le lien

<https://bit.ly/AMA-mar21>

Ask Me Anything | Sécurité
Demandez-moi n'importe quoi !

 **Posez une Question** >>

9 - 12 MAR
Jean François Pujol

Demandez-moi n'importe quoi
Microsoft Azure / AD :
Intégration sans heurts avec Cisco ISE

La communauté est disponible dans d'autres langues

Si vous parlez anglais, espagnol, portugais, russe, chinois ou japonais, vous pouvez participer aussi dans les autres communautés Cisco.

[Cisco Community](#)

Anglais

[Сообщество Cisco](#)

Russe

[Comunidad de Cisco](#)

Espagnol

[Comunidade da Cisco](#)

Portugais

[思科服务支持社区](#)

Chinois

[シスココミュニティ](#)

Japonais

Nous vous invitons à nous suivre dans les réseaux sociaux et à partager nos prochains événements

Cisco Community

- Facebook/CiscoSupportCommunity
- Twitter @cisco_support
- YouTube ciscosupportchannel
- LinkedIn Cisco Community
<https://www.linkedin.com/showcase/3544800/>
- Instagram ciscosupportcommunity
<https://www.instagram.com/ciscosupportcommunity/>



Votre avis nous
intéresse !



Veillez remplir le sondage qui
apparaîtra sur votre écran à la fin
de cette présentation.



Merci pour votre participation !



