

Configurez le portail d'invité ISE 2.1 avec PingFederate SAML SSO

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Aperçu d'écoulement](#)

[Écoulement prévu pour ce cas d'utilisation](#)

[Configurez](#)

[Étape 1. Préparez ISE pour utiliser un fournisseur externe d'identité SAML](#)

[Étape 2. Configurez le portail d'invité pour utiliser un fournisseur externe d'identité](#)

[Étape 3. Configurez PingFederate pour agir en tant que fournisseur d'identité pour le portail d'invité ISE](#)

[Étape 4. Importez les métadonnées d'IDP dans le profil externe de fournisseur d'IDP ISE SAML](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer la version 2.1 du Logiciel Cisco Identity Services Engine (ISE) afin de fournir des capacités simples d'On(SSO) de signe pour les utilisateurs portaux d'invité par le langage de balisage d'assertion de Sécurité (SAML).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Services d'invité de Logiciel Cisco Identity Services Engine.
- Connaissance de base au sujet de SAML SSO.

[Composants utilisés](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 2.1 de Logiciel Cisco Identity Services Engine
- Serveur de PingFederate 8.1.3.0 d'identité de ping comme identité Provider(IdP) SAML

Les informations contenues dans ce document ont été créées à partir des périphériques d'un

environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle configuration appliquée.

Aperçu d'écoulement

Le SAML est une norme de XML pour permuter des données d'authentification et d'autorisation entre les domaines de sécurité.

La spécification SAML définit trois rôles : le directeur (utilisateur d'invité), le fournisseur d'identité [IDP] (serveur fédéré d'IPing), et le fournisseur de services [fournisseur de services] (ISE).

Dans un SAML typique SSO circulent, le fournisseur de services demande et obtient une assertion d'identité à l'IDP. Basé sur ce résultat, ISE peut exécuter des décisions politiques pendant que l'IDP peut inclure des attributs configurables qu'ISE peut l'utiliser (c.-à-d. groupe et adresse e-mail associés à l'objet d'AD).

Écoulement prévu pour ce cas d'utilisation

1. Le commutateur d'accès Sans fil du contrôleur LAN (WLC) ou Est configuré pour un écoulement central typique de l'authentification Web (CWA).

Conseil : Trouvez les exemples de configuration pour des écoulements CWA dans la section Informations connexes au bas de l'article.

2. Le client se connecte et la session obtient authentifié contre ISE. L'accès au réseau Device(NAD) applique les paires de valeur d'attributs de réorientation (AVPs) retournées par ISE (l'URL-réorienter-acl et URL-réorientent).
3. Le client ouvre le navigateur, génère le trafic de HTTP ou HTTPS, et l'obtient réorienté au portail de l'invité d'ISE.
4. Une fois dans le portail le client pourra entrer dans les qualifications précédemment assignées d'invité (**sponsor créé**) et l'auto-disposition un nouveau compte d'invité ou employer ses qualifications d'AD pour ouvrir une session (**procédure de connexion des employés**) qui fournira simple se connectent des capacités par le SAML.
5. Une fois que l'utilisateur sélectionne l'option de la « procédure de connexion des employés », l'ISE vérifie s'il y a une assertion active associée à la session du navigateur de ce client contre l'IDP. S'il n'y a aucune session active, l'IDP imposera l'ouverture de session utilisateur. À cette étape l'utilisateur sera incité à entrer dans des qualifications d'AD dans le portail d'IDP directement.
6. L'IDP authentifie l'utilisateur par l'intermédiaire du LDAP et il crée une nouvelle assertion qui restera active pendant un temps configurable.

Note: Le ping fédéré par défaut applique une **Session Timeout de 60 minutes** (ceci signifie que s'il n'y a aucune demande de procédure de connexion SSO d'ISE en 60 minutes après l'authentification initiale la session est supprimée) et un **délai d'attente maximum de session de 480 minutes** (même si l'IDP a reçu des demandes constantes de procédure de connexion

SSO d'ISE pour cet utilisateur que la session expirera en 8 heures).

Tant que la session d'assertion est encore en activité, l'employé éprouvera SSO quand il utilise le portail d'invité. Une fois les temps de session, une nouvelle authentification de l'utilisateur sera imposée par l'IDP.

Configurez

Cette section discute les étapes de configuration pour intégrer ISE avec le ping fédéré et comment activer le navigateur SSO pour le portail d'invité.

Note: Bien que les diverses options et possibilités existent quand vous authentifiez des utilisateurs d'invité, non toutes les combinaisons sont décrites dans ce document. Cependant, cet exemple te fournit les informations nécessaires pour comprendre comment modifier l'exemple à la configuration précise que vous voulez réaliser.

Étape 1. Préparez ISE pour utiliser un fournisseur externe d'identité SAML

1. Sur Cisco ISE, choisissez la **gestion > la Gestion de l'identité > des sources extérieures d'identité > des fournisseurs d'id SAML**.
2. Cliquez sur **Add**.
3. Sous l'onglet de **General**, écrivez un **nom de fournisseur d'id**. Cliquez sur **Save**. Le reste de la configuration dans cette section dépend des métadonnées qui doit être importée de l'IDP dans les étapes postérieures.

Étape 2. Configurez le portail d'invité pour utiliser un fournisseur externe d'identité

1. Choisissez les **centres > l'accès invité de travail > configurent > des portails d'invité**.
2. Créez un nouveau portail et choisissez le **portail Auto-enregistré d'invité**.

Note: Ce ne sera pas le portail principal ce l'expérience utilisateur mais un subportail qui interagira avec l'IDP afin de vérifier l'état de session. Ce portail s'appelle SSOSubPortal.

3. Développez les **configurations portales** et choisissez **PingFederate** pour la **méthode d'authentification**.

4. **De l'ordre de source d'identité**, choisissez le **defined(PingFederate)** externe d'IDP SAML précédemment.

5. Développez les sections de **mises en page de bannière d'Acceptable Use Policy(AUP)** et de **POST-procédure de connexion** et désactivez chacun des deux.

L'écoulement portail est :

6. Sauvegardez les modifications.

7. Retournez aux portails d'invité et créez un neuf utilisant l'option **Auto-enregistrée de portail d'invité**.

Note: Ce sera le visible portail primaire au client. Le portail primaire utilisera le SSOSubportal comme interface entre ISE et l'IDP. Ce portail s'appelle PrimaryPortal.

8. Développez les **mis en page de procédure de connexion** et choisissez le **SSOSubPortal** précédemment créé sous « **permettent le portail suivant d'invité d'identité-fournisseur à utiliser pour la procédure de connexion** ».

9. Développez les **mis en page de bannière AUP et de POST-procédure de connexion de Politique d'Utilisation Acceptable** et décochez-les.

En ce moment l'écoulement portail devrait ressembler à ceci :

10. Choisissez la **personnalisation portails > les pages > la procédure de connexion**. Vous devriez maintenant avoir l'option de personnaliser les **options alternatives de procédure de connexion** (icône, texte, et ainsi de suite).

Note: Notez cela du côté droit, sous l'aperçu portail, l'option supplémentaire de procédure de connexion est visible.

11. Cliquez sur **Save**.

Maintenant les deux portails apparaissent sous la liste portails d'invité.

Étape 3. Configurez PingFederate pour agir en tant que fournisseur d'identité pour le portail d'invité ISE

1. Dans ISE, choisissez la **gestion > la Gestion de l'identité > des sources extérieures d'identité > des fournisseurs > PingFederate d'id SAML** et cliquez sur les **informations de fournisseur de services**.

2. Sous les **informations de fournisseur de services d'exportation, exportation de clic**.

3. Sauvegardez et extrayez le fichier zip généré. Le fichier XML contenu ici est utilisé pour créer le profil dans PingFederate dans les étapes postérieures.

Note: À partir de là, ce document couvre la configuration de PingFederate. Cette configuration est même pour de plusieurs solutions comme le portail de sponsor, le MyDevices, et les portails BYOD. (Ces solutions ne sont pas couvertes en cet article).

4. Ouvrez le portail d'admin de PingFederate (typiquement <https://ip:9999/pingfederate/app>).

5. Sous l'onglet de **configuration d'IDP > les connexions de fournisseur de services que la section choisissent créez nouveau**.

6. Sous le **type de connexion**, cliquez sur Next.

7. Sous des **possibilités de connexion**, cliquez sur Next.

8. Sous des **métadonnées d'importation**, cliquez sur la case d'option de **fichier**, le clic a choisi le **fichier** et choisit le fichier XML précédemment exporté d'ISE.

le résumé des métadonnées 9. Under, cliquent sur Next.

10. On la page des informations générales, sous le nom de la connexion, écrivent un nom (tel qu'ISEGuestWebAuth) et cliquent sur Next.

11. Sous le **navigateur SSO**, cliquez sur Configure le **navigateur SSO** et sous le **SAML les profils** vérifient les options et cliquent sur Next.

la vie de l'assertion 12. On cliquent sur Next.

la création de l'assertion 13. On cliquent sur Configure la **création d'assertion**.

le mappage de l'identité 14. Under choisissent la **norme** et cliquent sur Next.

15. Sur le **contrat d'attribut > étendez le contrat** écrivent la **messagerie d'attributs** et le **memberOf** et le clic **ajoutent**. Cliquez sur **Next** (Suivant).

La configuration de cette option permet au fournisseur d'identité pour passer le **MemberOf** et **pour envoyer des** attributs fournis par le Répertoire actif à ISE, qu'ISE peut utiliser plus tard comme condition pendant la décision politique.

exemple d'adaptateur de carte de clic de mappage de source de l'authentification 16. Under **nouvel**.

l'exemple de l'adaptateur 17. On choisissent l'**adaptateur de formulaire HTML**. Cliquez sur Next

18. Sous le **mappage les méthodes** choisissent la deuxième option vers le bas et cliquent sur Next.

19. Sur l'**attribut les sources et la consultation d'utilisateur** cliquent sur Add la **case de source d'attribut**.

20. Sous le **magasin de données** écrivez une description, et choisissez l'exemple de connexion de LDAP du **magasin de données actif** et définissez quel type de service d'annuaire c'est. S'il n'y a aucun **magasin de données** configuré pourtant le clic **parviennent des magasins de données** afin d'ajouter le nouveau citent.

21. Sous la **recherche de répertoire LDAP** définissez le **DN de base** pour la consultation d'utilisateur de LDAP dans le domaine et cliquez sur Next.

Note: C'est important car il définira le DN de base pendant la consultation d'utilisateur de LDAP. Un DN de base inexactement défini aura comme conséquence l'objet non trouvé dans le schéma de LDAP.

le filtre du LDAP 22. Under ajoutent la chaîne **sAMAccountName=\$ {nom d'utilisateur}** et cliquent sur Next.

23. Sous l'**exécution de contrat d'attribut** choisissez les options données et cliquez sur Next.

24. Vérifiez la configuration à la partie récapitulative et cliquez sur **fait**.
25. De retour dans l'**attribut la consultation de sources et d'utilisateur** cliquent sur Next.
26. Sous la **source de sécurité d'attribut** cliquez sur Next.
27. Sous l'**exécution de contrat d'attribut** choisissez ces options et cliquez sur Next.
28. Vérifiez la section et le clic de configuration en résumé **faits**.
29. De retour sur le **mappage de source d'authentification** cliquez sur Next.
30. Une fois que la configuration a été vérifiée sous le clic de page **récapitulative fait**.
31. De retour sur la **création d'assertion** cliquez sur Next.
32. Sous des **configurations de Protocol**, cliquez sur Configure les **configurations de Protocol**. En ce moment il devrait y avoir deux entrées déjà remplies. Cliquez sur **Next** (Suivant).
33. Sous SLO entretenez l'URLs cliquent sur Next.
34. Sur les attaches permises SAML, décochez les options OBJET FAÇONNÉ et SAVON et cliquez sur Next.
35. Dans le cadre de la stratégie de signature cliquez sur Next.
36. Dans le cadre de la stratégie de chiffrement cliquez sur Next.
37. Passez en revue la configuration dans la page récapitulative et cliquez sur **fait**.
38. De retour sur le navigateur les configurations SSO > de Protocol cliquent sur Next, valident la configuration, et cliquent sur **fait**.
39. L'onglet du navigateur SSO apparaît. Cliquez sur **Next** (Suivant).
40. Sous des **qualifications** cliquez sur Configure les **qualifications** et choisissez le certificat de signature à utiliser pendant l'IDP à la transmission ISE et vérifiez l'option **incluent le certificat dans la signature**. Cliquez ensuite sur **Next**.

Note: S'il n'y a aucun clic configuré par Certificats **gérez les Certificats** et suivez les demandes afin de générer un **certificat Auto-signé** à utiliser pour signer l'IDP aux transmissions ISE.

41. Validez la configuration sous la page récapitulative et cliquez sur **fait**.
42. De retour sur l'onglet de **qualifications** cliquez sur Next.
43. Sous le **lancement et le résumé** choisissez l'**ACTIVE d'état de la connexion**, validez le reste de la configuration, et cliquez sur **fait**.

Étape 4. Importez les métadonnées d'IDP dans le profil externe de fournisseur

d'IDP ISE SAML

1. Sous la console de gestion de PingFederate, choisissez la **configuration du serveur > les fonctions d'administration > l'exportation de métadonnées**. Si le serveur a été configuré pour de plusieurs rôles (IDP et fournisseur de services), choisissez l'option que **je suis l'identité Provider(IdP)**. Cliquez sur **Next** (Suivant).
2. Sous les **informations choisies** choisissez de mode de **métadonnées « à inclure dans les métadonnées manuellement »**. Cliquez sur **Next** (Suivant).
3. Sous **Protocol** cliquez sur Next.
4. Sur le **contrat d'attribut** cliquez sur Next.
5. Sous la **clé de signature** choisissez le certificat précédemment configuré sur le profil de connexion. Cliquez sur **Next** (Suivant).
6. Sous la **signature de métadonnées** choisissez le certificat de signature et le contrôle **incluent la clé publique de ce certificat dans l'élément d'information principale**. Cliquez sur **Next** (Suivant).
7. Sous le **certificat de cryptage XML** cliquez sur Next.

Note: L'option d'imposer le cryptage ici est jusqu'à l'admin de réseau.

8. Sous l'**exportation de clic de partie récapitulative**. Sauvegardez les métadonnées classent généré et puis cliquent sur **fait**.
9. Sous ISE, choisissez à la **gestion > à la Gestion de l'identité > des sources extérieures d'identité > des fournisseurs > PingFederate d'id SAML**.
10. Cliquez sur le **config de fournisseur d'identité > parcourent** et poursuivent pour importer les métadonnées enregistrées de l'exécution d'exportation de métadonnées de PingFederate.
11. Choisissez l'onglet de **groupes**, sous l'**attribut d'adhésion à des associations** ajoutez le **memberOf** et puis cliquez sur Add

Sous le nom de **dans l'assertion** ajoutez le nom unique que l'**IDP** devrait renvoyer quand l'attribut de **memberOf** est authentification récupérée de la forme LDAP. Dans ce cas le groupe configuré est lié au groupe de sponsor du MASSIF DE ROCHE et le DN pour ce groupe est comme suit :

Une fois que vous ajoutez le DN et le « nom description dans ISE » cliquent sur OK.

12. Choisissez l'onglet d'**attributs** et cliquez sur Add.

À cette étape, ajoutez l'attribut « messagerie » qu'est contenu dans le jeton SAML passé de l'IDP qui a basé sur la requête du ping au-dessus du LDAP, il devrait contenir l'attribut d'email pour cet objet.

Note: Étapes 11 et 12 s'assurent qu'ISE reçoit l'email d'objet d'AD et des attributs de MemberOf par l'IDP ouvrent une session l'action.

Vérifiez

1. Lancez le portail d'invité utilisant l'URL portail de test ou en suivant les CWA circulent. L'utilisateur aura les options d'entrer dans des qualifications d'invité, crée leur compte personnel, et procédure de connexion des employés.
2. **Procédure de connexion des employés de clic.** Puisqu'il n'y a aucune session active l'utilisateur sera réorienté au portail de procédure de connexion d'IDP.
3. Entrez dans les qualifications d'AD et le clic **se connectent**.
4. L'écran de connexion d'IDP réorientera l'utilisateur à la page portails de succès d'invité.
5. En ce moment, chaque fois que l'utilisateur revient à l'invité portail et choisit la « **procédure de connexion des employés** » on leur permettra dans le réseau tant que la session est encore en activité dans l'IDP.

Dépannez

N'importe quelle question d'authentification SAML sont enregistré sous ise-psc.log. Il y a un composant dédié (SAML) sous la **gestion > se connectant > configuration de log de debug > sélectionnent le noeud en question >** a placé le SAML composant **pour mettre au point de niveau.**

Vous pouvez accéder à ISE par le CLI et entrer dans la **queue d'ise-psc.log d'application de show logging de** commande et surveiller les événements SAML, ou vous pouvez télécharger ise-psc.log pour l'analyse approfondie sous des **exécutions > dépannez > des logs de téléchargement > sélectionnez l'onglet de logs de noeud > de debug ISE > le clic ise-psc.log** pour télécharger les logs.

```
2016-06-27 16:15:39,366 DEBUG [http-bio-14.36.157.210-8443-exec-3][  
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAMLUtils::isOracle() - checking whether IDP URL  
indicates that its OAM. IDP URL: https://14.36.147.1:9031/idp/sso.saml2  
2016-06-27 16:15:39,366 DEBUG [http-bio-14.36.157.210-8443-exec-3][  
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SPProviderId for PingFederate is: http://CiscoISE  
/5b4c0780-2da2-11e6-a5e2-005056a15f11  
2016-06-27 16:15:39,366 DEBUG [http-bio-14.36.157.210-8443-exec-3][  
cpm.saml.framework.impl.SAMLFacadeImpl -::::- ResponseValidationContext:  
    IdP URI: PingFederate  
    SP URI: http://CiscoISE/5b4c0780-2da2-11e6-a5e2-005056a15f11  
    Assertion Consumer URL: https://14.36.157.210:8443/portal/SSOLoginResponse.action  
    Request Id: _5b4c0780-2da2-11e6-a5e2-005056a15f11_DELIMITERportalId_EQUALS5b4c0780-2da2-  
11e6-a5e2-005056a15f11_SEMIportalSessionId_EQUALS309f733a-99d0-4c83-8  
b99-2ef6b76c1d4b_SEMI_DELIMITER14.36.157.210  
    Client Address: 14.0.25.62  
    Load Balancer: null  
2016-06-27 16:15:39,366 DEBUG [http-bio-14.36.157.210-8443-exec-3][  
cpm.saml.framework.validators.BaseSignatureValidator -::::- Determine the signing certificate  
2016-06-27 16:15:39,366 DEBUG [http-bio-14.36.157.210-8443-exec-3][  
cpm.saml.framework.validators.BaseSignatureValidator -::::- Validate signature to SAML standard  
with cert:CN=14.36.147.1, OU=TAC, O=Cisco, L=RTP, C=US serial:1465409531352  
2016-06-27 16:15:39,367 DEBUG [http-bio-14.36.157.210-8443-exec-3][  
org.opensaml.xml.signature.SignatureValidator -::::- Creating XMLSignature object  
2016-06-27 16:15:39,367 DEBUG [http-bio-14.36.157.210-8443-exec-3][  
org.opensaml.xml.signature.SignatureValidator -::::- Validating signature with signature
```



```
algorithm URI: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
2016-06-27 16:15:39,368 DEBUG [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.SAMLSignatureValidator -:::- Assertion signature validated
succesfully
2016-06-27 16:15:39,368 DEBUG [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.WebSSOResponseValidator -:::- Validating response
2016-06-27 16:15:39,368 DEBUG [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.WebSSOResponseValidator -:::- Validating assertion
2016-06-27 16:15:39,368 DEBUG [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.AssertionValidator -:::- Assertion issuer succesfully validated
2016-06-27 16:15:39,368 DEBUG [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.AssertionValidator -:::- Subject succesfully validated
2016-06-27 16:15:39,368 DEBUG [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.AssertionValidator -:::- Conditions succesfully validated
2016-06-27 16:15:39,368 DEBUG [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAML Response: validation succeeded for guest
IDPResponse
:
    IdP ID: PingFederate
    Subject: guest
    SAML Status Code:urn:oasis:names:tc:SAML:2.0:status:Success
    SAML Success:true
    SAML Status Message:null
    SAML email:guest@rtpaaa.net
    SAML Exception:null
2016-06-27 16:15:39,368 DEBUG [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- AuthenticatePortalUser - about to call
authenticateSAMLUser messageCode:null subject:guest
2016-06-27 16:15:39,375 DEBUG [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::- Authenticate SAML User - result:PASSED
```

[Informations connexes](#)

- [Authentification Web centrale avec le Cisco WLC et l'exemple de configuration ISE.](#)
- [Authentification Web centrale avec un exemple de configuration de commutateur et de Cisco Identity Services Engine.](#)
- [Notes en version pour le Logiciel Cisco Identity Services Engine, version 2.1](#)
- [Guide de l'administrateur de Logiciel Cisco Identity Services Engine, version 2.1](#)