Configuration et dépannage de SSO pour les agents et l'administrateur de partition dans ECE

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Informations générales
Configuration Steps
Configuration de l'approbation de partie de confiance pour ECE
Configuration d'un fournisseur d'identités
Création et importation de certificats
Configuration de l'authentification unique de l'agent
Définir l'URL du serveur Web/LB dans les paramètres de partition
Configuration de SSO pour les administrateurs de partition
<u>Dépannage</u>
Définition du niveau de suivi
Scénario de dépannage 1
<u>Erreur</u>
Analyse des journaux
Résolution
Scénario de dépannage 2
<u>Erreur</u>
Analyse des journaux
<u>Résolution</u>
Scénario de dépannage 3
Erreur_
Analyse des journaux
Résolution
Informations connexes

Introduction

Ce document décrit les étapes requises pour configurer l'authentification unique (SSO) pour les agents et les administrateurs de partition dans une solution ECE.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

Cisco Packaged Contact Center Enterprise (PCCE)

Cisco Unified Contact Center Enterprise (UCCE)

Chat et e-mail d'entreprise (ECE)

Microsoft Active Directory

Composants utilisés

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

Version UCCE : 12.6(1)

Version ECE : 12.6(1)

Service de fédération Microsoft Active Directory (ADFS) sur Windows Server 2016

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Les consoles de messagerie instantanée et de messagerie d'entreprise (ECE) sont accessibles en dehors de Finesse. Toutefois, l'authentification unique doit être activée pour permettre aux agents et aux superviseurs de se connecter à ECE via Finesse.

L'authentification unique peut également être configurée pour les nouveaux administrateurs de partition. Cela garantit que les nouveaux utilisateurs qui se connectent au bureau Administrateur Cisco ont accès à la console d'administration de messagerie et de conversation d'entreprise.

Points importants à noter à propos de l'authentification unique :

- Le processus de configuration d'un système pour l'authentification unique doit être effectué sur le noeud Sécurité au niveau de la partition par un utilisateur de partition avec les actions nécessaires : Afficher la sécurité des applications et Gérer la sécurité des applications.
- Pour que les superviseurs et les administrateurs puissent se connecter aux consoles autres que la console de l'agent, une fois l'authentification unique activée, vous devez fournir une URL externe valide de l'application dans les paramètres de partition. Voir Paramètres généraux de partition pour plus d'informations.
- Un certificat Java Keystore (JKS) est nécessaire pour configurer SSO afin de permettre aux utilisateurs ayant des rôles d'administrateur ou de superviseur de se connecter à la partition 1 d'ECE en dehors de Finesse à l'aide de leurs identifiants de connexion SSO. Consultez votre service informatique pour recevoir le certificat JKS.

- Un certificat SSL (Secure Sockets Layer) de Cisco IDS doit être importé sur tous les serveurs d'applications d'une installation. Pour obtenir le fichier de certificat SSL nécessaire, contactez votre service informatique ou l'assistance Cisco IDS.
- Le classement des serveurs de base de données pour Unified CCE est sensible à la casse. Le nom d'utilisateur dans la revendication retournée à partir de l'URL du point de terminaison des informations utilisateur et le nom d'utilisateur dans Unified CCE doivent être identiques. S'ils ne sont pas identiques, les agents SSO ne sont pas reconnus comme connectés et ECE ne peut pas envoyer la disponibilité des agents à Unified CCE.
- La configuration de SSO pour Cisco IDS affecte les utilisateurs qui ont été configurés dans Unified CCE pour l'authentification unique. Assurez-vous que les utilisateurs que vous souhaitez activer pour l'authentification unique dans ECE sont configurés pour l'authentification unique dans Unified CCE. Pour plus d'informations, consultez votre administrateur Unified CCE.



Remarque :

• Assurez-vous que les utilisateurs que vous souhaitez activer pour l'authentification unique dans ECE sont configurés pour l'authentification unique dans Unified CCE.

- Ce document spécifie les étapes à suivre pour configurer l'approbation de partie de confiance pour ECE dans un déploiement AD FS unique où le serveur de fédération de ressources et le serveur de fédération de comptes sont installés sur le même ordinateur.
- Pour un déploiement AD FS divisé, accédez au guide d'installation et de configuration ECE correspondant à la version correspondante.

Configuration Steps

Configuration de l'approbation de partie de confiance pour ECE

Étape 1

Ouvrez la console de gestion AD FS et accédez à AD FS > Relations d'approbation > Approbation de la partie de confiance.

Étape 2

Dans la section Actions, cliquez sur Ajouter une approbation de partie de confiance...

N AD FS				-	• x
🗌 File Action View Window Help					_ 8 ×
🗢 🔿 🗾 🖬 🖬					
AD FS	Relying Party Trusts			Actions	
> Service	Display Name	Enabled Type	Identifier	Relying Party Trusts	•
Relying Party Trusts				Add Relying Party Trust	
Claims Provider Trusts				View	•
Application Groups				New Window from Here	
				Refresh	
				7 Help	

Étape 3

Dans l'Assistant Ajouter une approbation de partie de confiance, cliquez sur Démarrer et effectuez les étapes suivantes :

a. Dans la page Sélectionner une source de données, sélectionnez l'option Saisir manuellement des données sur la partie à répondre et cliquez sur Suivant.

Select Data Source		
Steps	Select an option that this wizard will use to obtain data about this relving party:	
Welcome		
Select Data Source	Use this option to import the necessary data and certificates from a relying party organization that out	lishes
Specify Display Name	its federation metadata online or on a local network.	illarioa
Configure Certificate	Federation metadata address (host name or URL):	
Configure URL		
Configure Identifiers	Example: fs.contoso.com or https://www.contoso.com/app	
 Choose Access Control Policy Ready to Add Trust Finish 	 Import data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard with validate the source of the file. Federation metadata file location: Brows Inter data about the relying party manually Use this option to manually input the necessary data about this relying party organization. 	e
	< Previous Next > Cano	el

b. Dans la page Spécifier le nom d'affichage, indiquez le nom d'affichage de la partie de confiance. Cliquez sur Next (suivant).

🐐 Add Relying Party Trust W	izard	x
Specify Display Name		
Steps	Enter the display name and any optional notes for this relying party.	
Welcome	Display name:	
Select Data Source	ECE Console	
Specify Display Name	Notes:	
Configure Certificate	ECE 12.6.1	
Configure URL		
Configure Identifiers		
 Choose Access Control Policy 		~
Ready to Add Trust		
Finish		
		_
	< Previous Next > Cancel	

c. Dans la page Configurer l'URL :

i. Sélectionnez l'option Enable support for the SAML 2.0 Web SSO protocol.

ii. Dans le champ Relying Party SAML 2.0 SSO server URL, indiquez l'URL au format suivant : https://<Web-Server-Or-Load-Balancer-FQDN>/system/SAML/SSO/POST.controller

Steps AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If • Welcome WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party. • Select Data Source Enable support for the WS-Federation Passive protocol	🕸 Add Relying Party Trust W	izard X
Steps AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If Welcome WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party. Select Data Source Enable support for the WS-Federation Passive protocol	Configure URL	
● Configure Certificate The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol. ● Configure URL Relying party WS-Federation Passive protocol URL: ● Configure Identifiers	Steps Welcome Select Data Source Specify Display Name Configure Certificate Configure URL Configure Identifiers Ready to Add Trust Finish	AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Frust protocol is always enabled for a relying party. □ Enable support for the WS-Federation Passive protocol The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol URL: □ Example: https://fs.contoso.com/adfs/ls/ □ Enable support for the SAML 2.0 WebSSO protocol The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol. Relying party SAML 2.0 SSO service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol. Relying party SAML 2.0 SSO service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol. Relying party SAML 2.0 SSO service URL: https://ece126web1a.jo123.local/system/SAML/SSO/POST.controller] Example: https://www.contoso.com/adfs/ls/

d. Dans la page Configurer les identificateurs, indiquez l'identificateur d'approbation de la partie de confiance et cliquez sur Ajouter.

• La valeur doit être au format : https://<Web-Server-Or-Load-Balancer-FQDN>/

؋ Add Relying Party Trust Wi	zard	x
Configure Identifiers		
Steps Welcome	Relying parties may be identified by one or more unique identifier strings. Specify the identifier party trust.	s for this relying
Select Data Source	Relying party trust identifier:	
Specify Display Name	https://ece126web1a.jo123.local/	Add
Configure Certificate	Example: https://fs.contoso.com/adfs/services/trust	
Configure URL	Relying party trust identifiers:	
Configure Identifiers		Remove
 Choose Access Control Policy 		
Ready to Add Trust		
😑 Finish		
	< Previous Next >	Cancel

e. Dans la page Choisir une stratégie de contrôle d'accès, cliquez sur Suivant avec la valeur par défaut « Autoriser tout le monde ».

🐐 Add Relying Party Trust W	izard	x	c
Choose Access Contro	l Policy		
Steps	Choose an access control policy:	-	1
 Welcome Select Data Source Specify Display Name Configure Certificate Configure URL Configure Identifiers Choose Access Control Policy Ready to Add Trust Finish 	Name Permit everyone Permit everyone and require MFA Permit everyone and require MFA for specific group Permit everyone and require MFA from unauthenticated devices Permit everyone and require MFA, allow automatic device registr Permit everyone for intranet access Permit specific group ✓ III Policy Permit everyone III Policy III Policy III	Description Grant access to everyone. Grant access to everyone and require M Grant access to everyone and require M Grant access to the intranet users and re Grant access to everyone and require M Grant access to the intranet users. Grant access to users of one or more spone Solution of the intranet users of the or more spone Solution of the intranet users of the or more spone Solution of the intranet users of the or more spone Grant access to users of one or more spone Solution of the intranet users of the or more spone Solution of the intranet users of the intranet users of the or more spone Grant access to users of one or more spone Solution of the intranet users of the intranet users. Grant access to users of one or more spone Solution of the intranet users of the intranet users of the intranet users of the intranet users. Grant access to users of one or more spone Solution of the intranet users of the intrane	
	< Prev	rious Next > Cancel	

f. Dans la page Prêt à ajouter l'approbation, cliquez sur Suivant.

🐴 Add Relying Party Trust Wiz	ard							x
Ready to Add Trust								
Steps Welcome Select Data Source Specify Display Name Configure Cettificate Configure URL Configure Identifiers Choose Access Control Policy Ready to Add Trust Finish	The relying party to relying party to Specify the Relying p Monit Au This re < neve This re < neve	arty trust has ust to the A Identifiers monitoring s arty's federa or relying pa tomatically lying party's lying party v r >	been config D FS configu Encryption ettings for thi ation metadata rty update relying federation me vas last updat	ured. Review ration databa Signature s relying part a URL: g party etadata data red from fede	w the following settin ase. Accepted Claims y trust.	on:	Endpoints	add the
					< Previo	us Nex	d >	Cancel

g. Une fois l'approbation de la partie de confiance ajoutée, cliquez sur Fermer.

🐐 Add Relying Party Trust W	fizard	x
Finish		
Steps Welcome Select Data Source Specify Display Name Configure Certificate Configure URL Configure Identifiers Choose Access Control Policy	The relying party trust was successfully added. Configure claims issuance policy for this application	
 Ready to Add Trust Finish 		
	Close	

Dans la liste Approbations du fournisseur de confiance, sélectionnez l'approbation de la partie de confiance créée pour ECE et dans la section Actions, cliquez sur Propriétés.



Dans la fenêtre Propriétés, accédez à l'onglet Points de terminaison et cliquez sur le bouton Ajouter SAML.

ECE Console Pro	operties					×
Monitoring Organization	Identifiers Endpoints	Encryption Proxy End	Signatur Ipoints	re Acc Notes	cepted Clair Advance	ms ed
Specify the end	points to use fo	or SAML and	WS-Feder	ationPass	ive protoco	ols.
	rtion Consum	nae Der Endnoir	ex Віпа Ite	ing U	erauit	Re
https://ec	e126web1a.jo	123.1 0	POS	T N	lo	
				_		
Add SAML						
Add WS-Fede	eration		Rem	ove	Edit	
		ОК	Ca	ncel	Apply	

Dans la fenêtre Add an Endpoint, configurez comme indiqué :

- 1. Sélectionnez le type de point de terminaison Déconnexion SAML.
- 2. Spécifiez l'URL approuvée sous la forme https://<ADFS-server-FQDN>/adfs/ls/?wa=wsignoutcleanup1.0
- 3. Click OK.

Add an Endpoint

Endpoint type:		
SAML Logout	~	
Binding:		
POST	×	
Set the trusted URL	as default	
Index: 0		
Trusted URL:		
https://WIN-260MECJE	IC2.jo123.local/adfs/ls/?wa=wsignoutcleanup1	.0
Example: https://sts.com	ntoso.com/adfs/ls	
Response URL:		_
Example: https://sts.com	ntoso.com/logout	
	OK Cancel	

X

Étape 7

Dans la liste Fiducies de fournisseur de confiance, sélectionnez l'approbation créée pour ECE, et dans la section Actions cliquez sur Modifier la police d'assurance de demande.



Dans la fenêtre Modifier une police d'assurance de sinistre, sous l'onglet Règles de transformation d'émission, cliquez sur le bouton Ajouter une règle... et configurez comme indiqué :

a. Dans la page Choisir un type de règle, sélectionnez Envoyer les attributs LDAP en tant que revendications dans la liste déroulante, puis cliquez sur Suivant.

Edit Claim Issuance Policy for ECE Console	×	
Issuance Transform Rules		
The following transform rules specify the claims that will be sent to the relying part	ty.	
Order Rule Name Issued Claims		
	Ndd Transform Claim R	ule Wizard X
	Select Rule Template	9
	Steps	Select the template for the claim rule that you want to create from the following list. The description provides
	Choose Rule Type	details about each claim rule template.
	 Configure Claim Rule 	Claim rule template:
		Send LDAP Attributes as Claims
		Claim rule template description:
		Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.
Add Rule Edit Rule Remove Rule		
OK Cancel		
		< Previous Next > Cancel

- b. Sur la page Configurer la règle de revendication :
 - 1. Fournissez le nom de la règle de revendication et sélectionnez le magasin d'attributs.
 - 2. Définissez le mappage de l'attribut LDAP et du type de revendication sortante.
 - Sélectionnez Name ID comme nom de type de revendication sortante.
 - Cliquez sur Terminer pour revenir à la fenêtre Modifier une police d'assurance, puis cliquez sur OK.

🏘 Add Transform Claim Rule	Wizard	x
Configure Rule		
Configure Rule Steps a Choose Rule Type b Configure Claim Rule	You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from whether the extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule. Claim rule name: Account name to Name ID Rule template: Send LDAP Attributes as Claims Attribute store: Active Directory Mapping of LDAP attributes to outgoing claim types: DAP Attribute (Select or type to add more) User-Principal-Name Name ID	iich
	< Previous Finish Cancel	

Edit Claim Issuance Policy for ECE Console				
Issuance Transform Rules				
The following transform rules specify the claims that v	vill be sent to the relying party.			
Order Rule Name	Issued Claims			
1 Account name to Name ID	Name ID			
		A		
		T		
		₽.		
Add Rule Edit Rule Remove Rule				
	OK Cancel Ap	oly		

Dans la liste Approbations du fournisseur de confiance, double-cliquez sur l'approbation de partie de confiance ECE que vous avez créée.

Dans la fenêtre Propriétés qui s'ouvre, accédez à l'onglet Avancé et définissez l'algorithme de hachage sécurisé sur SHA-1 ou SHA-256. Cliquez sur OK pour fermer la fenêtre.



Remarque : cette valeur doit correspondre à la valeur 'Algorithme de signature' définie pour le 'Fournisseur de services' sous Configurations SSO dans ECE

Relying Party Trusts				
Display Name		Enabled	Туре	Identifier
ECE Console		Yes	WS-T	https://ece126web1a.jo123.local/
ECE Console Monitoring Organization Specify the Secure has	Properties Identifiers Encryption Endpoints Proxy End e secure hash algorithm to use sh algorithm: SHA-256	Signature Ac points Notes for this relying party	cepted Cla Advanc	x ims ced
	ОК	Cancel	Apply	y

Vérifiez et notez la valeur de l'identificateur de service de fédération.

 Dans la console de gestion AD FS, sélectionnez et cliquez avec le bouton droit sur AD FS > Modifier les propriétés du service de fédération > onglet Général > Identificateur du service de fédération



Remarque :

- Cette valeur doit être ajoutée exactement telle quelle lors de la configuration de la valeur « ID d'entité » pour le fournisseur d'identité sous Configurations SSO dans ECE.
- L'utilisation de http:// ne signifie PAS qu'ADFS n'est pas sécurisé, il s'agit simplement d'un identificateur.



Federation Service Properties	x
General Organization Events	
Federation Service display name:	
JO123 ADFS	
Example: Fabrikam Federation Service	
Federation Service name:	
WIN-260MECJBIC2.jo123.local	
Example: fs.fabrikam.com	
Federation Service identifier:	
http://WIN-260MECJBIC2.jo123.local/adfs/services/trust	
Example: http://fs.fabrikam.com/adfs/services/trust	
Web SSO lifetime (minutes): 480 🗘	
Enable delegation for service administration	
Delegate name:	
Edit	
Allow Local System account for service administration	
✓ Allow Local Administrators group for service administration	
OK Cancel Apply	
Tott Carlor (Pp)	

Configuration d'un fournisseur d'identités

Étape 11

Un certificat Java Keystore (JKS) est nécessaire pour configurer l'authentification unique afin de permettre aux utilisateurs ayant des rôles d'administrateur ou de superviseur de se connecter à une partition d'ECE en dehors de Finesse à l'aide de leurs identifiants de connexion à l'authentification unique.

Si vous souhaitez configurer SSO pour permettre aux utilisateurs ayant des rôles d'administrateur ou de superviseur de se connecter à la partition d'ECE en dehors de Finesse à l'aide de leurs identifiants de connexion SSO, le certificat JKS (Java Keystore) doit être converti en certificat de clé publique et configuré dans Confiance de la partie de confiance créé sur le serveur IdP pour ECE.

Consultez votre service informatique pour recevoir le certificat JKS.



Remarque : ces étapes s'appliquent aux systèmes utilisant ADFS comme fournisseur d'identité. D'autres fournisseurs d'identité peuvent utiliser différentes méthodes pour configurer le certificat de clé publique.

Voici un exemple de la manière dont un fichier JKS a été généré dans les travaux pratiques :

a. Générez JKS :



Remarque : le mot de passe de la banque de clés, le nom d'alias et le mot de passe de clé saisis ici sont utilisés lors de la configuration de « Service Provider » sous Configurations SSO dans ECE.

C.VIIcans\administrator 70123\kavton]_gankav_kavalg RSA_alias ara126wah1a sam]_kavstore C.VIamn\ara126wah1a sam] iks_kavsiza 2048_validity 1825
Enter keystore naskword:
Re-enter new password:
What is your first and last name?
[Unknown]: ece126app1a.jo123.local
What is the name of your organizational unit?
[Unknown]: TAC
What is the name of your organization?
[Unknown]: Cisco
What is the name of your City or Locality?
[Unknown]: RTP
What is the name of your State or Province?
[Unknown]: NC
What is the two-letter country code for this unit?
[Unknown]: US
Is CN=ece126app1a.jo123.local, OU=TAC, O=Cisco, L=RTP, ST=NC, C=US correct?
[no]: yes
Enter key password for <ece126web1a_sam1></ece126web1a_sam1>
(RETURN if same as keystore password):

b. Exportez le certificat :

Cette commande keytool exporte le fichier de certificat au format .crt avec le nom de fichier ece126web1a_saml.crt dans le répertoire C:\Temp.

keytool -exportcert -alias ece126web1a_saml -keystore C:\Temp\ece126web1a_saml.jks -rfc -file C:\Temp\e

Étape 12

Configuration d'un fournisseur d'identités

- 1. Sur la console de gestion AD FS, sélectionnez et cliquez avec le bouton droit sur l'approbation de la partie de confiance créée pour ECE.
- 2. Ouvrez la fenêtre Propriétés de l'approbation et sous l'onglet Signature, cliquez sur le bouton Ajouter.
- 3. Ajoutez le certificat public (fichier .crt généré à l'étape précédente) et cliquez sur OK.

Création et importation de certificats

Étape 13

Avant de configurer SSO pour utiliser Cisco IDS pour l'authentification unique des agents, le certificat Tomcat du serveur Cisco IDS doit être importé dans l'application.

a. Dans la console ECE Admin, sous le menu au niveau de la partition, cliquez sur l'option Security, puis sélectionnez Certificate Management dans le menu de gauche.



b. Dans l'espace Gestion des certificats, cliquez sur le bouton Nouveau et entrez les détails appropriés :

- Name : saisissez un nom pour le certificat.
- Description : ajoutez une description pour le certificat.
- Component Type : sélectionnez CISCO IDS.
- Import Certificate : pour importer le certificat, cliquez sur le bouton Search and Add et entrez les détails demandés :
- Certificate file : cliquez sur le bouton Browse et sélectionnez le certificat que vous souhaitez

importer. Les certificats peuvent uniquement être importés aux formats .pem, .der (BINARY) ou .cer/cert.

- Alias Name : fournissez un alias pour votre certificat.
- c. Cliquez sur Enregistrer

Partition	~			
۹		Create Certificate		
Access Restrictions	~	Name*	Cisco IDS Server	
udit Log		Description	Certificate for Cisco IdS Serv	/er
Certificate Management		2000.19.00.0		
ORS				
ata Masking	~	Component Type*	CISCO IDS	~
ich Text Content Policy		Import Certificate	ucce1261ids.cer	
ettings				
ingle Sign-On	~			

Configuration de l'authentification unique de l'agent

Étape 14

- Dans la console d'administration ECE, sous Menu au niveau de la partition, cliquez sur l'option Security, puis sélectionnez Single Sign-On > Configurations dans le menu de gauche.
- 2. Dans la liste déroulante Select Configuration, sélectionnez Agent et définissez la configuration sous l'onglet General :
- Enable Single Sign-On : cliquez sur le bouton Toggle pour activer l'authentification unique.
- Single Sign-On Type : sélectionnez Cisco IDS.

Enterprise Cha	at and Email									A O Partition	Administrator ~
Partition ~			Apps	Departments	Integration	Language Tools	Security	Services	Storage	System Resources	Tools User
٩	Configurations										
Access Restrictions ~ Attachments	Select Configuration Agent	v									
Audit Log	General SSO Configuration										
Certificate Management											
CORS	Name*	Agent Configuration									
Data Masking 🗸 🗸		Rights Right De Dasher other for									
Rich Text Content Policy	Description	agents									
Settings Single Sign-On Configurations	Enable Single Sign-On										
Licenses	Single Sign-On Type	Cisco IDS v									
Providers											
										Cance	Save

Cliquez sur l'onglet SSO Configuration et fournissez les détails de configuration :

a. Fournisseur OpenID Connect

URL du point de terminaison des informations utilisateur principal

- URL du point de terminaison des informations utilisateur du serveur Cisco IDS principal.
- Cette URL valide l'API jeton utilisateur/Informations utilisateur.
- Il est au format : <u>https://cisco-ids-1:8553/ids/v1/oauth/userinfo</u> où cisco-ids-1 indique le nom de domaine complet (FQDN) du serveur Cisco IDS principal.

Nom de revendication d'identité utilisateur

- Nom de la revendication renvoyé par l'URL du point de terminaison Informations utilisateur, qui identifie le nom d'utilisateur dans Unified ou Packaged CCE.
- Le nom de la demande et le nom d'utilisateur dans Unified ou Packaged CCE doivent correspondre.
- Il s'agit d'une des revendications obtenues en réponse à la validation du jeton Bearer.
- Si le nom d'utilisateur des agents dans Unified ou Packaged CCE correspond au nom principal de l'utilisateur, indiquez « upn » comme valeur du champ Nom de la revendication d'identité de l'utilisateur.
- Si le nom d'utilisateur des agents dans Unified ou Packaged CCE correspond au nom du compte SAM, indiquez « sub » comme valeur du champ Nom de la revendication d'identité de l'utilisateur.

URL du point de terminaison des informations utilisateur secondaire

- URL du point de terminaison Info utilisateur secondaire du serveur Cisco IDS.
- Il est au format : <u>https://cisco-ids-2:8553/ids/v1/oauth/userinfo</u> où cisco-ids-2 indique le nom de domaine complet (FQDN) du serveur Cisco IDS secondaire.

User Info Endpoint URL Method

- Méthode HTTP utilisée par ECE pour effectuer des appels de validation de jeton Bearer vers l'URL du point de terminaison Informations utilisateur.
- Sélectionnez POST dans la liste des options présentées (POST est sélectionné ici pour correspondre à la méthode du serveur IDS).

POST : méthode utilisée pour envoyer des données au serveur Cisco IDS au point d'extrémité spécifié.

Durée du cache de jeton d'accès (secondes)

- Durée, en secondes, pendant laquelle un jeton Bearer doit être mis en cache dans ECE.
- Les jetons de support pour lesquels les appels de validation sont réussis sont uniquement stockés dans les caches. (Valeur minimale : 1 ; valeur maximale : 30)

Autoriser la connexion SSO en dehors de Finesse

- Cliquez sur ce bouton bascule si vous souhaitez autoriser les utilisateurs ayant des rôles d'administrateur ou de superviseur à se connecter à la partition d'ECE en dehors de Finesse à l'aide de leurs identifiants de connexion SSO.
- Si cette option est activée, des informations doivent être fournies dans les sections Fournisseur d'identités et Fournisseur de services.
- Cela nécessite que votre configuration IdP autorise un serveur IdP partagé.



Partition	~			
٩		Configurations		
Access Restrictions Attachments	~	Select Configuration Agent	~	
Audit Log		General SSO Configuration		
Certificate Management		OpenId Connect Provider		
Data Masking Rich Text Content Policy	~	Primary User Info Endpoint URL* https://ids-fqdn:8553/ids/v1/oauth/u		
Settings		User Identity Claim Name*	upn	
Single Sign-On Configurations	^	Secondary User Info Endpoint URL		
Licenses		User Info Endpoint URL Method* POST		
Floviders		Access Token Cache Duration (Seconds)*	30	
		Allow SSO Login Outside Finesse		

b. Fournisseur d'identité

ID entité

• ID d'entité du serveur IdP.



Remarque : cette valeur doit correspondre exactement à la valeur « Federation Service Identifier » dans la console de gestion AD FS.

Q Access Restrictions ~ Attachments ~ Audit Log Certificate Management CORS Data Masking ~ Rich Text Content Policy ~	Configurations Select Configuration Agent General SSO Configuration Identity Provider Entity ID* http://WIN-260MECJBIC2.jo123.local	Federation Service Properties × General Organization Events Federation Service deplay name:
Settings Single Sign-On	Identity Provider Certificate*BEGIN CERTIFICATEMIIC8)C User Identity Location* SAML Subject Identifier	Enable delegation for service administration Delegate name: Edt
Licenses Providers	User Identity Attribute Name* Enable Encrypted Assertion	Allow Local System account for service administration Allow Local Administrators group for service administration
	Assertion Decryption Certificate* Enter Assertion Decryption Certificate	0

Certificat du fournisseur d'identité

- Certificat de clé publique.
- Le certificat doit commencer par « -----BEGIN CERTIFICATE----- » et se terminer par « -----END CERTIFICATE----- »
- Il s'agit du certificat de signature de jeton dans la console de gestion AD FS > Service > Certificats > Signature de jeton.

Allow SSO Login Outside Finesse		AD FS	Certificates		
Identity Provider		Service Attribute Stores Authentication Methods	Subject Service communications	Issuer	Effective Date
Entity ID*	http://WIN-260MECJBIC2.jo123.local	Certificates Claim Descriptions Device Registration	Token-decrypting CN=ADFS Encryption - WIN-260MECJBIC2 jo 123 local	CN=ADFS Encryption - W	1/31/2024
Identity Provider Certificate*	BEGIN CERTIFICATEMIICBJC	Scope Descriptions	Token-signing CN=ADFS Signing - WIN-260MECJBIC2 jo 123 Jocal	CN=ADFS Signing - WIN	1/31/2024
User Identity Location*	SAML Subject Identifier	Access Control Policies Relying Party Trusts			
User Identity Attribute Name*		Application Groups			
Enable Encrypted Assertion					
Assertion Decryption Certificate*	Enter Assertion Decryption Certificate				

Emplacement de l'identité utilisateur

- Sélectionnez SAML Subject Identifier pour définir l'emplacement de l'identité dans le certificat sur l'identificateur de sujet SAML par défaut, comme dans l'objet dans l'assertion SAML, par exemple, le nom d'utilisateur dans <saml : Subject>.
- Sélectionnez Attribut SAML pour affecter l'emplacement de l'identité à un attribut spécifique dans le certificat, par exemple, email.address. Fournissez l'attribut dans le champ Nom de l'attribut d'identité de l'utilisateur.

Nom d'attribut Identité utilisateur

- Applicable uniquement lorsque la valeur Emplacement de l'ID utilisateur est un attribut SAML.
- Cela peut être ajusté dans l'assertion SAML et utilisé pour sélectionner un attribut différent pour l'authentification des utilisateurs, comme une adresse e-mail.
- Il peut également être utilisé pour créer de nouveaux utilisateurs avec un attribut SAML.
- Par exemple, si un utilisateur est identifié par la valeur fournie dans l'attribut email.address et que la valeur de l'adresse e-mail fournie ne correspond à aucun utilisateur du système, un nouvel utilisateur est créé avec les attributs SAML fournis.

Activer l'assertion chiffrée (facultatif)

- Si vous souhaitez activer l'assertion chiffrée avec le fournisseur d'identité pour la connexion à la console, cliquez sur le bouton Basculer pour définir la valeur sur Activé.
- Si ce n'est pas le cas, définissez la valeur sur Désactivé.

Certificat De Déchiffrement D'Assertion

Si Activer l'assertion chiffrée est défini sur Activé, cliquez sur le bouton Rechercher et ajouter et confirmez votre choix pour modifier le certificat.

Fournissez les détails dans la fenêtre Certificat de déchiffrement d'assertion :

- Java Keystore File : indiquez le chemin d'accès de votre fichier Java Keystore. Ce fichier est au format .jks et contient la clé de déchiffrement dont le système a besoin pour accéder aux fichiers sécurisés par le fournisseur d'identité.
- Alias Name : identifiant unique de la clé de déchiffrement.
- Keystore Password : mot de passe requis pour accéder au fichier Keystore Java.
- Key Password : mot de passe requis pour accéder à la clé de déchiffrement de l'alias.



Remarque : le certificat doit correspondre dans l'onglet « Encryption » de l'approbation de la partie de confiance ECE configurée sur la console de gestion AD FS.

c. Fournisseur de services

Authentification initiée par le fournisseur de services

• Définissez le bouton bascule sur Activé.

ID entité

• Fournir l'URL externe de l'application ECE.

Service Provider Initiated Authentication Spec	ganization Endpoints Proxy Endpoints Notes Advanced pontoring Identifiers Encryption Signature Accepted Claims ecify the display name and identifiers for this relying party trust. Encryption Signature Accepted Claims
Entity ID* https://ece126web1a.jo123.local/	Display name: ECE Console
Request Signing Certificate*	Relying party identifier: Add
Signing Algorithm* SHA-256 V	Example: https://fs.contoso.com/adfs/services/trust Relying party identifiers:
Identity Provider Login URL* https://WIN-260MECJBIC2.jo123.loc	Remove Remove
Identity Provider Logout URL https://ece126web1a.jo123.local/def	

Demander un certificat de signature

- Un certificat JKS (Java Keystore) est nécessaire pour fournir les informations nécessaires.
- Téléchargez le fichier .jks à l'aide du nom d'alias et du mot de passe keystore/key générés à l'étape 11.



Remarque : le certificat téléchargé dans l'onglet « Signature » de l'approbation de partie de confiance ECE configurée sur la console de gestion AD FS doit correspondre.

Service Provider		ECE Console Properties
Service Provider Initiated Authentication		Organization Endpoints Proxy Endpoints Notes Advanced Monitoring Identifiers Encryption Signature Accepted Claims
Entity ID*	https://ece126web1a.jo123.local/	Specify the signature verification certificates for requests from this relying party. Subject Issuer Effective Date Expiratik
Request Signing Certificate*	••••	CN=ece126a, CN=ece126app, 1/31/2024 2:21: 1/29/20
Signing Algorithm*	SHA-256 ~	
Identity Provider Login URL*	https://WIN-260MECJBIC2.jo123.loc	
Identity Provider Logout URL	https://ece126web1a.jo123.local/def	

Algorithme de signature

- Définissez l'algorithme de signature pour le fournisseur de services.
- Si vous utilisez ADFS, cette valeur doit correspondre à l'algorithme sélectionné dans l'approbation de partie de confiance créée pour ECE sous l'onglet Avancé.

Service Provider		ECE Console Properties X
Service Provider Initiated Authentication		Monitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints Proxy Endpoints Notes Advanced
Entity ID*	https://ece126web1a.jo123.local/	Specify the secure hash algorithm to use for this relying party trust. Secure hash algorithm SHA-256
Request Signing Certificate*	••••	
Signing Algorithm*	SHA-256 ~	
Identity Provider Login URL*	https://WIN-260MECJBIC2.jo123.loc	
Identity Provider Logout URL	https://ece126web1a.jo123.local/def	

URL de connexion du fournisseur d'identité

- URL pour l'authentification SAML.
- Par exemple, pour ADFS, il s'agit de http://<ADFS>/adfs/ls.

URL de déconnexion du fournisseur d'identité

- URL vers laquelle les utilisateurs sont redirigés lorsqu'ils se déconnectent. Cette option est facultative et peut être n'importe quelle URL.
- Par exemple, les agents peuvent être redirigés vers <u>https://www.cisco.com</u> ou toute autre URL après la déconnexion SSO.

Étape 16

Cliquez sur Save (enregistrer)

Définir l'URL du serveur Web/LB dans les paramètres de partition

Étape 17

Assurez-vous que l'URL Web Server/LB correcte est entrée dans les paramètres de partition > sélectionnez l'onglet Apps et accédez à General Settings > External URL of the Application

cisco Enter	rprise Ch	at and Email				
Partition	~			Apps	Departments	Integration
٩		General Settings				
Chat & Messaging	~	٩				
Email	Ý	External URL of Application	https://ece126web1a.jo123.local			
Knowledge	~		Minimum characters allowed is 0. Maximum characters allowed is 100. Default value is https://external_application_url			
		Maximum number of records to display for search	100 10 - 500. Default value is 100			
		Maximum number of records to display for NAS search	9 1 - 100. Default value is 9			

Configuration de SSO pour les administrateurs de partition



Remarque :

- Cette étape s'applique uniquement à PCCE.
- Il s'agit du gadget ECE accessible dans l'interface Web d'administration de CCE https:///cceadmin.

Étape 18

Pour configurer SSO pour l'administrateur de partition

- Dans la console d'administration d'ECE, sous Menu au niveau de la partition, cliquez sur l'option Security, puis sélectionnez Single Sign-On > Configurations dans le menu de gauche.
- 2. Dans la liste déroulante Sélectionner la configuration, sélectionnez Administrateurs de partition et entrez les détails de configuration :

URL LDAP

- URL du serveur LDAP.
- Il peut s'agir de l'URL du contrôleur de domaine (par exemple, Idap://LDAP_server:389) ou de l'URL du catalogue global (par exemple, Idap://LDAP_server:3268) du serveur LDAP.
- La partition peut être ajoutée automatiquement au système lorsque ECE est accessible via la console d'administration CCE si ECE est configuré avec la recherche LDAP.
- Cependant, dans les déploiements Active Directory avec plusieurs domaines dans une seule forêt ou lorsque des UPN secondaires sont configurés, l'URL du contrôleur de domaine avec les ports LDAP standard 389 et 636 ne doit pas être utilisée.
- L'intégration LDAP peut être configurée pour utiliser l'URL de catalogue global avec les ports 3268 et 3269.



Remarque : il est recommandé d'utiliser l'URL du catalogue global. Si vous n'utilisez pas de catalogue global, une erreur dans les journaux ApplicationServer est la suivante.

Exception dans l'authentification LDAP <@>
javax.naming.PartialResultException : référence(s) de continuation non traitée(s) ;
nom restant 'DC=example,DC=com'

attribut de numéro de répertoire

- Attribut du nom unique qui contient le nom de connexion de l'utilisateur.
- Par exemple, userPrincipalName.

Base

- La valeur spécifiée pour Base est utilisée par l'application comme base de recherche.
- La base de recherche est l'emplacement de départ de la recherche dans l'arborescence du répertoire LDAP.
- Par exemple, DC=monentreprise, DC=com.

DN pour recherche LDAP

- Si votre système LDAP n'autorise pas la liaison anonyme, fournissez le nom distinctif (DN) d'un utilisateur qui dispose d'autorisations de recherche sur l'arborescence du répertoire LDAP.
- Si le serveur LDAP autorise la liaison anonyme, laissez ce champ vide.

Mot de passe

- Si votre système LDAP n'autorise pas la liaison anonyme, fournissez le mot de passe d'un utilisateur qui dispose d'autorisations de recherche sur l'arborescence du répertoire LDAP.
- Si le serveur LDAP autorise la liaison anonyme, laissez ce champ vide.

Étape 19

Cliquez sur Save (enregistrer)

La configuration de l'authentification unique pour les agents et les administrateurs de partition dans ECE est maintenant terminée.

Dépannage

Définition du niveau de suivi

- 1. Dans la console d'administration ECE, sous Menu au niveau de la partition, cliquez sur l'option Ressources système, puis sélectionnez Journaux de processus dans le menu de gauche.
- 2. Dans la liste des processus, sélectionnez le processus ApplicationServer > définir le niveau de trace souhaité dans le menu déroulant « Maximum Trace Level ».



Remarque :

- Pour le dépannage des erreurs de connexion SSO lors de la configuration initiale ou de la reconfiguration, définissez le suivi du processus ApplicationServer au niveau 7.
- Une fois l'erreur reproduite, redéfinissez le niveau de suivi sur le niveau par défaut
 4, pour éviter l'écrasement des journaux.

cisco Ente	erprise Ch	At and Email Partition Administrator -					
Partition	~	Apps Departments Integration Language Tools Security Services Storage System Resources Tools User					
٩		Q.					
Process Logs		Name	•	Description ©			
		ece126app1a:alarm-rules-process		ece126app1a:alarm-rules-process			
		ece126app1a:ApplicationServer		ece126app1a;ApplicationServer			
		ece126app1a:component-status		ece126app1a:component-status			
		ece126app1a:DatabaseMonitoring		ece126app1a:DatabaseMonitoring			
		ece126app1a:dsm-registry		ece126app1a:dsm-registry			
		ece126app1a:DSMController		ece126app1a:DSMController			
		ece128app1a.DSMControllerLaunchHelper		ece126app1a:DSMControllerLaunchHelper			
		ece126app1a:dx-process		ece126app1axdx-process			
		ece126app1a:EAAS-process		ece126app1a.EAAS-process			
		ece126app1a.EAMS-process		ece126app1a:EAMS-process			
		ece126app1a:MessagingServer		ece126app1a:MessagingServer			
		ece126app1a:monitor-process		ece126app1a:monitor-process			
		ece126app1a:ProcessLauncher		ece126app1a:ProcessLauncher			
		ece126app1a:purge-process		ece126app1a:purge-process			
		ece126app1a.report-process		ece126app1a:report-process			
		ece126app1a:rules-cache-process		ece126app1a:rules-cache-process			

uluih cisco

Enterprise Chat and Email

Partition ~		
٩	Edit Process Log: ece126app1a	:ApplicationServer
Process Logs	General Advanced Logging	
	Name	ece126app1a:ApplicationServer
	Description	ece126app1a:ApplicationServer
	Maximum Trace Level	4 - Info ^
	Log File Name	8 - Trace ^ 7 - Debug
	Maximum File Size	6 - Dbquery 5 - Perf
	Extensive Logging Duration	4 - Info 🗸 🗸
	Extensive Logging End Time	

Scénario de dépannage 1

Erreur

- Code d'erreur : 500
- Description de l'erreur : l'application ne peut pas se connecter à l'utilisateur pour le moment car la connexion au fournisseur d'identité a échoué.

Analyse des journaux

- Échec de la connexion IdP <samlp : Status><samlp : StatusCode Value="urn : oasis : names : tc : SAML : 2.0 : status : Responder" /></samlp : Status>
- Ici, l'état « Responder » indique qu'il y a un problème du côté AD FS dans ce cas, principalement avec le « certificat de signature de la demande » téléchargé sur la console d'administration ECE (configuration SSO > fournisseur de services) et le certificat téléchargé sur l'approbation de la partie de confiance ECE sous l'onglet « Signature ».
- Il s'agit du certificat qui est généré à l'aide du fichier Keystore Java.

Journaux du serveur d'applications - Niveau de suivi 7 :

<#root>

 $unmarshall {\tt AndValidateResponse:}$

2022-09-21 18:18:15.002 GMT+0000 <@> ERROR <@> [392364:qtp1158258131-392364] <@> ProcessId:3272 <@> PID 2022-09-21 18:18:15.002 GMT+0000 <@> INFO <@> [392364:qtp1158258131-392364] <@> ProcessId:3272 <@> PID:

L10N_USER_STATUS_CODE_ERROR:

2022-09-21 18:18:15.002 GMT+0000 <@> ERROR <@> [392364:qtp1158258131-392364] <@> ProcessId:3272 <@> PID at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.unmarshallAndValidateResponse(SAML2_0_ at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Han at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Han at com.egain.platform.module.security.sso.handler.OpenIDConnect_Handler.validateReqWithAttributes(OpenI at com.egain.platform.module.security.sso.admin.SSOAdministrator.validateRequestWithAttributes(SSOAdmin at com.egain.platform.module.security.sso.controller.SSOControllerServlet.doPost(SSOControllerServlet.j .

at java.lang.Thread.run(Thread.java:834) ~[?:?]

errorCode=500&errorString=The application is not able to login the user at this time as Identity Provide

2022-09-21 18:18:15.003 GMT+0000 <@> DEBUG <@> [392364:qtp1158258131-392364] <@> ProcessId:3272 <@> PID 2022-09-21 18:18:15.003 GMT+0000 <@> DEBUG <@> [392364:qtp1158258131-392364] <@> ProcessId:3272 <@> PID

Résolution

- Reportez-vous à la configuration « Request Signing Certificate » sous la section « Configuring Agent Single Sign-On - Service Provider ».
- Assurez-vous que le fichier Java Keystore .jks généré à l'étape 11 est chargé dans le champ

« Request Signing certificate » de la console d'administration ECE sous SSO Configuration
 > Select Configuration 'Agent' > onglet « SSO Configuration » > Service Provider > Request
 Signing certificate.

 Assurez-vous que le fichier .crt est téléchargé sous l'onglet « Signature » de l'approbation de la partie de confiance ECE (étape 12).

Scénario de dépannage 2

Erreur

- Code d'erreur : 400
- Description de l'erreur : le jeton de réponse SAML n'est pas valide : échec de la validation de la signature.

Analyse des journaux

 Cette erreur indique qu'il existe une incompatibilité dans le certificat entre le « certificat de signature de jeton » sur ADFS et le « certificat du fournisseur d'identité » sur la configuration de l'authentification unique ECE.

Journaux du serveur d'applications - Niveau de suivi 7 :

<#root>

Entering 'validateSSOCertificate' and validating the saml response against certificate:

2022-10-07 15:27:34.523 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID 2022-10-07 15:27:34.520 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID 2022-10-07 15:27:34.521 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID 2022-10-07 15:27:34.521 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID 2022-10-07 15:27:34.521 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID 2022-10-07 15:27:34.523 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID 2022-10-07 15:27:34.523 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID 2022-10-07 15:27:34.523 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID 2022-10-07 15:27:34.523 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID 2022-10-07 15:27:34.523 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID 2022-10-07 15:27:34.523 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID 2022-10-07 15:27:34.523 GMT+0000 <@> INF0 <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID 2022-10-07 15:27:34.523 GMT+0000 <@> INF0 <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID 2022-10-07 15:27:34.523 GMT+0000 <@> INF0 <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID 2022-10-07 15:27:34.523 GMT+0000 <@> INF0 <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID 2022-10-07 15:27:34.523 GMT+0000 <@> INF0 <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID 2022-10-07 15:27:34.523 GMT+0000 <@> INF0 <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID<202-10-07 15:27:34.523 GMT+0000 <@> INF0 <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID<202-10-07 15:27:34.523 GMT+0000 <@> INF0 <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID<202-10-07 15:27:34.523 GMT+0000 <@> INF0 <@> [537838:qtp1158258131-537838] <@> P

Error: Could not parse certificate: java.io.IOException: Incomplete data:

2022-10-07 15:27:34.523 GMT+0000 <@> ERROR <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID 2022-10-07 15:27:34.524 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID 2022-10-07 15:27:34.525 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID 2022-10-07 15:27:34.525 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID

Signature validation failed:

2022-10-07 15:27:34.525 GMT+0000 <@> ERROR <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID 2022-10-07 15:27:34.525 GMT+0000 <@> INFO <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID: 2022-10-07 15:27:34.525 GMT+0000 <@> ERROR <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID 2022-10-07 15:27:34.525 GMT+0000 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID

Résolution

- L'erreur affichée dans l'extrait de journal, 'Could not parse certificate: java.io.IOException: Incomplete data', indique que le contenu 'Identity Provider Certificate' n'est pas entré correctement
- Pour résoudre ce problème : dans AS FS Management > AD FS > Service > Certificates > Token-Signing > Export this certificate > ouvrez dans un éditeur de texte > copiez tout le contenu > collez sous le champ « Identity provider certificate » dans la configuration SSO > Save.
- Référez-vous à la configuration « Certificat du fournisseur d'identité » sous la section « Configuration de l'authentification unique de l'agent - Fournisseur d'identité » (Étape 15).

Scénario de dépannage 3

Erreur

- Code d'erreur : 401-114
- Description de l'erreur : Identité utilisateur introuvable dans l'attribut SAML.

Analyse des journaux

Journaux du serveur d'applications - Niveau de suivi 7 :

<#root>

getSSODataFromSAMLToken:

2024-02-01 01:44:32.081 GMT+0000 <@> ERROR <@> [1220:qtp815320891-1220] <@> ProcessId:7716 <@> PID:1 <@ 2024-02-01 01:44:32.081 GMT+0000 <@> TRACE <@> [1220:qtp815320891-1220] <@> ProcessId:7716 <@> PID:1 <@

L10N_USER_IDENTIFIER_NOT_FOUND_IN_ATTRIBUTE:

```
2024-02-01 01:44:32.081 GMT+0000 <@> ERROR <@> [1220:qtp815320891-1220] <@> ProcessId:7716 <@> PID:1 <@
com.egain.platform.module.security.sso.exception.SSOLoginException: null
at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.getSSODataFromSAMLToken(SAML2_0_Hand
at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.unmarshallAndValidateResponse(SAML2_
at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Ha
at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Ha
at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Ha
at com.egain.platform.module.security.sso.handler.SAML2_0_Handler.validateReqWithAttributes(SAML2_0_Ha
at com.egain.platform.module.security.sso.handler.OpenIDConnect_Handler.validateReqWithAttributes(SAML2_0_Ha
at com.egain.platform.module.security.sso.admin.SSOAdministrator.validateRequestWithAttributes(SSOAdmi
at com.egain.platform.module.security.sso.controller.SSOControllerServlet.doPost(SSOControllerServlet.
.
```

at java.lang.Thread.run(Thread.java:830) [?:?]

2024-02-01 01:44:32.083 GMT+0000 <@> DEBUG <@> [1220:qtp815320891-1220] <@> ProcessId:7716 <@> PID:1 <@ 2024-02-01 01:44:32.083 GMT+0000 <@> TRACE <@> [1220:qtp815320891-1220] <@> ProcessId:7716 <@> PID:1 <@

Résolution

- Cette erreur indique un problème/une non-correspondance de configuration dans les champs « Emplacement de l'identité de l'utilisateur » et « Nom de l'attribut d'identité de l'utilisateur ».
- Cochez et corrigez le 'User Identity Location' et le 'User Identity Attribute Name' dans la console d'administration ECE, sous Single Sign-On > Configurations > dans la liste déroulante Select Configuration, sélectionnez Agent > onglet SSO Configuration > Identity Provider (Étape 15).

Informations connexes

Il s'agit des documents clés que vous devez examiner en détail avant de commencer une installation ou une intégration ECE. Il ne s'agit pas d'une liste exhaustive des documents de la CEE.



Remarque :

- La plupart des documents ECE ont deux versions. Veuillez vous assurer que vous téléchargez et utilisez les versions qui sont destinées à PCCE. Le titre du document est soit pour Packaged Contact Center Enterprise, soit (Pour PCCE) ou (Pour UCCE et PCCE) après le numéro de version.
- Assurez-vous de consulter la page de démarrage de la documentation de Cisco Enterprise Chat and Email pour toute mise à jour avant toute installation, mise à niveau ou intégration.
- <u>https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/series.html</u>

Version ECE 12.6(1)

• Guide de l'administrateur de la messagerie et du chat d'entreprise

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.