Configuración y solución de problemas de SSO para agentes y administradores de particiones en ECE

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Configuration Steps
Configuración de Confianza de la Parte Confiadora para ECE
Configuración de un proveedor de identidad
Creación e importación de certificados
Configuración de Inicio de sesión único del agente
Establezca la URL del servidor Web/LB en la configuración de la partición
Configuración de SSO para Administradores de Partición
Resolución de problemas
Configuración del nivel de seguimiento
Situación de solución de problemas 1
Error
Análisis de registro
Resolución
Situación de solución de problemas 2
Error
Análisis de registro
Resolución
Situación de solución de problemas 3
Error
Análisis de registro
Resolución
Información Relacionada

Introducción

Este documento describe los pasos necesarios para configurar el inicio de sesión único (SSO) para agentes y administradores de particiones en una solución ECE.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

Cisco Packaged Contact Center Enterprise (PCCE)

Cisco Unified Contact Center Enterprise (UCCE)

Chat empresarial y correo electrónico (ECE)

Microsoft Active Directory

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

Versión de UCCE: 12.6(1)

Versión ECE: 12.6(1)

Microsoft Active Directory Federation Service (ADFS) en Windows Server 2016

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Se puede acceder a las consolas de chat y correo electrónico empresariales (ECE) fuera de Finesse; sin embargo, se debe habilitar SSO para que los agentes y supervisores puedan iniciar sesión en ECE a través de Finesse.

El inicio de sesión único también se puede configurar para los nuevos administradores de particiones. Esto garantiza que los nuevos usuarios que inician sesión en Cisco Administrator Desktop tengan acceso a Enterprise Chat and Email Administration Console.

Aspectos importantes que debe tener en cuenta sobre el inicio de sesión único:

- El proceso de configuración de un sistema para el inicio de sesión único debe realizarlo un usuario de la partición con las acciones necesarias en el nodo Seguridad de la aplicación y Administrar seguridad de la aplicación.
- Para que los supervisores y administradores inicien sesión en las consolas que no sean la consola de agente, una vez que se haya habilitado SSO, debe proporcionar una URL externa válida de la aplicación en la configuración de la partición. Consulte Configuración general de la partición para obtener más información.
- Se necesita un certificado de almacén de claves Java (JKS) para configurar SSO de modo

que los usuarios con funciones de administrador o supervisor puedan iniciar sesión en la partición 1 de ECE fuera de Finesse con sus credenciales de inicio de sesión de SSO. Póngase en contacto con el departamento de TI para recibir el certificado JKS.

- Se debe importar un certificado de Secure Sockets Layer (SSL) de Cisco IDS a todos los servidores de aplicaciones de una instalación. Para obtener el archivo de certificado SSL necesario, póngase en contacto con el departamento de TI o con el servicio de asistencia de Cisco IDS.
- La intercalación del servidor de base de datos para Unified CCE distingue entre mayúsculas y minúsculas. El nombre de usuario de la notificación devuelto por la dirección URL del extremo de información de usuario y el nombre de usuario de Unified CCE deben ser iguales. Si no son iguales, los agentes de inicio de sesión único no se reconocen como conectados y ECE no puede enviar la disponibilidad del agente a Unified CCE.
- La configuración de SSO para Cisco IDS afecta a los usuarios que se han configurado en Unified CCE para el inicio de sesión único. Asegúrese de que los usuarios que desea activar para SSO en ECE están configurados para SSO en Unified CCE. Póngase en contacto con el administrador de Unified CCE para obtener más información.



Nota:

- Asegúrese de que los usuarios que desea activar para SSO en ECE están configurados para SSO en Unified CCE.
- Este documento especifica los pasos para configurar la confianza de piezas de confianza para ECE en una implementación de AD FS única donde el servidor de federación de recursos y el servidor de federación de cuentas están instalados en el mismo equipo.
- Para una implementación de AD FS dividida, diríjase a la guía de instalación y configuración de ECE para la versión correspondiente.

Configuration Steps

Configuración de Confianza de la Parte Confiadora para ECE

Paso 1

Abra la consola de administración de AD FS y vaya a AD FS > Relaciones de confianza > Confianza de la persona de confianza.

Paso 2

En la sección Acciones, haga clic en Agregar confianza de usuario de confianza...

翰 AD FS					-			x
File Action View Window Help						[- 5	×
🗢 🔿 📧 🛿 🖬								
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				
				P Help				
	1		I					

Paso 3

En el asistente para agregar confianza de usuario de confianza, haga clic en Inicio y realice los pasos siguientes:

a. En la página Seleccionar origen de datos, seleccione la opción Introducir datos sobre la parte de respuesta manualmente y haga clic en Siguiente.

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.	nanca
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. En la página Especificar Nombre para Mostrar, proporcione un nombre para mostrar para el usuario de confianza. Haga clic en Next (Siguiente)

🐐 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. En la página Configurar URL:

i. Seleccione la opción Habilitar soporte para el protocolo SSO Web SAML 2.0.

ii. En el campo URL del servidor SSO SAML 2.0 del usuario de confianza, proporcione la URL con el formato: https://<FQDN de servidor web o equilibrador de carga>/system/SAML/SSO/POST.controller

🐴 Add Relying Party Trust Wiza	ard
Configure URL	
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-Trust protocol is always enabled for a relying party.

d. En la página Configurar identificadores, proporcione el identificador de confianza de usuario de confianza y haga clic en Agregar.

• El valor debe tener el formato: https://<FQDN de servidor web o equilibrador de carga>/

؋ 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. En la página Choose Access Control Policy, haga clic en next con el valor predeterminado de la política 'Permit everyone'.

🛯 🏘 Add Relying Party Trust Wi	zard	X
Choose Access Control	Policy	
Steps	Choose an access control policy:	
Welcome	Name	Description
Select Data Source	Permit everyone	Grant access to everyone.
Specify Display Name	Permit everyone and require MFA	Grant access to everyone and require M
Configure Certificate	Permit everyone and require MFA for specific group Permit everyone and require MFA from extranet access	Grant access to everyone and require M Grant access to the intranet users and re
Configure URL	Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and require M
Configure Identifiers	Permit everyone and require MFA, allow automatic device registr	Grant access to everyone and require M
Choose Access Control	Permit everyone for intranet access	Grant access to the intranet users.
Policy	Permit specific group	Grant access to users of one or more sp
 Ready to Add Trust Finish 	Verify and the second seco	user will be permitted access for this

f. En la página Preparado para agregar confianza, haga clic en Siguiente.

🐴 Add Relying Party Trust Wiza	ard							x
Ready to Add Trust								
Steps Welcome Select Data Source Specify Display Name Configure Certificate Configure URL Configure Identifiers Choose Access Control Policy Ready to Add Trust Finish	The relying party tr Monitoring Specify the Relying p Monitoring Monitoring 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 er >	been configu D FS configur Encryption ettings for this ation metadata rty update relying federation me vas last updat	Ired. Review ation databation Signature s relying part a URL:) party etadata data ed from fede	v the following settir ase. Accepted Claims y trust. was last checked eration metadata on	on:	lick Next to a	add the
					< Previo	ous Nex	d >	Cancel

g. Una vez agregada correctamente la confianza de usuario de confianza, haga clic en Cerrar.

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

En la lista Confianzas de proveedores de confianza, seleccione la confianza de usuario de confianza creada para ECE y, en la sección de acciones, haga clic en Propiedades.



En la ventana Propiedades, desplácese a la pestaña Terminales y haga clic en el botón Agregar SAML..

ECE Console Pro	operties					x
Monitoring Organization	Identifiers Endpoints	Encryption Proxy Enc	Signatu Ipoints	ire Ad Notes	ccepted Clai Advanc	ms ed
Specify the endp	points to use fo	or SAML and	WS-Fede	erationPa	ssive protoci	ols.
	rtion Consun	na ner Endpoir	ex ыло nts	aing	Detault	Re
https://ec	e126web1a.jo	123.I 0	PO:	ST	No	
<	1	11				>
Add SAML]					
Add WS-Fede	eration		Ren	nove	Edit	
		ОК	Ca	ancel	Apply	

En la ventana Add an Endpoint, configure como se indica:

- 1. Seleccione el tipo de terminal como cierre de sesión de SAML.
- 2. Especifique la URL de confianza como https://<ADFS-server-FQDN>/adfs/ls/?wa=wsignoutcleanup1.0
- 3. Click OK.

Add an Endpoint

Endpoint type:	
SAML LOGOUE	· · · · · · · · · · · · · · · · · · ·
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

х

Paso 7

En la lista Confianza de proveedores, seleccione la confianza creada para ECE y, en la sección de acciones, haga clic en Editar póliza de seguro de reclamación.



En la ventana Editar póliza de seguro de reclamación, en la pestaña Reglas de transformación de emisión, haga clic en el botón Agregar regla... y configure como se muestra:

a. En la página Choose Rule Type (Elegir tipo de regla), seleccione Send LDAP Attributes as Claims (Enviar atributos LDAP como notificaciones) en el menú desplegable y haga clic en Next (Siguiente).

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		
	🐐 Add Transform Claim R	Kule Wizard X
	Select Rule Templat	e
	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 reiying 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. En la página Configurar regla de reclamación:
 - 1. Proporcione el nombre de la regla de reclamación y seleccione el almacén de atributos.
 - 2. Defina la asignación del atributo LDAP y el tipo de notificación saliente.
 - Seleccione Name ID como el nombre del tipo de notificación saliente.
 - Haga clic en Finalizar para volver a la ventana Editar póliza de seguro de reclamación y, a continuación, haga clic en Aceptar.

🏘 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

En la lista Confianzas de proveedores de confianza, haga doble clic en la confianza de usuario de confianza de ECE que ha creado.

En la ventana Propiedades que se abre, vaya a la ficha Avanzadas y establezca el algoritmo hash seguro en SHA-1 o SHA-256. Haga clic en Accept (Aceptar) para cerrar la ventana.



Nota: este valor debe coincidir con el valor del 'algoritmo de firma' establecido para el 'proveedor de servicios' en Configuraciones de SSO en ECE

Relying Party Trusts				
Display Name		Enabled	Туре	Identifier
ECE Console		Yes	WS-T	https://ece126web1a.jo123.local/
ECE Console ECE Console F Monitoring Organization Specify the Secure has	Properties Identifiers Encryption S Endpoints Proxy Endpo secure hash algorithm to use for h algorithm: SHA-256	Yes Signature Ac sints Notes r this relying party	WS-T cepted Cla Advance trust.	https://ece126web1a.jo123.local/
	ОК	Cancel	Apph	y

Verifique y anote el valor del Identificador del Servicio de federación.

 En la consola de administración de AD FS, seleccione AD FS > Editar propiedades del servicio de federación > ficha General > Identificador del servicio de federación y haga clic con el botón secundario del mouse en él



Nota:

- Este valor debe agregarse exactamente tal como se indica al configurar el valor "Id. de entidad" para el proveedor de identidad en Configuraciones de SSO en ECE.
- El uso de http:// NO significa que ADFS no sea seguro, sino simplemente un identificador.



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	

Configuración de un proveedor de identidad

Paso 11

Se necesita un certificado de almacén de claves Java (JKS) para configurar SSO de modo que los usuarios con funciones de administrador o supervisor puedan iniciar sesión en la partición de ECE fuera de Finesse con sus credenciales de inicio de sesión de SSO.

Si desea configurar SSO para permitir que los usuarios con roles de administrador o supervisor

inicien sesión en la partición de ECE fuera de Finesse con sus credenciales de inicio de sesión de SSO, el certificado de almacén de claves Java (JKS) debe convertirse en certificado de clave pública y configurarse en Confianza de usuario de confianza creada en el servidor IdP para ECE.

Póngase en contacto con el departamento de TI para recibir el certificado JKS.



Nota: estos pasos se aplican a los sistemas que utilizan ADFS como proveedor de identidad. Otros proveedores de identidad pueden tener diferentes métodos para configurar el certificado de clave pública.

A continuación se muestra un ejemplo de cómo se generó un archivo JKS en el laboratorio:

a. Generar JKS:

keytool -genkey -keyalg RSA -alias ece126web1a_saml -keystore C:\Temp\ece126web1a_saml.jks -keysize 204



Nota: La contraseña del almacén de claves, el nombre de alias y la contraseña de clave introducidos aquí se utilizan al configurar la configuración del proveedor de servicios en Configuraciones de SSO en ECE.



b. Exportar el certificado:

Este comando keytool exporta el archivo de certificado en formato .crt con el nombre de archivo

ece126web1a_saml.crt al directorio C:\Temp.

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

Paso 12

Configuración de un proveedor de identidad

- 1. En la consola de administración de AD FS, seleccione y haga clic con el botón secundario del mouse (ratón) en la confianza de usuario de confianza creada para ECE.
- 2. Abra la ventana Propiedades de la confianza y, en la ficha Firma, haga clic en el botón Agregar.
- 3. Agregue el certificado público (archivo .crt generado en el paso anterior) y haga clic en Aceptar.

Creación e importación de certificados

Paso 13

Antes de configurar SSO para utilizar Cisco IDS para el inicio de sesión único para agentes, el certificado Tomcat del servidor de Cisco IdS debe importarse a la aplicación.

a. En la consola de administración de ECE, en Menú de nivel de partición, haga clic en la opción Seguridad y luego seleccione Administración de certificados en el menú del lado izquierdo.



b. En el espacio Administración de certificados, haga clic en el botón Nuevo e introduzca los detalles adecuados:

- Nombre: escriba un nombre para el certificado.
- Descripción: agregue una descripción para el certificado.
- Tipo de componente: Seleccione CISCO IDS.
- Importar certificado: para importar el certificado, haga clic en el botón Buscar y agregar e introduzca los detalles solicitados:
- Archivo de certificado: Haga clic en el botón Browse (Examinar) y seleccione el certificado

que desea importar. Los certificados sólo se pueden importar en los formatos .pem, .der (BINARY) o .cer/cert.

- Nombre de alias: introduzca un alias para el certificado.
- c. Haga clic en Guardar

cisco Enterpr	ise Cr			
Partition	~			
٩		Create Certificate		
Access Restrictions	~	Name*	Cisco IDS Server	
Attachments				
Audit Log		Description	Certificate for Cisco IdS Serve	er
Certificate Management		Description		
CORS				
Data Masking	~	Component Type*	CISCO IDS	~
Rich Text Content Policy		Import Certificate	ucce1261ids.cer	
Settings				
Single Sign-On	~			

Configuración de Inicio de sesión único del agente

Paso 14

- En la consola de administración de ECE, en el menú de nivel de partición, haga clic en la opción Security y, a continuación, seleccione Single Sign-On > Configurations en el menú de la izquierda.
- 2. En el menú desplegable Seleccionar configuración, seleccione Agente y establezca la configuración en la ficha General:
- Activar inicio de sesión único: haga clic en el botón Alternar para activar el inicio de sesión único.
- Tipo de inicio de sesión único: Seleccione Cisco IDS.

Enterprise Ch	at and Email								A O Partition	Administrator \sim
Partition ~			Apps Departr	ments Integration	Language Tools	Security	Services	Storage	System Resources	Tools User
٩	Configurations									
Access Restrictions ~ Attachments	Select Configuration Agent	~								
Audit Log	General SSO Configuration									
Certificate Management										
CORS	Name*	Agent Configuration								
Data Masking 🗸 🗸		State State State State State								
Rich Text Content Policy	Description	single sign-On Contiguration for agents								
Settings Single Sign-On	Enable Single Sign-On									
Licenses	Single Sign-On Type	Cisco IDS v								
Providers										
100000										
									Cance	Save

Haga clic en la pestaña SSO Configuration y proporcione los detalles de la configuración:

a. Proveedor de OpenID Connect

URL de terminal de información de usuario principal

- La URL de terminal de información del usuario del servidor IDS de Cisco principal.
- Esta URL valida el token de usuario/API de información de usuario.
- Está en el formato: <u>https://cisco-ids-1:8553/ids/v1/oauth/userinfo</u>, donde cisco-ids-1 indica el nombre de dominio completamente calificado (FQDN) del servidor principal de Cisco IDS.

Nombre de reclamación de identidad de usuario

- Nombre de la notificación devuelta por la dirección URL del terminal de información del usuario, que identifica el nombre de usuario en Unified o Packaged CCE.
- El nombre de la reclamación y el nombre de usuario de Unified o Packaged CCE deben coincidir.
- Esta es una de las notificaciones obtenidas en respuesta a la validación del token portador.
- Si el nombre de usuario de los agentes de Unified o Packaged CCE coincide con el nombre principal de usuario, proporcione "upn" como valor del campo Nombre de reclamación de identidad de usuario.
- Si el nombre de usuario de los agentes de Unified o Packaged CCE coincide con el nombre de cuenta SAM, proporcione "sub" como valor del campo Nombre de reclamación de identidad de usuario.

URL de terminal de información de usuario secundario

- La URL del terminal de información del usuario secundario del servidor IDS de Cisco.
- Está en el formato: <u>https://cisco-ids-2:8553/ids/v1/oauth/userinfo</u>, donde cisco-ids-2 indica el nombre de dominio completamente calificado (FQDN) del servidor secundario de Cisco IDS.

Método URL de terminal de información de usuario

- El método HTTP utilizado por ECE para realizar llamadas de validación de token portador a la URL de terminal de información de usuario.
- Seleccione POST en la lista de opciones presentadas (POST se selecciona aquí para coincidir con el método del servidor IDS).

POST: método utilizado para enviar datos al servidor IDS de Cisco en el extremo especificado.

Duración de caché de token de acceso (segundos)

- La duración, en segundos, durante la cual un token portador debe almacenarse en caché en ECE.
- Los tokens portadores para los que las llamadas de validación son correctas sólo se almacenan en cachés. (Valor mínimo: 1; valor máximo: 30)

Permitir inicio de sesión SSO fuera de Finesse

- Haga clic en este botón Alternar si desea permitir que los usuarios con funciones de administrador o supervisor inicien sesión en la partición de ECE fuera de Finesse con sus credenciales de inicio de sesión de SSO.
- Si se activa, se debe proporcionar información en las secciones Proveedor de identidad y Proveedor de servicios.
- Esto requiere que su configuración de IdP permita un servidor de IdP compartido.



Partition	~		
٩		Configurations	
Access Restrictions Attachments	~	Select Configuration Agent	~
Audit Log		General SSO Configuration	1
CORS		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 ~
Providers		Access Token Cache Duration (Seconds)*	30
		Allow SSO Login Outside Finesse	

b. Proveedor de identidad

ID de entidad

• Id. de entidad del servidor IdP.



Nota: este valor debe coincidir exactamente con el valor 'Identificador de servicio de federación' de la consola de administración de AD FS.

٩	Configurations	Federation Service Properties X
Access Restrictions v Attachments Audit Log Certificate Management	Select Configuration Agent General SSO Configuration	Federation Service display name: JO123 ADFS Example: Fabricam Federation Service Federation Service name: WIN-260MECJ8IC2 jo123 local Example: fs fabricam com
CORS Data Masking ~ Rich Text Content Policy Settings	Identity Provider Entity ID* Identity Provider Certificate* Id	Federation Service identifier: http://WIN-260MECJ8/C2/a123.local/adfs/services/http:// Example: http://fs.fabrikam.com/adfs/services.http:// Web SS0 lifetime (minutes): 480 © Enable delegation for service administration
Single Sign-On A	User Identity Location* SAML Subject Identifier	Delegate name:
Licenses Providers	User Identity Attribute Name* Enable Encrypted Assertion	New Local System account for service administration New Local Administrators group for service administration
	Assertion Decryption Certificate* Enter Assertion Decryption Certificate	

Certificado del proveedor de identidad

- El certificado de clave pública.
- El certificado debe comenzar con "-----BEGIN CERTIFICATE-----" y terminar con "-----END CERTIFICATE-----"
- Este es el certificado de firma de token en la Consola de administración de AD FS > Servicio > Certificados > Firma de token.

Allow SSO Login Outside Finesse		AD FS	Certificates		
Identity Provider		Service Attribute Stores Authentication Methods	Subject Service communications	CNHo123-WIN-260MEC I	Effective Date
Entity ID*	http://WIN-260MECJBIC2.jo123.local	Certificates Claim Descriptions Device Registration	Token-decrypting Token-		1/31/2024
Identity Provider Certificate*	BEGIN CERTIFICATEMIIC8JC	Scope Descriptions	Token-signing CN=ADFS Signing - WIN-260MECJBIC2 jo123 local	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				

Ubicación de identidad de usuario

- Seleccione SAML Subject Identifier para establecer la ubicación de identidad en el certificado con el identificador de asunto SAML predeterminado, como en el asunto de la afirmación SAML, por ejemplo, el nombre de usuario en <saml:Subject>.
- Seleccione Atributo SAML para asignar la ubicación de identidad a un atributo específico del certificado, por ejemplo, email.address. Proporcione el atributo en el campo Nombre de atributo de identidad de usuario.

Nombre de atributo de identidad de usuario

- Sólo se aplica cuando el valor de Ubicación de ID de usuario es un atributo SAML.
- Esto se puede ajustar dentro de la afirmación SAML y se puede utilizar para seleccionar un atributo diferente para la autenticación de usuarios, como una dirección de correo electrónico.
- También se puede utilizar para crear nuevos usuarios con un atributo SAML.
- Por ejemplo, si se identifica a un usuario mediante el valor proporcionado en el atributo email.address y el valor de la dirección de correo electrónico proporcionada no coincide con ningún usuario del sistema, se crea un nuevo usuario con los atributos SAML proporcionados.

Habilitar aserción cifrada (opcional)

- Si desea activar la aserción cifrada con el proveedor de identidad para el inicio de sesión en la consola, haga clic en el botón Toggle (Alternar) para establecer el valor en Enabled (Activado).
- Si no es así, establezca el valor en Disabled (Desactivado).

Certificado de descifrado de aserción

Si Habilitar aserción cifrada está establecido en Habilitado, haga clic en el botón Buscar y agregar y confirme su elección para cambiar el certificado.

Proporcione los detalles en la ventana Certificado de descifrado de aserción:

- Archivo de Almacén de Claves Java: Introduzca la ruta del archivo del almacén de claves Java. Este archivo tiene el formato .jks y contiene la clave de descifrado que el sistema necesita para acceder a los archivos protegidos por el proveedor de identidad.
- Nombre de Alias: Identificador exclusivo de la clave de descifrado.
- Contraseña del Almacén de Claves: Contraseña necesaria para acceder al archivo de almacén de claves Java.
- Key Password (Contraseña de clave): Contraseña necesaria para acceder a la clave de descifrado del alias.



Nota: debe coincidir con el certificado de la ficha 'Cifrado' de la confianza de usuario de confianza de ECE configurada en la consola de administración de AD FS.

c. Proveedor de servicios

Autenticación iniciada por el proveedor de servicios

• Establezca el botón de alternancia en Activado.

ID de entidad

• Proporcione la URL externa de la aplicación ECE.

Service Provider			ECE Console Properties X
Service Provider Initiated Authentication			Organization Endpoints Proxy Endpoints Notes Advanced Monitoring Identifiers Encryption Signature Accepted Claims Specify the display name and identifiers for this relying party trust. Specify the display name and identifiers Specify the display name and identifiers Accepted Claims
Entity ID*	https://ece126web1a.jo123.local/		Display name: ECE Console
Request Signing Certificate*	****	•	Relying party identifier: Add
Signing Algorithm*	SHA-256 ~]	Example: https://fs.contoso.com/adfs/services/trust Relying party identifiers: Inters://ecc128web1a.jo123.jocal/
Identity Provider Login URL*	https://WIN-260MECJBIC2.jo123.loc		
Identity Provider Logout URL	https://ece126web1a.jo123.local/def		

Solicitar certificado de firma

- Se necesita un certificado de almacén de claves Java (JKS) para proporcionar la información necesaria.
- Cargue el archivo .jks con el nombre de alias y la contraseña del almacén de claves/clave generados en el paso 11.



Nota: debe coincidir con el certificado cargado en la ficha "Firma" de la confianza de usuario de confianza de ECE configurada en la consola de administración de AD FS.

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 Expirative
Request Signing Certificate*	5	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	

Algoritmo de firma

- Establezca el algoritmo de firma para el proveedor de servicios.
- Si utiliza ADFS, este valor debe coincidir con el algoritmo seleccionado en la confianza de usuario de confianza creada para ECE en la ficha Avanzadas.

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 inicio de sesión del proveedor de identidad

- La URL para la autenticación SAML.
- Por ejemplo, para ADFS, sería <u>http://<ADFS>/adfs/ls</u>.

URL de cierre de sesión del proveedor de identidad

- Dirección URL a la que se redirige a los usuarios al cerrar sesión. Esta opción es opcional y puede ser cualquier URL.
- Por ejemplo, los agentes se pueden redirigir a <u>https://www.cisco.com</u> o a cualquier otra URL después de cerrar la sesión de SSO.

Paso 16

Haga clic en Save (Guardar).

Establezca la URL del servidor Web/LB en la configuración de la partición

Paso 17

Asegúrese de ingresar la URL correcta del servidor Web/LB en la configuración de la partición > seleccione la pestaña Aplicaciones y navegue hasta Configuración general > URL externo de la aplicación

cisco Ente	rprise Ch	at and Email				
Partition	~			Apps	Departments	Integration
٩		General Settings				
Chat & Messaging	~	× Q.				
Email v		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			

Configuración de SSO para Administradores de Partición



Nota:

- Este paso se aplica sólo a PCCE.
- Se trata del gadget ECE al que se accede desde la interfaz WEB de administración de CCE https:///cceadmin.

Paso 18

Para configurar SSO para el administrador de particiones

- En la consola de administración de ECE, en el menú de nivel de partición, haga clic en la opción Seguridad y, a continuación, seleccione Inicio de sesión único > Configuraciones en el menú de la izquierda.
- 2. En el menú desplegable Seleccionar configuración, seleccione Administradores de partición e introduzca los detalles de configuración:

URL LDAP

- La URL del servidor LDAP.
- Puede ser la URL del controlador de dominio (por ejemplo, ldap://LDAP_server:389) o la URL del catálogo global (por ejemplo, ldap://LDAP_server:3268) del servidor LDAP.
- La partición se puede agregar automáticamente al sistema cuando se accede a ECE a través de la consola de administración de CCE si ECE está configurado con búsqueda LDAP.
- Sin embargo, en las implementaciones de Active Directory con varios dominios en un único bosque o donde se configuran UPN alternativos, no se debe utilizar la URL del controlador de dominio con los puertos LDAP estándar 389 y 636.
- La integración LDAP se puede configurar para utilizar la URL del catálogo global con los puertos 3268 y 3269.



Nota: se recomienda utilizar la URL de catálogo global. Si no utiliza un GC, un error en los registros de ApplicationServer es el siguiente.

 Excepción en la autenticación LDAP <@> javax.aming.PartialResultException: referencias de continuación sin procesar; nombre restante 'DC=ejemplo,DC=com'

atributo DN

- Atributo del DN que contiene el nombre de inicio de sesión del usuario.
- Por ejemplo, userPrincipalName.

Base

- La aplicación utiliza el valor especificado para Base como base de búsqueda.
- La base de búsqueda es la ubicación inicial para la búsqueda en el árbol de directorios LDAP.
- Por ejemplo, DC=miempresa, DC=com.

DN para búsqueda LDAP

- Si el sistema LDAP no permite el enlace anónimo, proporcione el nombre distinguido (DN) de un usuario que tenga permisos de búsqueda en el árbol de directorios LDAP.
- Si el servidor LDAP permite el enlace anónimo, deje este campo en blanco.

Contraseña

- Si su sistema LDAP no permite el enlace anónimo, proporcione la contraseña de un usuario que tenga permisos de búsqueda en el árbol de directorios LDAP.
- Si el servidor LDAP permite el enlace anónimo, deje este campo en blanco.

Paso 19

Haga clic en Save (Guardar).

Con esto finaliza la configuración de inicio de sesión único para agentes y administradores de particiones en ECE.

Resolución de problemas

Configuración del nivel de seguimiento

- 1. En la consola de administración de ECE, en el menú de nivel de partición, haga clic en la opción Recursos del sistema y, a continuación, seleccione Registros de proceso en el menú de la izquierda.
- 2. En la lista de procesos, seleccione el proceso ApplicationServer > establezca el nivel de seguimiento deseado en el menú desplegable 'Maximum Trace Level'.



Nota:

- Para solucionar los errores de inicio de sesión de SSO durante la instalación inicial o la reconfiguración, establezca el seguimiento de procesos de ApplicationServer en el nivel 7.
- Una vez que se reproduzca el error, vuelva a establecer el nivel de seguimiento en el nivel 4 predeterminado para evitar que se sobrescriban los registros.

Enterprise C	Chat and Email Partition Administrator ~					
Partition ~	Apps Departments Integration Language Tools Security Services Storage System Resources Tools User					
Q.	۵,					
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				
	ece126app1a:DSMControllerLaunchHelper	ece126app1a.DSMControllerLaunchHelper				
	ece126app1a:dx-process	ece126app1a:dx-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				

ululu 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	

Situación de solución de problemas 1

- Código de error: 500
- Descripción del error: la aplicación no puede iniciar sesión en el usuario en este momento porque se ha producido un error en el inicio de sesión del proveedor de identidad.

Análisis de registro

- Error de inicio de sesión IdP <samlp:Status><samlp:StatusCode
 Value="urn:oasis:names:tc:SAML:2.0:status:Responder" /></samlp:Status>
- En este caso, el estado "Respondedor" indica que hay algún problema en el lado de AD FS, en este caso, principalmente con el "Solicitar certificado de firma" cargado en la consola de administración de ECE (Configuración de SSO > Proveedor de servicios) y el certificado cargado en el Fideicomiso de confianza de ECE en la pestaña "Firma".
- Este es el certificado que se genera con el archivo de almacén de claves Java.

Registros del servidor de aplicaciones - Nivel de seguimiento 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

Resolución

- Consulte la configuración de "Solicitar certificado de firma" en la sección "Configuración del inicio de sesión único del agente: proveedor de servicios".
- Asegúrese de que el archivo .jks del almacén de claves Java generado en el paso 11 se

carga en el campo "Solicitar certificado de firma" en la consola de administración de ECE en Configuración de SSO > Seleccionar configuración 'Agente' > ficha 'Configuración de SSO' > Proveedor de servicios > Solicitar certificado de firma.

• Asegúrese de que el archivo .crt se carga en la pestaña "Firma" de la ECE Relying Party Trust (Paso 12).

Situación de solución de problemas 2

Error

- Código de error: 400
- Descripción del error: el token de respuesta de SAML no es válido: no se pudo validar la firma.

Análisis de registro

 Este error indica que hay una discordancia en el certificado entre el 'Certificado de firma de token' en ADFS y el 'Certificado del proveedor de identidad' en la configuración de SSO de ECE.

Registros del servidor de aplicaciones - Nivel de seguimiento 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 15:27:34.521 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 <@> DEBUG <@> [537838:qtp1158258131-537838] <@> ProcessId:3272 <@> PID

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

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

Resolución

- El error que aparece en el fragmento de registro, 'No se pudo analizar el certificado: java.io.IOException: Incomplete data', indica que el contenido de 'Certificado del proveedor de identidad' no se ha introducido correctamente
- Para resolver esto: en la Administración de AS FS > AD FS > Servicio > Certificados > Firma de token > Exportar este certificado > abra en un editor de texto > copie todo el contenido > pegue en el campo 'Certificado del proveedor de identidad' en la configuración de SSO > Guardar.
- Consulte la configuración del 'Certificado del proveedor de identidad' en la sección 'Configuración del inicio de sesión único del agente - Proveedor de identidad' (Paso 15).

Situación de solución de problemas 3

Error

- Código de error: 401-114
- Descripción del error: identidad de usuario no encontrada en el atributo SAML.

Análisis de registro

Registros del servidor de aplicaciones - Nivel de seguimiento 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 <@

Resolución

- Este error indica un problema de configuración o una falta de coincidencia en los campos 'Ubicación de identidad de usuario' y 'Nombre de atributo de identidad de usuario'.
- Verifique y corrija la 'Ubicación de identidad del usuario' y el 'Nombre de atributo de identidad del usuario' en la consola de administración de ECE, en Inicio de sesión único > Configuraciones > en el menú desplegable Seleccionar configuración, seleccione Agente > ficha Configuración de SSO > Identificar proveedor (Paso 15).

Información Relacionada

Estos son los documentos clave que debe revisar a fondo antes de iniciar cualquier instalación o integración de ECE. No se trata de una lista completa de documentos de la CEPE.



Nota:

- La mayoría de los documentos ECE tienen dos versiones. Asegúrese de descargar y utilizar las versiones correspondientes a PCCE. El título del documento es para Packaged Contact Center Enterprise o (para PCCE) o (para UCCE y PCCE) después del número de versión.
- Asegúrese de consultar la página de inicio de la documentación de Cisco Enterprise Chat y Email para ver si hay alguna actualización antes de realizar cualquier instalación, actualización o integración.
- <u>https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/series.html</u>

ECE Versión 12.6(1)

• Guía del administrador de correo electrónico y chat empresarial

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).