# Konfiguration und Fehlerbehebung bei SSO für Agenten und Partitionsadministrator in ECE

# Inhalt

Einleitung
<u>Voraussetzungen</u>
Anforderungen
Verwendete Komponenten
Hintergrundinformationen
Konfigurationsschritte
<u>rtoningurationsschillte</u>
Konfigurieren der Vertrauenswürdigkeit der vertrauenden Partei für ECE
Konfigurieren eines Identitätsanbieters
Erstellen und Importieren von Zertifikaten
Konfigurieren der einmaligen Anmeldung für den Agent
Festlegen der Webserver-/LB-URL in den Partitionseinstellungen
Konfigurieren von SSO für Partitionsadministratoren
Fehlerbehebung
Trace-Ebene festlegen
Fehlerbehebung - Szenario 1
<u>Fehler</u>
Protokollanalyse
Auflösung
Fehlerbehebung - Szenario 2
<u>Fehler</u>
Protokollanalyse
Auflösung
Fehlerbehebung - Szenario 3
<u>Fehler</u>
Protokollanalyse
Auflösung
Zugehörige Informationen

# Einleitung

In diesem Dokument werden die erforderlichen Schritte zur Konfiguration von Single Sign-On (SSO) für Agents und Partitionsadministratoren in einer ECE-Lösung beschrieben.

# Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

Cisco Packaged Contact Center Enterprise (PCCE)

Cisco Unified Contact Center Enterprise (UCCE)

Enterprise Chat und E-Mail (ECE)

**Microsoft Active Directory** 

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

UCCE-Version: 12.6(1)

ECE-Version: 12.6(1)

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

# Hintergrundinformationen

Der Zugriff auf ECE-Konsolen (Enterprise Chat und E-Mail) ist auch außerhalb von Finesse möglich. Allerdings muss SSO aktiviert sein, damit sich Agenten und Supervisoren über Finesse bei ECE anmelden können.

Single Sign-On kann auch für neue Partitionsadministratoren konfiguriert werden. So wird sichergestellt, dass neue Benutzer, die sich beim Cisco Administrator-Desktop anmelden, Zugriff auf die Enterprise Chat- und E-Mail-Verwaltungskonsole erhalten.

Wichtige Hinweise zur einmaligen Anmeldung:

- Der Prozess der Konfiguration eines Systems f
  ür die einmalige Anmeldung muss vom Partitionsbenutzer auf Partitionsebene f
  ür den Sicherheitsknoten mit den erforderlichen Aktionen ausgef
  ührt werden: Anwendungssicherheit anzeigen und Anwendungssicherheit verwalten.
- Damit sich Supervisoren und Administratoren bei anderen Konsolen als der Agentenkonsole anmelden können, müssen Sie nach der Aktivierung von SSO in den Partitionseinstellungen eine gültige externe URL der Anwendung angeben. Weitere Informationen finden Sie unter Allgemeine Partitionseinstellungen.
- Für die Konfiguration von SSO ist ein Java Keystore (JKS)-Zertifikat erforderlich, damit sich Benutzer mit Administrator- oder Supervisor-Rollen bei Partition 1 von ECE außerhalb von

Finesse mit ihren SSO-Anmeldedaten anmelden können. Wenden Sie sich an Ihre IT-Abteilung, um das JKS Zertifikat zu erhalten.

- Ein Secure Sockets Layer (SSL)-Zertifikat von Cisco IDS muss in alle Anwendungsserver einer Installation importiert werden. Um die erforderliche SSL-Zertifikatsdatei zu erhalten, wenden Sie sich an Ihre IT-Abteilung oder den Cisco IDS-Support.
- Bei der DB-Serversortierung für Unified CCE wird die Gro
  ß- und Kleinschreibung ber
  ücksichtigt. Der Benutzername im Anspruch, der von der Benutzerinfo-Endpunkt-URL zur
  ückgegeben wird, und der Benutzername in Unified CCE m
  üssen identisch sein. Wenn diese nicht identisch sind, werden Single Sign-On-Agenten nicht als angemeldet erkannt, und die ECE kann die Agentenverf
  ügbarkeit nicht an Unified CCE senden.
- Die Konfiguration von SSO f
  ür Cisco IDS wirkt sich auf Benutzer aus, die in Unified CCE f
  ür Single Sign-On konfiguriert wurden. Stellen Sie sicher, dass die Benutzer, die Sie f
  ür SSO in ECE aktivieren m
  öchten, f
  ür SSO in Unified CCE konfiguriert sind. Weitere Informationen erhalten Sie von Ihrem Unified CCE-Administrator.



Anmerkung:

• Stellen Sie sicher, dass die Benutzer, die Sie für SSO in ECE aktivieren möchten,

für SSO in Unified CCE konfiguriert sind.

- In diesem Dokument werden die Schritte zum Konfigurieren von Relying Part Trust f
  ür ECE in einer einzelnen AD FS-Bereitstellung beschrieben, bei der Resource Federation Server und Account Federation Server auf demselben Computer installiert sind.
- Für eine AD FS-Split-Bereitstellung navigieren Sie zum Leitfaden für die Installation und Konfiguration von ECE für die jeweilige Version.

# Konfigurationsschritte

Konfigurieren der Vertrauenswürdigkeit der vertrauenden Partei für ECE

Schritt 1

Öffnen Sie die AD FS-Verwaltungskonsole, und navigieren Sie zu AD FS > Trust Relationships > Relying Party Trust.

Schritt 2

Klicken Sie im Abschnitt "Aktionen" auf Vertrauenswürdigkeit für vertrauende Partei hinzufügen...

N AD FS			_ D 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
			Q Refresh
			I Help
	1		

Schritt 3

Klicken Sie im Assistenten zur Vertrauensstellung für vertrauende Parteien hinzufügen auf Start, und führen Sie die folgenden Schritte aus:

a. Wählen Sie auf der Seite "Datenquelle auswählen" die Option Daten über die Antwortpartei manuell eingeben aus, und klicken Sie auf Weiter.

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

b. Geben Sie auf der Seite Anzeigenamen angeben einen Anzeigenamen für die vertrauende Partei an. Klicken Sie auf Next (Weiter).

🐐 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		
<ul> <li>Choose Access Control Policy</li> </ul>		~
Ready to Add Trust		
Finish		
	< Previous Next > Cancel	

c. Auf der Seite "URL konfigurieren":

i. Wählen Sie die Option Enable support for the SAML 2.0 Web SSO protocol.

ii. Geben Sie im Feld "Relying Party SAML 2.0 SSO server URL" die URL im folgenden Format an: https://<Web-Server-Or-Load-Balancer-FQDN>/system/SAML/SSO/POST.controller

🐐 Add Relying Party Trust Wizard		×
Configure URL		
Steps       AL         • Welcome       W.         • Select Data Source       Image: Specify Display Name         • Configure Certificate       Image: Configure URL         • Configure Identifiers       Image: Choose Access Control Policy         • Ready to Add Trust       Image: Configure Identifiers         • Finish       Image: Configure Identifiers	D FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If S-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the RLs to use. Support for the WS-Trust 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 URLs Relying party 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 SSO service URL: https://ece126web1a.jo123.local/system/SAML/SSO/POST.controller Example: https://www.contoso.com/adfs/ls/	

d. Geben Sie auf der Seite Kennzeichner konfigurieren den Vertrauensbezeichner der vertrauenden Partei an, und klicken Sie auf Hinzufügen.

Der Wert muss das folgende Format haben: https://<Webserver-Or-Load-Balancer-FQDN>/

؋ Add Relying Party Trust Wi	zard	×
Configure Identifiers		
Steps	Relying parties may be identified by one or more unique identifier strings. Specify the identifier	s for this relying
Welcome	party trust.	
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
<ul> <li>Choose Access Control Policy</li> </ul>		
Ready to Add Trust		
Finish		
	< Previous Next >	Cancel

e. Klicken Sie auf der Seite Choose Access Control Policy (Zugriffskontrollrichtlinie auswählen) mit dem Standardwert 'Permit everyone' (Jeden zulassen) auf Next (Weiter).

🐐 Add Relying Party Trust Wiz	rard		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	e M
Configure Certificate	Permit everyone and require MFA for specific group	Grant access to everyone and require	e M
Configure URI	Permit everyone and require MFA from extranet access Permit everyone and require MFA from unauthenticated devices	Grant access to the intranet users an Grant access to everyone and require	are e M
Configure Identifiers	Permit everyone and require MFA, allow automatic device registr	Grant access to everyone and require	e M
	Permit everyone for intranet access	Grant access to the intranet users.	
Choose Access Control Policy	Permit specific group	Grant access to users of one or more	spi
<ul> <li>Peodute Add Taut</li> </ul>	< III		>
<ul> <li>Finish</li> </ul>	Permit everyone         I do not want to configure access control policies at this time. No application.	user will be permitted access for this rious Next > Cancel	

f. Klicken Sie auf der Seite Bereit zur Vertrauensstellung hinzufügen auf Weiter.

🐴 Add Relying Party Trust Wiza	ard							x
Ready to Add Trust								
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	The relying party to relying party to Monitoring Specify the Relying p Monit Monit Au This re < neve	arty trust has ust to the A Identifiers monitoring s warty's federa or relying party dying party v er >	s been config D FS configu Encryption settings for thi ation metadata inty update relying federation me vas last updat	ured. Review ration databa Signature s relying part a URL: g party etadata data ed from fede	v the following settinase. Accepted Claims y trust.	on:	Endpoints	add the
	<u> </u>				< Previo	ous Nex	d >	Cancel

g. Wenn die Vertrauensstellung der vertrauenden Seite erfolgreich hinzugefügt wurde, klicken Sie auf Schließen.

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

Wählen Sie in der Liste Vertrauenswürdigkeit des vertrauenden Anbieters die

Vertrauenswürdigkeit der vertrauenden Partei aus, die für ECE erstellt wurde, und klicken Sie im Aktionsbereich auf Eigenschaften.



Navigieren Sie im Eigenschaftenfenster zur Registerkarte Endpunkte, und klicken Sie auf die Schaltfläche SAML hinzufügen...

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 te	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	

Konfigurieren Sie im Fenster Endpunkt hinzufügen wie folgt:

- 1. Wählen Sie als Endpunkttyp SAML Logout (SAML-Abmeldung) aus.
- 2. Geben Sie die vertrauenswürdige URL als https://<ADFS-server-FQDN>/adfs/ls/?wa=wsignoutcleanup1.0 an.
- 3. Klicken Sie auf OK.

# Add an Endpoint

Endpoint type:	
SAML Logout	~
Binding:	
POST	¥
Set the trusted URL	as default
Index: 0	
Trusted URL:	
https://WIN-260MECJE	BIC2.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

## Schritt 7

Wählen Sie in der Liste Vertrauenswürdige Anbieter die für ECE erstellte Vertrauensstellung aus, und klicken Sie im Aktionsbereich auf Anspruchsversicherungsrichtlinie bearbeiten.



Klicken Sie im Fenster "Versicherungspolice für Ansprüche bearbeiten" auf der Registerkarte "Ausstellungstransformationsregeln" auf die Schaltfläche Regel hinzufügen... und konfigurieren Sie wie folgt:

a. Wählen Sie auf der Seite Regeltyp auswählen aus dem Dropdown-Menü die Option LDAP-Attribute als Ansprüche senden, und klicken Sie auf Weiter.



- b. Auf der Seite Anspruchsregel konfigurieren:
  - 1. Geben Sie den Namen der Anspruchsregel an, und wählen Sie den Attributspeicher aus.
  - 2. Definieren Sie die Zuordnung des LDAP-Attributs und des ausgehenden Anspruchstyps.
  - Wählen Sie als ausgehenden Anspruchstypnamen Name ID aus.
  - Klicken Sie auf Fertig stellen, um zum Fenster "Versicherungsrichtlinie für Ansprüche bearbeiten" zurückzukehren, und klicken Sie dann auf 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		x
Issuance Transform Rules		
The following transform rules specify the claims that will be sent to the relying party.		
Order Rule Name Issued Claims		
1 Account name to Name ID Name ID		
	4	
	-	p.
Add Rule Edit Rule Remove Rule		
OK Cancel	Apply	,

Doppelklicken Sie in der Liste Vertrauenswürdiger Anbieter auf die von Ihnen erstellte Vertrauenswürdigkeit der vertrauenden ECE-Partei.

Öffnen Sie im Eigenschaftenfenster die Registerkarte Erweitert, und legen Sie den sicheren Hashalgorithmus auf SHA-1 oder SHA-256 fest. Klicken Sie auf OK, um das Fenster zu schließen.



Hinweis: Dieser Wert muss mit dem Wert übereinstimmen, der unter "SSO Configurations" (SSO-Konfigurationen) in ECE für den "Service Provider" (Dienstanbieter) als 'Signing-Algorithmus' festgelegt wurde.

Relying Party Trusts				
Display Name		Enabled	Туре	Identifier
ECE Console		Yes	WS-T	https://ece126web1a.jo123.local/
ECE Console Pro	perties			×
Monitoring I	Identifiers Encryption Sig	gnature Ac	cepted Cla	ims
Organization	Endpoints Proxy Endpoint	ts Notes	Advanc	ced
Specify the se	cure hash algorithm to use for th	his relying party	rtrust.	
Secure hash a	algorithm: SHA-256			✓
	ОК	Cancel	Appl	у

Überprüfen und notieren Sie den Wert für die Verbunddienstkennung.

 Klicken Sie in der AD FS-Verwaltungskonsole mit der rechten Maustaste auf AD FS > Eigenschaften des Verbunddiensts bearbeiten > Registerkarte Allgemein > Verbunddienstkennung



Anmerkung:

- Dieser Wert muss genau wie beim Konfigurieren des Werts für die Entitäts-ID für den Identitätsanbieter unter SSO-Konfigurationen in ECE hinzugefügt werden.
- Die Verwendung von http:// bedeutet NICHT, dass ADFS nicht sicher ist. Es handelt sich hierbei lediglich um einen Bezeichner.



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	

# Konfigurieren eines Identitätsanbieters

Schritt 11

Für die Konfiguration von SSO ist ein Java Keystore (JKS)-Zertifikat erforderlich, damit sich Benutzer mit Administrator- oder Supervisor-Rollen mit ihren SSO-Anmeldedaten bei der ECE-Partition außerhalb von Finesse anmelden können.

Wenn Sie SSO so konfigurieren möchten, dass sich Benutzer mit Administrator- oder Supervisor-

Rollen bei der Partition von ECE außerhalb von Finesse mit ihren SSO-Anmeldedaten anmelden können, muss das Java Keystore (JKS)-Zertifikat in ein Public Key-Zertifikat konvertiert und in Relying Party Trust (Vertrauenswürdigkeit der Partei) konfiguriert werden, das auf dem IdP-Server für ECE erstellt wurde.

Wenden Sie sich an Ihre IT-Abteilung, um das JKS Zertifikat zu erhalten.



Hinweis: Diese Schritte gelten für Systeme, die ADFS als Identitätsanbieter verwenden. Andere Identitätsanbieter können unterschiedliche Methoden zur Konfiguration von Zertifikaten mit öffentlichem Schlüssel verwenden.

Das folgende Beispiel zeigt, wie eine JKS-Datei in der Übung generiert wurde:

a. JKS generieren:

![](_page_24_Picture_0.jpeg)

Hinweis: Das hier eingegebene Kennwort für den Schlüsselspeicher, der Aliasname und das Schlüsselkennwort werden beim Konfigurieren der Konfiguration für den Dienstanbieter unter SSO-Konfigurationen in ECE verwendet.

![](_page_24_Figure_2.jpeg)

b. Exportieren Sie das Zertifikat:

Dieser keytool-Befehl exportiert die Zertifikatsdatei im .crt-Format mit dem Dateinamen

ece126web1a\_saml.crt in das Verzeichnis C:\Temp.

keytool -exportcert -alias ece126web1a\_saml -keystore C:\Temp\ece126web1a\_saml.jks -rfc -file C:\Temp\e

Schritt 12

Konfigurieren eines Identitätsanbieters

- 1. Wählen Sie in der AD FS-Verwaltungskonsole die Vertrauensstellung der vertrauenden Seite aus, die für ECE erstellt wurde, und klicken Sie mit der rechten Maustaste darauf.
- 2. Öffnen Sie das Eigenschaftenfenster für die Vertrauensstellung, und klicken Sie auf der Registerkarte Signatur auf die Schaltfläche Hinzufügen.
- 3. Fügen Sie das öffentliche Zertifikat (die .crt-Datei, die im vorherigen Schritt generiert wurde) hinzu, und klicken Sie auf OK.

## Erstellen und Importieren von Zertifikaten

Schritt 13

Vor der Konfiguration von SSO zur Verwendung von Cisco IDS für Single Sign-On für Agents muss das Tomcat-Zertifikat vom Cisco IdS-Server in die Anwendung importiert werden.

a. Klicken Sie in der ECE-Administratorkonsole im Menü auf Partitionsebene auf die Option Sicherheit, und wählen Sie dann im Menü auf der linken Seite die Option Zertifikatsverwaltung aus.

Enterprise Ch	at and Email			A O Partition Ac	ministrator ~
Partition ~		Apps	Departments Integration Language Tools	Security Services Storage System Resources	Tools User
۵,	à.				New
Access Restrictions	Name ÷	Component Type	Description	Expire Date	
Attachments	No items to display in list.				
Audit Log					
Certificate Management					
CORS					
Data Masking 🗸 🗸					
Rich Text Content Policy					
Settings					
Single Sign=On v					

b. Klicken Sie im Bereich Zertifikatsverwaltung auf die Schaltfläche Neu, und geben Sie die entsprechenden Details ein:

- Name: Geben Sie einen Namen für das Zertifikat ein.
- Beschreibung: Fügen Sie eine Beschreibung für das Zertifikat hinzu.
- Komponententyp: Wählen Sie CISCO IDS aus.
- Zertifikat importieren: Um das Zertifikat zu importieren, klicken Sie auf die Schaltfläche Suchen und Hinzufügen, und geben Sie die erforderlichen Details ein:

- Zertifikatsdatei: Klicken Sie auf die Schaltfläche Durchsuchen, und wählen Sie das Zertifikat aus, das Sie importieren möchten. Die Zertifikate können nur im Format .pem, .der (BINARY) oder .cer/cert importiert werden.
- Aliasname: Geben Sie einen Alias für Ihr Zertifikat an.
- c. Klicken Sie auf Speichern

ahaha

cisco Littorp	inse Cr	hat and Email		
Partition	~			
٩		Create Certificate		
Access Restrictions Attachments	~	Name*	Cisco IDS Server	
Audit Log		Description	Certificate for Cisco IdS Sen	ver
Certificate Management		Description		
CORS		0	0/000 /00	
Data Masking	~	Component Type*	CISCO IDS	~
Rich Text Content Policy		Import Certificate	ucce1261ids.cer	
Settings				
Cianta Cian On	~			

# Konfigurieren der einmaligen Anmeldung für den Agent

#### Schritt 14

- 1. Klicken Sie in der ECE-Administratorkonsole im Menü auf Partitionsebene auf die Option Sicherheit, und wählen Sie dann im Menü auf der linken Seite die Option Einmalige Anmeldung > Konfigurationen aus.
- 2. Wählen Sie im Dropdown-Menü "Konfiguration auswählen" den Agenten aus, und legen Sie die Konfiguration auf der Registerkarte Allgemein fest:
- Single Sign-On aktivieren: Klicken Sie auf die Schaltfläche "Umschalten", um SSO zu aktivieren.
- Single Sign-On Type: Wählen Sie Cisco IDS aus.

Enterprise Ch	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	~									
Audit Log	General SSO Configuration										
Certificate Management											
CORS	Name*	Agent Configuration									
Data Masking 🗸 🗸		Sinala Sian - On Continuation for									
Rich Text Content Policy	Description	agents									
Single Sign-On A	Enable Single Sign-On										
Licenses	Single Sign-On Type	Cisco IDS 🗸 🗸									
Providers											
										Cance	Save

Klicken Sie auf die Registerkarte SSO-Konfiguration, und geben Sie die Konfigurationsdetails an:

a. OpenID-Verbindungsanbieter

URL des Endpunkts für primäre Benutzerinformationen

- Die Endpunkt-URL für die Benutzerinformationen des primären Cisco IDS-Servers.
- Diese URL validiert die Benutzertoken-/Benutzerinfo-API.
- Das Format ist wie folgt: <u>https://cisco-ids-1:8553/ids/v1/oauth/userinfo</u>, wobei cisco-ids-1 den FQDN (Fully Qualified Domain Name) des primären Cisco IDS-Servers angibt.

Anspruchsname der Benutzeridentität

- Der Name des Anspruchs, der von der URL des Benutzerinformationsendpunkts zurückgegeben wird, der den Benutzernamen in Unified oder Packaged CCE identifiziert.
- Der Anspruchsname und der Benutzername in Unified oder Packaged CCE müssen übereinstimmen.
- Dies ist einer der Ansprüche, die als Reaktion auf die Validierung des Trägertokens erhalten wurden.
- Wenn der Benutzername der Agenten in Unified oder Packaged CCE mit dem Namen des Benutzerprinzips übereinstimmt, geben Sie "upn" als Wert für das Feld "Anspruchsname der Benutzeridentität" an.
- Wenn der Benutzername der Agenten in Unified oder Packaged CCE mit dem SAM-Kontonamen übereinstimmt, geben Sie als Wert für das Feld "User Identity Claim Name" (Anspruchname für Benutzeridentität) den Wert "sub" an.

URL des Endpunkts für sekundäre Benutzerinformationen

- Die URL des Info Endpoint des sekundären Benutzers des Cisco IDS-Servers.
- Das Format ist wie folgt: https://cisco-ids-2:8553/ids/v1/oauth/userinfo, wobei cisco-ids-2 den

FQDN (Fully Qualified Domain Name) des sekundären Cisco IDS-Servers angibt.

URL-Methode für Benutzerinfo-Endpunkt

- Die HTTP-Methode, die von ECE zum Durchführen von Validierungsaufrufen für Trägertoken an die URL des Endpunkts für Benutzerinformationen verwendet wird.
- Wählen Sie in der angezeigten Optionsliste POST aus (POST wird hier ausgewählt, um zur Methode des IDS-Servers zu passen).

POST: Methode zum Senden von Daten an den Cisco IDS-Server am angegebenen Endpunkt.

Cache-Dauer des Zugriffstokens (Sekunden)

- Die Dauer in Sekunden, für die ein Träger-Token in ECE zwischengespeichert werden muss.
- Trägertoken, für die Validierungsaufrufe erfolgreich sind, werden nur im Cache gespeichert. (Mindestwert: 1; Höchstwert: 30)

SSO-Anmeldung außerhalb von Finesse zulassen

- Klicken Sie auf diese Schaltfläche "Umschalten", wenn Benutzer mit Administrator- oder Supervisor-Rollen sich bei der Partition von ECE außerhalb von Finesse mit ihren SSO-Anmeldedaten anmelden sollen.
- Wenn diese Funktion aktiviert ist, müssen Informationen in den Abschnitten "Identitätsanbieter" und "Dienstanbieter" bereitgestellt werden.
- Dies erfordert, dass Ihre IdP-Konfiguration einen gemeinsamen IdP-Server zulässt.

![](_page_29_Picture_0.jpeg)

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 v
Providers		Access Token Cache Duration (Seconds)*	30
		Allow SSO Login Outside Finesse	

## b. Identitätsanbieter

Entitäts-ID

• Element-ID des IdP-Servers.

![](_page_30_Picture_0.jpeg)

Hinweis: Dieser Wert muss genau dem Wert 'Federation Service Identifier' in der AD FS-Verwaltungskonsole entsprechen.

۹	Configurations	Federation Service Properties X
Access Restrictions ~	Select Configuration Agent ~	Federation Service diaplay name: [J0123 ADFS Example: Software Federation Service Federation Service name:
Certificate Management	General SSO Configuration Identity Provider	WIN-260MECJBIC2.0123.local Example: fs fabrikan.com Extension: Sension kilettifer
Data Masking v	Entity ID*	http://WIN-260MECJ8IC2jo123.local/adfs/services.htust Example: http://fs/abrikam.com/adfs/services.htust
tich Text Content Policy Settings	Identity Provider Certificate*	Web SSO lifetime (minutes): 480 0
ingle Sign-On A Configurations	User Identity Location* SAML Subject Identifier	Deegae name:
Licenses Providers	User Identity Attribute Name*	Allow Local System account for service administration  Allow Local Administrations group for service administration
	Assertion Decryption Certificate* Enter Assertion Decryption Certificate	

Zertifikat des Identitätsanbieters

- Das Public-Key-Zertifikat.
- Das Zertifikat muss mit "-----BEGIN CERTIFICATE-----" beginnen und mit "-----END CERTIFICATE-----" enden.
- Dies ist das Tokensignaturzertifikat in der AD FS-Verwaltungskonsole > Dienst > Zertifikate > Tokensignatur.

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	Claim Descriptions Tol	Token-decrypting CN=ADFS Encryption - WIN-260MECJBIC2 jo 123 Jocal	CN=ADFS Encryption - W	1/31/2024
Identity Provider Certificate*	BEGIN CERTIFICATEMIIC8jC	Scope Descriptions	Token-signing Token-Signing - WIN-260MECJBIC2 jo123 local	CN=ADFS Signing - WIN	1/31/2024
User Identity Location*	SAML Subject Identifier	<ul> <li>Access Control Policies</li> <li>Relying Party Trusts</li> <li>Claims Provider Trusts</li> </ul>			
User Identity Attribute Name*		Application Groups			
Enable Encrypted Assertion	•				
Assertion Decryption Certificate*	Enter Assertion Decryption Certificate				

#### Standort der Benutzeridentität

- Wählen Sie SAML Subject Identifier (SAML-Betreff-ID) aus, um den Identitätsspeicherort im Zertifikat auf die standardmäßige SAML Subject Identifier (SAML-Betreff-ID) festzulegen, wie im Betreff in der SAML Assertion, z. B. dem Benutzernamen im <saml:Subject>.
- Wählen Sie SAML-Attribut aus, um den Identitätsspeicherort einem bestimmten Attribut im Zertifikat zuzuweisen, z. B. email.address. Geben Sie das Attribut in das Feld Name des Benutzeridentitätsattributs ein.

Name des Benutzeridentitätsattributs

- Gilt nur, wenn der Wert für den Standort der Benutzer-ID ein SAML-Attribut ist.
- Dies kann innerhalb der SAML-Assertion angepasst werden und verwendet werden, um ein anderes Attribut f
  ür die Authentifizierung von Benutzern auszuw
  ählen, z. B. eine E-Mail-Adresse.
- Es kann auch verwendet werden, um neue Benutzer mit einem SAML-Attribut zu erstellen.
- Wenn beispielsweise ein Benutzer anhand des im Attribut email.address angegebenen Werts identifiziert wird und der angegebene Wert der E-Mail-Adresse mit keinem Benutzer im System übereinstimmt, wird ein neuer Benutzer mit den angegebenen SAML-Attributen erstellt.

Verschlüsselte Aussage aktivieren (optional)

- Wenn Sie die verschlüsselte Assertion mit dem Identitätsanbieter für die Konsolenanmeldung aktivieren möchten, klicken Sie auf die Schaltfläche Umschalten, und legen Sie den Wert auf Aktiviert fest.
- Andernfalls setzen Sie den Wert auf Disabled (Deaktiviert).

Assertion-Entschlüsselungszertifikat

Wenn "Verschlüsselte Assertion aktivieren" auf "Aktiviert" gesetzt ist, klicken Sie auf die Schaltfläche Suchen und Hinzufügen, und bestätigen Sie, dass Sie das Zertifikat ändern möchten.

Geben Sie die Details im Fenster Assertion Decryption Certificate (Assertionsentschlüsselungszertifikat) an:

- Java Keystore File (Java-Keystore-Datei): Geben Sie den Dateipfad Ihrer Java Keystore-Datei an. Diese Datei hat das Format .jks und enthält den Entschlüsselungsschlüssel, den das System benötigt, um auf Dateien zuzugreifen, die durch den Identity Provider gesichert sind.
- Aliasname: Der eindeutige Bezeichner für den Entschlüsselungsschlüssel.
- Keystore Password: Das Kennwort, das für den Zugriff auf die Java Keystore-Datei erforderlich ist.
- Key Password (Schlüsselkennwort): Das Kennwort, das für den Zugriff auf den Entschlüsselungsschlüssel des Alias erforderlich ist.

![](_page_32_Picture_5.jpeg)

Hinweis: Dies muss mit dem Zertifikat auf der Registerkarte "Encryption" (Verschlüsselung) der konfigurierten ECE-Vertrauensstellung der vertrauenden Partei auf der AD FS-Verwaltungskonsole übereinstimmen.

#### c. Dienstleister

Vom Dienstanbieter initiierte Authentifizierung

• Legen Sie die Umschaltfläche auf Enabled (Aktiviert) fest.

#### Entitäts-ID

• Geben Sie die externe URL der ECE-Anwendung an.

Service Provider				ECE Console P	Properties				×
Service Provider Initiated Authentication				Organization Monitoring Specify the dis	Endpoints Identifiers splay name and	Proxy End Encryption didentifiers for	dpoints N Signature this relying pa	lotes Acc arty trust	Advanced epted Claims
Entity ID*	https://ece126web1a.jo123.local/			Display nam ECE Consol	ne: le				
Request Signing Certificate*			0	Relying part	ty identifier:				Add
Signing Algorithm*	SHA-256 ~	•		Example: ht Relying part	tps://fs.contos ty identifiers:	co.com/adfs/s	ervices/trust		Deserve
Identity Provider Login URL*	https://WIN-260MECJBIC2.jo123.loc			mipsinece	120web1a.jo1.	23306817			Remove
Identity Provider Logout URL	https://ece126web1a.jo123.local/def								

#### Signaturzertifikat anfordern

- Ein Java Keystore (JKS)-Zertifikat ist erforderlich, um die erforderlichen Informationen bereitzustellen.
- Laden Sie die JKS-Datei mit dem Aliasnamen und dem Schlüsselspeicher/Schlüsselkennwort hoch, die in Schritt 11 generiert wurden.

![](_page_34_Picture_0.jpeg)

Hinweis: Dies muss mit dem Zertifikat übereinstimmen, das auf die Registerkarte "Signature" der konfigurierten ECE Relying Party Trust auf der AD FS-Verwaltungskonsole hochgeladen wurde.

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*	••••	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	

Signaturalgorithmus

- Legen Sie den Signaturalgorithmus für den Dienstanbieter fest.
- Bei Verwendung von ADFS muss dieser Wert mit dem Algorithmus übereinstimmen, der in der Vertrauensstellung der vertrauenden Seite ausgewählt wurde, die für ECE auf der Registerkarte "Advanced" (Erweitert) erstellt wurde.

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*	****	0		
Signing Algorithm*	SHA-256 🗸			
Identity Provider Login URL*	https://WIN-260MECJBIC2.jo123.loc			
Identity Provider Logout URL	https://ece126web1a.jo123.local/def			

Anmelde-URL des Identitätsanbieters

- Die URL für die SAML-Authentifizierung.
- Für ADFS ist dies beispielsweise <u>http://<ADFS>/adfs/ls</u>.

Abmelde-URL des Identitätsanbieters

- Die URL, zu der Benutzer beim Abmelden umgeleitet werden. Dies ist optional und kann eine beliebige URL sein.
- Agenten können beispielsweise nach der SSO-Abmeldung an https://www.cisco.com oder eine andere URL umgeleitet werden.

Schritt 16

Klicken Sie auf Save (Speichern).

Festlegen der Webserver-/LB-URL in den Partitionseinstellungen

Schritt 17

Stellen Sie sicher, dass der richtige Webserver/LB-URL unter Partitionseinstellungen eingegeben wurde. Wählen Sie die Registerkarte Apps aus, und navigieren Sie zu Allgemeine Einstellungen > Externe URL der Anwendung.

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

# Konfigurieren von SSO für Partitionsadministratoren

![](_page_36_Picture_2.jpeg)

Anmerkung:

- Dieser Schritt gilt nur für PCCE.
- Dies gilt für das ECE-Gadget, auf das über die CCE-Admin-Webschnittstelle https:///cceadmin zugegriffen wird.

## Schritt 18

So konfigurieren Sie SSO für den Partitionsadministrator

- Klicken Sie in der ECE-Administratorkonsole im Menü auf Partitionsebene auf die Option Sicherheit, und wählen Sie dann im Menü links die Option Einmalige Anmeldung > Konfigurationen aus.
- 2. Wählen Sie im Dropdown-Menü "Konfiguration auswählen" die Option "Partitionsadministratoren" aus, und geben Sie die Konfigurationsdetails ein:

### LDAP-URL

- Die URL des LDAP-Servers.
- Dabei kann es sich um die URL des Domänencontrollers (z. B. Idap://LDAP\_server:389) oder die URL des globalen Katalogs (z. B. Idap://LDAP\_server:3268) des LDAP-Servers handeln.
- Die Partition kann dem System automatisch hinzugefügt werden, wenn über die CCE-Verwaltungskonsole auf ECE zugegriffen wird, wenn ECE mit LDAP-Suche konfiguriert wurde.
- In Active Directory-Bereitstellungen mit mehreren Domänen in einer Gesamtstruktur oder bei denen alternative UPNs konfiguriert sind, darf die Domänencontroller-URL mit den standardmäßigen LDAP-Ports 389 und 636 jedoch nicht verwendet werden.
- Die LDAP-Integration kann für die Verwendung der URL des globalen Katalogs mit den Ports 3268 und 3269 konfiguriert werden.

![](_page_38_Picture_0.jpeg)

Hinweis: Es wird empfohlen, die URL des globalen Katalogs zu verwenden. Wenn Sie keinen GC verwenden, wird ein Fehler in den ApplicationServer-Protokollen wie folgt angezeigt.

 Ausnahme bei LDAP-Authentifizierung <@> javax.naming.PartialResultException: Nicht verarbeitete(r) Fortsetzungsverweis(e); verbleibender Name "DC=example,DC=com"

## **DN-Attribut**

- Das Attribut des DN, der den Benutzernamen enthält.
- Beispiel: userPrincipalName.

#### Basis

- Der für Base angegebene Wert wird von der Anwendung als Suchbasis verwendet.
- Die Suchbasis ist der Ausgangspunkt für die Suche in der LDAP-Verzeichnisstruktur.
- Beispiel: DC=mycompany, DC=com.

#### DN für LDAP-Suche

- Wenn Ihr LDAP-System keine anonyme Bindung zulässt, geben Sie den Distinguished Name (DN) eines Benutzers ein, der über Suchberechtigungen für die LDAP-Verzeichnisstruktur verfügt.
- Wenn der LDAP-Server eine anonyme Bindung zulässt, lassen Sie dieses Feld leer.

Kennwort

- Wenn Ihr LDAP-System keine anonyme Bindung zulässt, geben Sie das Kennwort eines Benutzers ein, der über Suchberechtigungen für die LDAP-Verzeichnisstruktur verfügt.
- Wenn der LDAP-Server eine anonyme Bindung zulässt, lassen Sie dieses Feld leer.

### Schritt 19

Klicken Sie auf Save (Speichern).

Damit ist die Konfiguration der einmaligen Anmeldung für Agenten und Partitionsadministratoren in ECE abgeschlossen.

# Fehlerbehebung

## Trace-Ebene festlegen

- 1. Klicken Sie in der ECE-Admin-Konsole im Menü auf Partitionsebene auf die Option Systemressourcen und wählen Sie dann im Menü auf der linken Seite die Option Prozessprotokolle aus.
- Wählen Sie aus der Liste der Prozesse den ApplicationServer-Prozess aus > legen Sie die gewünschte Ablaufverfolgungsebene im Dropdown-Menü "Maximale Ablaufverfolgungsebene" fest.

![](_page_40_Picture_0.jpeg)

Anmerkung:

- Um die SSO-Anmeldefehler während der Ersteinrichtung oder Neukonfiguration zu beheben, legen Sie die Ablaufverfolgung des ApplicationServer-Prozesses auf Ebene 7 fest.
- Sobald der Fehler reproduziert wurde, setzen Sie die Ablaufverfolgungsebene auf die Standardebene 4 zurück, um das Überschreiben der Protokolle zu vermeiden.

Enterprise Cl	hat and Email	🐥 🔕 Partition Administrator ~			
Partition 👻	Apps Departm	nents Integration Language Tools Security Services Storage System Resources Tools User			
à.	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			
	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 A	dvanced Logging		
	Name		ece126app1a:ApplicationServer	
	Description		ece126app1a:ApplicationServer	
	Maximum Trace Le	vel	4 - Info	^
	Log File Name		8 - Trace 7 - Debug	^
	Maximum File Size		6 - Dbquery 5 - Perf	
	Extensive Logging	Duration	4 - Info	~ <b>,</b>
	Extensive Logging	End Time		

# Fehlerbehebung - Szenario 1

Fehler

- Fehlercode: 500
- Fehlerbeschreibung: Die Anwendung kann sich beim Benutzer derzeit nicht anmelden, da die Identity Provider-Anmeldung fehlgeschlagen ist.

#### Protokollanalyse

- Fehler bei der IdP-Anmeldung <samlp:Status><samlp:StatusCode</li>
   Value="urn:oasis:names:tc:SAML:2.0:status:Responder" /></samlp:Status>
- Hier zeigt der Status "Responder" an, dass ein Problem auf AD FS-Seite vorliegt in diesem Fall primär mit dem auf der ECE-Admin-Konsole hochgeladenen "Request Signing Certificate" (SSO-Konfiguration > Service Provider) und dem auf der Registerkarte "Signature" in die ECE Relying Party Trust hochgeladenen Zertifikat.
- Dies ist das Zertifikat, das mit der Java Keystore-Datei generiert wird.

Anwendungsserver-Protokolle - Ablaufverfolgungsebene 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

#### Auflösung

- Weitere Informationen finden Sie in der Konfiguration "Request Signing Certificate" im Abschnitt "Configuring Agent Single Sign-On Service Provider".
- Stellen Sie sicher, dass die in Schritt 11 generierte JKS-Datei für den Java Keystore in das

Feld "Request Signing certificate" auf der ECE-Administratorkonsole unter SSO Configuration > Select Configuration 'Agent' > 'SSO Configuration' (SSO-Konfiguration auswählen) > Service Provider > Request Signing certificate hochgeladen wird.

• Stellen Sie sicher, dass die CRT-Datei auf der Registerkarte "Signature" der Vertrauensstellung der ECE-vertrauenden Partei hochgeladen wird (Schritt 12).

#### Fehlerbehebung - Szenario 2

#### Fehler

- Fehlercode: 400
- Fehlerbeschreibung: Das SAML-Antworttoken ist ungültig: Die Signaturüberprüfung ist fehlgeschlagen.

#### Protokollanalyse

• Dieser Fehler weist darauf hin, dass das Zertifikat nicht mit dem Token-Signaturzertifikat von ADFS und dem Identitätsanbieter-Zertifikat der ECE SSO-Konfiguration übereinstimmt.

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

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

#### Auflösung

- Der Fehler im Protokollausschnitt 'Zertifikat konnte nicht analysiert werden: java.io.IOAusnahme: Unvollständige Daten' weist darauf hin, dass der Inhalt des 'Identity Provider Certificate' nicht richtig eingegeben wurde.
- So beheben Sie dieses Problem: Auf der AS FS-Verwaltung > AD FS > Dienst > Zertifikate > Token-Signing > Dieses Zertifikat exportieren > in einem Texteditor öffnen > alle Inhalte kopieren > unter "Identity Provider Certificate" in der SSO-Konfiguration einfügen > Speichern.
- Weitere Informationen finden Sie in der Konfiguration für das "Identity Provider Certificate" im Abschnitt "Configuring Agent single sign-on Identity Provider" (Schritt 15).

### Fehlerbehebung - Szenario 3

Fehler

- Fehlercode: 401-114
- Fehlerbeschreibung: Die Benutzeridentität wurde im SAML-Attribut nicht gefunden.

#### Protokollanalyse

Anwendungsserver-Protokolle - Ablaufverfolgungsebene 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.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 <@

Auflösung

- Dieser Fehler weist auf ein Konfigurationsproblem/eine Diskrepanz in den Feldern "User Identity Location" (Standort der Benutzeridentität) und "User Identity Attribute Name" (Attributname der Benutzeridentität) hin.
- Überprüfen und korrigieren Sie den 'User Identity Location' und den 'User Identity Attribute Name' in der ECE-Admin-Konsole unter Single Sign-On > Configurations > im Dropdown-Menü "Select Configuration" die Option Agent > SSO Configuration tab > Identify Provider (Schritt 15).

# Zugehörige Informationen

Dies sind die wichtigsten Dokumente, die vor der Installation oder Integration von ECE eingehend geprüft werden müssen. Dies ist keine umfassende Liste von ECE-Dokumenten.

![](_page_46_Picture_0.jpeg)

Anmerkung:

- Die meisten ECE-Dokumente haben zwei Versionen. Bitte stellen Sie sicher, dass Sie die Versionen für PCCE herunterladen und verwenden. Der Dokumenttitel enthält entweder für Packaged Contact Center Enterprise oder (für PCCE) oder (für UCCE und PCCE) die Versionsnummer.
- Überprüfen Sie vor der Installation, dem Upgrade oder der Integration auf der Startseite der Cisco Enterprise Chat- und E-Mail-Dokumentation auf Updates.
- https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chatemail/series.html

ECE-Version 12.6(1)

• Administratorhandbuch für Enterprise-Chat und -E-Mails

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.