Integration von ECE mit PCCE in Version 12.0 und höher

Inhalt

Einführung

Dieses Dokument beschreibt die Schritte zur Integration von Enterprise Chat und E-Mail (ECE) in Packaged Contact Center Enterprise (PCCE) in Version 12.0 und höher.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Enterprise Chat und E-Mail (ECE) 12.x
- Packaged Contact Center Enterprise (PCCE) 12.x

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- ECE 12.5(1)
- PCCE 12.5(1)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Mit der PCCE-Version 12.0 wurde eine neue Verwaltungsschnittstelle eingeführt, die Single Pane of Glass (SPOG) genannt wird. Fast die gesamte Verwaltung des Contact Centers und der zugehörigen Anwendungen erfolgt nun über diese Schnittstelle. Um ECE und PCCE richtig zu integrieren, müssen Sie mehrere Schritte ausführen, die für diese Integration einzigartig sind. Dieses Dokument führt Sie durch diesen Prozess.

Terminologie

In diesem Dokument werden diese Begriffe verwendet.

- Enterprise Chat und E-Mail (ECE) - ECE ist ein Produkt, mit dem E-Mail- und Chat-Anfragen genauso an Contact Center-Agenten weitergeleitet werden können wie Sprachanrufe.
- Single Pane of Glass (SPOG) - SPOG ist die Methode, mit der die PCCE-Administration in Version 12.0 und höher ausgeführt wird. SPOG ist eine vollständige Neufassung des CCE Administration Tools, das in Versionen vor 12.0 verwendet wurde.
- Zertifizierungsstelle (Certificate Authority, CA) - Eine Stelle, die digitale Zertifikate gemäß einem PKI-Modell (Public Key Infrastructure) ausstellt. Es gibt zwei Arten von CAs, auf die Sie stoßen können.Öffentliche Zertifizierungsstelle - Eine öffentliche Zertifizierungsstelle verfügt über ihre Stamm- und Zwischenzertifikate, die in den meisten Browsern und Betriebssystemen enthalten sind. Zu den gängigen öffentlichen CAs gehören IdenTrust, DigiCert, GoDaddy und GlobalSign.Private CA - Eine private CA ist eine, die innerhalb eines Unternehmens existiert. Einige private CAs werden von öffentlichen CAs signiert, aber meistens handelt es sich dabei um eigenständige CAs, und die Zertifikate, die sie ausstellen, werden nur von Computern in dieser Organisation als vertrauenswürdig eingestuft.Innerhalb eines der beiden CA-Typen gibt es zwei Typen von CA-Servern.Root CA Server - Der Root CA Server signiert sein eigenes Zertifikat. Bei der standardmäßigen, mehrschichtigen PKI-Bereitstellung ist die Root CA offline und kann nicht darauf zugegriffen werden. Die Root-CA dieses Modells gibt auch nur Zertifikate für einen anderen CA-Server aus, der als Erweiterte Zertifizierungsstelle bezeichnet wird. Einige Unternehmen verwenden nur eine Single-Tier-

Zertifizierungsstelle. In diesem Modell gibt die Stammzertifizierungsstelle Zertifikate aus, die für die Verwendung durch eine andere Entität als einen anderen CA-Server bestimmt sind.Erweiterte CA-Server - Der Zwischenserver oder der ausstellende CA-Server gibt Zertifikate aus, die für die Verwendung durch eine andere Einheit als einen anderen CA-Server bestimmt sind.

- Microsoft Management Console (MMC) - Eine in Microsoft Windows enthaltene Anwendung, die das Laden verschiedener Snap-Ins ermöglicht. Mithilfe der Snap-Ins können Sie eine benutzerdefinierte Konsole für die Serververwaltung erstellen. Windows enthält viele verschiedene Snap-Ins. Eine kurze Liste von Beispielen enthält Zertifikate, Geräte-Manager, Datenträgerverwaltung, Ereignisanzeige und Dienste.
- Network Load Balancer (NLB) - Ein Gerät oder eine Anwendung, das bzw. die mehreren physischen Ressourcen für Endbenutzer mit einem gemeinsamen physischen Namen bereitstellt. NLBs werden häufig für Webanwendungen und -dienste verwendet. NLBs können auf viele Arten implementiert werden. Bei Verwendung mit ECE muss der NLB so konfiguriert werden, dass Benutzersitzungen mithilfe von Cookie-Einfügen oder einer gleichwertigen Methode zum selben physischen Back-End-Webserver zurückkehren. Dies wird als Haftsitzung mit Cookie-Insert bezeichnet. Sticky Session bezieht sich einfach auf die Fähigkeit eines Load Balancers, eine Benutzersitzung für alle Interaktionen an denselben physischen Back-End-Server zurückzugeben. Secure Sockets Layer (SSL) Passthrough - SSL-Passthrough ist eine Methode, bei der die SSL-Sitzung zwischen dem Endbenutzergerät und dem physischen Webserver, dem die Benutzersitzung zugewiesen wurde, besteht. SSL-Passthrough erlaubt kein Einfügen von Cookies, da die HTTP-Sitzung jederzeit physisch verschlüsselt ist. Die meisten NLBs unterstützen eine Haftsitzung mit SSL Passthrough mithilfe von Stangentabellen, die den ServerHello- und clienthello-Teil der Sitzungseinrichtung überwachen und die eindeutigen Werte in einer Tabelle speichern. Wenn die nächste Anforderung, die diesen Werten entspricht, dem NLB angezeigt wird, kann die Stick-Tabelle verwendet werden, um die Sitzung an denselben Back-End-Server zurückzugeben.SSL-Offload - Wenn ein NLB für die SSL-Offload konfiguriert ist, gibt es zwei SSL-Sitzungen oder -Tunnel, die für eine bestimmte Endbenutzersitzung vorhanden sind. Die erste Adresse besteht zwischen dem Endbenutzergerät und der virtuellen IP (VIP), die auf dem NLB für die Website konfiguriert ist. Die zweite ist zwischen der Back-End-IP-Adresse des NLB und dem physischen Webserver, dem die Sitzung des Benutzers zugewiesen ist. SSL-Offload unterstützt Cookie-Insert, da der HTTP-Stream vollständig entschlüsselt wird, während auf dem NLB zusätzliche HTTP-Cookies eingefügt und Sitzungsprüfungen durchgeführt werden können. SSL-Offloads werden häufig verwendet, wenn die Webanwendung kein SSL benötigt, sondern aus Sicherheitsgründen erfolgt. Die aktuellen ECE-Versionen unterstützen den Zugriff auf die Anwendung in einer Nicht-SSL-Sitzung nicht.

Erforderliche Schritte

Es gibt mehrere Voraussetzungen, die erfüllt sein müssen, bevor Sie mit der Integration der beiden Systeme beginnen.

- Minimaler PCCE-Patch-Level Version 12.0(1) - ES37Version 12.5(1) - Derzeit kein Mindestumfang für Basisfunktionen
  WebEx Experience Management (WXM) Analyzer-Funktion erfordert ES7
- ECE-Patch-Level mindestens Es wird empfohlen, dass ECE die neueste verfügbare

Engineering Special (ES) ausführt.Version 12.0(1) - ES3 + ES3_ET1aVersion 12.5(1) - Derzeit kein Mindestumfang für Basisfunktionen
WXM Analyzer-Funktion erfordert ES1

- Konfigurationselemente Stellen Sie sicher, dass Sie die ECE_Email-, ECE_Chat- und ECE_Outbound Media Routing Domains (MRDs) der richtigen Anwendungsinstanz zuordnen.Für das PCCE 2000 Agent-Bereitstellungsmodell ist die Anwendungsinstanz MultiChannel.Für das PCCE 4000/12000 Agent-Bereitstellungsmodell besteht die Anwendungsinstanz in Form von {site}_{peripherer_set}_{application_instance}.
  Wenn Sie PCCE mit dem Standortnamen Main (Main), einem Peripheriegerät (PS1) und einer Anwendungsinstanz als Multichannel installiert haben, lautet der Name der Anwendungsinstanz Main_PS1_Multichannel.**Hinweis**: Beim Namen der Anwendungsinstanz wird Groß- und Kleinschreibung unterschieden. Stellen Sie sicher, dass Sie den Namen korrekt eingeben, wenn Sie den ECE-Webserver zum Bestand hinzufügen.

Integrationsschritte

Die Details zu allen Schritten in diesem Dokument sind in der Dokumentation für ECE und PCCE enthalten, aber sie sind nicht in einer Liste aufgeführt und auch nicht alle in demselben Dokument enthalten. Weitere Informationen finden Sie unter den am Ende dieses Dokuments enthaltenen Links.

Schritt 1: Konfigurieren von SSL-Zertifikaten

Sie müssen ein Zertifikat für die Verwendung durch den ECE-Webserver generieren. Sie können ein selbstsigniertes Zertifikat verwenden, aber es ist oft einfacher, ein Zertifizierungsstellen-signiertes Zertifikat zu verwenden. Selbstsignierte Zertifikate sind nicht weniger sicher als Zertifizierungsstellen signierte Zertifikate, es gibt weniger Schritte zum Erstellen des Zertifikats. Wenn das Zertifikat jedoch ausgetauscht werden muss, müssen Sie daran denken, das neue Zertifikat in die Java-Tastaturen auf allen PCCE Administration-Datenservern hochzuladen. Wenn Sie ein Zertifikat mit CA-Vorzeichen verwenden, müssen Sie nur die Root- und ggf. Zwischenzertifikate in die Keystores hochladen.

Wenn Ihre Bereitstellung mehrere Webserver umfasst, müssen Sie diese Richtlinien durchgehen. Die für die Konfiguration eines Netzwerk Load Balancers erforderlichen Schritte werden in diesem Dokument nicht behandelt. Wenden Sie sich bei Bedarf an Ihren Load Balancer-Anbieter.

Ein Load Balancer ist nicht erforderlich, vereinfacht jedoch die Implementierung erheblich.

Der Zugriff auf die ECE-Anwendung auf jedem Webserver muss unabhängig von der verwendeten Load Balancer-Methode SSL verwenden.

Der Load Balancer kann entweder als SSL-Passthrough oder SSL-Offload konfiguriert werden.

Wenn SSL-Passthrough ausgewählt ist, muss Folgendes ausgeführt werden: Sie müssen alle Zertifikatsvorgänge auf einem Server ausführen.

Nach der ordnungsgemäßen Konfiguration des Zertifikats müssen Sie das Zertifikat exportieren und sicherstellen, dass der private Schlüssel in eine PFX-Datei (Personal Information Exchange) aufgenommen wird.

Sie müssen die PFX-Datei auf alle anderen Webserver in der Bereitstellung kopieren und anschließend in IIS importieren.

Wenn SSL Offload ausgewählt wird, kann jeder Webserver mit einem eigenen SSL-Zertifikat konfiguriert werden.

> **Hinweis**: Wenn Sie mehrere Webserver haben und SSL-Passthrough auf Ihrem Webserver auswählen oder wenn Sie ein gemeinsames Zertifikat auf allen Servern haben möchten, müssen Sie einen Webserver auswählen, um Schritt 1 auszuführen, und das Zertifikat dann auf alle anderen Webserver importieren.
> Wenn Sie SSL Offload auswählen, müssen Sie diese Schritte auf allen Webservern ausführen. Sie müssen auch ein Zertifikat generieren, das auf dem Load Balancer verwendet werden kann.

Schritt 1.1: Erstellen eines Zertifikats

Sie können diesen Abschnitt überspringen, wenn Sie bereits ein Zertifikat erstellt oder erhalten haben. Wählen Sie andernfalls eine der beiden Optionen aus.

Option 1: Verwenden eines selbstsignierten Zertifikats

1. Navigieren Sie zu IIS Administration.
2. Wählen Sie den Servernamen in der Struktur Verbindungen auf der linken Seite aus.
3. Suchen Sie im mittleren Bereich nach **Serverzertifikaten**, und doppelklicken Sie auf diese, um sie zu öffnen.
4. Wählen Sie **selbst signiertes Zertifikat erstellen...** im Bereich Aktionen rechts.
5. Wählen Sie im Fenster **Selbstsigniertes Zertifikat erstellen** einen Namen aus, und geben Sie im Feld **Angezeigter Name für das Zertifikat angeben** einen Namen ein: Box. Mit diesem Namen wird das Zertifikat im Auswahlprozess im nächsten Hauptschritt angezeigt. Dieser Name muss nicht mit dem gebräuchlichen Namen des Zertifikats übereinstimmen und hat keinen Einfluss darauf, wie das Zertifikat für den Endbenutzer angezeigt wird.
6. Stellen Sie sicher, dass **Personal** im Feld **Zertifikatsspeicher für das neue Zertifikat auswählen aktiviert ist:** aus.
7. Wählen Sie **OK**, um das Zertifikat zu erstellen.
8. Fahren Sie mit dem nächsten wichtigen Schritt fort, dem **Bind-Zertifikat an Website**.

Option 2: Verwenden eines Zertifikats mit CA-Vorzeichen

Für Zertifikate mit CA-Vorzeichen müssen Sie eine CSR-Anfrage (Certificate Signing Request) erstellen. Die CSR ist eine Textdatei, die dann an die Zertifizierungsstelle gesendet wird, wo sie signiert ist. Anschließend wird das signierte Zertifikat zusammen mit den erforderlichen Zertifizierungsstellenzertifikaten zurückgegeben und die CSR-Nummer erfüllt. Sie können dies über die IIS-Administration oder die Microsoft Management Console (MMC) tun. Die IIS-Verwaltungsmethode ist viel einfacher, da keine speziellen Kenntnisse erforderlich sind. Sie können jedoch nur die Felder konfigurieren, die im Subject-Attribut des Zertifikats enthalten sind, und die Bitlänge ändern. MMC erfordert zusätzliche Schritte und dass Sie über umfassende Kenntnisse aller Felder verfügen, die in einem gültigen CSR erforderlich sind. Es wird dringend empfohlen, MMC nur zu verwenden, wenn Sie über moderate bis fachkundige Erfahrung bei der Erstellung und Verwaltung von Zertifikaten verfügen. Wenn für die Bereitstellung der Zugriff auf

ECE durch mehr als einen vollqualifizierten Namen erforderlich ist oder Sie einen Teil des Zertifikats außer dem Betreff und der Bitlänge ändern müssen, müssen Sie die MMC-Methode verwenden.

1. Über IIS-Administration Verwenden Sie diese Schritte, um über den IIS-Manager eine CSR-Anfrage (Certificate Signing Request) zu generieren.Navigieren Sie zu IIS Administration.Wählen Sie den Servernamen in der Struktur Verbindungen auf der linken Seite aus.Suchen Sie im mittleren Bereich nach **Serverzertifikaten**, und doppelklicken Sie auf diese, um sie zu öffnen.Wählen Sie **Zertifikatsanforderung erstellen.. aus.** im Bereich Aktionen rechts. Der Assistent **zum Anfordern von Zertifikaten** wird angezeigt.Geben Sie auf der Seite **Eigenschaften** für **eindeutige Namen** die Werte im Formular für Ihr System ein. Alle Felder müssen eingegeben werden. Wählen Sie **Weiter**, um fortzufahren.Lassen Sie auf der Seite **Eigenschaften** für **kryptografische Dienstanbieter** die Standardauswahl für **Kryptografiedienstanbieter:**. Ändern Sie die **Bit-Länge:** auf einen Wert von mindestens **2048**. Wählen Sie **Weiter**, um fortzufahren.Wählen Sie auf der Seite **Dateiname** einen Speicherort für die CSR-Datei aus.Übergeben Sie die Datei an die CA. Wenn Sie das signierte Zertifikat erhalten haben, kopieren Sie es auf den Webserver, und fahren Sie mit dem nächsten Schritt fort.Wählen Sie am gleichen Speicherort im IIS-Manager im Bereich **Aktionen** die Option **Complete Certificate Request** (**Abschlusszertifikatanforderung**) aus. Der Assistent wird angezeigt.Wählen Sie auf der Seite **Response der Zertifizierungsstelle angeben** das von Ihrer Zertifizierungsstelle bereitgestellte Zertifikat aus. Geben Sie einen Namen in das Feld **Freundlicher Name** ein. Mit diesem Namen wird das Zertifikat im Auswahlprozess im nächsten Hauptschritt angezeigt. Vergewissern Sie sich, dass **im Feld Zertifikatsspeicher für das neue Zertifikat auswählen Folgendes angezeigt wird:** -Dropdown-Menü auf **Persönlich** eingestellt.Wählen Sie **OK**, um den Zertifikatshochladen abzuschließen.Fahren Sie mit dem nächsten wichtigen Schritt fort, dem **Bind-Zertifikat an Website**.
2. über Microsoft Management Console (MMC) Verwenden Sie diese Schritte, um eine CSR-Anfrage über MMC zu generieren. Mit dieser Methode können Sie jeden Aspekt der CSR-Anfrage anpassen.Klicken Sie mit der rechten Maustaste auf die Schaltfläche Start, und wählen Sie Ausführen aus.Geben Sie **mmc** in das Feld Ausführen ein, und wählen Sie **OK aus**.Fügen Sie das Certificate-Snap-In dem MMC-Fenster hinzu. Wählen Sie **Datei** und dann **Snap-In hinzufügen/entfernen aus...**. Das Feld **Snap-Ins hinzufügen oder entfernen** wird angezeigt.Suchen Sie in der Liste links nach **Zertifikaten**, und wählen Sie **Hinzufügen >**. Das Snap-In Certificates wird angezeigt.Wählen Sie die Option **Computerkonto** und dann **Weiter >**.Stellen Sie sicher, dass der **lokale Computer: (der Computer, auf dem diese Konsole installiert ist)** auf der Seite **Computer auswählen** ausgewählt ist, wählen Sie **Beenden** aus.Wählen Sie **OK**, um das Feld **Snap-Ins hinzufügen oder entfernen** zu schließen.CSR erstellen Erweitern Sie im linken Teilfenster **Zertifikate (Lokaler Computer)** und dann **Personal**, und wählen Sie den Ordner **Zertifikate aus**.Klicken Sie mit der rechten Maustaste auf den Ordner **Zertifikate**, und navigieren Sie zu **Alle Aufgaben > Erweiterte Vorgänge >**, und wählen Sie dann **Benutzerdefinierte Anforderung erstellen aus...**. Der Assistent **für die Zertifikatsregistrierung** wird angezeigt.Wählen Sie im Einführungsbildschirm **Weiter** aus.Wählen Sie auf der Seite **Select Certificate Enrollment Policy (Richtlinie für die Zertifikatsregistrierung** auswählen) die Option **Proceed without enrollment policy (Ohne Registrierungs-Richtlinie fortsetzen**) aus, die unter **Custom Request (Benutzerdefinierte Anforderung)** aufgelistet ist, und wählen Sie dann **Next (Weiter)**.Stellen Sie auf der Seite **Benutzerdefinierte Anforderung** sicher, dass die ausgewählte **Vorlage (Keine Vorlage) CNG-**

Schlüssel ist und das **Anforderungsformat** für Ihre CA geeignet ist. **PKCS #10** funktioniert mit der Microsoft CA. Wählen Sie **Weiter**, um zur nächsten Seite zu gelangen.Wählen Sie auf der Seite **Zertifikatinformationen** das Dropdown-Menü neben dem Wort **Details aus**, und wählen Sie dann die Schaltfläche **Eigenschaften** aus. Das Formular **Zertifikateigenschaften** wird angezeigt.Alle Optionen für das Formular **Eigenschaften** für **Zertifikate** werden nicht in den Anwendungsbereich dieses Dokuments aufgenommen. Weitere Informationen finden Sie in der Microsoft-Dokumentation. Hier sind einige Hinweise und Tipps auf diesem Formular. Stellen Sie sicher, dass Sie alle erforderlichen Werte im **Betreffnamen** eingeben**:** Abschnitt des **Betreffs:** TabulatorStellen Sie sicher, dass der für **Common name** angegebene Wert auch im **Alternativnamen** angegeben ist**:** AbschnittLegen Sie den **Typ fest:** in **DNS**, geben Sie die URL in den **Wert:** und anschließend die Schaltfläche **Hinzufügen >** auswählen.Wenn Sie mehrere URLs für den Zugriff auf die ECE verwenden möchten, geben Sie jeden alternativen Namen in diesem Feld an, und wählen Sie **Add >** nachher aus.Stellen Sie sicher, dass die **Schlüsselgröße** auf der Registerkarte **Privater Schlüssel** auf einen Wert größer als 1024 festgelegt ist.Wenn Sie das Zertifikat für die Verwendung auf mehreren Webservern exportieren möchten, wie es häufig bei einer HA-Installation der Fall ist, stellen Sie sicher, dass Sie **Privaten Schlüssel exportieren** auswählen. Wenn Sie dies nicht tun, kann das Zertifikat zu einem späteren Zeitpunkt nicht exportiert werden.Die von Ihnen eingegebenen Werte und die von Ihnen ausgewählten Werte werden nicht validiert. Sie müssen sicherstellen, dass Sie alle erforderlichen Informationen angeben, oder die Zertifizierungsstelle kann die CSR-Anfrage nicht abschließen.Wenn Sie alle Auswahlen ausgewählt haben, **OK**, um zum Assistenten zurückzukehren. Wählen Sie **Weiter**, um zur nächsten Seite zu gelangen.Klicken Sie auf **Wo möchten Sie die Offline-Anfrage speichern?** einen Dateinamen an einem Speicherort aus, auf den Sie zugreifen können. Für die meisten CAs sollten Sie **Base 64** als Format auswählen.Übergeben Sie die Datei an Ihre CA. Wenn sie es signiert und Ihnen das Zertifikat zurückgegeben haben, kopieren Sie das Zertifikat auf den Webserver, und fahren Sie mit den letzten Schritten fort.Navigieren Sie im MMC-Snap-In für die Zertifikatsverwaltung zu **Certificates (Local Computer) > Personal**, klicken Sie mit der rechten Maustaste auf **Certificates**, und wählen Sie **All Tasks > Import.. (Alle Aufgaben > Importieren..) aus.**. Der **Assistent zum Importieren von Zertifikaten** wird angezeigt.Wählen Sie im Einführungsbildschirm **Weiter** aus.Wählen Sie im Bildschirm **Datei für den Import** das Zertifikat aus, das von Ihrer CA signiert wurde, und wählen Sie dann **Weiter**.Wählen Sie **Alle Zertifikate im folgenden Speicher platzieren aus**.Stellen Sie sicher, dass **Personal** im **Zertifikatsspeicher** ausgewählt ist**:** und dann **Weiter** auswählen.Überprüfen Sie den letzten Bildschirm, und wählen Sie dann **Fertig stellen**, um den Import abzuschließen.Sie können jetzt die MMC-Konsole schließen. Wenn Sie aufgefordert werden, die Konsoleneinstellungen zu speichern, können Sie **Nein** auswählen. Dies hat keinen Einfluss auf den Zertifikatsimport.Fahren Sie mit dem nächsten wichtigen Schritt fort, dem **Bind-Zertifikat an Website**.

Schritt 1.2: Binden des Zertifikats an die Website

Vorsicht: Sie müssen sicherstellen, dass das Feld Hostname leer bleibt und die Option Servernamenindizierung vorschreiben nicht im Feld Seitenbindung bearbeiten aktiviert ist. Wenn eine dieser Optionen konfiguriert ist, schlägt SPOG fehl, wenn versucht wird, mit ECE zu kommunizieren

1. Öffnen Sie den IIS-Manager (Internetinformationsdienste), wenn Sie dies zuvor noch nicht getan haben.
2. Navigieren Sie im Bereich **Verbindungen** links zu **Sites,** und wählen Sie **Standardwebsite aus**. Stellen Sie sicher, dass Sie den korrekten Sitenamen auswählen, wenn Sie einen anderen Sitenamen als die Standardwebsite verwendet haben.
3. **Bindungen** auswählen**..** im **Aktionsbereich** rechts. Das Feld **Site Bindings** wird angezeigt. Wenn keine Zeile mit **Type**, **https** und **Port**, **443** vorhanden ist, führen Sie die folgenden Schritte aus. Andernfalls fahren Sie mit dem nächsten Hauptschritt fort. Wählen Sie **Hinzufügen.. aus.** -Schaltfläche, wird das Feld **Site-Bindung hinzufügen** angezeigt.Wählen Sie **https** im **Typ:** angezeigt.Stellen Sie sicher, dass die **IP-Adresse:** zeigt **Alle nicht zugewiesenen** Geräte und den **Port an:** ist **443**.Vergewissern Sie sich, dass Sie den **Hostnamen** verlassen**:** -Feld leer und die Option **Servernamenangabe** anfordern deaktiviert.Im **SSL-Zertifikat:** im Dropdown-Menü den Zertifikatsnamen auswählen, der dem zuvor erstellten entspricht. Wenn Sie sich nicht sicher sind, welches Zertifikat Sie auswählen möchten, verwenden Sie **Select...** Schaltfläche zum Anzeigen und Durchsuchen der auf dem Server vorhandenen ZertifikateVerwenden Sie die **Ansicht...** um das ausgewählte Zertifikat anzuzeigen und zu überprüfen, ob die Details korrekt sind.Wählen Sie **OK**, um die Auswahl zu speichern.Wählen Sie die Zeile aus, in der in der Spalte Typ die Option **https** angezeigt wird, und wählen Sie anschließend **Bearbeiten...** -Taste. Das Feld **Seitenbindung bearbeiten** wird angezeigt. Stellen Sie sicher, dass die **IP-Adresse:** zeigt **Alle nicht zugewiesenen** Geräte und den **Port an:** ist **443**.Stellen Sie sicher, dass der **Hostname** ist leer gelassen worden, und die Option **Servernamenangabe** anfordern ist nicht aktiviert.Im **SSL-Zertifikat:** im Dropdown-Menü den Zertifikatsnamen auswählen, der dem zuvor erstellten entspricht. Wenn Sie sich nicht sicher sind, welches Zertifikat Sie auswählen möchten, verwenden Sie **Select...** Schaltfläche zum Anzeigen und Durchsuchen der auf dem Server vorhandenen ZertifikateVerwenden Sie die **Ansicht...** um das ausgewählte Zertifikat anzuzeigen und zu überprüfen, ob die Details korrekt sind.Wählen Sie **OK**, um die Auswahl zu speichern.Wählen Sie **Close** aus, um zum IIS-Manager zurückzukehren.
4. Sie können den IIS-Manager jetzt schließen.

Schritt 2: Partitionsadministrator-SSO konfigurieren

Mit der Partitionsadministrator-SSO-Konfiguration kann ECE automatisch ein Benutzerkonto auf Partitionsebene für jeden Administrator erstellen, der das ECE-Gadget in SPOG öffnet.

> **Hinweis**: Sie müssen die Partition Administrator SSO konfigurieren, auch wenn Sie nicht vorhaben, die Agent- oder Supervisor-SSO zu aktivieren.

Schritt 2.1: Rufen Sie das Active Directory (AD)-Zertifikat ab, und erstellen Sie einen Keystore.

Dieser Schritt ist erforderlich, um die jüngsten von Microsoft angekündigten Sicherheitsänderungen zu beheben.

Weitere Informationen finden Sie unter https://support.microsoft.com/en-us/help/4520412/2020-ldap-channel-binding-and-ldap-signing-requirements-for-windows.

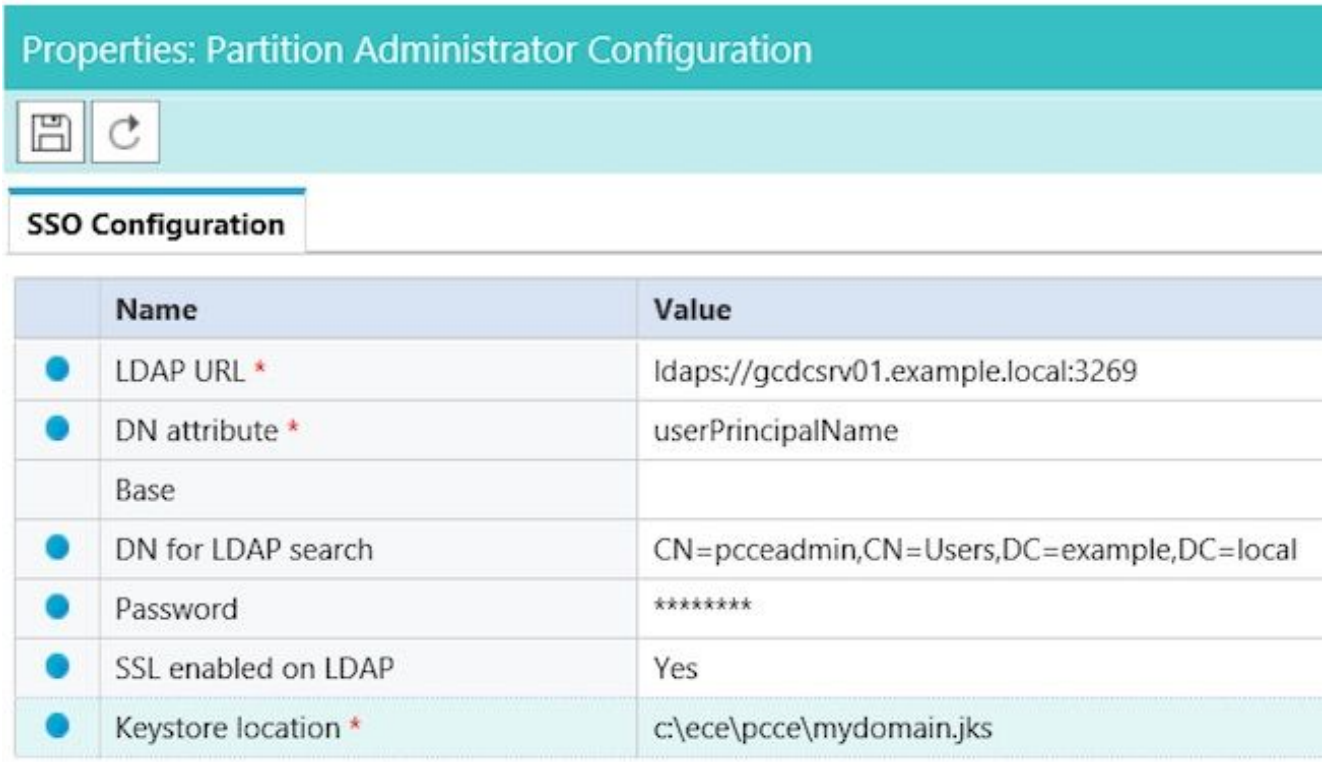
1. Rufen Sie das SSL-Zertifikat im Base 64-Format von Ihrem AD-Server ab, den Sie im

Partitionsadministratorkonfigurationsformular angeben.
2. Kopieren Sie die Zertifikatsdatei auf einen der Anwendungsserver.
3. Öffnen Sie eine RDP-Sitzung auf dem Anwendungsserver, auf den Sie das Zertifikat kopiert haben.
4. Erstellen Sie wie folgt einen neuen Java-Keystore. Öffnen Sie auf dem Anwendungsserver eine Eingabeaufforderung.Wechseln Sie in das Verzeichnis ECE Java Development Kit (JDK) bin.Führen Sie diesen Befehl aus. Ersetzen Sie die Werte nach Bedarf.
keytool -import -trustcacerts -alias mydomaincontroller -file C:\temp\domainctl.crt -keystore c:\ece\pcce\mydomain.jks -storepass MyP@ssword
5. Kopieren Sie den Keystore auf allen anderen Anwendungsservern in Ihrer Umgebung auf denselben Pfad.

Schritt 2.2: Konfigurieren der ECE mit LDAP-Zugriffsinformationen (AD Lightweight Directory Access Protocol)

1. Navigieren Sie auf einer Workstation oder einem Computer mit **Internet Explorer 11** zur URL der Geschäftsparte. **Tipp**: Die Business-Partition wird auch als Partition 1 bezeichnet. Bei den meisten Installationen kann der Zugriff auf die Business-Partition über eine URL erfolgen, die ähnlich ist: https://ece.example.com/default.
2. Melden Sie sich als **PA** an, und geben Sie das Kennwort für Ihr System an.
3. Wenn Sie sich erfolgreich angemeldet haben, wählen Sie den **Verwaltungs**-Link auf der ursprünglichen Konsole aus.
4. Navigieren Sie wie folgt zum Ordner **SSO-Konfiguration**: **Administration > Partition: default > Security > SSO and Provisioning**.
5. Wählen Sie im oberen Teilfenster rechts den Eintrag **Partitionsverwaltungskonfiguration** aus.
6. Geben Sie im unteren Bereich rechts die Werte für Ihr Lightweight Directory Access Protocol (LDAP) und AD ein. **LDAP-URL**: Verwenden Sie als Best Practice den Namen eines Global Catalog (GC) Domain Controller.
Wenn Sie keinen GC verwenden, sehen Sie möglicherweise einen Fehler in den ApplicationServer-Protokollen wie folgt.
Ausnahme bei der LDAP-Authentifizierung <@>
javax.naming.PartialResultException: Nicht verarbeitete Kontinuitätsreferenzen; verbleibender Name "DC=example,DC=com" Der nicht sichere globale Katalogport ist 3268.Der sichere globale Katalogport ist 3269.**DN-Attribut** - Dies muss userPrincipalName sein.**Base** - Dies ist nicht erforderlich, wenn Sie einen GC verwenden. Andernfalls müssen Sie das korrekte LDAP-Basisformat angeben.**DN für die LDAP-Suche** - Wenn Ihre Domäne keine anonyme Bindung zulässt, müssen Sie den Distinguished Name eines Benutzers angeben, der an LDAP gebunden und die Verzeichnisstruktur durchsucht werden kann.
Tipp: Die einfachste Methode, den richtigen Wert für den Benutzer zu finden, ist die Verwendung des Tools Active Directory-Benutzer und -Computer. Aktivieren Sie **Erweiterte Funktionen** im Menü **Ansicht**.Navigieren Sie zum Benutzerobjekt, klicken Sie mit der rechten Maustaste, und wählen Sie **Eigenschaften aus**.Wählen Sie die Registerkarte **Attribute** aus.Wählen Sie die Schaltfläche **Filtern**, und wählen Sie **Nur Attribute mit Werten anzeigen aus**.Suchen Sie **distinquishedName** in der Liste, und doppelklicken Sie dann auf, um den Wert anzuzeigen.Markieren Sie den angezeigten Wert, kopieren Sie ihn und fügen Sie ihn in einen Texteditor ein.Kopieren Sie den Wert aus der Textdatei, und fügen Sie ihn in das Feld **DN für die LDAP-Suche ein**.
Der Wert sollte ähnlich sein wie bei "CN=pcceadmin", "CN=Users", "DC=example",

"DC=local".**Passwort** - Wenn Ihre Domäne keine anonyme Bindung zulässt, müssen Sie das Passwort für den angegebenen Benutzer angeben.**SSL aktiviert auf LDAP** - Dieses Feld sollte für die meisten Kunden als Pflichtfeld angesehen werden.**Keystore-Speicherort** - Dies sollte der Speicherort des Keystore sein, in den Sie das SSL-Zertifikat aus AD importiert haben. Im Beispiel ist dies c:\ece\pcce\mydomain.jks, wie im Bild gezeigt:



7. Wählen Sie das Symbol der Diskette aus, um die Änderungen zu speichern.

Schritt 3: Konfigurationsdatei validieren

Der Abschluss dieses Abschnitts ist für alle 12.0-Installationen obligatorisch. Für alle anderen Versionen als 12.0 können Sie diesen Abschnitt überspringen.
Es gibt zwei weitere Szenarien mit allen Versionen, in denen dieser Schritt möglicherweise erforderlich ist. Die erste ist, wenn die ECE in einer Hochverfügbarkeits-Konfiguration installiert wurde. Der zweite und häufigere Fall ist, wenn der Hostname des Webservers nicht mit dem Namen übereinstimmt, den Sie für den Zugriff auf die ECE verwenden. Wenn Sie z. B. den ECE-Webserver auf einem Server mit dem Hostnamen UCSVRECEWEB.example.com installieren, Benutzer jedoch mit dem URL chat.example.com auf die ECE-Webseiten zugreifen, muss dieser Abschnitt abgeschlossen werden. Wenn der Hostname des Servers und die URL, mit der Sie auf ECE zugreifen, identisch sind und Sie die Version 12.5 oder höher installiert haben, können Sie diesen Schritt überspringen und den Abschnitt beenden.

Ersetzen Sie {ECE_HOME} durch den physischen Ort, an dem Sie ECE installiert haben. Wenn Sie zum Beispiel ECE unter **C:\Cisco** installiert haben, ersetzen Sie {ECE_HOME} durch **C:\Cisco** an jedem Speicherort.

Tipp: Verwenden Sie einen Texteditor wie Notepad++ anstelle von Notepad oder Wordpad, da diese die Zeilenenden nicht richtig interpretieren.

1. Öffnen Sie eine Remotedesktop-Sitzung mit allen ECE-Webservern in Ihrer Bereitstellung.
2. Navigieren Sie zu diesem Pfad, **{ECE_HOME}\eService\templates\finesse\gadget\spog**.

3. Suchen Sie die Datei **spog_config.**jsfile, und erstellen Sie eine Sicherungskopie an einem sicheren Speicherort.
4. Öffnen Sie die aktuelle **spog_config.**jsfile in einem Texteditor.
5. Suchen Sie diese beiden Posten, und aktualisieren Sie sie entsprechend Ihrer Bereitstellung.
   Beim Web_server_Protocol muss es sich um https handeln. Falls erforderlich, müssen Sie es aktualisieren.
   Aktualisieren Sie den Namen web_server_name, damit er dem vollqualifizierten Namen entspricht, den Sie für den Zugriff auf ECE zugewiesen haben. Beispiel: **ece.example.com**
   var web_server_protocol = "https";var web_server_name = "ece.example.com";
6. Speichern Sie die Änderungen.
7. Wiederholen Sie diese Schritte auf allen anderen Webservern in Ihrer Bereitstellung.

Schritt 4: ECE zum PCCE-Bestand hinzufügen

Ab 12.0 bietet PCCE 3 verschiedene Bereitstellungsoptionen: 2000 Agent (2K Agent), 4000 Agent (4K Agent) und 12000 Agent (12K Agent). Diese drei Bereitstellungsoptionen können in zwei Gruppen aufgeteilt werden: 2K Agent und 4K/12K Agent. Sie sind auf diese Weise voneinander getrennt, da sie in SPOG verschiedene grundlegende Unterschiede aufweisen. Dieser Absatz folgt einem sehr allgemeinen Vergleich der beiden Methoden. Dieses Dokument enthält keine spezifischen Schritte zum Hinzufügen einer Komponente zum Inventar. Detaillierte Informationen zu diesem Prozess finden Sie unter den Links am Ende dieses Dokuments. Dieser Abschnitt behandelt spezifische Details, die überprüft werden müssen, wenn Sie ECE zu PCCE hinzufügen. In diesem Dokument wird außerdem davon ausgegangen, dass die PCCE-Installation abgeschlossen ist und Sie auf andere Aspekte der Lösung zugreifen und diese konfigurieren können.

- 2.000 Agenten-Bereitstellung Die Erstkonfiguration der PCCE-Komponenten erfolgt vollständig über die CCE-Administration und ist automatisiertNeue Komponenten werden über ein Popup-Feld auf der Bestandsseite hinzugefügt, in dem Sie die Details wie die IP oder den Hostnamen und die erforderlichen Anmeldeinformationen oder die komponentenspezifische Konfiguration eingeben.
- 4000- und 1200-Agenten-Bereitstellung Ein Großteil der Erstkonfiguration spiegelt die für UCCE verwendeten Schritte wider.Die Komponenten werden über eine CSV-Datei (Comma Separated Values) hinzugefügt, die Sie von der CCE-Verwaltung herunterladen, nach der jeweiligen Installation füllen und dann hochladen.Bei der Erstbereitstellung müssen einige spezifische Komponenten in die erste CSV-Datei aufgenommen werden.Komponenten, die bei der Ersteinrichtung des Systems nicht hinzugefügt wurden, werden mithilfe von CSV-Dateien hinzugefügt, die die erforderlichen Informationen enthalten

Schritt 4.1: Laden Sie das ECE-Webserverzertifikat in den Java Keystore hoch.

1. Wenn selbstsignierte Zertifikate verwendet werden Öffnen Sie eine Remotedesktopverbindung mit dem primären, Seite-A-Administrationsdatenserver (ADS).Öffnen Sie Internet Explorer 11 als Administrator, und navigieren Sie zur ECE-Geschäftspartition.Wählen Sie auf der rechten Seite der URL-Leiste das Symbol eines Vorhängeschlosss aus, und wählen Sie dann **Zertifikate anzeigen aus**.Wählen Sie im Feld **Zertifikat** die Registerkarte **Details** aus.Wählen Sie **In Datei kopieren aus...** am unteren Ende der Registerkarte.Wählen Sie im **Assistenten für den Zertifikatsexport** die Option **Weiter**, bis

die Seite **Dateiformat exportieren angezeigt wird**. Stellen Sie sicher, dass Sie das **Base-64-codierte X.509 (.CER)** Format auswählen.Speichern Sie das Zertifikat an einem Speicherort wie **c:\Temp\certificates** auf dem ADS-Server, um den Export abzuschließen.Kopieren Sie das Zertifikat auf alle anderen ADS-Server.Öffnen Sie eine administrative Eingabeaufforderung.Wechseln Sie in das Java-Hauptverzeichnis und dann in das Verzeichnis bin. Auf das Java-Hauptverzeichnis kann wie folgt zugegriffen werden. **cd %JAVA_HOME%\bin**Sichern Sie die aktuelle Datei **für** die **Warnmeldungen**. Kopieren Sie die Datei mit **den** Akerts von **%JAVA_HOME%\lib\security** an einen anderen Speicherort.Führen Sie diesen Befehl aus, um das zuvor gespeicherte Zertifikat zu importieren. Wenn das Schlüsselwort nicht 'change eit' ist, aktualisieren Sie den Befehl, damit er mit Ihrer Installation übereinstimmt.
keytool -keystore ../lib/security/cacerts -storepass changeit -import -alias <FQDN ECE-Server> -file <Ort, an dem Sie das Zertifikat gespeichert haben>Starten Sie den ADS-Server neu.Wiederholen Sie die Schritte 8-12 für die anderen ADS-Server.

2. Bei Verwendung von Zertifikaten mit CA-Vorzeichen Rufen Sie das Root- und Zwischenzertifikat im DER/PEM-Format ab, und kopieren Sie sie an einen Speicherort wie **C:\Temp\certificates** auf allen ADS-Servern. **Hinweis**: Wenden Sie sich an Ihren CA-Administrator, um diese Zertifikate zu erhalten. Öffnen Sie eine Remotedesktopverbindung mit dem primären, Seite-A-ADS.Öffnen Sie eine administrative Eingabeaufforderung.Wechseln Sie in das Java-Hauptverzeichnis und dann in das Verzeichnis bin. Auf das Java-Hauptverzeichnis kann wie folgt zugegriffen werden. **cd %JAVA_HOME%\bin**Sichern Sie die aktuelle Datei **für** die **Warnmeldungen**. Kopieren Sie die Datei mit **den** Akerts von **%JAVA_HOME%\lib\security** an einen anderen Speicherort.Führen Sie diesen Befehl aus, um das zuvor gespeicherte Zertifikat zu importieren. Wenn das Schlüsselwort nicht 'change eit' ist, aktualisieren Sie den Befehl, damit er mit Ihrer Installation übereinstimmt.
keytool -keystore ../lib/security/cacerts -storepass changeit -trustcacerts -import -alias <Name des CA-Roots> -file <Ort, an dem Sie das Root-Zertifikat gespeichert haben>Wiederholen Sie Schritt 6. und die Zwischenzertifizierung einzuführen, sofern vorhanden.Starten Sie den ADS-Server neu.Wiederholen Sie die Schritte 2-12 für alle anderen ADS-Server.

Schritt 4.2: Hinzufügen des ECE-Datenservers zum Bestand

- Während der Datenserver im Systeminventar vorhanden sein muss, erfolgt keine direkte Kommunikation zwischen den PCCE ADS und dem Datenserver.
- Wenn ECE bei der Bereitstellung mit 1.500 Agenten bereitgestellt wird, ist der Datenserver der Dienstserver.
- Wenn ECE in einer HA-Konfiguration installiert ist, sollten beide Services-Server hinzugefügt werden.

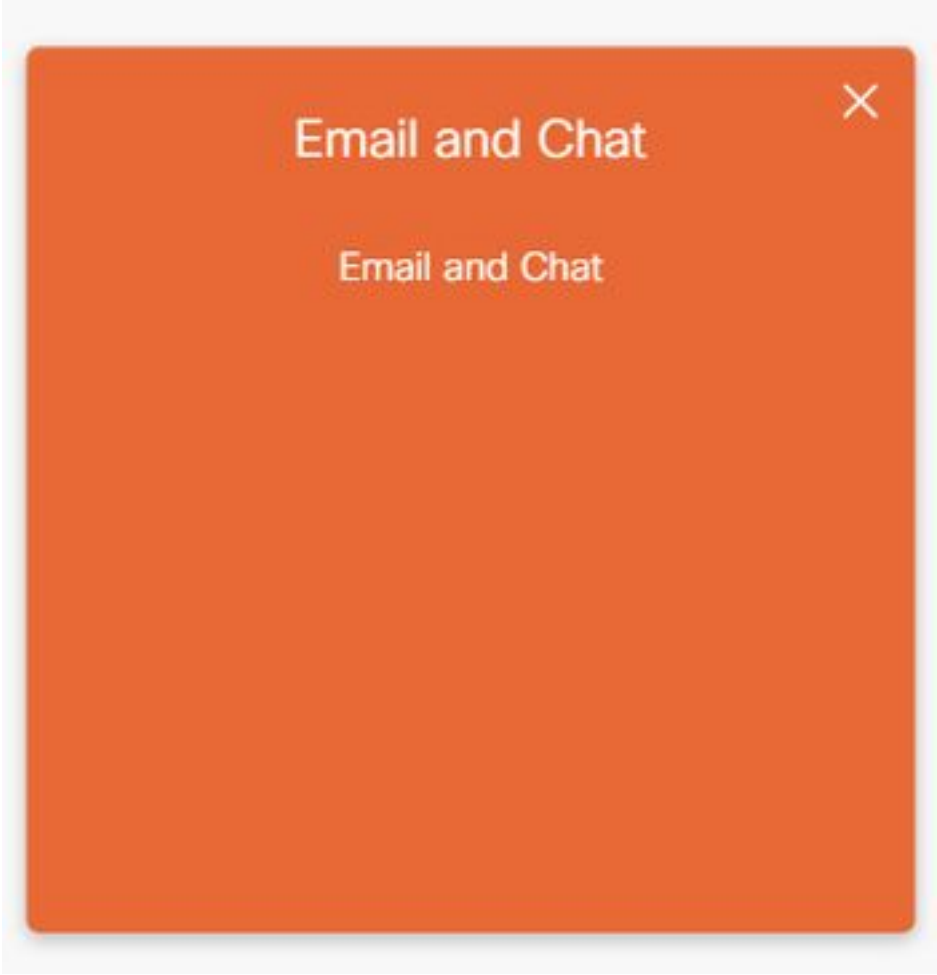
Schritt 4.3: Hinzufügen des ECE-Webservers zum Bestand

- Stellen Sie sicher, dass Sie den Webserver mit dem vollqualifizierten Namen hinzufügen. Dieser Name muss entweder mit dem im ECE-Zertifikat angegebenen gemeinsamen Namen übereinstimmen oder als einer der SANs (Subject Alternative Name) aufgeführt sein.Sie dürfen nicht nur den Hostnamen oder die IP-Adresse verwenden.

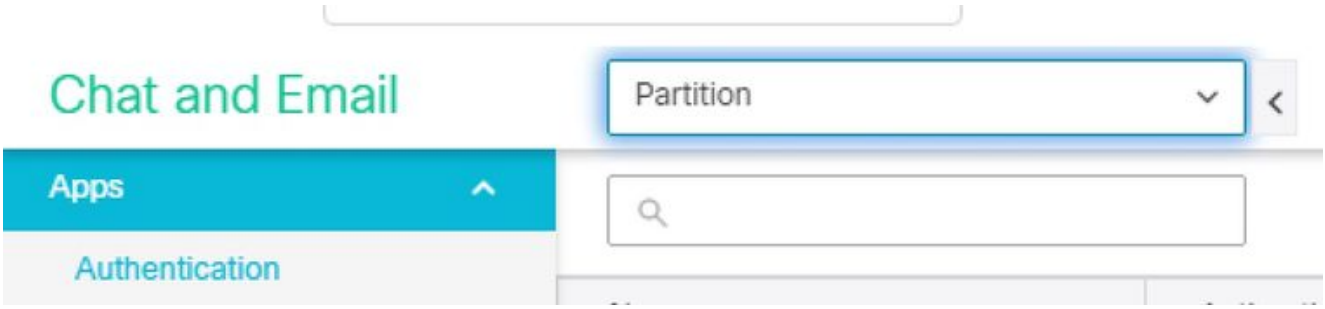
- Der Benutzername und das Kennwort für die ECE müssen die PA-Anmeldeinformationen sein.
- Stellen Sie sicher, dass die Anwendungsinstanz korrekt ist. Beim Namen der Anwendungsinstanz wird Groß- und Kleinschreibung unterschieden.Für 2000 Agent-PCCE-Bereitstellungen ist die Anwendungsinstanz MultiChannelFür 4000/12000-Agent-PCCE-Bereitstellungen enthält die Anwendungsinstanz den Standort- und Peripheriegerätesatz als Teil des Namens.
- Wenn ECE mit mehr als einem Webserver installiert wird, z. B. in der Bereitstellung mit 1.500 Agenten oder in einer Bereitstellung mit 400 Agenten HA, können Sie entweder die URL verwenden, die auf Ihren Load Balancer verweist, oder die URL, die auf jeden einzelnen Webserver verweist, als vollqualifizierter Name des Webservers.
- Wenn Sie über mehr als eine ECE-Bereitstellung verfügen oder wenn Sie jeden einzelnen Webserver in der Bereitstellung mit mehr als einem hinzufügen möchten, wählen Sie den richtigen Webserver, wenn Sie das ECE-Gadget in SPOG öffnen.

Schritt 5: Integration von ECE mit PCCE

1. Melden Sie sich bei der CCE-Verwaltung als Administrator an.
2. Wählen Sie die **E-Mail- und Chat-**Karte und anschließend den Link **E-Mail und Chat** wie im Bild gezeigt aus.



3. Überprüfen Sie den aktuell ausgewählten Server im Dropdown-Menü Device Name (Gerätename). Wenn Sie beide Webserver in einer HA-Installation hinzugefügt haben, können Sie einen der beiden Webserver auswählen. Wenn Sie zu einem späteren Zeitpunkt eine zweite ECE-Bereitstellung zu Ihrem System hinzufügen, stellen Sie sicher, dass Sie den entsprechenden Server auswählen, bevor Sie fortfahren.
4. Wählen Sie im Dropdown-Menü neben **Chat und E-Mail** die Option **Partition** oder **Global** wie im Bild gezeigt aus.

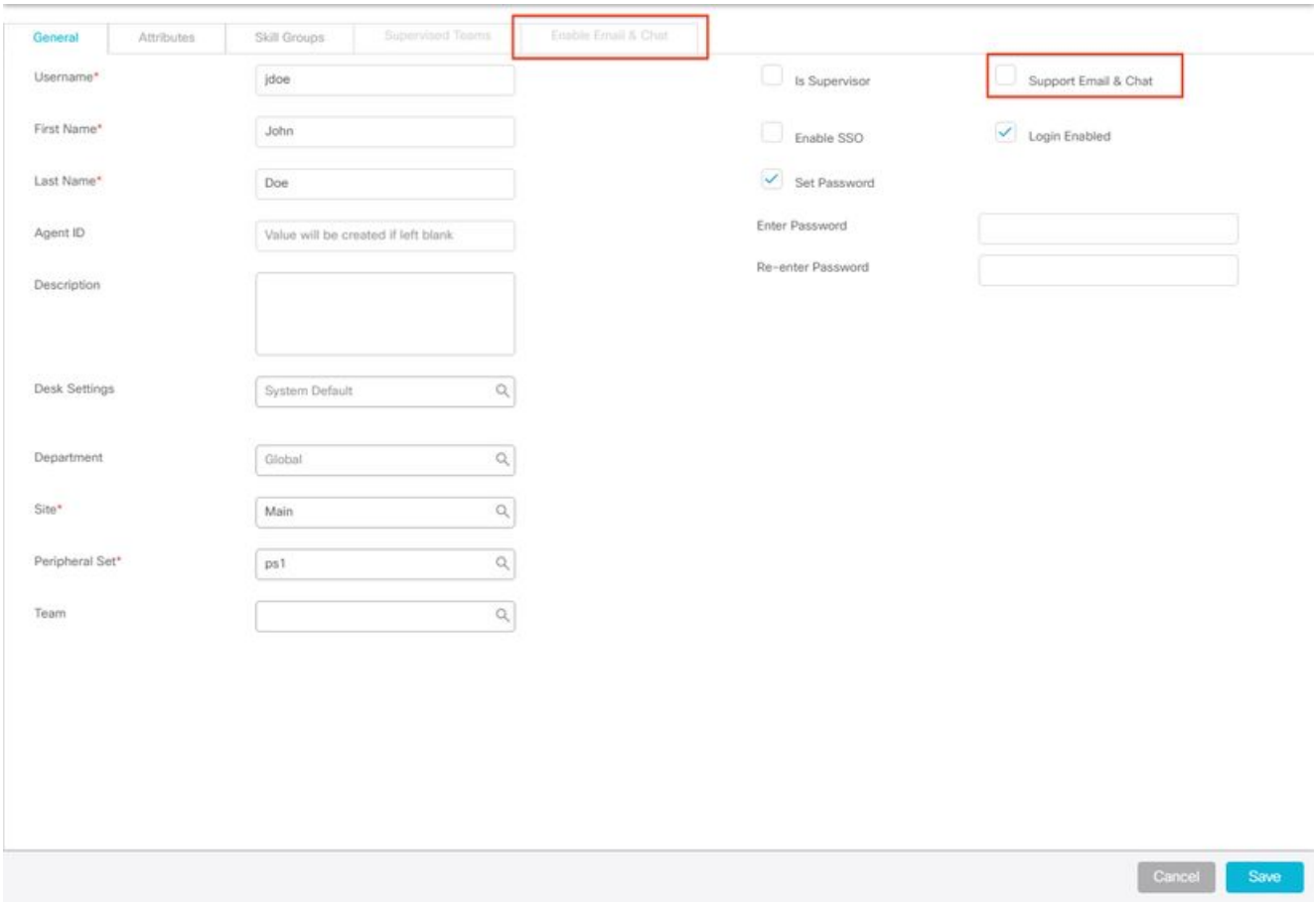


5. Wählen Sie im oberen Menü die Option **Integration (Integration) aus**, wählen Sie dann den Pfeil neben **Unified CCE** und wählen Sie den zweiten **Unified CCE** wie im Bild gezeigt aus.

6. Füllen Sie die Werte auf der Registerkarte **AWDB-Details** für Ihre Installation aus, und wählen Sie dann die Schaltfläche **Speichern**.
7. Wählen Sie die Registerkarte **Konfiguration aus**, und schließen Sie dies wie folgt ab. Wählen Sie das Dropdown-Menü neben **Anwendungsinstanz** aus, und wählen Sie die für ECE erstellte Anwendungsinstanz aus. **Hinweis**: Dies darf nicht die Anwendungsinstanz sein, die mit UQ beginnt.Wählen Sie den grünen Kreis mit der weißen Pluszeichen-Taste aus. Agenten-PG auswählen. Wählen Sie die Agenten-PGs (oder Agenten-PGs, wenn mehrere Agenten vorhanden sind) aus.Wählen Sie **Speichern aus**, sobald Sie alle Agenten-PGs hinzugefügt haben. **Warnung**: Wenn Sie **Speichern** ausgewählt haben, ist das System dauerhaft mit PCCE verbunden und kann nicht rückgängig gemacht werden. Wenn in diesem Abschnitt Fehler gemacht werden, müssen Sie ECE deinstallieren vollständig und alle Datenbanken löschen und dann ECE installieren, als ob es sich um eine Neuinstallation handelt.

Schritt 6: ECE-Integration überprüfen

1. Überprüfen Sie in der CCE-Verwaltung, ob in der oberen Statusleiste keine Warnmeldungen angezeigt werden. Wenn Alerts vorhanden sind, wählen Sie das Wort **Alerts aus**, und überprüfen Sie die Bestandsseite, um sicherzustellen, dass keine der Alerts für die ECE-Server vorhanden sind.
2. Wählen Sie **Benutzer** und dann **Agenten** in der Navigationsleiste links aus.
3. Wählen Sie einen Agenten aus der Liste aus, und überprüfen Sie dies. Sie sollten nun ein neues Kontrollkästchen für **Support-E-Mail und -Chat** auf der Registerkarte **Allgemein** sehen.Sie sollten nun eine neue Registerkarte mit der Bezeichnung **E-Mail und Chat aktivieren** sehen, wie im Bild gezeigt.



4. Aktivieren Sie einen Testagenten für ECE. Aktivieren Sie das Kontrollkästchen **E-Mail- und Chat-Support**, und beachten Sie, dass die Registerkarte **E-Mail und Chat aktivieren** nun aktiviert werden kann.Wählen Sie die Registerkarte **E-Mail und Chat aktivieren**, und geben Sie im Feld **Bildschirmname** einen Wert an.Wählen Sie **Speichern**, um den Benutzer zu aktualisieren.Sie sollten eine Erfolgsmeldung erhalten.
5. Überprüfen Sie, ob ECE aktualisiert wurde. Wählen Sie die Navigationstaste **Übersicht aus**, und wählen Sie dann die **E-Mail- und Chat-**Karte und den Link aus.Wählen Sie im Dropdown-Menü neben **Chat und E-Mail** den Namen aus, der der Abteilung des Agenten entspricht. **Hinweis**: Die Service-Abteilung in ECE besitzt alle Objekte, die der Global-Abteilung in PCCE angehören. Der Abteilungsname Service ist daher ein reservierter Wert.Wählen Sie im oberen Menü **Benutzerverwaltung** und anschließend **Benutzer** im Menü unter **Chat und E-Mail aus**.Überprüfen Sie, ob der neue Agent in der Liste angezeigt wird.

Fehlerbehebung

Es wird empfohlen, mehrere Tools herunterzuladen und auf den ECE-Servern zu belassen. Dadurch wird die Fehlerbehebung und Wartung der Lösung im Laufe der Zeit deutlich vereinfacht.

- Ein Texteditor wie Notepad++
- Archivierungstool wie 7-Zip
- Eine der vielen Tail-for-Windows-Programme
  Einige Beispiele: E-Mail - https://www.baremetalsoft.com/baretail/Tail für Win32 - http://tailforwin32.sourceforge.net/

Um Integrationsprobleme zu beheben, müssen Sie zunächst einige wichtige Protokolldateien und deren Speicherort kennen.

1. ## Dateinamen und Speicherorte auf der ECE

   Es gibt viele Protokolle im ECE-System. Dies sind nur die Protokolle, die Ihnen bei der Fehlerbehebung im Zusammenhang mit der Integration am meisten helfen.

   Serverschlüssel:C = Kollidierter ServerA = AnwendungsserverS = Services ServerM = Messaging-ServerDie meisten Protokolldateien haben auch zwei weitere Protokolle, die ihnen zugeordnet sind.eg_log_{SERVERNAME}_{PROCESS}.log - Primäres Prozessprotokolleg_log_dal_connpool_{SERVERNAME}_{PROCESS}.log - Nutzung des Verbindungspoolseg_log_query_timeout_{SERVERNAME}_{PROCESS}.log - Wird aktualisiert, wenn eine Abfrage aufgrund eines Zeitüberschreitungsfehlers fehlschlägt
2. ## Dateinamen und Speicherorte auf PCCE

   Die PCCE-Protokolle für Integrationsprobleme befinden sich alle auf der Seite-A-ADS. Nachfolgend sind die Protokolle aufgeführt, die bei der Behebung von Integrationsproblemen am wichtigsten sind. Jede dieser Optionen befindet sich unter **C:\icm\tomcat\logs**.

   Von diesen Protokollen werden die ersten drei am häufigsten angefordert und geprüft.Verwenden Sie diese Schritte, um Ablaufverfolgungsebenen festzulegen und die erforderlichen Protokolle zu sammeln.
3. ## Konfiguration der Ablaufverfolgungsebene

   Dieser Abschnitt gilt nur für ECE. Die von PCCE benötigten Protokolle haben ihren Trace-Level von Cisco festgelegt und können nicht geändert werden. Navigieren Sie auf einer Workstation oder einem Computer mit **Internet Explorer 11** zur URL der Systempartition. **Tipp**: Die Systempartition wird auch als Partition 0 bezeichnet. Bei den meisten Installationen kann auf die Systempartition über eine URL wie https://ece.example.com/system zugegriffen werden.Melden Sie sich als **sa** an, und geben Sie das Kennwort für Ihr System an.Wenn Sie sich erfolgreich angemeldet haben, wählen Sie den Link **System** auf der ursprünglichen Konsole aus.Erweitern Sie auf der Seite **System** die Option **System > Gemeinsam genutzte Ressourcen > Protokollierung > Prozesse.**Suchen Sie im oberen rechten Bereich den Prozess, der die Ablaufverfolgungsebene ändern soll, und wählen Sie ihn aus.
   Hinweis: In einem HA-System und in einem System mit mehr als einem Anwendungsserver werden Prozesse mehrmals aufgeführt. Um sicherzustellen, dass Sie die Daten erfassen, legen Sie die Ablaufverfolgungsebene für alle Server fest, die den Prozess enthalten.Wählen Sie im unteren rechten Teilfenster das Dropdown-Menü für **Maximum trace level (Maximale Ablaufverfolgungsebene) aus,** und wählen Sie den entsprechenden Wert aus.
   In ECE sind 8 Ablaufverfolgungsebenen definiert. Die 4 in dieser Liste sind diejenigen, die am häufigsten verwendet werden. 2 - Fehler - Standard-Ablaufverfolgungsebene für Prozesse4 - Info - Trace-Level, der allgemein für die Problemlösung verwendet wird6 -

Dbquery - ist häufig hilfreich, um Probleme zu einem frühen Zeitpunkt der Einrichtung oder komplexere Probleme zu diagnostizieren.7 - Debuggen - Sehr ausführliche Ausgabe, nur bei den komplexesten Problemen erforderlich**Hinweis**: Bei 6 - Dbquery sollte kein Prozess über einen längeren Zeitraum aufbewahrt werden, im Allgemeinen nur mit TAC-Anleitung.Die meisten Prozesse sollten auf der Ablaufverfolgungsebene bleiben, 2-Fehler. Wenn Sie Stufe 7 oder 8 auswählen, müssen Sie auch eine maximale Dauer auswählen. Wenn die maximale Dauer eingehalten wird, kehrt die Ablaufverfolgungsebene zur letzten festgelegten Ebene zurück.
Nachdem das System eingerichtet wurde, ändern Sie diese vier Prozesse in die Ablaufverfolgungsebene 4.EAAS-ProzessEAMS-Prozessdx-Prozessrx-processWählen Sie das Speichersymbol aus, um die neue Ablaufverfolgungsebene festzulegen.

4. ## Erfassen von Protokolldateien

Öffnen Sie eine Remotedesktop-Sitzung mit dem Server, auf dem der Prozess Protokolle erstellt, die erforderlich sind.Navigieren Sie zum Speicherort der Protokolldatei. ECE-Server Protokolle werden wie folgt geschrieben:Standardmäßig sind Protokolle geschriebene Dateien mit einer maximalen Größe von 5 MB.Wenn eine Protokolldatei den konfigurierten Höchstwert erreicht, wird sie im Format {LOGNAME}.log umbenannt.{#}ECE behält die vorherigen 49 Protokolldateien sowie die aktuelle Datei beiDas aktuelle Protokoll endet immer mit.log und keine Nummer danachProtokolle werden weder archiviert noch komprimiertDie meisten Protokolle haben eine gemeinsame Struktur.Protokolldateien verwenden <@>, um Abschnitte zu trennen.Protokolle werden immer in GMT+0000 Zeit geschriebenECE-Protokolle befinden sich je nach Installation an verschiedenen Stellen.400 Agenten-Bereitstellungen Einseitig Server: Zusammengefasster ServerStandort: **{ECE_HOME}\eService_RT\logs**Hohe Verfügbarkeit Server: Beide Server sind zusammengefasstStandort: **{ECE_HOME}\eService\logs**Das Verzeichnis, das für die DFS-Freigabe (Distributed File System) erstellt wurde, enthält nur Protokolle für Installation und Upgrades.Nur der Server, der die DSM-Rolle (Distributed Systems Manager) besitzt, schreibt Protokolle für die Komponenten, die Teil der Services-Rolle sind Die Besitzer der DSM-Rolle finden Sie auf der Registerkarte "Prozesse" des Windows Task-Managers. Es gibt 10-15 Java-Prozesse auf diesem Server, die nicht auf dem Sekundärserver ausgeführt werden.Zu den Komponenten von DSM gehören: EAAS, EAMS, Retriever, Dispatcher, Workflow usw.1.500 Agenten-Bereitstellungen Protokolle auf dem Server, der die Rolle hostetStandort: **{ECE_HOME}\eService\logs**Mit Ausnahme des Services-Servers werden alle Server für alle Prozesse, die der Komponente zugeordnet sind, betrieben und schreiben ProtokolleBei einer Bereitstellung mit hoher Verfügbarkeit wird der Services-Server in einer Aktiv/Standby-Konfiguration betrieben.Nur der Server, der Eigentümer der DSM-Rolle ist, schreibt ProtokolleDer Besitzer der DSM-Rolle kann anhand der Anzahl der Prozesse identifiziert werden, die im Windows Task-Manager angezeigt werden. Es gibt 10-15 Java-Prozesse, die auf dem primären Server und nur 4 Java-Prozesse auf dem sekundären Server ausgeführt werden.PCCE-Server Die erforderlichen Protokolle von PCCE finden Sie unter

C:\icm\tomcat\logsTomcat-Protokolle werden nicht übernommen oder archiviertProtokolle werden in lokaler Serverzeit geschriebenSammeln Sie alle Protokolle, die nach der Feststellung des Problems erstellt oder geändert wurden.
Eine vollständige Erläuterung der Protokolle und der festgestellten Probleme geht über den Rahmen dieses Dokuments hinaus. Einige häufige Fragen, welche Aspekte überprüft werden müssen, und einige mögliche Lösungen sind wie folgt: Zertifikatbezogene Probleme Zertifikat nicht importiert Verhalten: Wenn Sie versuchen, das ECE-Gadget in SPOG zu öffnen, sehen Sie den Fehler "Beim Laden der Seite ist ein Fehler aufgetreten. Wenden Sie sich an den Administrator."Prüfung: Die Katalina meldet sich bei PCCE für ähnliche Fehler an. javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: Fehler beim Erstellen des PKIX-Pfads: sun.security.provider.certpath.SunCertPathBuilderException: kann keinen gültigen Zertifizierungspfad für das angeforderte Ziel finden.Auflösung: Stellen Sie sicher, dass Sie das ECE-Webserver-Zertifikat oder die entsprechenden Zertifizierungsstellenzertifikate in den Vorlagenspeicher der ADS importiert haben.Nicht übereinstimmendes Zertifikat Verhalten: Wenn Sie versuchen, das ECE-Gadget in SPOG zu öffnen, sehen Sie einen Fehler, der anzeigt, dass der gemeinsame Name oder der alternative Subjektname des Zertifikats nicht mit dem konfigurierten Namen übereinstimmt.Prüfung: Überprüfen des SSL-ZertifikatsAuflösung: Stellen Sie sicher, dass entweder das Feld "Common Name" im Betreff oder eines der DNS-Felder im Betreff Alternativer Name den vollqualifizierten Namen enthält, den Sie als Webserver-Namen in SPOG eingegeben haben.Systemprobleme Dienst nicht gestartet Verhalten: Wenn Sie versuchen, das ECE-Gadget in SPOG zu öffnen, sehen Sie die Fehlermeldung "Die Webseite unter https://{url} ist möglicherweise vorübergehend nicht erreichbar oder sie hat sich dauerhaft in eine neue Adresse verschoben."Prüfung: Überprüfen Sie, ob der Windows-Dienst - Cisco Service auf allen ECE-Servern mit Ausnahme des Webservers gestartet wurde. Überprüfen Sie die Stammprotokolle auf dem Anwendungsserver auf Fehler.Auflösung: Starten Sie den Cisco Service für alle ECE-Services.Konfigurationsproblem LDAP-Konfiguration Verhalten: Wenn Sie versuchen, das ECE-Gadget in SPOG zu öffnen, sehen Sie den Fehler "Beim Laden der Seite ist ein Fehler aufgetreten. Wenden Sie sich an den Administrator."Prüfung: Erhöhen Sie die Ablaufverfolgungsebene des Anwendungsservers auf Ebene 7 - Debuggen, versuchen Sie dann erneut, die Anmeldung durchzuführen, und überprüfen Sie das Anwendungsserverprotokoll. Suchen Sie das Wort LDAP.Auflösung: Überprüfen Sie die LDAP-Konfiguration für die Partition Administrator-SSO, um sicherzustellen, dass sie korrekt ist.

Zugehörige Informationen

Dies sind die wichtigsten Dokumente, die Sie gründlich prüfen müssen, bevor Sie eine ECE-Installation oder -Integration starten. Dies ist keine umfassende Liste von ECE-Dokumenten.

Vorsicht: Die meisten ECE-Dokumente haben zwei Versionen. Bitte stellen Sie sicher, dass Sie die für PCCE vorgesehenen Versionen herunterladen und verwenden. Der Titel des Dokuments lautet entweder **für Packaged Contact Center Enterprise** oder **(für PCCE)** oder **(für UCCE und PCCE)** nach der Versionsnummer.

Überprüfen Sie, ob Sie die Startseite für die Cisco Enterprise Chat- und E-Mail-Dokumentation vor der Installation, dem Upgrade oder der Integration auf Updates überprüfen.

https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/series.html

- 12,0 Installations- und Konfigurationsleitfaden für Enterprise Chat und E-MailUpgrade-Leitfaden für Enterprise Chat und E-MailAdministratorhandbuch für Enterprise-Chat- und E-Mail-Funktionen
- 12,5 Installations- und Konfigurationsleitfaden für Enterprise Chat und E-MailUpgrade-Leitfaden für Enterprise Chat und E-MailAdministratorhandbuch für Enterprise-Chat- und E-Mail-Funktionen