Introduction à Cisco Unified Intelligence Center

Vue d'ensemble

Cisco Unified Intelligence Center constitue une plate-forme de création de rapports pour les utilisateurs des produits Cisco Contact Center. C'est une application Web qui fournit des rapports et des tableaux de bord sur des données historiques, en temps réel et en direct.

Unified Intelligence Center permet d'atteindre les principaux objectifs suivants :

- Obtenir des données à partir de la base de données de la solution de base. La solution de base peut consister en n'importe lequel des produits Contacts Center.
- Vous permettre de créer des requêtes personnalisées pour extraire des données spécifiques.
- Personnaliser la présentation visuelle des rapports.
- Personnalise les données du rapport.
- Permettre à différents groupes de personnes de visualiser des données spécifiques à leur fonction.

Accès à Unified Intelligence Center

L'URL pour se connecter à l'application de création de rapports Unified Intelligence Center est :

HTTPS

https://<HOST>:8444/cuicui/Main.jsp

Où HOST représente le nom DNS d'un nœud Unified Intelligence Center.

Remarque Cisco Unified Intelligence Center ne prend pas en charge HTTP. Depuis Cisco Unified Intelligence Center version 12.6 (1), le port 8081 n'est pas pris en charge.

Cisco Unified Intelligence Center version 12.6 (1) prend en charge le message d'ouverture de session personnalisé pour les utilisateurs. Si votre administrateur a défini les messages d'ouverture de session personnalisés, le message est affiché sur la page **Se connecter**.

Remarque Les messages d'ouverture de session personnalisés ne sont pas affichés pour les utilisateurs qui se connectent à l'aide de la SSO (authentification unique).

Paramètres régionaux par défaut dans Unified Intelligence Center

Remarque Pour spécifier des paramètres régionaux, installez le pack linguistique.

Le premier accès à Cisco Unified Intelligence Center affiche la page de connexion aux paramètres régionaux du navigateur. Pour modifier les paramètres régionaux, cliquez sur le nom d'utilisateur dans le coin supérieur droit de l'écran et sélectionnez les paramètres régionaux requis dans la liste déroulante.

Lorsque vous sélectionnez des paramètres régionaux, le navigateur conserve ces informations, même lorsque vous vous déconnectez, puis vous connectez à nouveau à Cisco Unified Intelligence Center au sein du même navigateur.

Tableau 1 : Langues prises en charge

Portugais (Brésil)	Chinois (Simplifié)	Chinois (traditionnel)	Danois	Néerlandais
Anglais (États-Unis)	Français (France)	Allemand	Italien	Japonais
Coréen	Russe	Espagnol (Espagne)	Suédois	Polonais
Turc	Finnois	Norvégien	Čeština (tchèque)	Bulgare
Català (Catalan)	Hrvatski (croate)	Magyar (hongrois)	Slovenčina (slovaque)	Slovenščina (slovène)
Српски (serbe)	Română (roumain)			

Synchroniser le cluster

L'administrateur de configuration du système peut utiliser la fonction Synchroniser le cluster (lien sous le nom d'utilisateur dans le coin supérieur droit de l'écran de votre interface utilisateur) pour notifier tous les nœuds du cluster d'effacer leur mémoire cache locale. Cette action synchronise et vide toutes les mémoires cache du cluster. Une fois la mémoire cache locale effacée, chaque nœud est obligé de directement accéder à la base de données pour obtenir les informations demandées.

Chaque nœud reçoit de nouvelles données à partir de la base de données. Les données sont automatiquement placées dans la mémoire cache locale pour y être accessibles lors des requêtes futures. Les données demeurent cohérentes dans la base de données et il n'y a aucune perte d'informations.

Pour plus d'informations, consultez la section *Mise en cache Unified Intelligence Center* dans le *Guide d'administration du Cisco Unified Intelligence Center* à l'adresse https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.

La prise en charge du navigateur et les certificats auto-signés

Unified Intelligence Center prend en charge :

- Internet Explorer 11 (en mode natif avec Windows 10)
- Firefox ESR 68 et versions ultérieures ESR
- Edge Chromium (Microsoft Edge V79 et versions ultérieures)
- Chrome 76.0.3809 et versions ultérieures

Remarque Dans les navigateurs mentionnés ci-dessus, assurez-vous de fermer manuellement la fenêtre d'acceptation des certificats pour charger les rapports de données en direct.

Certificats auto-signés

Assurez-vous que les fenêtres contextuelles sont activées pour Cisco Unified Intelligence Center.

Une fois que vous avez saisi l'URL de Cisco Unified Intelligence Center dans votre navigateur, vous pouvez ajouter un certificat en procédant comme suit :

Installer un certificat sur un système d'exploitation Windows :

La procédure d'ajout d'un certificat varie pour chaque navigateur. Pour chaque navigateur, procédez comme suit :

Internet Explorer

Remarque Si vous utilisez un client Windows, et êtes connecté en tant qu'utilisateur Windows, vous devez exécuter Internet Explorer en tant qu'administrateur pour installer les certificats de sécurité. Dans le menu Démarrer, cliquez à droite sur Internet Explorer et sélectionnez Exécuter en tant qu'administrateur.

Contactez votre administrateur si vous n'avez pas les permissions nécessaires pour installer les certificats de sécurité.

1. Une page s'affiche pour indiquer que le certificat de sécurité du site Web pose problème. Cliquez sur **Poursuivre sur ce site Web (non recommandé)** pour ouvrir la page de connexion Cisco Unified Intelligence Center. L'écran d'ouverture de session apparaît avec une erreur de certificat dans la barre d'adresse.
2. Cliquez sur l'erreur de certificat qui apparait dans la barre d'adresse, puis cliquez sur **Afficher les certificats**.
3. Dans la boîte de dialogue **Certificat**, cliquez sur **Installer un certificat** pour ouvrir **l'Assistant Importation de certificat**.
4. Dans **l'assistant Importation de certificat**, cliquez sur **Suivant**.
5. Sélectionnez **Placer tous les certificats dans le magasin suivant**, puis cliquez sur **Naviguer**.
6. Sélectionnez **Autorités de certification racines de confiance**, puis cliquez sur **OK**.
7. Cliquez sur **Suivant**, puis sur **Terminer**. Une boîte de dialogue **Avertissement de sécurité** s'affiche.
8. Cliquez sur **Oui** pour installer le certificat. La boîte de dialogue **Importer le certificat** apparaît.
9. Cliquez sur **OK** et fermez la boîte de dialogue **Importer le certificat**.
10. Saisissez vos nom d'utilisateur et mot de passe, et cliquez sur **Connexion**.

Remarque Pour supprimer l'erreur de certificat du bureau, vous devez fermer et rouvrir votre navigateur.

Firefox

1. Une page apparaît qui indique par un avertissement que cette connexion n'est pas fiable.
2. Sur l'onglet du navigateur, cliquez sur **Je comprends les risques** > **Ajouter une exception**.
3. Dans la boîte de dialogue **Ajouter une exception**, assurez-vous que la case **Enregistrer l'exception de façon permanente** est cochée.
4. Cliquez sur **Confirmer l'exception de sécurité**.

   La page d'avertissement se ferme automatiquement.
5. Saisissez vos nom d'utilisateur et mot de passe, et cliquez sur **Connexion**.

Répétez les étapes précédentes pour tous les liens de certificat. Après avoir accepté tous les certificats, le processus de connexion s'achève.

Chrome et Edge Chromium(Microsoft Edge)

1. Une page s'affiche avec un avertissement qui indique qu'il y a un problème avec le certificat de sécurité de votre site web.

   Dans Chrome, cliquez sur **Avancé** > **Continuer vers < nom d'hôte > (non sécurisé)**.

   Dans Microsoft Edge, cliquez sur **Avancé** > **Continuer vers < nom d'hôte > (non sécurisé)**.

   La page de connexion s'ouvre et une erreur de certificat apparaît dans la barre d'adresse de votre navigateur.

2. Cliquez sur l'**erreur de certificat**, puis sur

   Dans Chrome, cliquez sur **Certificat (non valide)**.

   Dans Microsoft Edge, cliquez sur **Certificat (non valide)**.

   La boîte de dialogue **Certificat** apparaît.

3. Dans l'onglet **Détails**, cliquez sur **Copier dans un fichier**.

   La boîte de dialogue **Assistant Exportation de certificat** s'ouvre.

4. Cliquez sur **Suivant**.

5. Conservez la sélection par défaut **Binaire codé DER X. 509 (. CER)** et cliquez sur **Suivant**.

6. Cliquez sur **Parcourir** et sélectionnez le dossier dans lequel vous souhaitez enregistrer le certificat.

7. Saisissez un **nom de fichier** reconnaissable et cliquez sur **Enregistrer**.

8. Cliquez sur **Suivant**.

9. Cliquez sur **Terminer**.

   Un message d'exportation réussie apparaît.

10. Cliquez sur **OK** et fermez l' **Assistant d'exportation de certificat**.

11. Accédez au dossier dans lequel vous avez enregistré le fichier de certificat (fichier .cer), cliquez avec le bouton droit sur le fichier, puis cliquez sur **Installer le certificat**.

    La boîte de dialogue **Assistant Exportation de certificat** s'ouvre.

12. Conservez l'**utilisateur actuel** de la sélection par défaut et cliquez sur **Suivant**.

13. Sélectionnez **Placer tous les certificats dans le magasin suivant**, puis cliquez sur **Naviguer**.

    La boîte de dialogue **Sélectionner un magasin de certificats** apparaît.

14. Sélectionnez **Autorités de certification racines de confiance**, puis cliquez sur **OK**.

15. Cliquez sur **Suivant**.

16. Cliquez sur **Terminer**.

    Une boîte de dialogue **d'avertissement de sécurité** s'affiche vous demandant si vous souhaitez installer le certificat.

17. Cliquez sur **Oui**. Une boîte de dialogue d'**importation de certificat**, qui indique que l'importation a réussi, s'affiche.

18. Cliquez sur **OK**.

19. Saisissez vos nom d'utilisateur et mot de passe, et cliquez sur **Connexion**.

Fermez le navigateur et connectez-vous à Cisco Unified Intelligence Center. L'erreur de sécurité n'apparaît pas dans la barre d'adresses.

Installer les certificats sur MacOS :

La procédure de téléchargement d'un certificat varie pour chaque navigateur. Pour chaque navigateur, procédez comme suit :

Chrome et Edge Chromium(Microsoft Edge)

1. Une page d'avertissement apparaît qui indique que votre connexion n'est pas privée. Pour ouvrir la page de connexion de Cisco Unified Intelligence Center,

   Dans Chrome, cliquez sur **Avancé** > **Continuer vers < nom d'hôte > (non sécurisé)**.

   Dans Microsoft Edge, cliquez sur **Avancé** > **Continuer vers < nom d'hôte > (non sécurisé)**.
2. Cliquez sur l'erreur de certificat qui apparaît dans la barre d'adresse, puis

   Dans Chrome, sélectionnez **Certificat (non valide)**.

   Dans Microsoft Edge, sélectionnez **Certificat (non valide)**.

   Une boîte de dialogue de certificat s'affiche avec les détails du certificat.
3. Faites glisser l' icône du **certificat** sur le bureau.
4. Double cliquez sur le certificat. L'application **Keychain Access** s'ouvre.
5. Dans le volet de droite de la boîte de dialogue Keychain, naviguez jusqu'au certificat, cliquez avec le bouton droit sur le certificat, puis sélectionnez **Obtenir des informations** à partir des options répertoriées. Une boîte de dialogue s'affiche avec davantage d'informations sur le certificat.
6. Développez **Approuver**. Dans le menu déroulant **Lors de l'utilisation de ce certificat**, sélectionnez **Toujours approuver**.
7. Fermez la boîte de dialogue contenant plus d'informations sur le certificat. Une boîte de dialogue de confirmation s’affiche.
8. Authentifiez la modification d u trousseau Keychains en fournissant un mot de passe.
9. Le certificat est maintenant approuvé et l'erreur de certificat n'apparaît pas dans la barre d'adresse.

Firefox

1. Dans votre navigateur Firefox, saisissez l'URL de Cisco Unified Intelligence Center. Une page d'avertissement s'affiche et indique qu'il y a un risque de sécurité.
2. Cliquez sur **Avancé**, puis sur le lien **Afficher le certificat**. La boîte de dialogue **Visionneuse de certificat** apparaît.
3. Cliquez sur **Détails** , puis cliquez sur **Exporter**. Enregistrez le certificat (**fichier .crt**) dans un dossier local.

Remarque Si l'option de fichier **.crt** n'est pas disponible, sélectionnez l'option **.der** pour enregistrer le certificat.

4. Dans le menu, sélectionnez **Firefox** > **Préférences**. La page **Préférences** s'affiche.

5. Dans le volet de gauche, sélectionnez **Confidentialité et sécurité**.
6. Faites défiler jusqu'à la section **Certificats** et cliquez sur **Afficher les certificats...**. La fenêtre **Gestionnaire de certificat** s'affiche.
7. Cliquez sur **Importer** et sélectionnez le certificat.
8. Le certificat est maintenant autorisé et l'erreur de certificat n'apparaît pas dans la barre d'adresse.

Prise en charge de la résolutions d'écran

Prise en charge de la résolution d'écran pour Cisco Unified Intelligence Center : 1366 x 768 ou supérieure.