Cisco Unified Intelligence Center の概要

概要

Cisco Unified Intelligence Center は、Cisco Contact Center 製品のユーザのためのレポーティング プラットフォームです。これは、履歴レポート、リアルタイムレポート、ライブデータレポート、およびダッシュボードを提供する、Web ベースのアプリケーションです。

Unified Intelligence Center は、主に次の目的に使用できます。

- ベース ソリューションのデータベースからデータを取得する。あらゆる Contact Center 製品をベース ソリューションとして使用できます。
- 特定のデータを取得するカスタム クエリの作成を可能にする。
- レポートの視覚的表示をカスタマイズする。
- レポートデータをカスタマイズする。
- さまざまなグループのユーザに、その役割に応じて特定のデータが表示されるようにする。

Unified Intelligence Center 次のタスクを実行できるユーザインターフェイス:

- レポートを作成および表示する。
- 選択したインターバルでレポートを実行するようスケジュール設定する。
- レポートおよびレポートフォルダのインポートとエクスポートを行う。

Unified Intelligence Center へのアクセス

Unified Intelligence Centerレポートアプリケーションにログインするための URLは。

HTTPS

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

この場合、HOST は Unified Intelligence Center のノードの DNS 名を表します。

Unified Intelligence Center はデフォルトでは HTTP をサポートしていません。コマンドライン インターフェイスから [cuic プロパティ（cuic properties）] > [http 有効（http-enabled）] の順に選択して [オン（on）] に設定することで、HTTP を有効にすることができます。HTTP が有効の場合、Unified Intelligence Center はログイン ページを HTTPS でロードします。ログイン成功後、Unified Intelligence Center はメイン ページを HTTP でロードします。

HTTP

http://<HOST>:8081/cuicui/Main.jsp

この場合、HOST は Unified Intelligence Center のノードの DNS 名を表します。

[http 有効（http-enabled）] が [オフ（off）] の場合、Unified Intelligence Center はすべての HTTP 要求を HTTPS にリダイレクトします。

（注） パーマリンクは HTTP でも HTTPS でも機能します。

Unified Intelligence Center のデフォルト ロケール

（注） ロケールを指定するには、言語パックをインストールします。

Cisco Unified Intelligence Center に初めてアクセスした場合は、ブラウザ ロケールにサインイン ページが表示されます。ロケールを変更するには、画面の右上隅にあるユーザ名をクリックし、ドロップダウン リストから必要なロケールを選択します。

ロケールを選択すると、ブラウザにそのロケール情報が保持されます。これは、サインアウトした後に同じブラウザで Cisco Unified Intelligence Center に再度サインインした場合でも保持されます。

表 *1*: サポートされている言語

ポルトガル語（ブラジル）	中国語（簡体字）	中国語（繁体字）	デンマーク語	オランダ語

英語（米国）	フランス語（フランス）	ドイツ語	イタリア語	日本語
韓国語	ロシア語	スペイン語（スペイン）	スウェーデン語	ポーランド語
トルコ語	フィンランド語	ノルウェー語	Čeština（チェコ語）	ブルガリア語
Català（カタロニア語）	Hrvatski（クロアチア語）	Magyar（ハンガリー語）	Slovenčina（スロバキア語）	slovenščina（スロベニア語）
Српски（セルビア語）	Română（ルーマニア語）			

クラスタの同期

システム設定の管理者は、クラスタ機能の同期 (ユーザインターフェイス画面の右上隅のユーザ名の下にあるリンク) を使用することによって、クラスタ内のすべてのノードに対してローカルキャッシュをクリアするように通知することができます。このアクションでは、クラスタ内のすべてのキャッシュを同期して空にします。ローカル キャッシュがクリアされると、各ノードは要求された情報をデータベースから直接取得せざるをえなくなります。

各ノードは、データベースから新しいデータを取得します。データは自動的にローカルキャッシュに入れられ、将来のリクエストの際にアクセスされます。データベース内のデータの一貫性は維持されるため、情報の損失はありません。

詳細については、*Cisco Unified Intelligence Center* アドミニストレーションガイド*Unified Intelligence Center* キャッシュ セクション
https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html
を参照してください。

ブラウザサポートと自己署名証明書

Unified Intelligence Center は、以下をサポートします。

- Internet Explorer 11（Windows 10 のネイティブモード）
- Firefox ESR 52 以上の ESR
- Edge Chromium（Microsoft Edge V79 以降）
- Chrome 60 以上

（注） アクセスするには OAMP、Internet Explorer 11 互換モードが必要です。Chrome のサポートは新しいユーザ インターフェイスのみが対象です。

自己署名証明書

Cisco Unified Intelligence Center に対してポップアップが有効になっていることを確認します。

Cisco Unified Intelligence Center の URL をブラウザに入力した後、以下の手順を実行して証明書を追加します。

Windows オペレーティングシステムでの証明書のインストール：

証明書の追加手順はブラウザによって異なります。各ブラウザでの手順を次に示します。

Internet Explorer

（注） Windows クライアントを使用して Windows ユーザとしてサインインしている場合は、管理者として Internet Explorer を実行して、セキュリティ証明書をインストールする必要があります。[スタート（Start）] メニューで、[Internet Explorer] を右クリックし、[管理者として実行（Run as Administrator）] を選択します。

セキュリティ証明書をインストールするために必要なアクセス許可がない場合は、管理者に問い合わせてください。

1. Web サイトのセキュリティ証明書に問題があるという警告がページに表示されます。[このサイトの閲覧を続行する（推奨されません）（Continue to this website (not recommended)）] リンクをクリックして、Cisco Unified Intelligence Center のサインインページを開きます。サインイン画面が表示され、アドレスバーに証明書エラーが表示されます。
2. アドレスバーに表示された証明書エラーをクリックし、[証明書の表示（View Certificates）] をクリックします。
3. [証明書（Certificate）] ダイアログボックスで、[証明書のインストール（Install Certificate）] をクリックして、証明書のインポートウィザードを開きます。
4. 証明書のインポートウィザードで、[次へ（Next）] をクリックします。
5. [証明書をすべて次のストアに配置する（Place all certificates in the following store）] を選択し、[参照（Browse）] をクリックします。
6. [信頼されたルート証明機関（Trusted Root Certification Authorities）] を選択し、[OK] をクリックします。
7. [次へ（Next）] をクリックしてから、[終了（Finish）] をクリックします。[セキュリティの警告（Security Alert）] ダイアログボックスが表示されます。

8. [はい（Yes）] をクリックして証明書をインストールします。[証明書のインポート（Certificate Import）] ダイアログボックスが表示されます。
9. [OK] をクリックし、[証明書のインポート（Certificate Import）] ダイアログボックスを閉じます。
10. ログイン情報を入力し、[サインイン（Sign In）] をクリックします。

（注） デスクトップから証明書エラーを削除するには、ブラウザを閉じて開き直す必要があります。

Firefox

1. この接続は信頼できないという警告がページに表示されます。
2. ブラウザのタブで、[リスクを容認する（I Understand the Risks）] > [例外の追加（Add Exception）] をクリックします。
3. [例外の追加（Add Exception）] ダイアログボックスで、[次回以降にもこの例外を有効にする（Permanently store this exception）] チェックボックスをオンにします。
4. [セキュリティ例外の確認（Confirm Security Exception）] をクリックします。

   警告ページが自動的に閉じます。
5. ログイン情報を入力し、[サインイン（Sign In）] をクリックします。

すべての証明書リンクについて上記の手順を繰り返します。すべての証明書を受け入れたら、サインインプロセスは完了です。

Chrome および Edge Chromium（Microsoft Edge）

1. Web サイトのセキュリティ証明書に問題があるという警告がページに表示されます。

   Chrome では、[詳細設定（Advanced）] > [<Hostname>にアクセスする（安全ではありません）（Proceed to <Hostname> (unsafe)）] をクリックします。

   Microsoft Edge では、[詳細設定（Advanced）] > [<Hostname>に進む（安全ではありません）（Proceed to <Hostname> (unsafe)）] をクリックします。

   サインインページが開き、ブラウザのアドレスバーに証明書エラーが表示されます。
2. 証明書エラーをクリックし、次の手順を実行します。

   Chrome では、[証明書（無効）（Certificate (Invalid)）] をクリックします。

   Microsoft Edge では、[証明書（無効）（Certificate (not valid)）] をクリックします。

   [証明書（Certificate）] ダイアログボックスが表示されます。
3. [詳細（Details）] タブで、[ファイルにコピー（Copy to File）] をクリックします。

   [証明書のエクスポートウィザード（Certificate Import Wizard）] ダイアログボックスが表示されます。

4. [次へ（Next）] をクリックします。
5. デフォルトの選択である [DER encoded binary X.509 (.CER)] のままにして、[次へ（Next）] をクリックします。
6. [参照（Browse）] をクリックし、証明書の保存先フォルダを選択します。
7. わかりやすいファイル名を入力し、[保存（Save）] をクリックします。
8. [次へ（Next）] をクリックします。
9. [Finish] をクリックします。

   エクスポートが正常に完了したことを知らせるメッセージが表示されます。
10. [OK] をクリックし、[証明書のエクスポートウィザード（Certificate Export Wizard）] を閉じます。
11. 証明書ファイル（.cer ファイル）を保存したフォルダを参照し、ファイルを右クリックして、[証明書のインストール（Install Certificate）] をクリックします。

    [証明書のインポートウィザード（Certificate Import Wizard）] ダイアログボックスが表示されます。
12. デフォルトの選択である [現在のユーザ（Current User）] のままにして、[次へ（Next）] をクリックします。
13. [証明書をすべて次のストアに配置する（Place all certificates in the following store）] を選択し、[参照（Browse）] をクリックします。

    [証明書ストアの選択（Select Certificate Store）] ダイアログボックスが表示されます。
14. [信頼されたルート証明機関（Trusted Root Certification Authorities）] を選択し、[OK] をクリックします。
15. [次へ（Next）] をクリックします。
16. [Finish] をクリックします。

    証明書をインストールするかどうかをたずねる [セキュリティ警告（Security Warning）] ダイアログボックスが表示されます。
17. **[はい（Yes）]** をクリックします。インポートの成功を通知する [証明書のインポート（Certificate Import）] ダイアログボックスが表示されます。
18. [OK] をクリックします。
19. ログイン情報を入力し、[サインイン（Sign In）] をクリックします。

ブラウザを閉じ、Cisco Unified Intelligence Center にサインインします。アドレスバーにセキュリティエラーが表示されなくなります。

macOS での証明書のインストール：

証明書のダウンロード手順はブラウザによって異なります。各ブラウザでの手順を次に示します。

Chrome および Edge Chromium（Microsoft Edge）

1. 接続がプライベートでないという警告ページが表示されます。Cisco Unified Intelligence Center のサインインページを開くには、次の手順を実行します。

   Chrome では、[詳細設定（Advanced）] > [<Hostname>にアクセスする（安全ではありません）（Proceed to <Hostname> (unsafe)）] をクリックします。

   Microsoft Edge では、[詳細設定（Advanced）] > [<Hostname>に進む（安全ではありません）（Proceed to <Hostname> (unsafe)）] をクリックします。

2. アドレスバーに表示された証明書エラーをクリックし、次の手順を実行します。

   Chrome では、[証明書（無効）（Certificate (Invalid)）] を選択します。

   Microsoft Edge では、[証明書（無効）（Certificate (Not Valid)）] を選択します。

   証明書の詳細を含む証明書ダイアログボックスが表示されます。

3. [証明書（Certificate）] アイコンをデスクトップにドラッグします。
4. 証明書をダブルクリックします。キーチェーンアクセスアプリケーションが開きます。
5. キーチェーンのダイアログの右ペインで、証明書を参照して右クリックし、表示されたオプションから [情報を取得（Get Info）] を選択します。証明書の詳細な情報を含むダイアログが表示されます。
6. [信頼（Trust）] を展開します。[この証明書を使用するとき（When using this certificate）] ドロップダウンから [常に信頼（Always Trust）] を選択します。
7. 証明書の詳細な情報を含むダイアログボックスを閉じます。確認用のダイアログボックスが表示されます。
8. パスワードを入力してキーチェーンの変更を認証します。
9. これで証明書が信頼され、アドレスバーに証明書エラーが表示されなくなります。

Firefox

1. Firefox ブラウザで、Cisco Unified Intelligence Center の URL を入力します。セキュリティリスクがあるという警告ページが表示されます。
2. [詳細（Advanced）] をクリックし、[証明書を確認（View Certificate）] リンクをクリックします。[証明書ビューア（Certificate Viewer）] ダイアログボックスが表示されます。
3. [詳細（Details）] をクリックし、[エクスポート（Export）] をクリックします。証明書（**.crt** ファイル）をローカルフォルダに保存します。

（注） **.crt** ファイルのオプションを使用できない場合は、**.der** オプションを選択して証明書を保存します。

4. メニューから、[Firefox] > [設定（Preferences）] を選択します。[設定（Preferences）] ページが表示されます。
5. 左側のペインで、[プライバシーとセキュリティ（Privacy & Security）] を選択します。
6. [証明書（Certificates）] セクションまでスクロールし、[証明書を表示...（View Certificates...）] をクリックします。[証明書マネージャ（Certificate Manager）] ウィンドウが表示されます。
7. [インポート（Import）] をクリックし、証明書を選択します。
8. これで証明書が承認され、アドレスバーに証明書エラーが表示されなくなります。

スクリーン解像度サポート

Cisco Unified Intelligence Center のサポートされている画面解像度：1366 x 768 以上。