システム設定

Settingsでは、ActiveServerインスタンスのシステム設定を構成できます。**Settings**には以下の3つのタブがあります：

- システム
- セキュリティー
- ActiveMerchantから移行

システム

システムには3つのセクションがあります。

サーバーURL

- **External URL** - 認証コールバックおよび製品のアクティブ化に使用される、外部からアクセス可能なURL。URLには、 `https://"あなたのActiveServerドメイン名":"サーバーポート番号"` の形式で入力できます。 `https://paymentgateway.com:8443` 等。URLの `サーバーポート番号` は、**ActiveServer**設定ファイルで設定された（使用されているプロトコルに応じて） `as.server.http.port` または `as.server.https.port` の値です。

> **警告**
>
> **外部URL**を更新すると、各国際ブランドのDirectory Server設定の3DSサーバーURLが更新されます。いずれかの国際ブランドの**3DSサーバーURL**の値が空の場合、新しい**外部URL**値とHTTPSリスニングポートを足した値が自動的に設定されます。 **3DSサーバーURL**値が既に設定されている場合、変更は行われません。
>
> この自動更新は、これらのURLの形式は一般的に同じであるため、セットアッププロセスを支援するための機能です。アーキテクチャーのセットアップによって**3DSサーバーURL**に個別のURLが割り当てられている場合、取引を実行する前にこの設定を更新する必要があります。

> **注釈**
>
> ロードバランサーがセットアップされていた場合、このURLは上記のURLパターンとは異なる場合があり、構成された別の管理UIインターフェイスURLになる場合があります。 **外部URL**用のロードバランサーが上記のサーバーポートにリクエストを転送していることを確認してください。
>
> 例： URL `https://paymentgateway.com` がサーバーコールバック用に設定され、 `https://admin.paymentgateway.com` が管理UIインターフェースリクエスト用に設定されている場合、 `https://paymentgateway.com` が**外部URL**に使用されます。

- **API URL** - 認証APIおよび管理API呼び出しの受信に使用されるオプションのURL。このURLのドメイン名は、API（x.509）の認証用のクライアント証明書の生成にも使用されます。入力されない場合、デフォルトで**ActiveServer**はクライアント証明書の生成に外部URLのドメイン名を使用します。このURLは外部からアクセス可能である必要はありません。URLの形式は**外部URL**と同じで、ポート番号を指定できます。
- **Admin URL** - Eメールを利用したユーザーのアクティブ化とパスワードのリセット手順に使用されるオプションのURL。この値は、**ActiveServer**の設定ファイルにAdmin portが有効と設定される場合のみ入力できます。Admin portが有効と設定され、この値が空白の場合は、localhostドメインと指定されたAdmin portが使用されます。ですがこの場合、リモートホストからドメインへアクセスする際に問題が発生します。Admin portが無効と設定される場合、**External URL**に入力されたドメイン名が使用されます。このURLは外部からアクセスできなくても支障はありません。

> **重要**
>
> 上記のURLの場合、システム機能が正しく実行されることを確認するためにURL妥当性確認が実行されます。妥当性確認では、URLに**パス**または**クエリ文字列**が含まれていないことを確認します。
>
> 例： `https://domainname<:port>` は妥当性確認に成功しますが、 `https://domainname<:port>/path?queryString` は失敗します。

ログ

- **Log level** - コンソール出力およびシステムログの詳細度。利用可能な値(右に行くほど詳細度が上がります）：**ERROR** > **INFO** > **DEBUG**.
- **Enable message content logs** - 有効化されると、ActiveServer は 3DS メッセージの内容をログに残します。

API構成

API構成セクションでは、インスタンスのAPIバージョンのシステム管理が可能です。現在、サポートされているAPIバージョンが表示され、認証APIV1を無効にする機能が提供されています。

APIv1 の無効化

APIv1 のサポートが廃止日を迎えたため、APIv2 のみを使用するようシステムを更新すべく、APIv1を無効にする機能が提供されました。 APIv2 には下記のような改善点が数多く含まれます：

- 完全な PAN は保存されなくなり、PCI セキュリティ監査要件の軽減が見込まれています。
- 加盟店ごとの暗号化キーが不要になり、取引処理並びにデータベース及び HSM アクセスのための性能が向上しました。
- 取引格納のためのデータ構造が改善されました。

API V2への移行は、認証API V1を無効にし、すべてのトランザクションをAPI V2に変換する**一方向**のプロセスであり、元に戻すことはできません。 **移行する前に3DSリクエスターをアップグレードしてAPI V2トランザクションのみを使用し、問題がないことを確認することを強くお勧めします。**

API V1を無効にするボタンを選択すると、次のプロセスが実行されます。

1. すべての認証APIV1リクエストは、エラーコード「1027 Unsupported API version」を返すようになります。したがって、3DSリクエスターはAPI V1リクエストを送信できなくなります。
2. 加盟店によって実行されるトランザクションの暗号化に使用されるデータキーは、新しい加盟店が作成されたときに作成されなくなります。認証API V2は、加盟店ごとのキーを使用せず、トランザクションデータの暗号化にマスターキーとデータキーを使用したエンベロープ暗号化を使用します。
3. バックグラウンドで移行プロセスが開始され、API v1で保存されたPANが切り捨てられ、データ形式がAPI V2に変更されます（データベースから使用されなくなったテーブルの削除を含む）。移行するトランザクションの数は、管理UIに表示されます。 **APIv1トランザクションの数**のカウンターが「0」に達すると移行プロセスのが完了を意味しています。

データキーの削除

既存の加盟店毎のデータキーまたはキーストアファイルは、ActiveServerによって自動的に**削除されません**。移行プロセスが終了したら、HSM、ローカル、またはS3バケットのキーは不要になったため、いつでも手動で削除できます。

HSMを使用している場合は、接頭辞 `REQ_` が付いているキーエイリアスを削除できます。キーエイリアスの前に `AS_` または `MASTER_` が付いているキーは**削除しないでください**。

SunJCEローカルまたはS3キーストアタイプでActiveServerを使用している場合は、`as_<UUID>.jks` の形式のキーストアファイルを削除できます。 `as_sys_<UUID>.jks` または `as_master_key.jks` キーストアファイルを**削除しないでください**。

> **注釈**
>
> KMSキーストアタイプを利用している場合はAPIV1はデフォルトで無効になっているため、APIV1の無効化プロセスは適用されません。

セキュリティー

- **Session timeout (読み取り専用)** - 有効期限が切れ、ユーザーにログイン認証情報の再入力を要求するまでの、ログイン・セッションが有効な間隔。デフォルトのセッションは900秒(15分)に設定されています。この設定を変更する場合は `application-prod.properties` に以下の行を追加してインスタンスを再起動させて下さい。

  ```
  as.settings.session-timeout={単位　秒}
  ```

  例：　セッションのタイムアウト時間を1800秒(30分)に設定したい場合は `as.settings.session-timeout=1800` と追加して下さい。

  > **重要**
  >
  > 値は300 ~ 3600秒までの整数が設定可能です。

- **Session failed attempts** - セッション・ロック時間で指定された期間ログインが一時的に無効化されるまでの失敗ログイン試行回数。一定時間経過後、正しい認証情報を指定することでセッションを再確立できます（単位： 試行回数）。
- **Session lock time** - 失敗ログイン試行回数を超えた場合にユーザーがロックされる間隔（単位： 分）
- **Password expiry period** - 新しいパスワードの作成が要求されるまでの、パスワードが有効な日数（単位： 日数）
- **Password history check** - 特定のパスワードを再度利用できるようになるまで一意のパスワードの使用が要求される数 （単位： 一意のパスワード数）
- **Force two factor login** - サーバー上の**すべての**ユーザーに対して2要素認証を**enable**（有効化）**disable**（無効化）します。ActiveServerでは、ユーザーに2要素認証を提供するのにGoogle認証システムを使用しています。この設定が**有効化**されると、アカウントで2要素認証がまだセットアップされていないユーザーは、システム機能を使用する前に、次回ログイン時に2要素認証をセットアップすることが強制されます。Google認証システムのセットアップの手順が画面上に表示されます。

データ暗号化鍵ローテーション

現在のシステム用の暗号鍵（システム情報の暗号化に使用）の作成日を表示し、ユーザーが[**Rotate key**]を選択することで使用する、鍵をローテーションできます。新しいシステムの関連データは、新しいデータ暗号鍵を使用して暗号化されます。

マスター暗号鍵のローテーション

現在のマスター暗号キー（認証API v2トランザクションの認証値の暗号化に使用）の作成日とキーエイリアスを表示します。 [**Rotate key**]を選択して、ユーザー鍵をローテーションできます。ただし、キーローテーションは、マスターキーが保護するデータには影響しません。マスターキーが生成したデータ暗号鍵をローテーションしたり、マスターキーで保護されているデータを再暗号化したりすることはありません。

HSM

この機能を使用すると、変更された場合にユーザーがHSM PINを更新できます。

- **Full file name and path of PKCS#11 library** - この値は `application-prod.properties` から読み取られ、 `application-prod.properties` ファイルを更新し、サーバーを再起動することでのみ変更できます。
- **Slot number of HSM** - この値は `application-prod.properties` から読み取られ、 `application-prod.properties` ファイルを更新し、サーバーを再起動することでのみ変更できます。
- **HSM PIN** - 新しいHSM PINを入力できます。

Test HSM connectionボタンを選択すると、入力した**HSM PIN**を使用したHSMへの接続が試行されます。テストが成功すると、システムによって"HSM connection successful"というメッセージが表示されます。失敗した場合は"Invalid HSM Pin"と表示されます。

Updateボタンを選択すると、**HSM PIN**の値でデータベースが更新されます。**更新後はサーバーの再起動が必要です**。

> **警告**
>
> HSM PINテストの結果にかかわらず、HSM PINは更新されます。これは、必要に応じて、HSM PINが変更される前に、**ActiveServer**データベースを更新できるようにするためです。誤ったHSM PINを使用すると取引が失敗するため、システムを更新する前に正しいPINが入力されていることを確認してください。

> **Version 1.0.4**
>
> この機能はバージョン1.0.4リリースで追加されました。

ActiveMerchantから移行

ActiveMerchant　Migrationタブでは、**ビジネス管理者**ユーザーがGPayments**ActiveMerchant**（3DS1 MPI）から加盟店とアクワイアラーをインポートして、3DS1から3DS2への移行をを可能にします。

移行機能の詳細については、 ActiveMerchantからの移行ガイドをご確認下さい。