Security Server 設定ガイド

目次

1. はじめに

本書では Security Server の設定方法について説明します。

1.1 対象読者

本書は、PlanetCross ソフトウェアのインストール、操作、管理を行う PlanetCross Security Server システム管理者を対象としています。

1.2 必要な技能

本書は、Linux サーバーの管理、コンピューターネットワーク、および PlanetCross の動作原理について中級程度の知識をお持ちの方を対象としています。

1.3 PlanetCross Security Server

Security Server の主な機能は、リクエストの証拠能力を担保した上で、リクエストを仲介することです。

Security Server は、ポートの一方がパブリックインターネットに接続され、他方が組織内ネットワークの情報システムに接続されています。Security Server は SOAP プロトコルをサポートする特殊なアプリケーションファイアウォールとして考えることもできます。そのため、他のプロトコルを仲介するファイアウォールなどと並行して設定する必要があります。

Security Server には、クライアントとサービスプロバイダーの間のメッセージ交換を保護する機能があります。

- パブリックインターネットを通じて送信されるメッセージは、デジタル署名と暗号化によって保護されます。
- サービスプロバイダーの Security Server は受信するメッセージに対してアクセス制御を行います。データにアクセスできるのは、サービスプロバイダーと適切な契約を結んだユーザーだけに制限されます。

システム全体の可用性を高めるために、サービスユーザーとサービスプロバイダーの Security Server は、次のように冗長化できます。

- サービスユーザーはリクエストをするために、複数台の Security Server を並行して動作させることができます。
- サービスプロバイダーがサービスを提供するために複数台の Security Server をネットワークに接続する場合、リクエストは複数のサーバーにロードバランシング(負荷分散)されます。
- サービスプロバイダーの一台の Security Server がオフラインになると、リクエストは自動的に利用可能な他の Security Server に振り分けられます。

Security Server は、グローバルコンフィギュレーションを提供する Central Server にも依存します。

1.4 PlanetCross のコンセプト

- **グローバルコンフィギュレーション**

  Security Server によって PlanetCross Central Server から定期的にダウンロードされる XML ファイルからなります。グローバルコンフィギュレーションは、以下を含みます。

- トラストアンカーのアドレスと公開鍵(認証サービスの CA およびタイムスタンプサービス)
- 中間認証局の公開鍵
- OCSP サービスのアドレスと公開鍵 (*Authority Information Access* 拡張により利用できない場合)
- PlanetCross メンバーとそのサブシステムに関する情報
- PlanetCross に登録されているメンバーの Security Server のアドレス
- PlanetCross に登録されている Security Server の認証用証明書に関する情報
- PlanetCross に登録されている Security Server のクライアントに関する情報
- グローバルアクセス権グループに関する情報
- PlanetCross システムパラメーター

- **メンバークラス**

  共通のユニットの下で同様の特性を持つ PlanetCross メンバーをグループ化します。たとえば、国の機関は"GOV"メンバークラスの下にグループ化され、民間組織は"COM"のメンバークラス下にグループ化されます。

- **メンバーコード**

  特定の PlanetCross メンバーと 1 対 1 で関連付きます。特定のメンバークラス内のユニークな文字の組み合わせです。メンバーコードはメンバーの存続期間中は変更されません。たとえば、エストニアの組織や国の機関のメンバーコードは事業登録番号です。

- **Security Server クライアント**

  Security Server との関係が PlanetCross 監督機関に登録されており、PlanetCross サービスを使用および/または提供するために Security Server を使用する PlanetCross メンバーのサブシステムです。

- **Security Server の所有者**

  特定の Security Server を法的に担当する PlanetCross メンバーです。Security Server の所有者は、太字のフォントで Security Server クライアントリスト("Configuration" -> "Security Server Clients") に表示されます。
  サブシステムは、PlanetCross メンバーの情報システムの一部を表します。PlanetCross メンバーは、PlanetCross サービスを使用または提供するために、情報システムをサブシステムとして登録しなければなりません。

  - サブシステムは、PlanetCross サービスの提供と使用の面において自立しています。PlanetCross メンバーのサブシステムのアクセス権は独立しています。一つのサブシステムに与えられたアクセス権は、メンバーの他のサブシステムのアクセス権には影響しません。
  - サブシステムによって提供されるサービスは、メンバーの他のサブシステムによって提供されるサービスから独立しています。

  PlanetCross サービスを使用または提供する際に、サブシステムから送信されたメッセージに署名するため、サブシステムを管理するメンバーの署名用証明書が使用されます。
  PlanetCross メンバーは、複数のサブシステムを一台の Security Server に関連付けることができ、一つのサブシステムは複数台の Security Server に関連付けることができます。

- **PlanetCross 証明書**

  PlanetCross 監督機関で承認された認証サービスプロバイダーが発行します。PlanetCross 証明書は、次のいずれかになります。

  - **署名用証明書** - PlanetCross メンバーに発行され、Security Server が交換するデータにデジタル署名するために使用します。
  - **認証用証明書** - Security Server に対して発行され、Security Server の間のセキュアな通信チャネルを確立するために使用します。

- **PlanetCross インスタンス**

  ID は異なる PlanetCross インスタンスを識別します。各インスタンスには識別コードが割り当てられています。たとえば、エストニアの開発インスタンスのコードは "ee-dev" であり、プロダクションインスタンスのコードは "EE" です。

- **PlanetCross メンバー**

  PlanetCross に参加し、そのサービスプロバイダーおよび/またはユーザーの能力によって PlanetCross の機能を使用する法人あるいは人です。

- **PlanetCross のメッセージ**

  PlanetCross メッセージプロトコルに基づいて記述されたサービスリクエストとレスポンスです。サービスを利用または提供する情報システムと Security Server 間で交換されます。

2. ユーザー管理

2.1 ユーザーのロール(役割)

Security Server は、次のユーザーのロールをサポートします。

- **セキュリティ担当者**(xroad-security-officer) - 鍵設定、鍵、および証明書の管理を含むセキュリティポリシーとセキュリティ要件を担当します。
- **登録担当者**(xroad-registration-officer) - Security Server クライアントの登録と削除を担当します。
- **サービス管理者**(xroad-service-administrator) - サービスのデータとアクセス権を管理します。
- **システム管理者**(xroad-system-administrator) - Security Server のインストール、設定、およびメンテナンスを担当します。
- **Security Server オブザーバー**(xroad-securityserver-observer) - 設定の編集アクセス権なしで Security Server の状態を閲覧することができます。このロールを通じて、ユーザーに Security Server の管理ユーザーインターフェイスへの読み取り専用アクセスを提供することができます。

一人のユーザーは複数のロールを持つことができ、複数のユーザーが同じロールを持つこともできます。各ロールには、システムのインストール時に作成された対応するシステムグループがあります。

以後、ガイドの各適用セクションは、特定のアクションを実行するためにどのユーザーロールが必要かを示します。

記載例) ＜アクセス権: セキュリティ担当者＞

ログインしているユーザーに特定のタスクを実行する権限がない場合、アクションを開始するボタンは非表示になります(対応するキーボードの組み合わせやマウスアクションを使用してタスクを実行することもできません)。許可されたデータとアクションのみが表示され、ユーザーが利用できます。

2.2 ユーザーの管理

ユーザー管理は、root ユーザー権限においてコマンドラインで実行されます。

2.2.1 ユーザーの追加

新しいユーザーを追加するには、次のコマンドを入力します。

```
$ sudo adduser username
```


2.2.2 ユーザー権限の設定

作成したユーザーに権限を付与するには、該当するシステムグループに追加します。たとえば、次のようにします。

```
$ sudo adduser username xroad-security-officer
$ sudo adduser username xroad-registration-officer
$ sudo adduser username xroad-service-administrator
$ sudo adduser username xroad-system-administrator
$ sudo adduser username xroad-securityserver-observer
```

ユーザー権限は、xroad-jetty サービス再起動後にのみ適用されます。

2.2.3 ユーザー権限の削除

ユーザー権限を削除するためには、該当するシステムグループからユーザーを削除します。たとえば、次のようにします。

```
$ sudo deluser username xroad-security-officer
```

2.2.4 ユーザーの削除

ユーザーを削除するには、次のように入力します。

```
$ sudo deluser username
```


3. Security Server クライアントの管理

重要	**PlanetCross** サービスを使用または提供するには、Security Server クライアントが **PlanetCross** 監督機関によって承認された認証サービスプロバイダーに認証される必要があります。 また、クライアントとクライアントが使用する Security Server 間の関連付けを **PlanetCross** 監督機関に登録しなければなりません。

このセクションでは、Security Server のクライアントの管理について、説明します。

【注記】
Security Server のクライアントは、Security Server の所有者とは異なります。所有者の情報は、Security Server のインストール時に登録されます。所有者の詳細については、『Security Server インストールガイド』を参照してください。

3.1 Security Server クライアントの状態

クライアントには以下の状態があります。

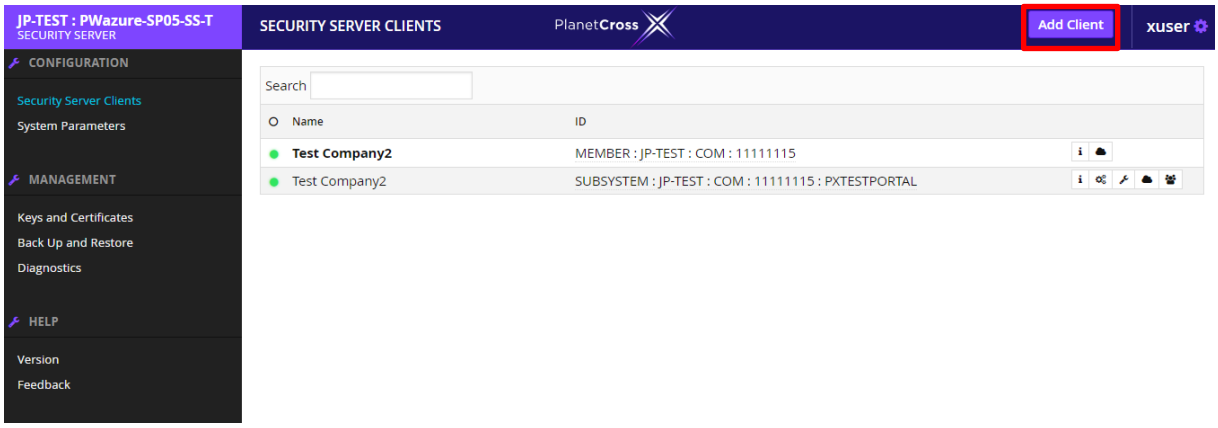
状態	説明
 保存済	クライアントの情報が入力され、Security Server に保存済であることを示します。ただし、クライアントと Security Server 間の関連付けは、PlanetCross 監督機関に登録されていない状態です。(関連付けがデータ入力前に Central Server に登録されている場合、クライアントはデータ入力後に「登録済」状態になります)。 「保存済」の状態から、クライアントは次の状態に移行できます。 ・「登録中」: クライアントの登録リクエストが Security Server から送信された場合。 ・「削除済」: クライアントの情報が Security Server の設定から削除された場合。
 登録中	クライアントの登録リクエストは Security Server から Central Server に送信されたが、クライアントと Security Server の関連付けはまだ PlanetCross 監督機関によって承認されていない状態です。 「登録中」状態から、クライアントは次の状態に遷移できます。 ・「登録済」: クライアントと Security Server 間の関連が PlanetCross 監督機関によって承認された場合。 ・「削除中」: クライアント削除リクエストが Security Server から提出された場合。
 登録済	クライアントと Security Server 間の関連付けが、PlanetCross 監督機関で承認されている状態です。 この状態では、クライアントは PlanetCross サービスを提供し、使用することができます(他のすべての条件が満たされていることが前提)。 「登録済」の状態から、クライアントは次の状態に遷移できます。 ・「グローバルエラー」: クライアントと Security Server の間の関連が PlanetCross 監督機関によって取り消された場合。 ・「削除中」: クライアント削除リクエストが Security Server から送信された場合。

状態	説明
グローバルエラー	クライアントと Security Server 間の関連付けが Central Server で取り消された状態です。 「グローバルエラー」の状態から、クライアントは次の状態に遷移できます。 ・「登録済」: クライアントと Security Server 間の関連付けが Central Server に復元された場合(例えば、クライアントと Security Server 間の関連付けがエラーのために失われた場合)。 ・「削除済」: クライアントの情報が Security Server の設定から削除された場合。
削除中	クライアントの削除リクエストが Security Server から送信された状態です。 「削除中」の状態から、クライアントは次の状態に遷移できます。 「削除済」: クライアントの情報が Security Server の設定から削除された場合。

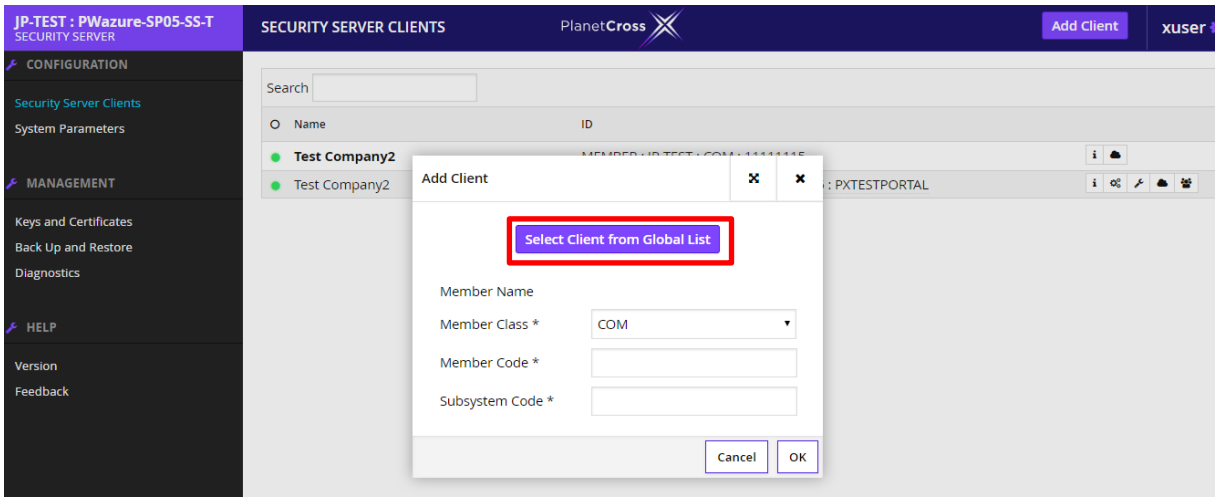
3.2 Security Server へのクライアントの追加

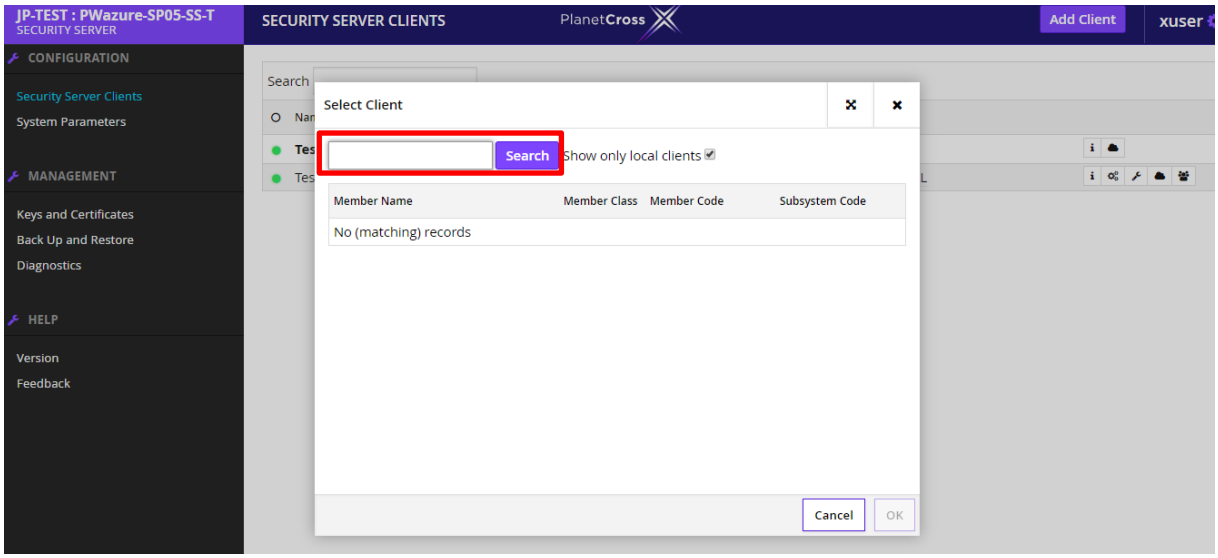
Security Server にクライアントを追加します。＜アクセス権: 登録担当者＞

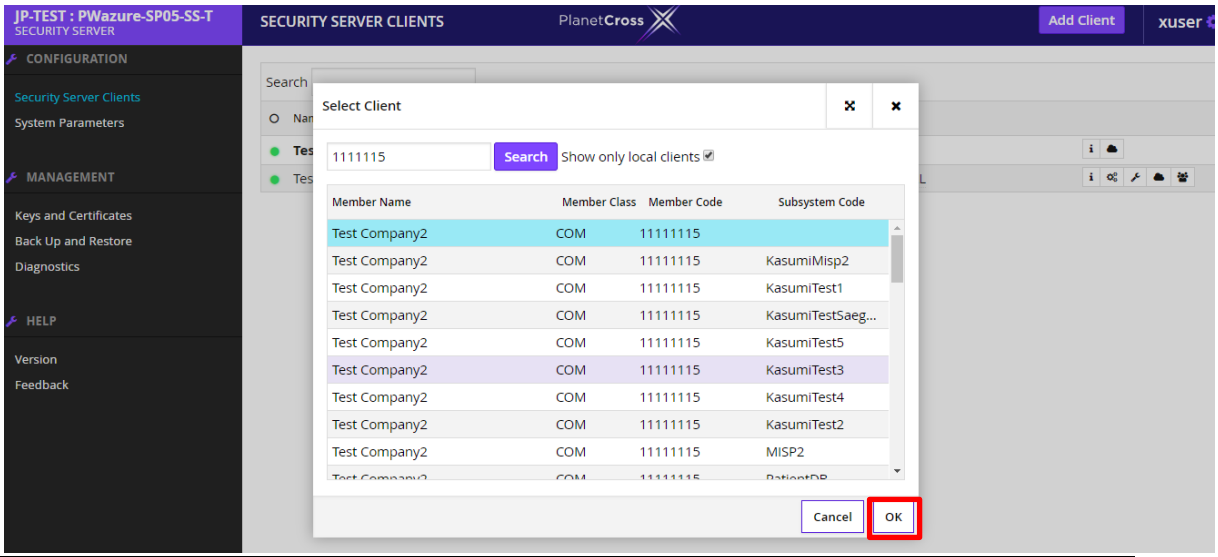
1. **[Configuration]**メニューで、**[Security Server Clients]**を選択します。

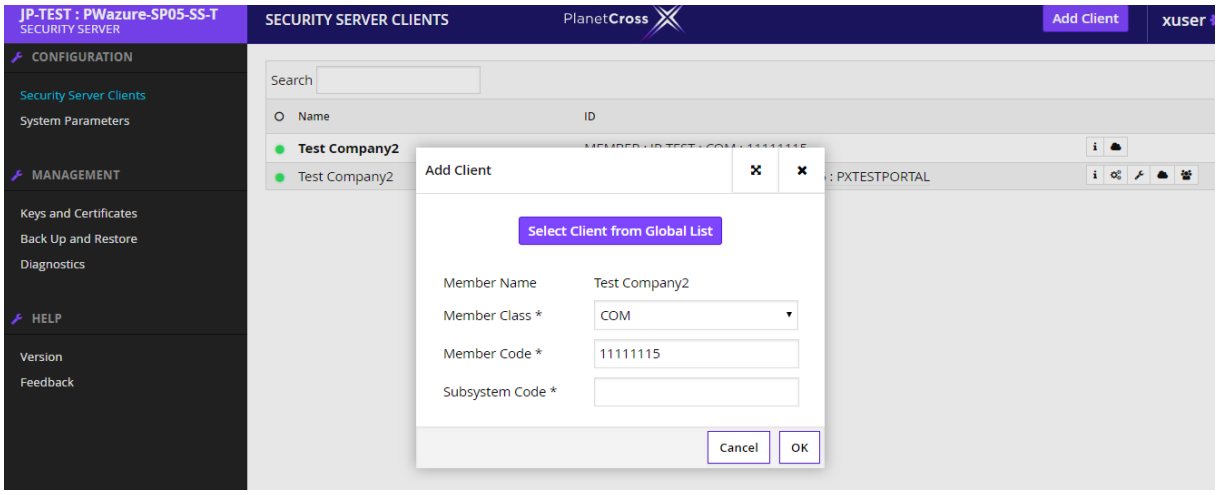


2. **[Add Client]**をクリックします。
開いたウィンドウで、クライアントの情報を手動で入力するか、または**[Select Client from Global List]**をクリックし、すべての PlanetCross メンバーとそのサブシステムの中からクライアントの情報を探します。

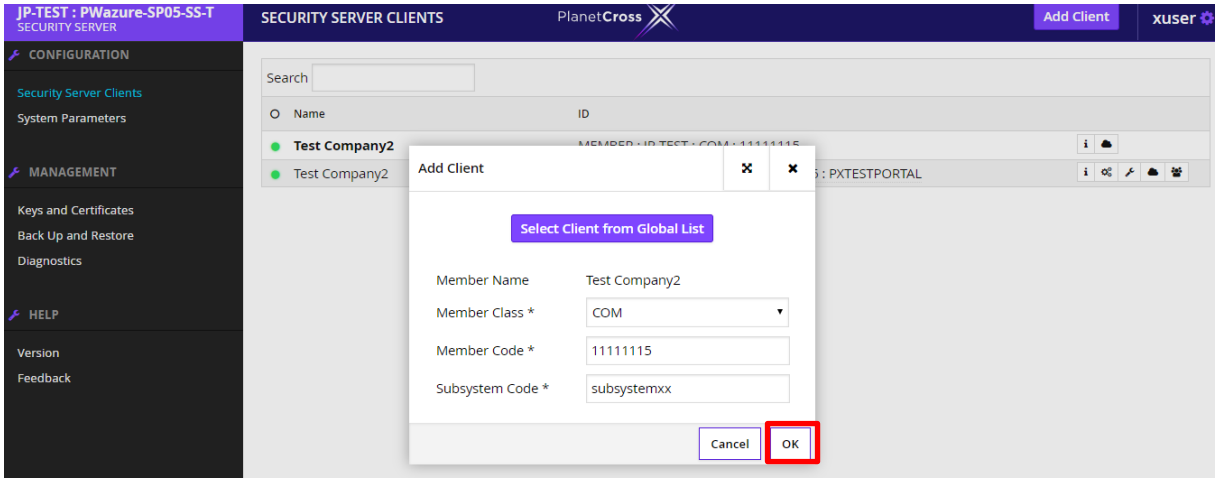


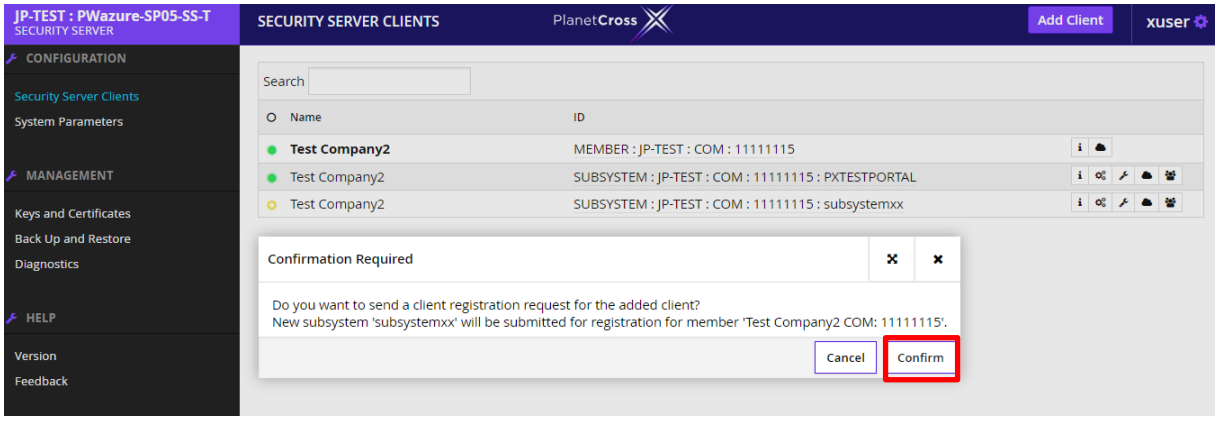






3. クライアントの情報を入力したら、**[OK]**をクリックし、**[Confirm]**をクリックします。
新しいクライアントは、「保存済」状態で Security Server クライアントのリストに追加されます。





3.3 Security Server クライアントの署名用鍵と証明書の設定

Security Server クライアントが PlanetCross を介して交換されるメッセージに署名するためには、署名用鍵と証明書を設定する必要があります。

【注記】
・証明書はサブシステムには発行されません。サブシステムは、サブシステムの所有者(すなわち、PlanetCross メンバー)の証明書を使用します。
・同じ Security Server に登録されている PlanetCross メンバーのサブシステムは、メッセージを署名するのに同じ署名用証明書を使用します。既にメンバーの署名用証明書を含む場合、そのメンバーのサブシステムを追加するときに、新しい署名用鍵および/または証明書を設定する必要はありません。

3.4 PlanetCross 監督機関に Security Server クライアントを登録する

Security Server クライアントを PlanetCross 監督機関に登録するには、次の手順を実行します。

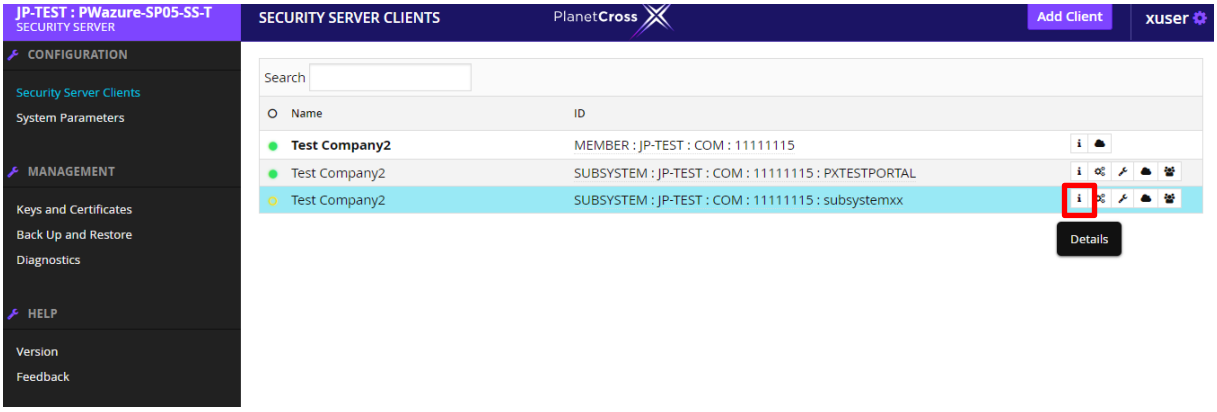
1. Security Server クライアント登録リクエストを Security Server から送信します。
2. クライアントの登録リクエストを、PlanetCross インスタンスの組織手順に従って PlanetCross 監督機関に送信します。

登録リクエストは、PlanetCross 監督機関によって承認される必要があります。

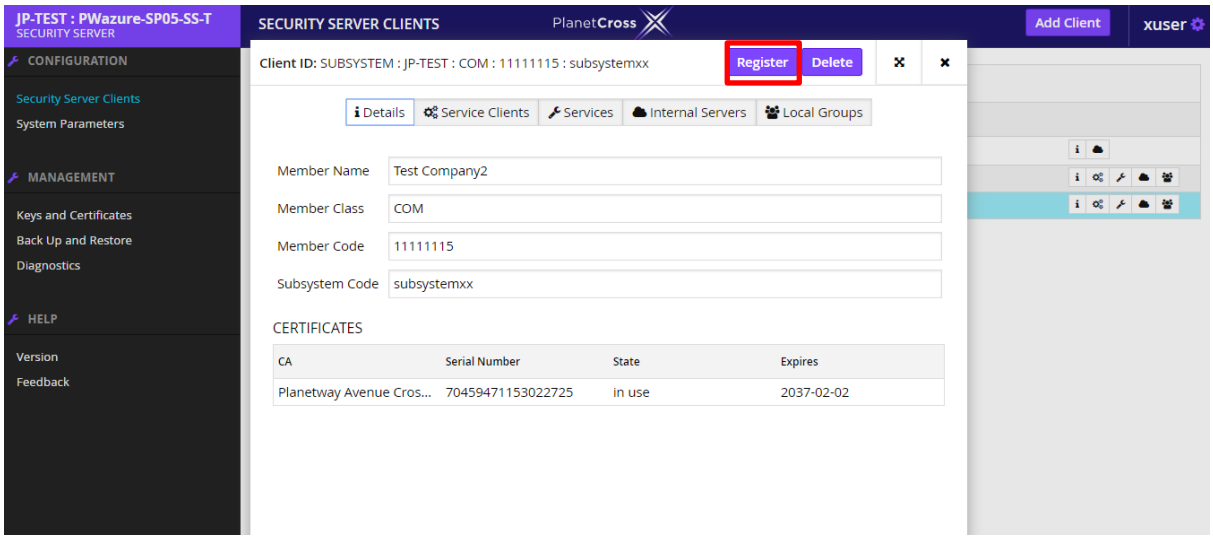
3.4.1 Security Server クライアントの登録

クライアント登録リクエストを送信するためには、次の手順を実行します。
＜アクセス権: 登録担当者＞

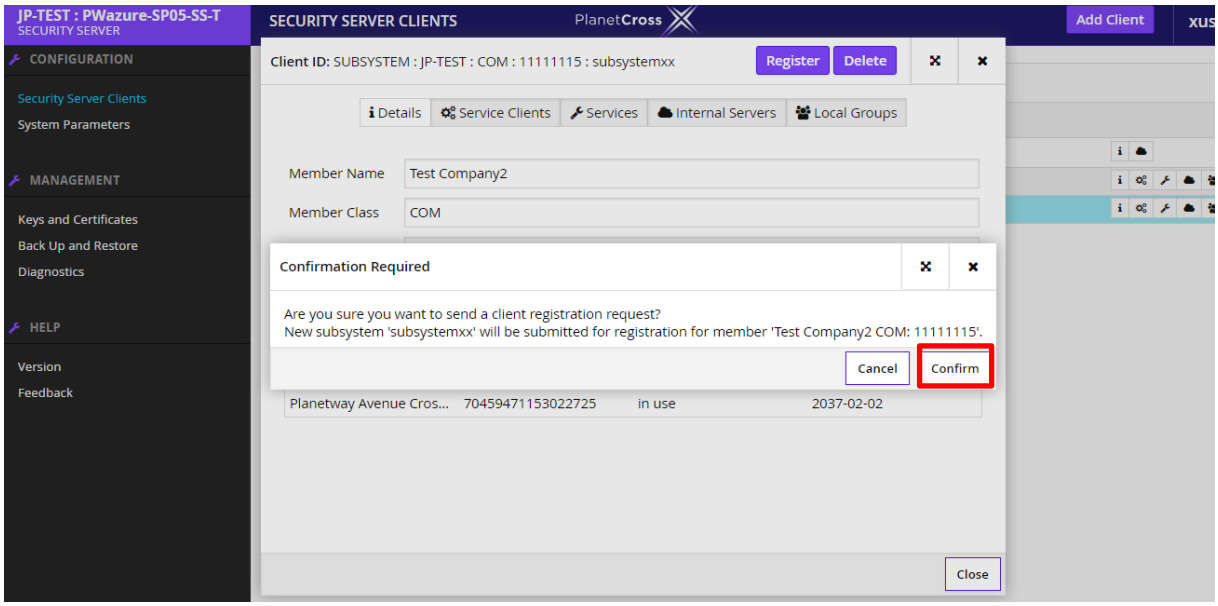
1. **[Configuration]**メニューで、**[Security Server Clients]**を選択します。
2. Security Server クライアントのリストから「保存済」状態のクライアントを選択します。



3. **[Details]**アイコンをクリックし、開いたウィンドウで**[Register]**をクリックします。



4. **[Confirm]**をクリックしてリクエストを送信します。



リクエストを送信すると、「Request sent」というメッセージが表示され、クライアントの状態は「登録中」に設定されます。 PlanetCross 監督機関が登録を承認した後に、クライアントの状態は「登録済」に設定され、登録プロセスは完了します。

3.5 Security Server からクライアントの削除

Security Server からクライアントを削除すると、クライアントに関連するすべての情報(WSDL、サービス、アクセス権、必要であれば証明書)もサーバーから削除されます。

【注記】
1 クライアントが削除された場合でも、その署名用証明書が Security Server に登録された他のクライアント、たとえば削除されたクライアントが属する PlanetCross メンバーの他のサブシステムによって使用されている場合には、署名用証明書を削除することは推奨しません。

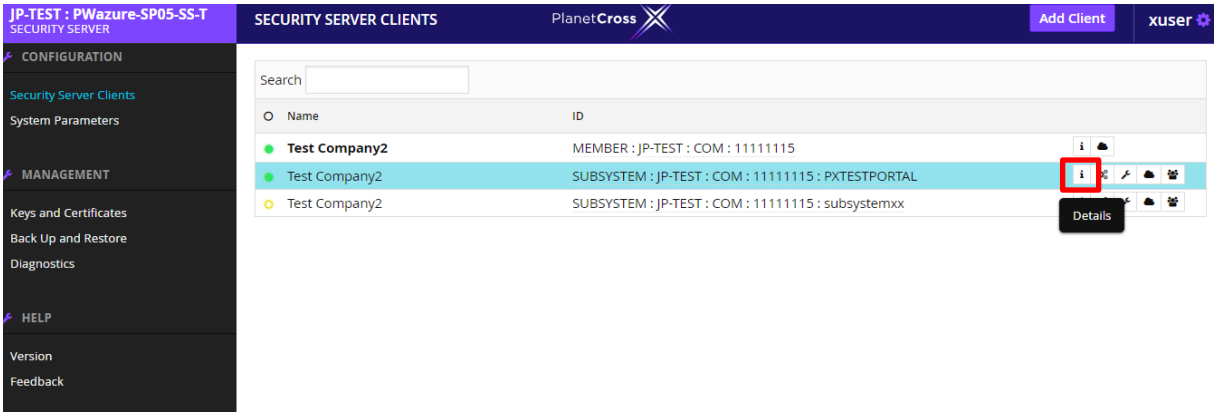
PlanetCross 監督機関に登録済みまたは登録中状態と表示されるクライアントは、削除する前に登録解除する必要があります。登録解除イベントは、Security Server から Security Server クライアント削除リクエストを Central Server に送信します。

3.5.1 クライアントの登録を解除する

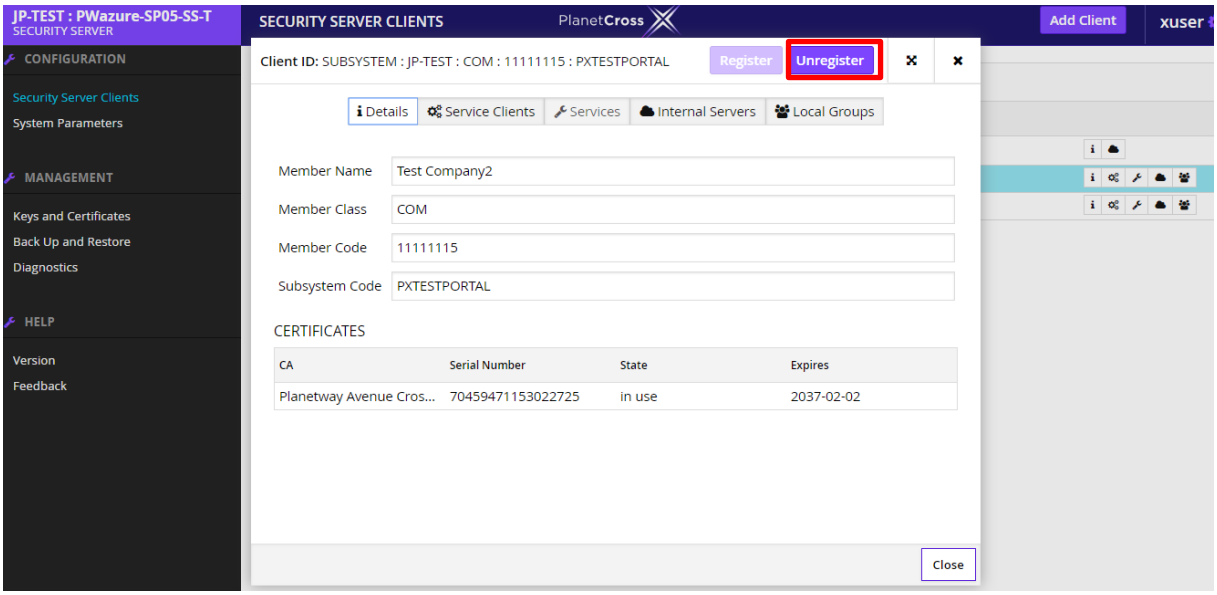
クライアントの登録を解除するには、次の手順を実行します。＜アクセス権: 登録担当者＞

1. **[Configuration]**メニューで、**[Security Server Clients]**を選択します。

2. サーバーから削除したいクライアントを選択し、クライアントの行の**[Details]**アイコンをクリックします。



3. 表示されたウィンドウで、**[Unregister]**をクリックし、**[Confirm]**をクリックします。



Security Server は、自動的にクライアント削除リクエストを Central Server に送信し、Central Server はそれを受信すると Security Server とクライアント間の関連付けを削除します。

4. 削除リクエストの Central Server への送信についての通知が表示されるので、クライアントの情報(証明書を除く)を削除するか確認します。

   クライアントの情報をすぐに削除したい場合は、**[Confirm]**をクリックします。
   クライアントの証明書を削除するオプションが表示されます。
   証明書を削除するには、もう一度**[Confirm]**をクリックします。

   クライアントの情報を保持したい場合は、**[Cancel]**をクリックします。
   クライアントは、メッセージを仲介することができず PlanetCross 監督機関に再度登録することができない「削除中」状態に移行します。

5. 「削除中」状態のクライアントの情報を削除するには、クライアントの行の**[Details]**アイコンをクリックします。
   クライアントを選択し、開いたウィンドウで**[Delete]**をクリックして、**[Confirm]**をクリックします。

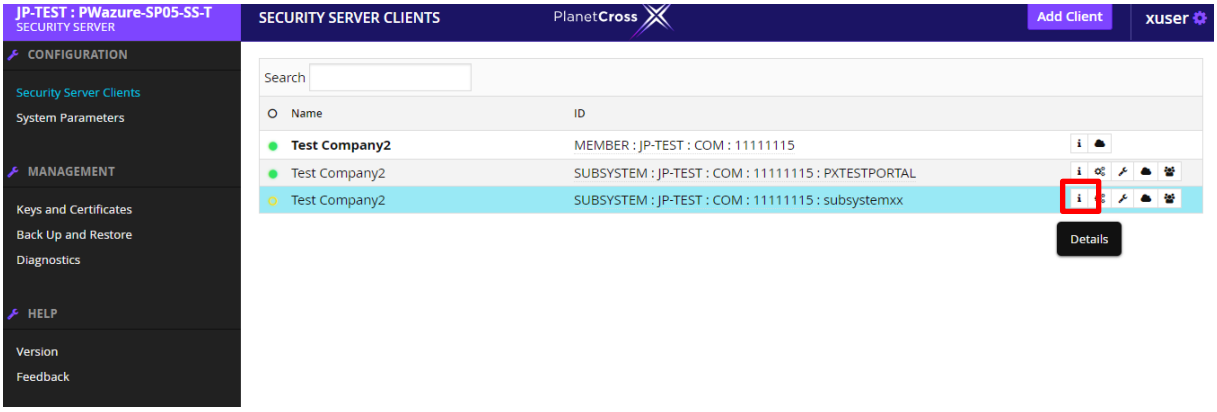
【注記】
Security Server を介し削除リクエストを送信することなく、登録されたクライアントを Central Server から登録削除することができます。この方法では、クライアントを担当する Security Server の管理者は、登録を解除するクライアントに関する情報を含むリクエストを Central Server の管理者に送信する必要があります。クライアントが Security Server からの削除リクエストなしで Central Server から削除された場合、クライアントは Security Server に「グローバルエラー」状態で表示されます。

3.5.2 クライアントを削除する

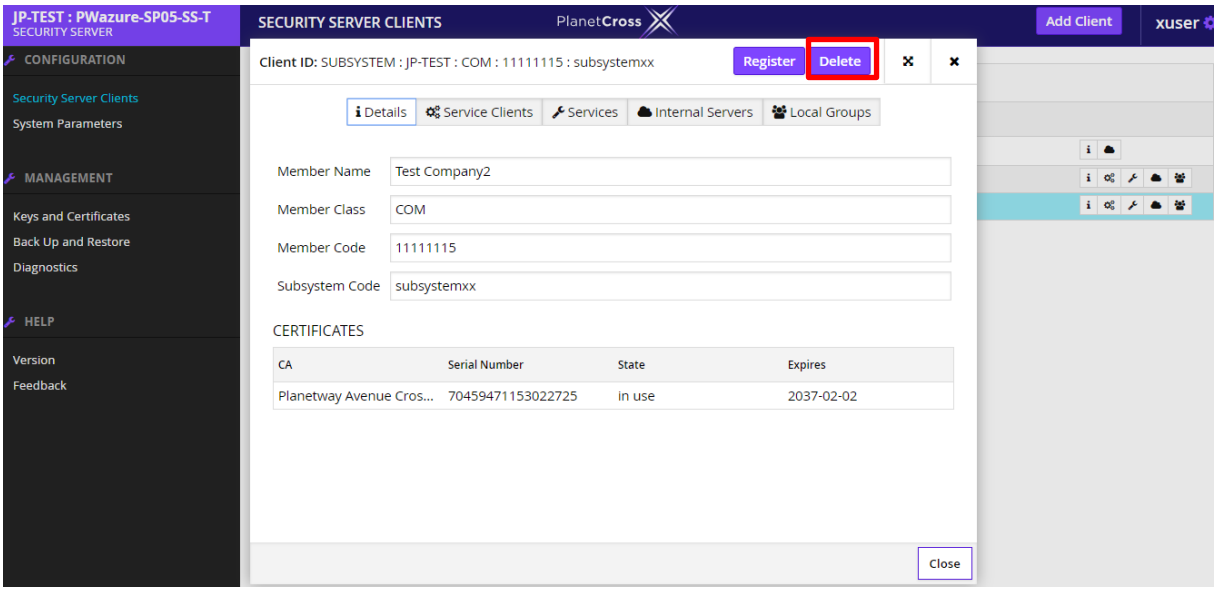
Security Server クライアントは、状態が「保存済」、「グローバルエラー」または「削除中」であれば削除できます。「登録済」または「登録中」の状態にあるクライアントは、削除する前に登録解除する必要があります。
クライアントを削除するには、次の手順を実行します。＜アクセス権: 登録担当者＞

1. **[Configuration]**メニューで、**[Security Server Clients]**を選択します。

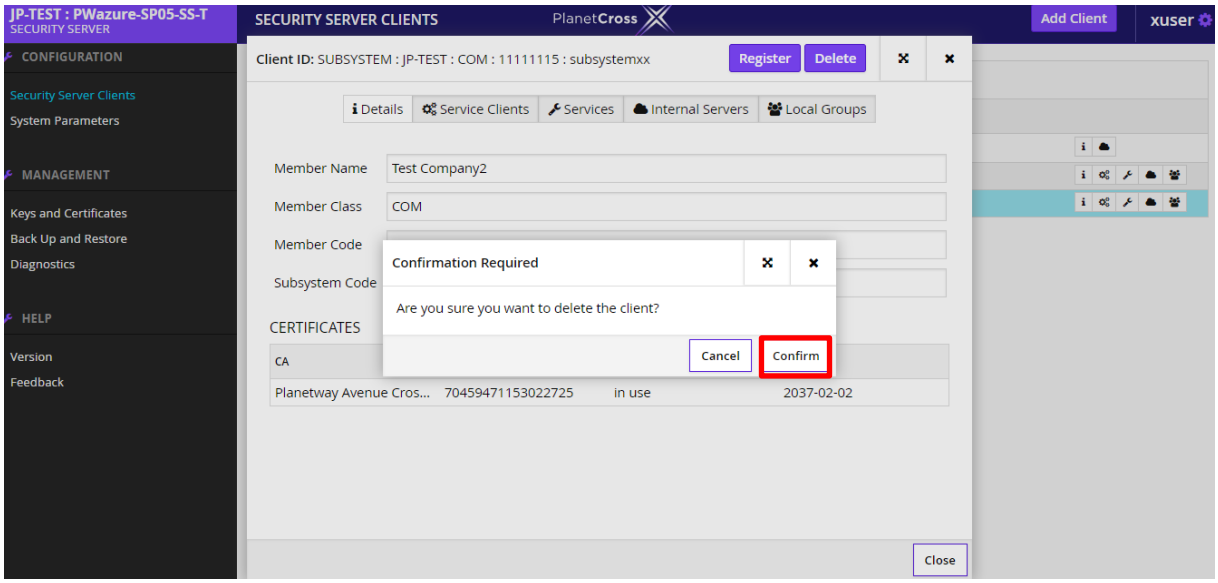
2. Security Server から削除したいクライアントをテーブルから選択し、その行の**[Details]**アイコンをクリックします。



3. 開いたウィンドウで、**[Delete]**をクリックします。



4. **[Confirm]**をクリックして削除を確認します。

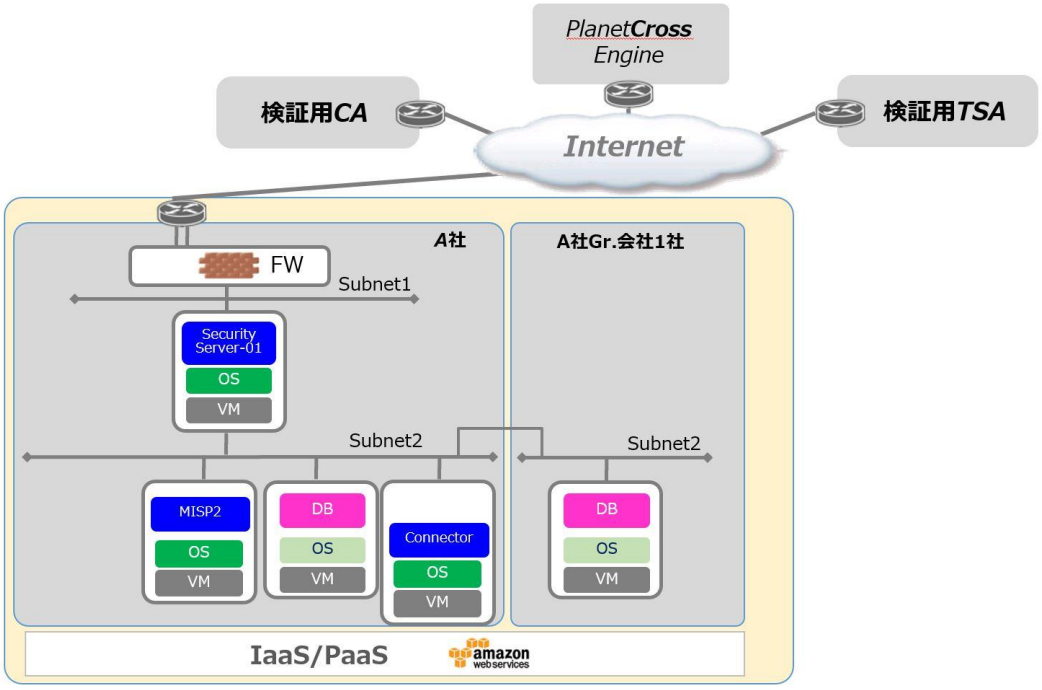


3.6 Security Server に複数のメンバーを登録する

Security Server に複数のメンバーを登録する場合に必要な手順を記載します。

3.6.1 複数社で1セットの Security Server を利用する場合

以下は、グループ本社およびグループ 5 社が AWS を利用しており、Security Server は 1 セットのみでグループ各社の DB 連携する場合の例です。



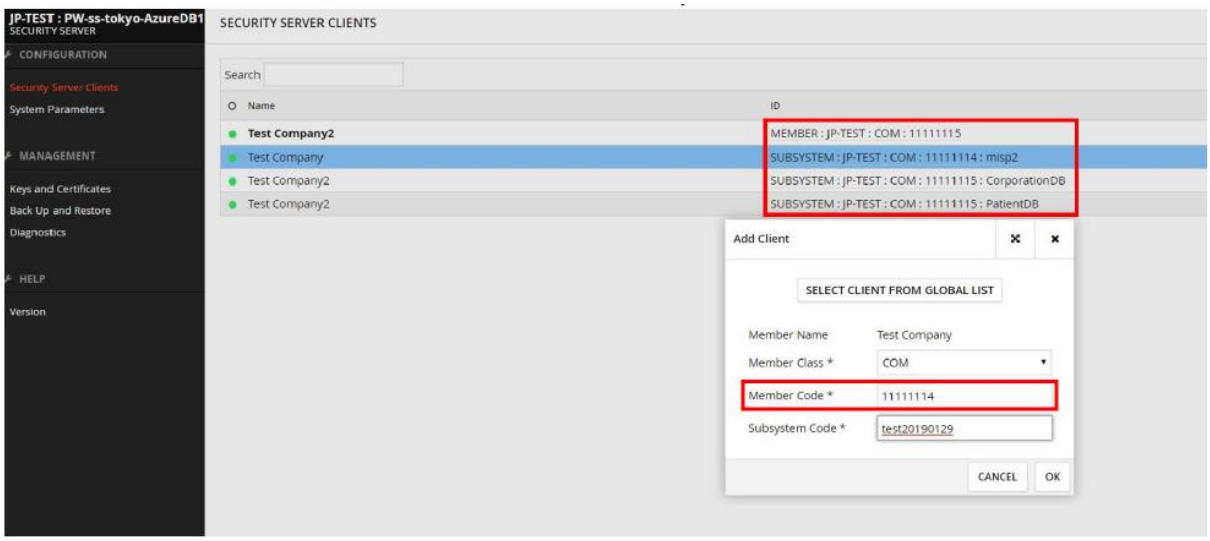
1. Member Code 登録を複数社分行います。

   PlanetCross Engine 側に登録をする依頼を実施します。

2. 各社分の Member Code で Subsystem Client を作成します。

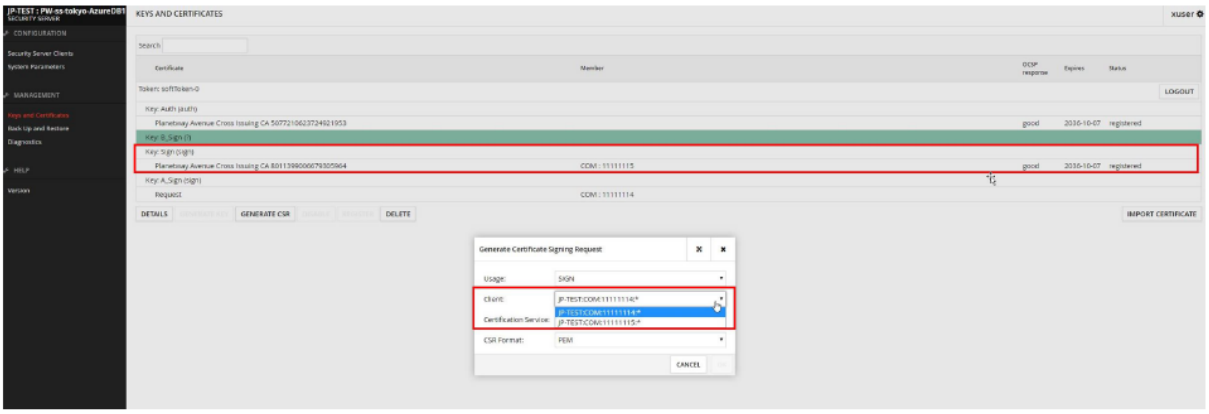
   (1) [Security Server Clients] > [Add client]を実行します。

(2) Security Server 自体の Member Code とは別の各社分の Member Code で Subsystem Client を作成します。



3. 各社分の Member Code の証明書をインポートします。

(1) [Keys and Certificates]で Sign key を作成します。
(2) [Generate CSR]で各社の Member Code を指定した CSR を作成します。



(3) CSR を基に作成された証明書をインポートして完了します。

4. セキュリティトークン、鍵、および証明書の管理

4.1 セキュリティトークン、鍵、および証明書の状態

オブジェクト(トークン、鍵または証明書)の可用性を表示するために、「Keys and Certificates」画面では次の背景色が使用されます。

背景色	状態
黄色	オブジェクトは Security Server で利用可能ですが、オブジェクトの情報は Security Server の設定に保存されていない状態です。 たとえば、スマートカードがサーバーに接続されてはいますが、スマートカードの証明書がサーバーにインポートされていない可能性があります。 黄色の背景にある証明書は、メッセージの仲介には使用できません。
白	オブジェクトは Security Server で利用可能であり、オブジェクトの情報は Security Server の設定に保存されています。 白い背景の証明書は、メッセージの仲介に使用できます。
グレー	オブジェクトは Security Server で利用できません。 グレーの背景にある証明書は、メッセージの仲介には使用できません。

【注記】
鍵デバイスおよび鍵の情報は次のいずれかの時点で自動的に設定に保存されます。
- 鍵デバイスおよび鍵に関連する証明書が Security Server にインポートされた場合
- 鍵の CSR が作成される場合

同様に、鍵デバイスおよび鍵の情報は、最後の関連する証明書または CSR が削除された後に、Security Server 設定から自動的に削除されます。

4.2 証明書の登録状態

登録状態は、証明書の PlanetCross システムにおける使用可否およびどのように使用できるかを示します。
「Keys and Certificates」画面では、「状態」列に証明書の登録状態(「削除済み」を除く)が表示されます。

4.2.1 署名用証明書の登録状態

Security Server の署名用証明書は、次の登録状態のいずれかになります。

登録状態	説明
登録済	証明書が Security Server にインポートされ、その設定に保存されました。 「登録済」状態の署名用証明書は、PlanetCross メッセージに署名するために使用できます。
削除済	サーバー設定から証明書が削除されました。 証明書が「削除済」状態であり、Security Server に接続されているハードウェアキーデバイスに格納されている場合、証明書は黄色い背景に表示されます。

4.2.2 認証用証明書の登録状態

Security Server の認証用証明書は、次の登録状態のいずれかになります。

登録状態	説明
保存済	証明書が Security Server にインポートされ、その設定に保存されたが、登録用に送信されていません。この状態から、証明書は次の状態に遷移します。 ・「登録中」: Security Server から Central Server に認証用証明書の登録リクエストが送信された場合。 ・「削除済」: Security Server 設定から認証用証明書の情報が削除された場合。
登録進行中	認証用証明書の登録リクエストが作成され、Central Server に送信されましたが、証明書と Security Server 間の関連付けはまだ承認されていません。この状態から、証明書は次の状態に遷移します。 ・「登録済み」: 認証用証明書と Security Server との間の関連付けが PlanetCross 監督機関によって承認された場合。 ・「削除中」: 証明書削除リクエストが Central Server に送信済みの場合。ユーザーは、認証用証明書の削除リクエストの送信が失敗した場合でも、この状態に強制的に遷移できます。
 登録済み	認証用証明書と Security Server の間の関連付けが Central Server で承認されています。この状態の認証用証明書を使用して、PlanetCross メッセージを交換するためのセキュアなデータ交換チャネルを確立することができます。この状態から、証明書は次の状態に遷移できます。 ・「グローバルエラー」: 認証用証明書と Security Server の間の関連付けが Central Server で取り消された場合。 ・「削除中」: 証明書の削除リクエストが Central Server に送信されている場合。ユーザーは、認証用証明書削除リクエストの送信が失敗しても、この状態に遷移することを強制することができます。
 グローバルエラー	認証用証明書と Security Server の間の関連付けが Central Server で取り消された場合。この状態から、証明書は次の状態に遷移できます。 ・「登録済」: 認証用証明書と Security Server の間の関連付けが Central Server に復元された場合(例えば、クライアントと Security Server の間の関連付けがエラーのために失われた場合)。 ・「削除済」: Security Server 設定から認証用証明書の情報が削除された場合。
 削除中	認証用証明書の登録リクエストが作成され、Central Server に送信されました。この状態から、証明書は次の状態に遷移できます。 ・「削除済」: Security Server 設定から認証用証明書の情報が削除された場合。
削除済	証明書が Security Server 設定から削除されました。

4.3 証明書の有効性状態

有効性状態は、証明書が PlanetCross システムから独立して使用できるか、またどのように使用できるかを示します。
Keys and Certificates 画面では、証明書の有効性状態を **OCSP** レスポンス欄に表示します。有効性状態(「無効」を除く)は「登録済」状態にある証明書の場合に表示します。

Security Server の証明書は、次のいずれかの有効性状態になります。

有効性状態	説明
不明 (有効情報がない)	証明書に有効な OCSP レスポンスがない(OCSP レスポンス有効期間は PlanetCross 監督機関によって設定される)または最後の OCSP レスポンスが "不明"(レスポンダがリクエストされた証明書について知らない)またはエラーだった場合。
中断	証明書に関する最後の OCSP レスポンスが「中断」されました。
有効	証明書に関する最後の OCSP レスポンスが「有効」でした。「有効」状態の証明書のみを使用して、メッセージに署名し、Security Server の間の接続を確立することができます。
期限切れ	証明書の有効終了日が過ぎました。証明書はアクティブではなく、この証明書についての OCSP クエリーは実行しません。
取消済	証明書に関する最後の OCSP レスポンスが "Revoked" でした。証明書はアクティブではなく、この証明書についての OCSP クエリーは実行しません。
無効	ユーザーは証明書を無効とマークしました。証明書はアクティブではなく、この証明書についての OCSP クエリーは実行しません。

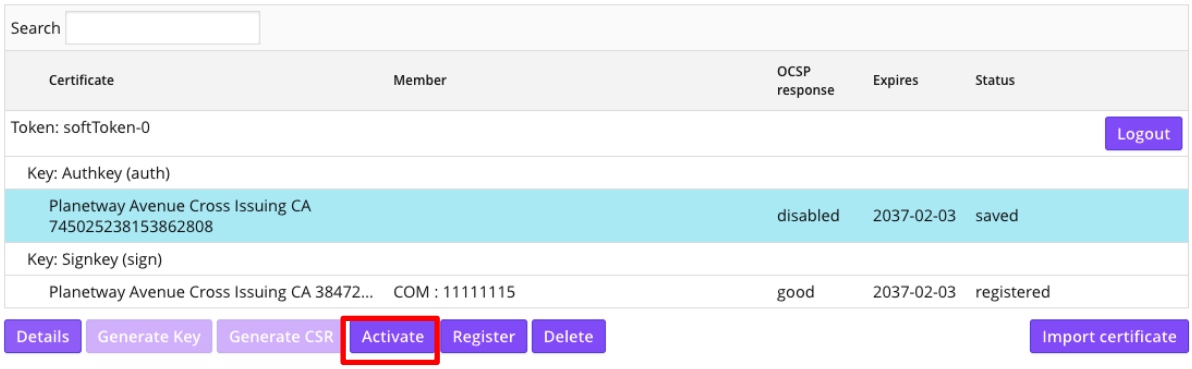
4.4 証明書の有効化と無効化

無効な証明書は、メッセージの署名や Security Server の間のセキュアなチャネルの確立(認証)には使用できません。証明書が無効になっている場合、「鍵と証明書」テーブルの「OCSP レスポンス」欄のステータスは「無効」です。

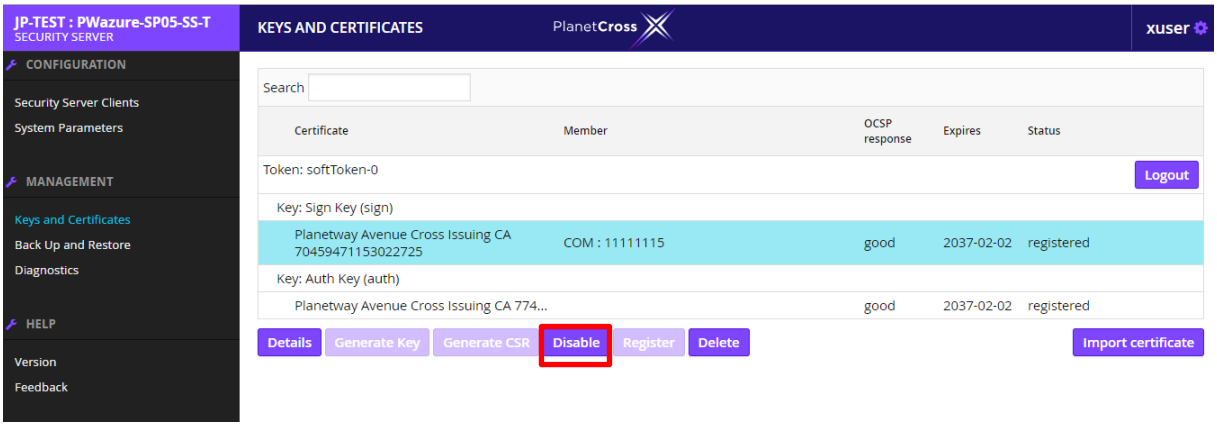
証明書を有効または無効にするには、次の手順を実行します。
＜アクセス権：認証用証明書の場合:セキュリティ担当者＞
＜アクセス権：署名用証明書の場合:セキュリティ担当者、登録担当者＞

1. **[Management]**メニューで、**[Keys and Certificates]**を選択します。

2. 証明書を有効にするためには、テーブルから無効の証明書を選択し、**[Activate]**をクリックします。



証明書を無効にするには、テーブルから有効な証明書を選択し、**[Disable]**をクリックします。



4.5 認証用鍵と証明書の設定と登録

Security Server は、複数の認証用鍵および証明書を持つことができます(例えば、認証用鍵の変更中の場合)。

別の認証用鍵と証明書の設定、認証用証明書の登録方法については、『Security Server インストールガイド』を参照してください。

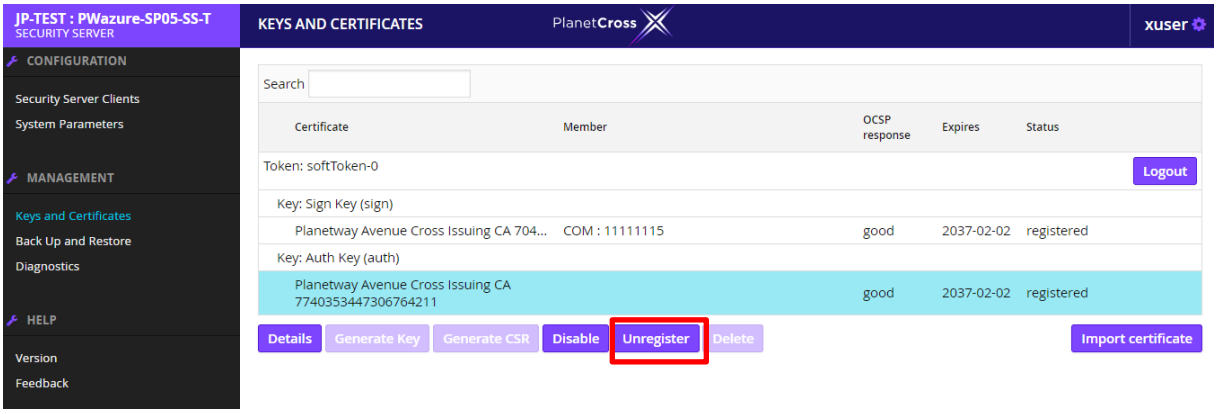
4.6 証明書の削除

PlanetCross 監督機関で「登録済み」または「登録中」状態にある認証用証明書は、削除する前に登録解除する必要があります。登録解除イベントは、Security Server から Central Server への認証用証明書の削除リクエストを送信します。

4.6.1 認証用証明書の登録を解除する

認証用証明書の登録を解除するには、次の手順を実行します。
＜アクセス権: セキュリティ担当者＞

1. **[Management]**メニューで、**[Keys and Certificates]**を選択します。
2. 「登録済み」または「登録中」の状態の認証用証明書を選択し、**[Unregister]**をクリックします。



その後、認証用証明書の削除リクエストが PlanetCross Central Server に自動的に送信され、Central Server ではそれを受け取ると、認証用証明書を削除します。
リクエストが正常に送信された場合、「リクエスト送信済」というメッセージが表示され、認証用証明書が「削除中」状態に移行します。

【注記】
登録された認証用証明書は、Security Server を介して削除リクエストを送信することなくても、Central Server から削除することができます。この場合、Security Server の管理者は、削除する認証用証明書に関する情報を含むリクエストを Central Server の管理者に送信する必要があります。Security Server からの削除リクエストなしで Central Server から認証用証明書が削除された場合、その証明書は Security Server で「グローバルエラー」状態で表示されます。

4.6.2 証明書または CSR 通知の削除

システム設定に保存している認証用証明書は、状態が「保存済み」、「グローバルエラー」または「削除中」であれば削除できます。署名用証明書および CSR 通知は、常にシステム設定から削除できます。

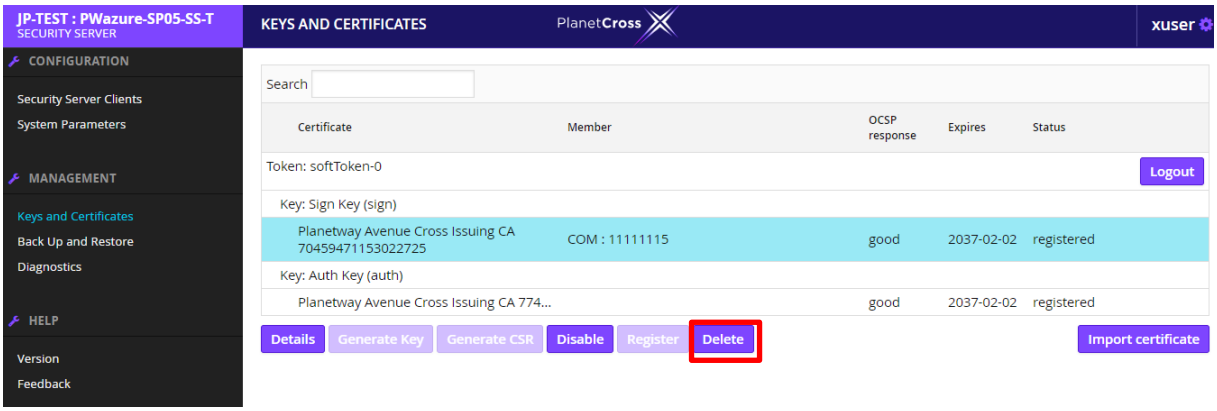
証明書がハードウェアセキュリティトークンに格納されている場合、削除は次の **2** つのレベルで動作します。

- 証明書がサーバー設定に保存されている場合、削除は証明書をサーバー設定から削除しますが、セキュリティトークンからは削除しません。
- 証明書がサーバー設定に保存されていない場合(証明書の背景が黄色の場合)、削除は証明書をセキュリティトークンから削除します(トークンがこの動作をサポートしていることが前提)。

証明書または **CSR** 通知を削除するためには、次の手順を実行します。
＜アクセス権：認証用証明書の場合: セキュリティ担当者＞
＜アクセス権：署名用証明書の場合: セキュリティ担当者、登録担当者＞

1. **[Management]**メニューで、**[Keys and Certificates]**を選択します。

2. テーブルから証明書または CSR 通知を選択し、**[Delete]**をクリックします。



3. **[Confirm]**をクリックして、削除を確認します。

4.7 鍵を削除する

警告	サーバー設定から鍵を削除すると、その鍵に関連付けているすべての証明書(および CSR 通知)も削除されます。

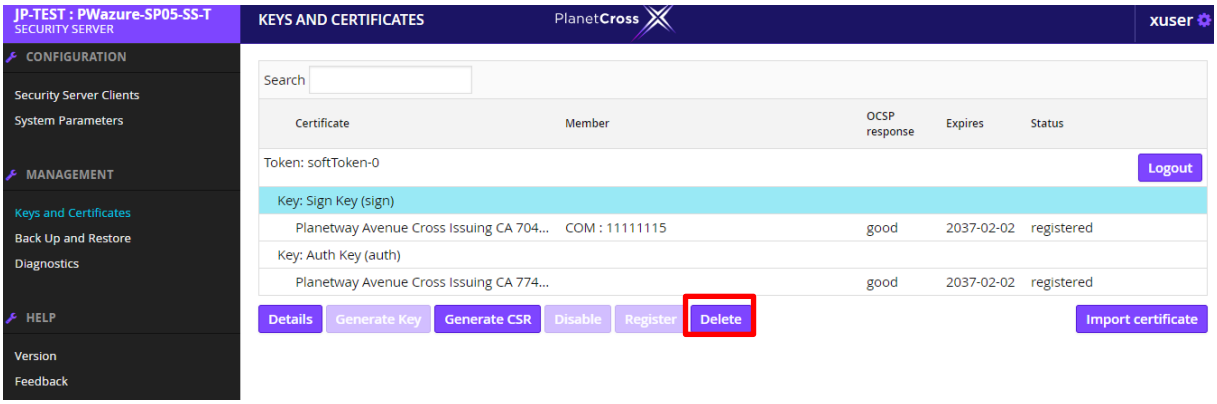
鍵の削除は次の **2** つのレベルで動作します。

- 鍵がサーバー設定に保存されている場合、削除はサーバー設定から鍵を削除(および関連する証明書)しますが、セキュリティトークンからは削除しません。
- 鍵がサーバー設定に保存していない場合(鍵の背景が黄色の場合)、削除はセキュリティトークンから鍵を削除します(トークンがこの動作をサポートしていることを前提)。

鍵を削除するためには、次の手順を実行します。
＜アクセス権：認証用鍵の場合: セキュリティ担当者＞
＜アクセス権：署名用鍵の場合: セキュリティ担当者、登録担当者＞
＜アクセス権：役割を持たない鍵の場合: セキュリティ担当者、登録担当者＞

1. **[Management]**メニューで、**[Keys and Certificates]**を選択します。

2. 鍵を選択し、**[Delete]**をクリックします。



3. **[Confirm]**をクリックし、鍵(および関連する証明書)の削除を確認します。

5. サービス設定

5.1 PlanetCross サービス

サービスは 2 つのレベルで管理されます。

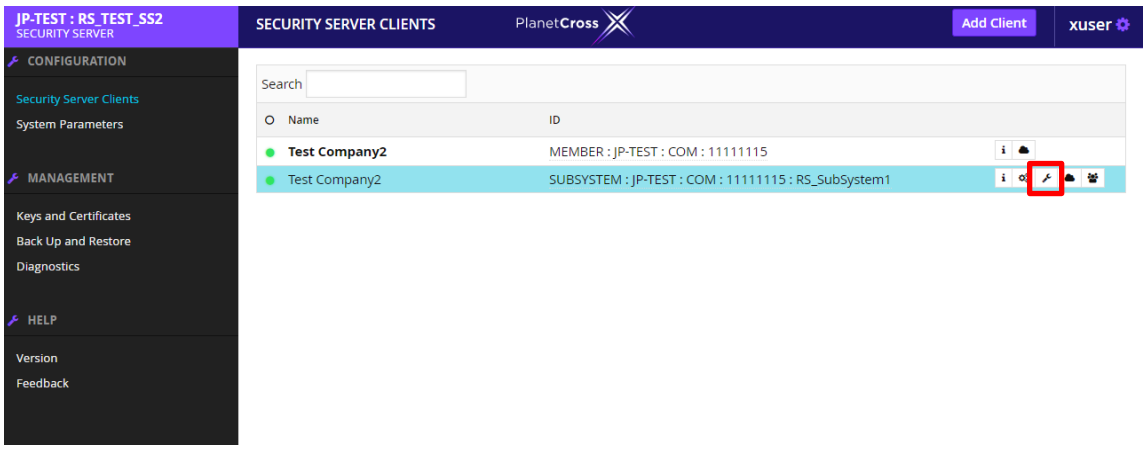
- サービスの追加、削除、および無効化は WSDL レベルで実行します。
- サービスアドレス、内部ネットワーク接続方法、およびサービスタイムアウト値は、サービスレベルで設定されます。ただし、一つのサービスの設定を同じ WSDL 内の他のすべてのサービスに簡単に拡張できます。

5.2 WSDL の追加

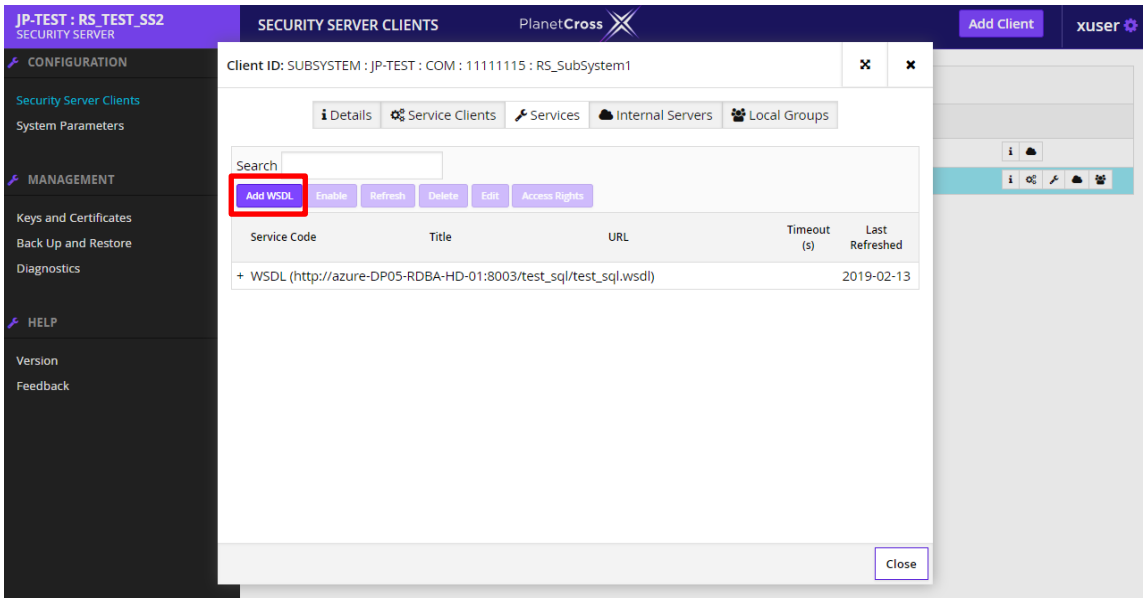
新しい WSDL ファイルが追加されると、Security Server はそこからサービス情報を読み取り、その情報をサービス一覧に表示します。サービスコード、タイトル、アドレスは WSDL から読み込まれます。

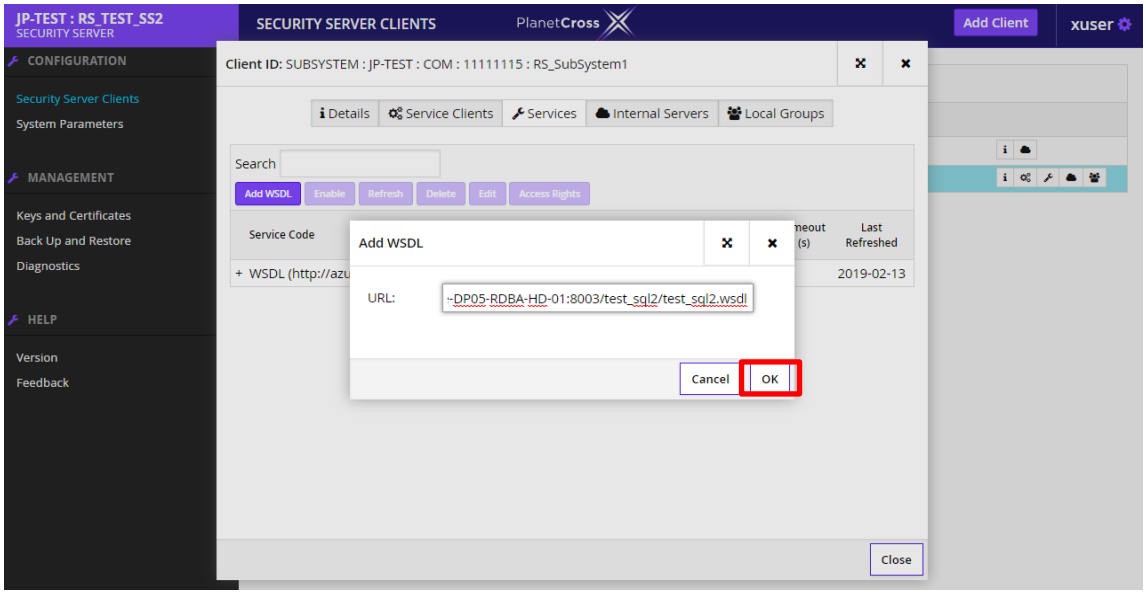
WSDL を追加するためには、次の手順を実行します。＜アクセス権: サービス管理者＞

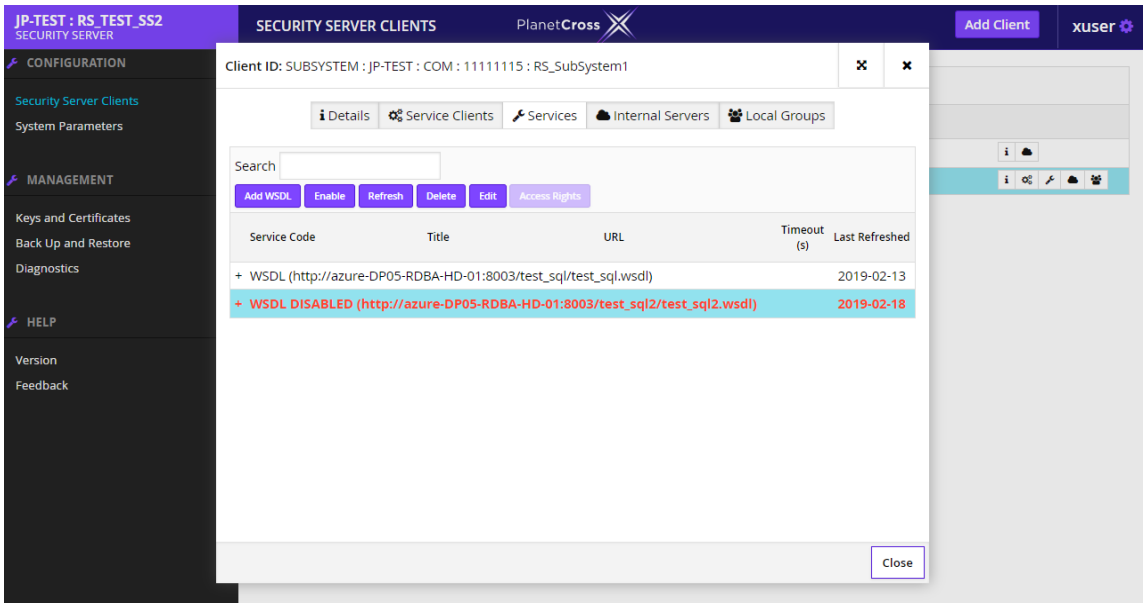
1. [Configuration]メニューで[Security Server Clients]を選択し、テーブルからクライアントを選択し、その行の[Services]アイコンをクリックします。



2. [Add WSDL]をクリックし、表示されたウィンドウに WSDL アドレスを入力して、[OK]をクリックします。
WSDL とそれに含まれるサービスに関する情報が一覧に追加されます。デフォルトでは、WSDL は無効状態で追加されます。







WSDL に含まれるサービスの一覧を表示するには、次の手順を実行します。

- WSDL 行の前にある + 記号をクリックして、リストを展開します。

5.3 WSDL の更新

更新後、Security Server は WSDL ファイルを WSDL アドレスから Security Server に再読み込みし、再読み込みされたファイルのサービス情報を既存のサービスと照合してチェックします。新しい WSDL のサービスの構成に現在のバージョンと比較して変更があれば、警告が表示され、更新を続けるかキャンセルするかを選択します。

WSDL を更新するには、次の手順を実行します。＜アクセス権: サービス管理者＞

1. [Configuration]メニューで[Security Server Clients]を選択し、一覧からクライアントを選択し、その行の[Services]アイコンをクリックします。

2. 更新したい WSDL を一覧から選択し、[Refresh]をクリックします。
   新しい WSDL に Security Server の現行の WSDL と比較して変更がある場合、警告が表示されます。

3. 警告が表示された場合、更新を続行するには、[Continue]をクリックします。

WSDL が更新される際、既存のサービスの設定は上書きされません。

5.4 WSDL の有効化と無効化

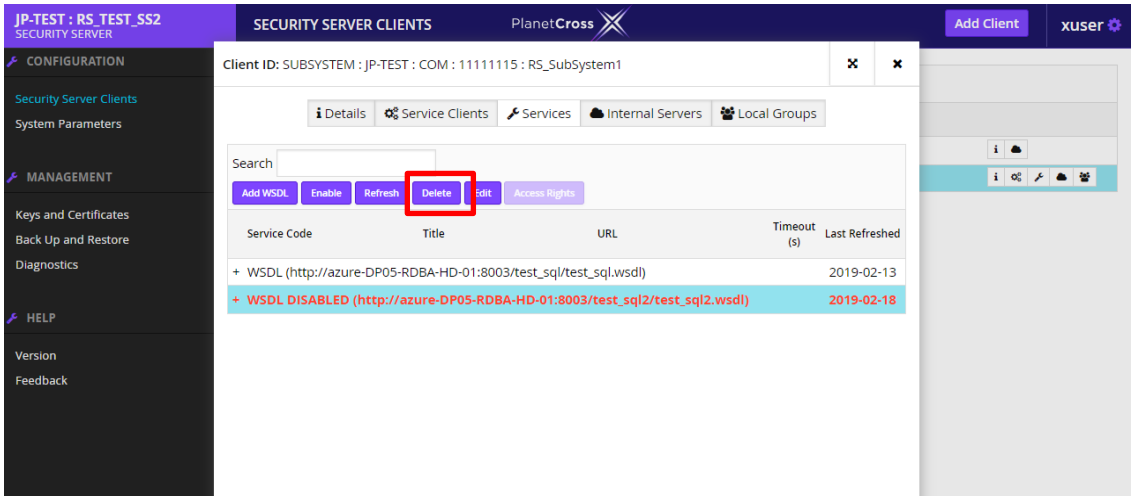
無効な WSDL はサービス一覧に赤で表示され、「Disabled」の注記が表示されます。

無効な WSDL で記述されたサービスはサービスクライアントからアクセスできません。そのようなサービスにアクセスしようとすると、Security Server の管理者が WSDL を無効化した時に入力した情報を含むエラーメッセージが返信されます。

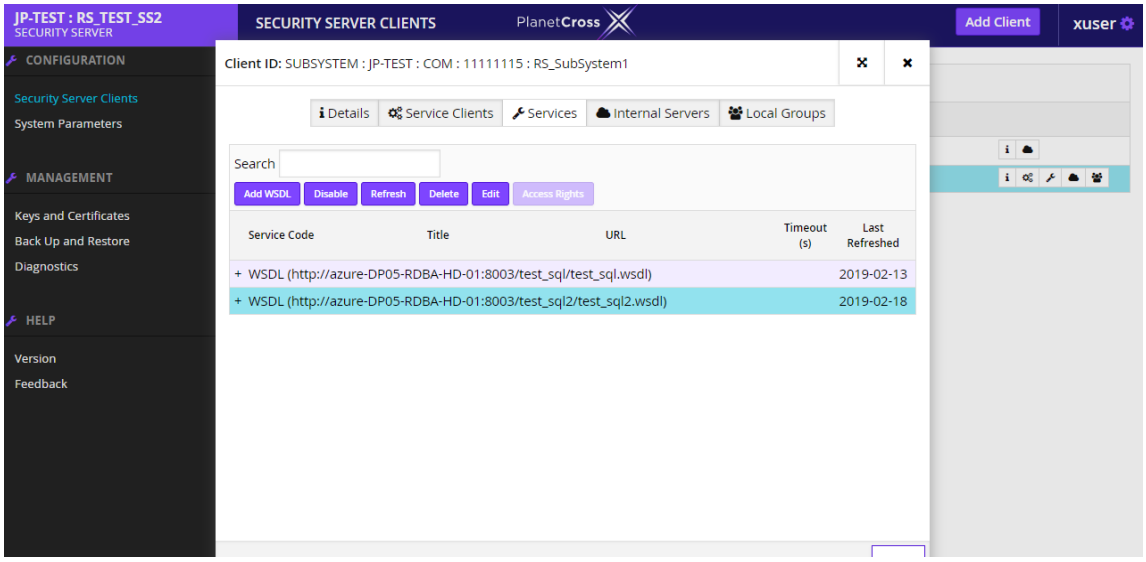
WSDL が有効化されると、そこに記述されているサービスにはユーザーがアクセスできるようになります。したがって、WSDL を有効にする前に、すべてのサービスのパラメーターが正しく設定されているかを確認する必要があります。

WSDL を有効化するためには、次の手順を実行します。＜アクセス権: サービス管理者＞

1. [Configuration]メニューで[Security Server Clients]を選択し、一覧からクライアントを選択し、その行の[Services]アイコンをクリックします。
2. 一覧から無効な WSDL を選択し、[Enable]をクリックします。



ボタンを押した後、黒文字となり、有効となります。



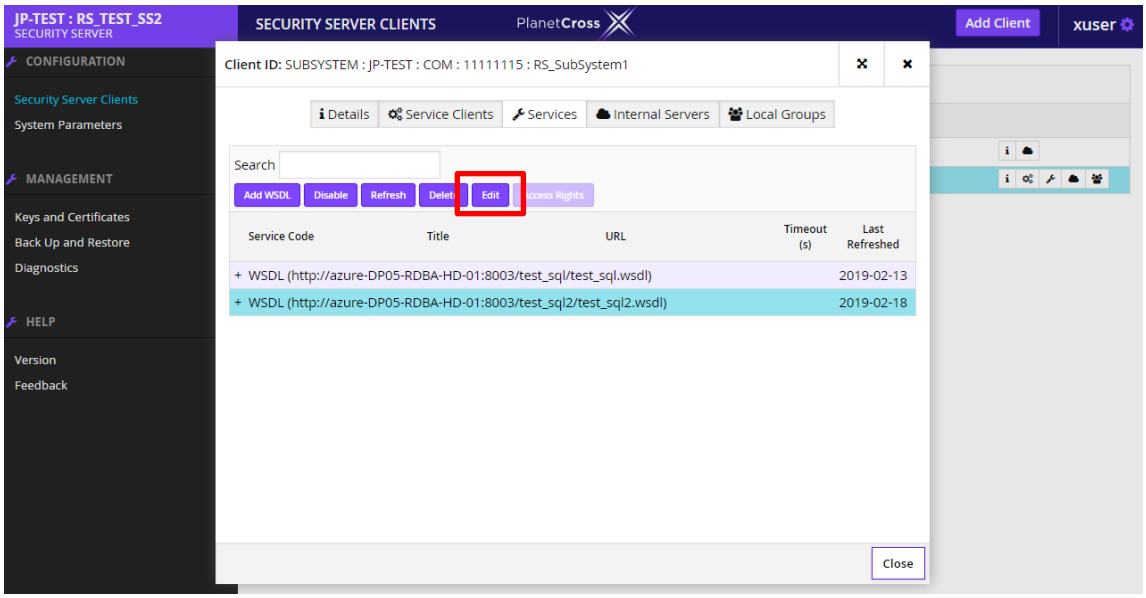
WSDL を無効化するためには、以下の手順を実行します。

1. [Configuration]メニューで[Security Server Clients]を選択し、一覧からクライアントを選択し、その行の[Services]アイコンをクリックします。
2. WSDL を無効化するためには、一覧から有効な WSDL を選択し、[Disable]をクリックします。
3. 表示されたウィンドウで、エラーメッセージを入力します。
   エラーメッセージは、WSDL のサービスにアクセスしようとするクライアントに表示されます。
4. 最後に[OK]をクリックします。

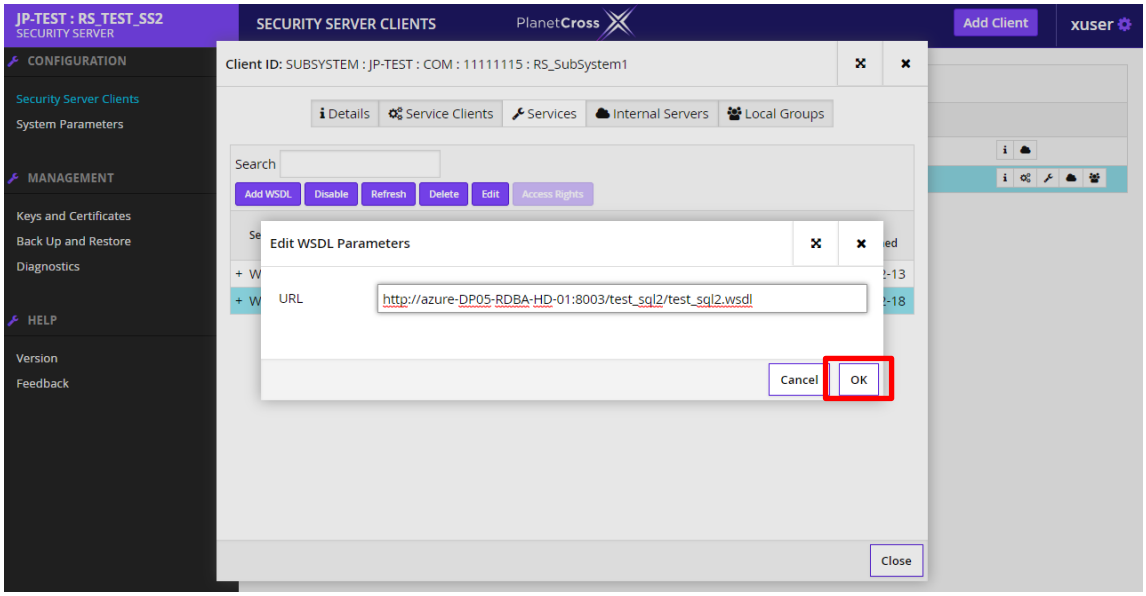
5.5 WSDL のアドレスの変更

WSDL アドレスを変更するためには、次の手順を実行します。<アクセス権: サービス管理者>

1. [Configuration]メニューで[Security Server Clients]を選択し、一覧からクライアントを選択し、その行の[Services]アイコンをクリックします。
2. 一覧から、アドレスを変更したい WSDL を選択し、[Edit]をクリックします。



3. 表示されたウィンドウで、WSDL アドレスを編集して[OK]をクリックします。
アドレスを変更すると、WSDL が更新されます。

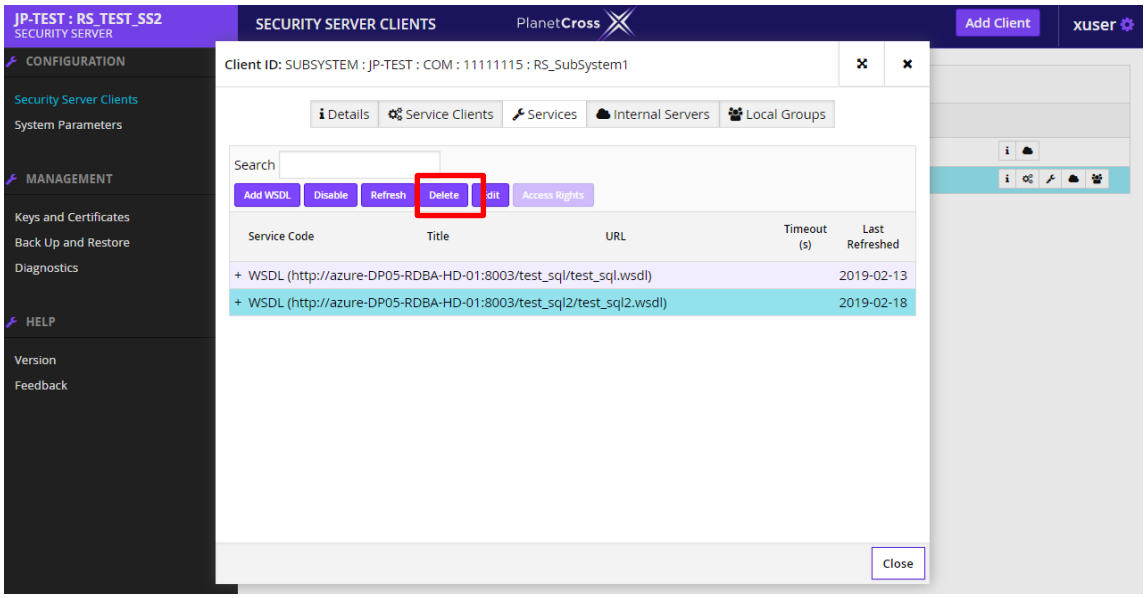


5.6 WSDL の削除

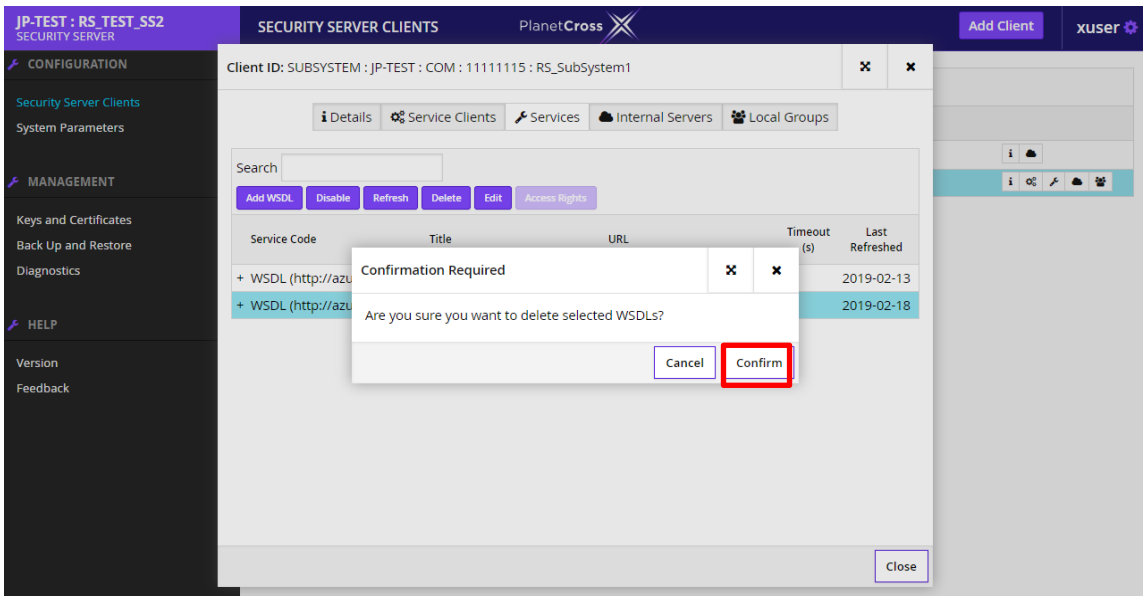
WSDL が削除されると、アクセス権を含めて WSDL に記述されているサービスに関連するすべての情報が削除されます。

WSDL を削除するには、次の手順を実行します。<アクセス権: サービス管理者>

1. [Configuration]メニューで[Security Server Clients]を選択し、一覧からクライアントを選択し、その行の[Services]アイコンをクリックします。
2. 削除したい WSDL を一覧から選択し、[Delete]をクリックします。



3. 表示されたウィンドウで[Confirm]をクリックして削除を確認します。



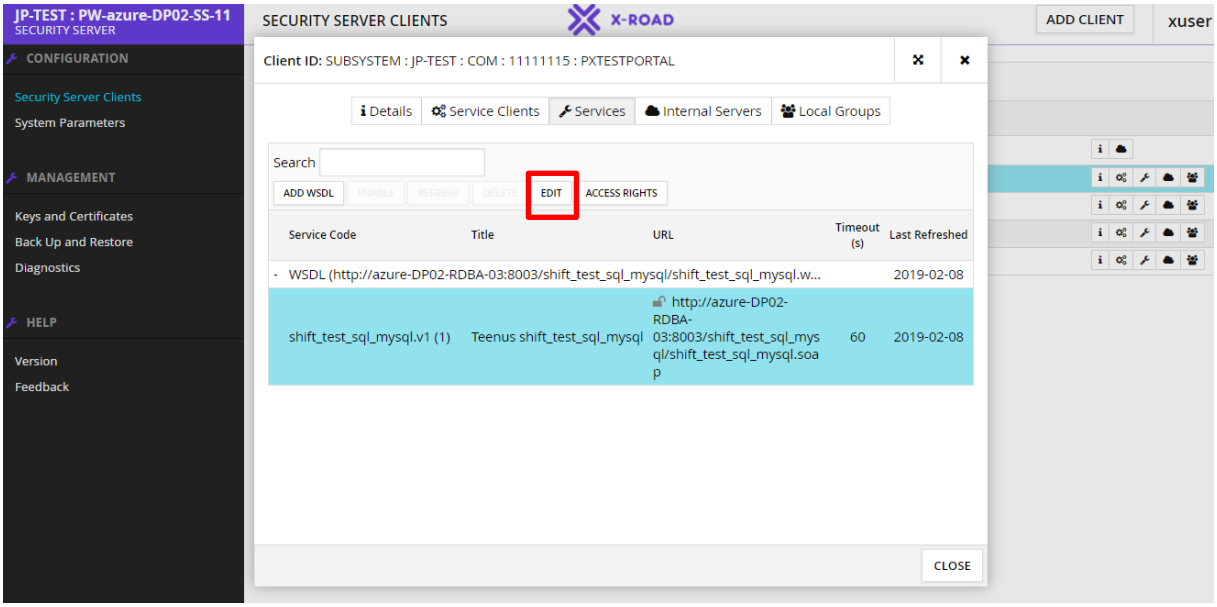
5.7 サービスパラメーターの変更

サービスパラメーターには以下の項目があります。

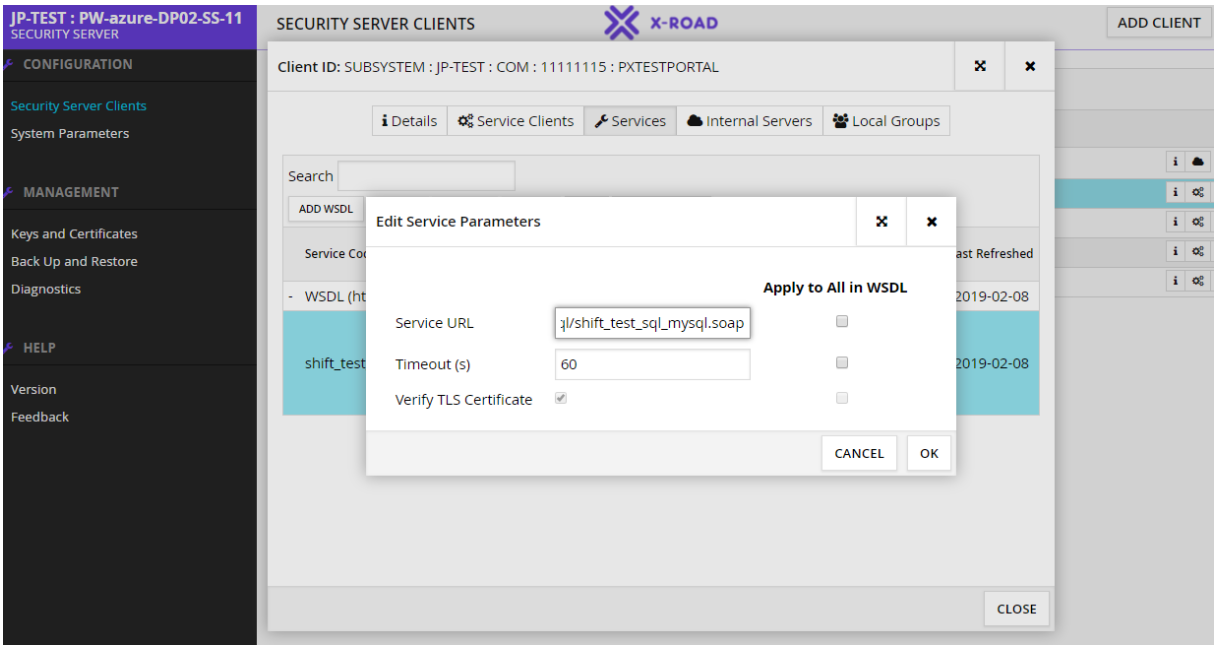
- **サービス URL** - サービスを対象とするリクエストを送信する URL
- **タイムアウト** - データベースへのリクエストの最長時間(秒単位)
- **TLS 証明書の確認** - TLS 接続が確立された時に、証明書の検証の有無をトグルする

サービスパラメーターを変更するには、次の手順を実行します。
＜アクセス権: サービス管理者＞

1. [Configuration]メニューで[Security Server Clients]を選択し、一覧からクライアントを選択し、その行の[Services]アイコンをクリックします。
2. 一覧からサービスを選択し、[Edit]をクリックします。



3. 表示されたウィンドウで、サービスパラメーターを設定します。
選択したパラメーターを同じ WSDL に記述されているすべてのサービスに適用するためには、[Apply to All in WSDL]欄で、このパラメーターの横にあるチェックボックスを選択します。



4. [OK]をクリックします。
設定したパラメーターが適用されます。

6. アクセス権の管理

アクセス権は、以下のアクセス権の対象に付与することができます。

- **PlanetCross メンバーのサブシステム**
- **グローバルアクセス権グループ** - グローバルグループは、PlanetCross 監督機関で作成されます。グループにアクセス権が付与されている場合は、そのすべてのグループメンバーにも適用されます。
- **ローカルアクセス権グループ** - アクセス管理を簡素化するために、Security Server の各クライアントはローカルアクセス権グループを作成できます。グループにアクセス権が付与されている場合は、そのすべてのグループメンバーにも適用されます。

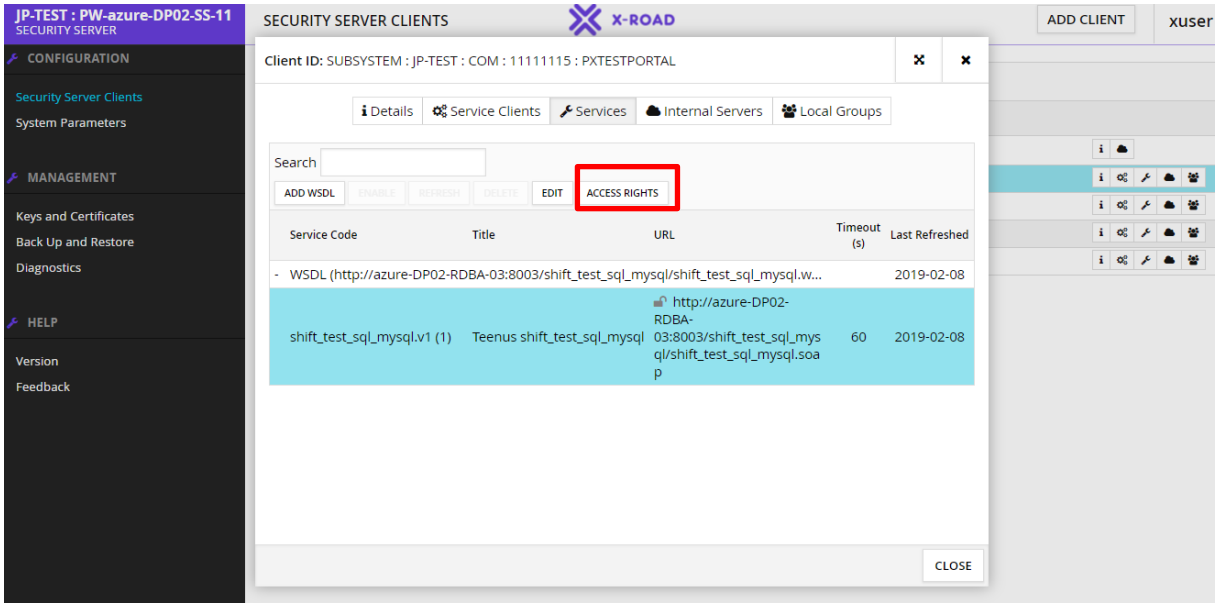
Security Server のアクセス権を管理するには、2 つのオプションがあります。

- **サービスベースアクセス権管理** - 複数のサービスクライアントに対して単一のサービスを公開/非公開する必要がある場合。
- **サービスクライアントベースアクセス権管理** - 単一のクライアントが複数のサービスを公開/非公開する必要がある場合。

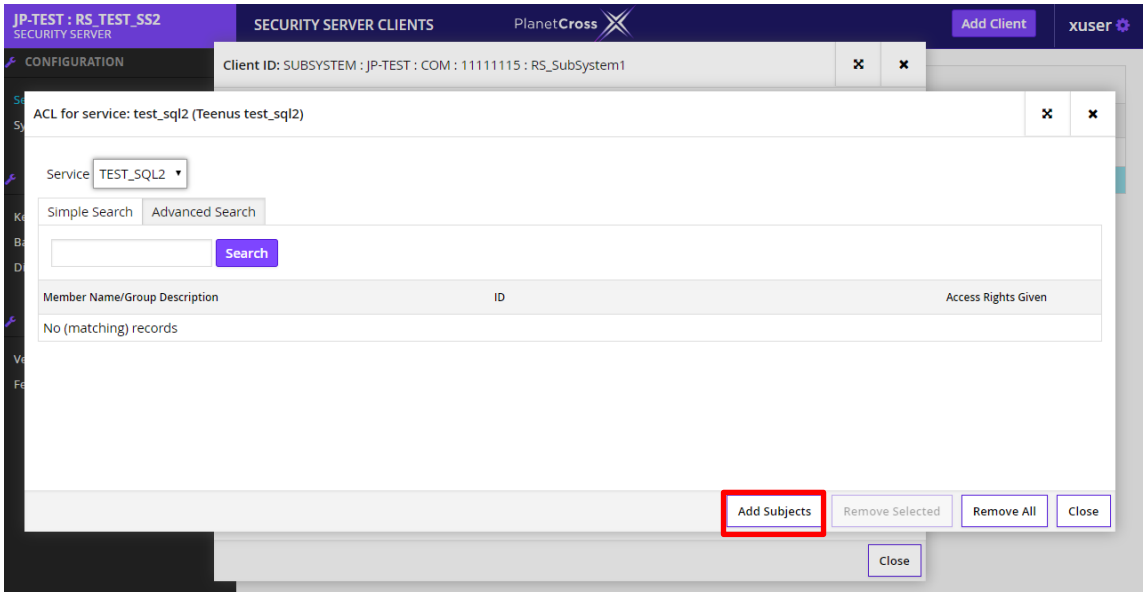
6.1 サービスのアクセス権の変更

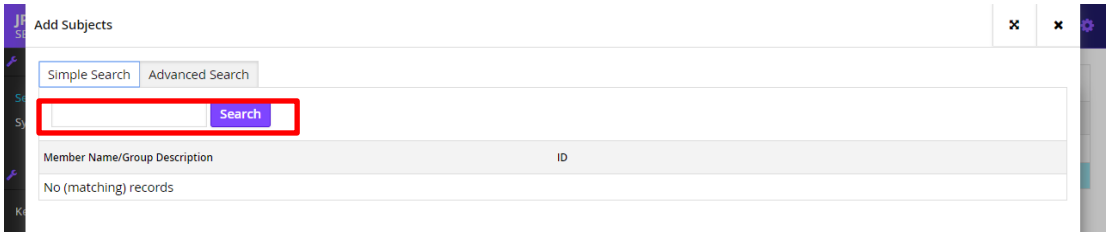
サービスのアクセス権を変更するためには、次の手順を実行します。
＜アクセス権: サービス管理者＞

1. [Configuration]メニューで[Security Server Clients]を選択し、一覧からクライアントを選択し、その行の[Services]アイコンをクリックします。
2. 一覧からサービスを選択し、[Access Rights]をクリックします。
表示されたウィンドウで、アクセス権一覧には、選択したサービスにアクセスできるすべての PlanetCross サブシステムおよびグループに関する情報が表示されます。

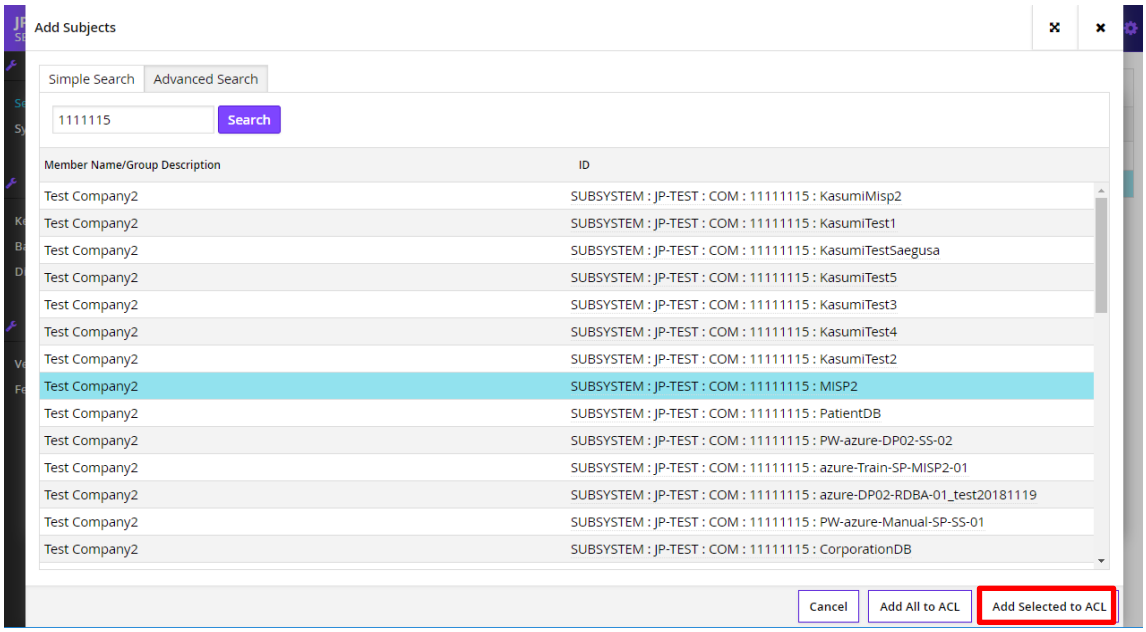


3. サブジェクト(PlanetCross サブシステムまたはグループ)にサービスのアクセス権を追加するためには、[Add Subject]をクリックします。
サブジェクト検索ウィンドウが表示されます。PlanetCross の監督機関に登録されているすべてのサブシステムとグローバルグループ、および Security Server クライアントのローカルグループの中から検索できます。

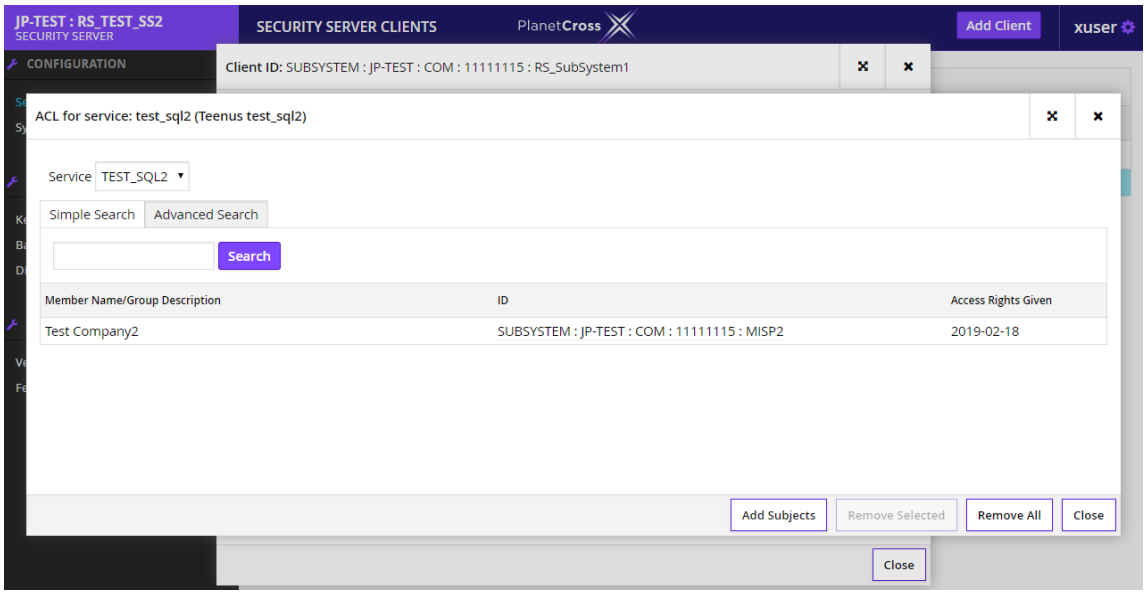




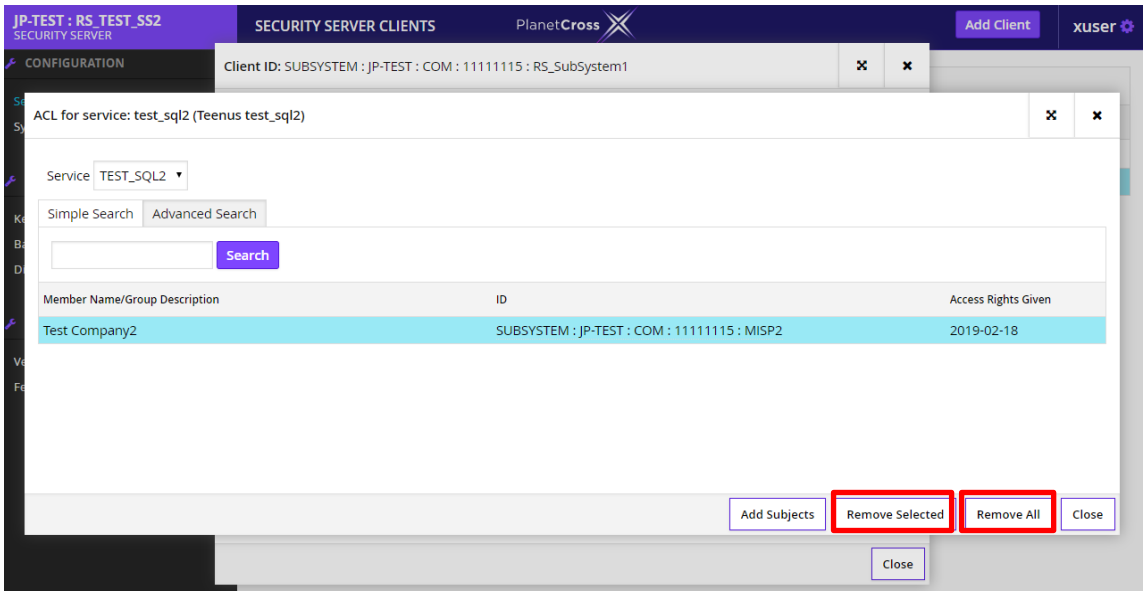
一覧から 1 つまたは複数のサブジェクトを選択し、[Add Selected to ACL**]をクリックします。検索結果のすべてのサブジェクトにアクセス権を付与するには、[Add All to ACL*]をクリックします。



ボタンを押した後、アクセス権のあるサブジェクトを確認できます。



4. アクセス権のサブジェクトを削除するには、アクセス権一覧の対応する行を選択して、[Remove Selected]をクリックします。
アクセス権リストをクリアする(つまり、すべてのサブジェクトを削除する)ためには、[Remove All]をクリックします。

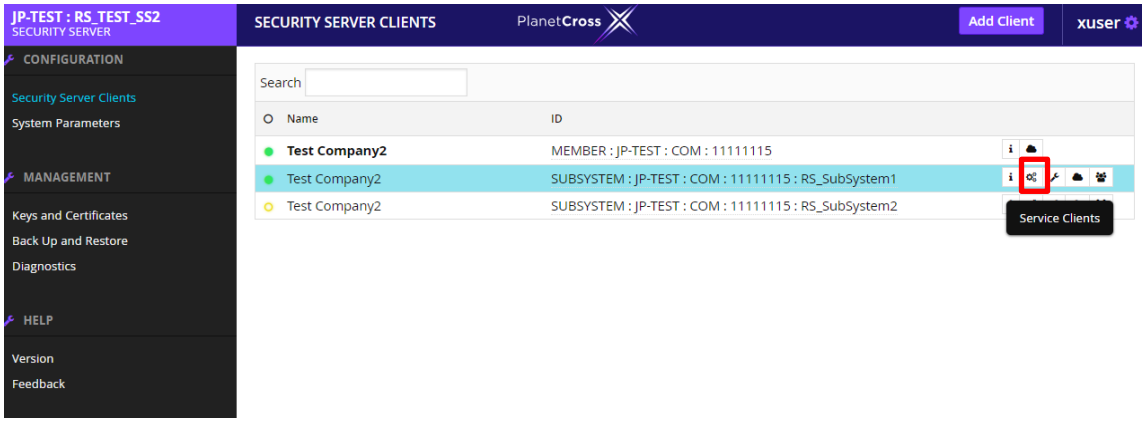


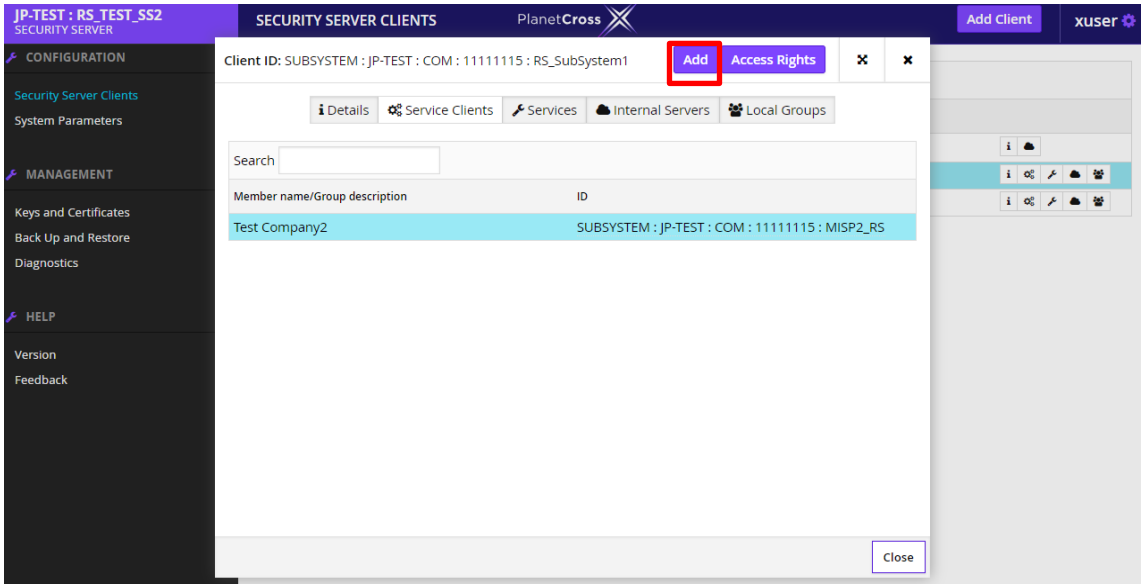
6.2 サービスクライアントの追加

サービスクライアント画面(Configuration -> Security Server Clients -> Service Clients)は、この Security Server クライアントによって媒介されるサービスのすべてのアクセス権サブジェクトを表示します。つまり、PlanetCross サブシステムまたはグループにこのクライアントのサービスへのアクセス権が付与されている場合、この画面にサブジェクトが表示されます。

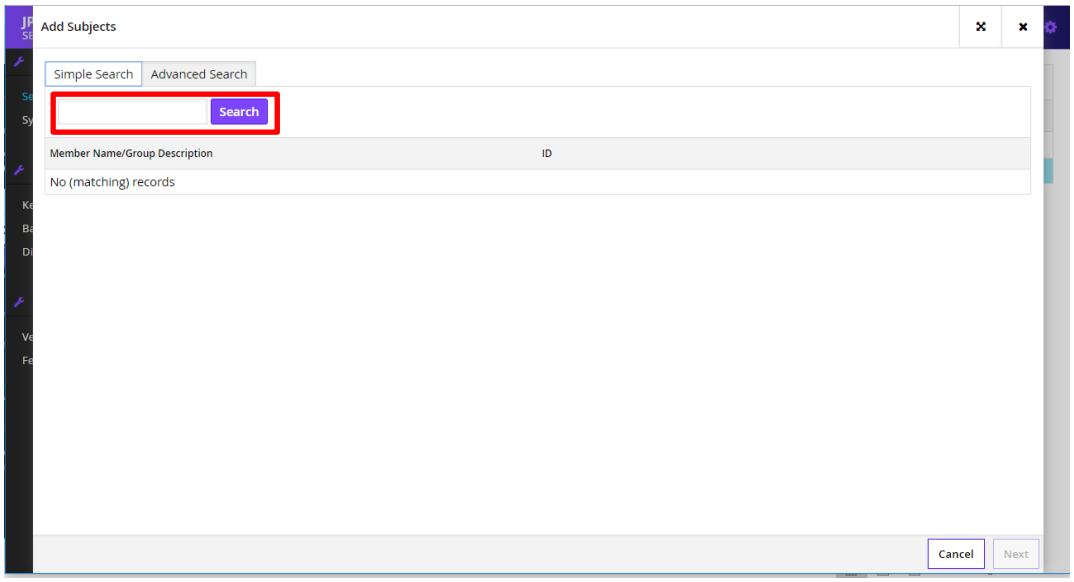
サービスクライアントを追加するには、次の手順を実行します。
＜アクセス権: サービス管理者＞

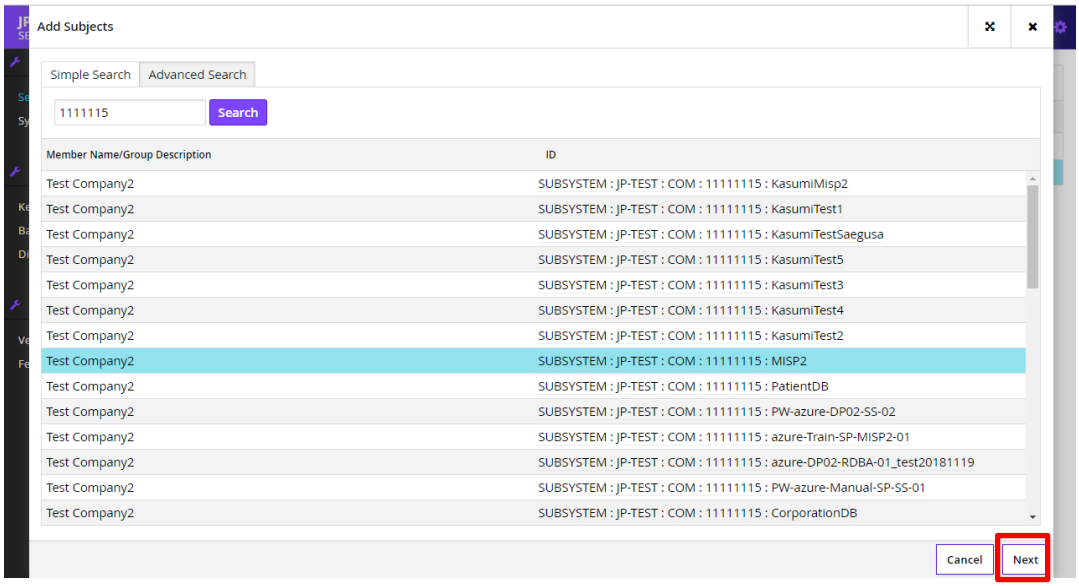
1. [Configuration]メニューで、[Security Server Clients]を選択します。
2. 一覧からクライアントを選択し、[Service Clients]アイコンをクリックし、次に、[Add]をクリックします。



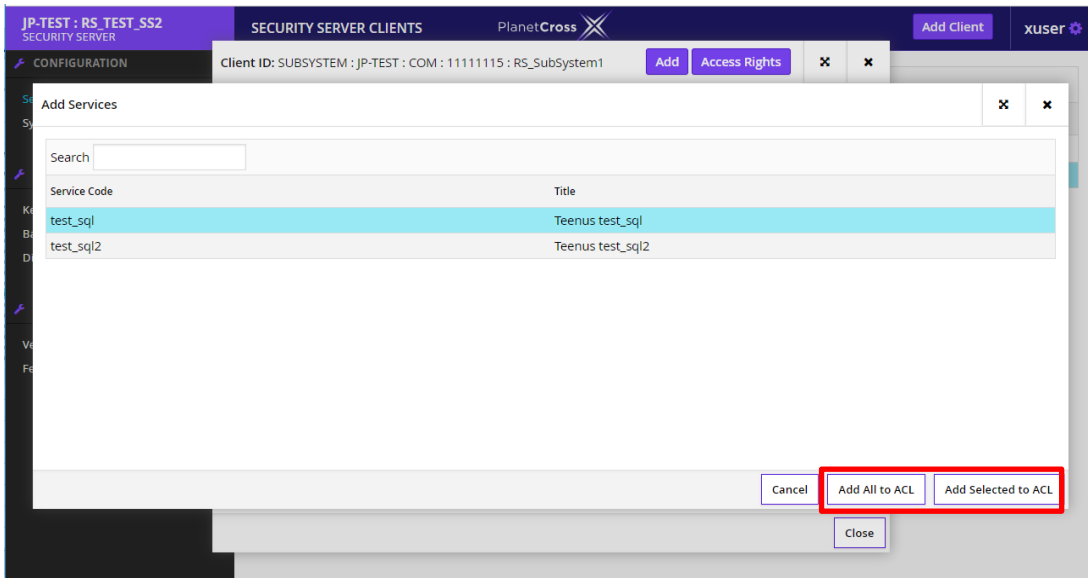


3. 表示されたウィンドウで、アクセス権を付与したいサブジェクト(サブシステム、ローカルまたはグローバルグループ)を見つけて選択し、[Next]をクリックします。

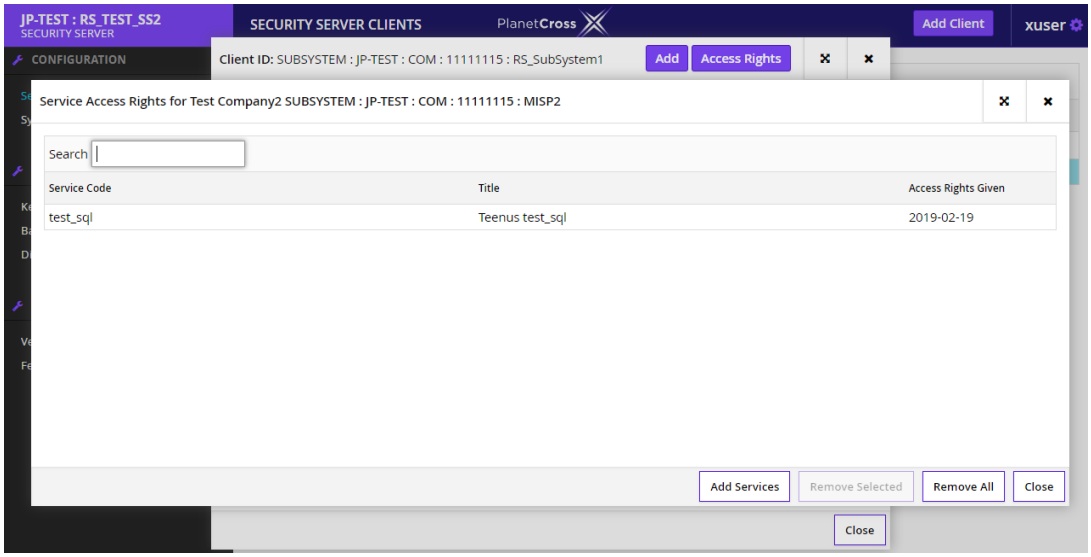




4. 選択したサブジェクトにアクセス権を付与したいサービスを探します。
5. [Add Selected to ACL]をクリックして、選択したサービスへのアクセス権をこのサブジェクトに付与します。または、[Add All to ACL]をクリックして、フィルタ内のすべてのサービスに対するアクセス権をサブジェクトに付与します。



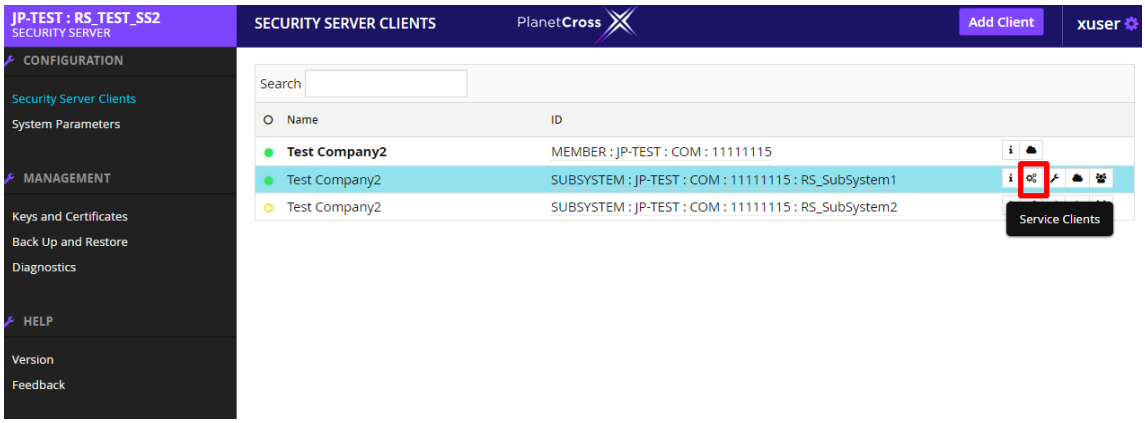
サブジェクトがサービスクライアントのリストに追加した後に、アクセス権を変更できるクライアントアクセス権ビューが表示されます。



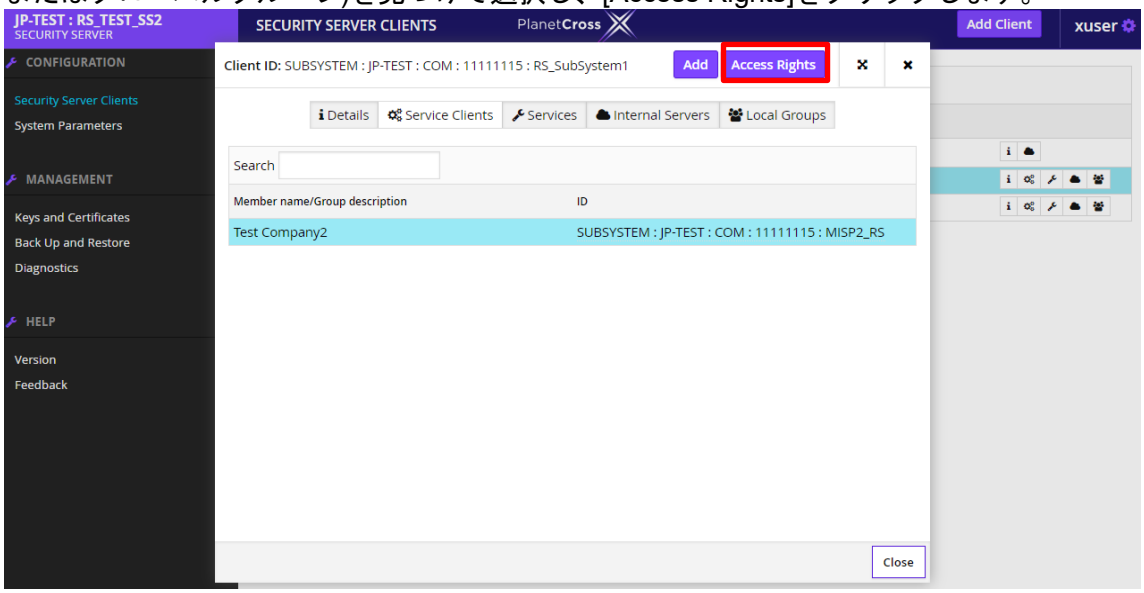
6.3 サービスクライアントのアクセス権の変更

サービスクライアントのアクセス権を変更するためには、次の手順を実行します。
＜アクセス権: サービス管理者＞

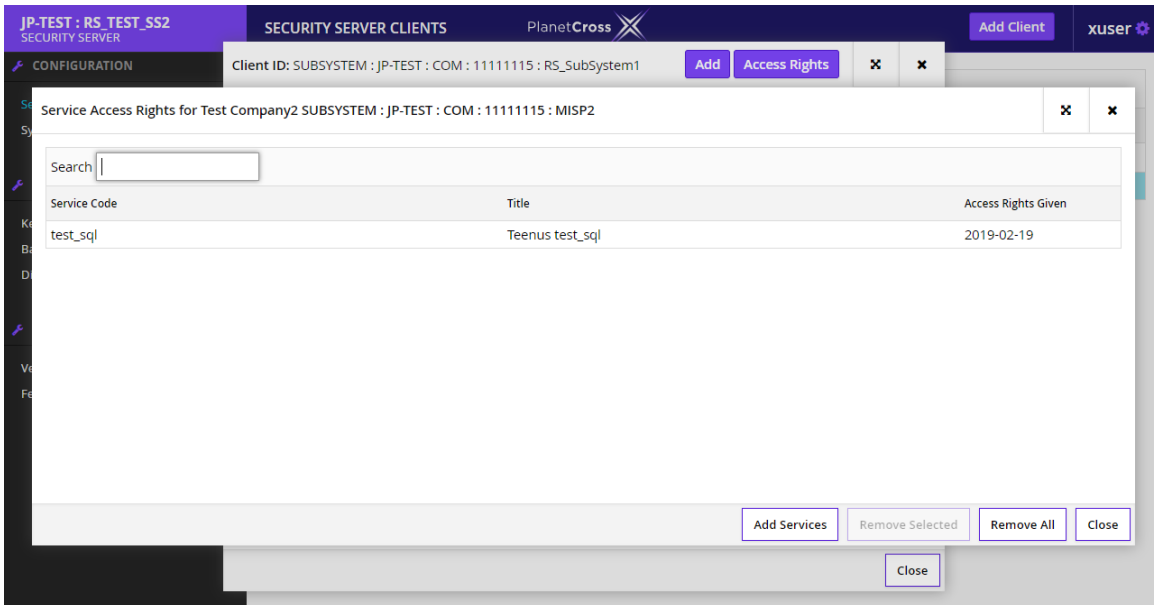
1. [Configuration]メニューで[Security Server Clients]を選択し、一覧からクライアントを選択し、その行の[Service Clients]アイコンをクリックします。



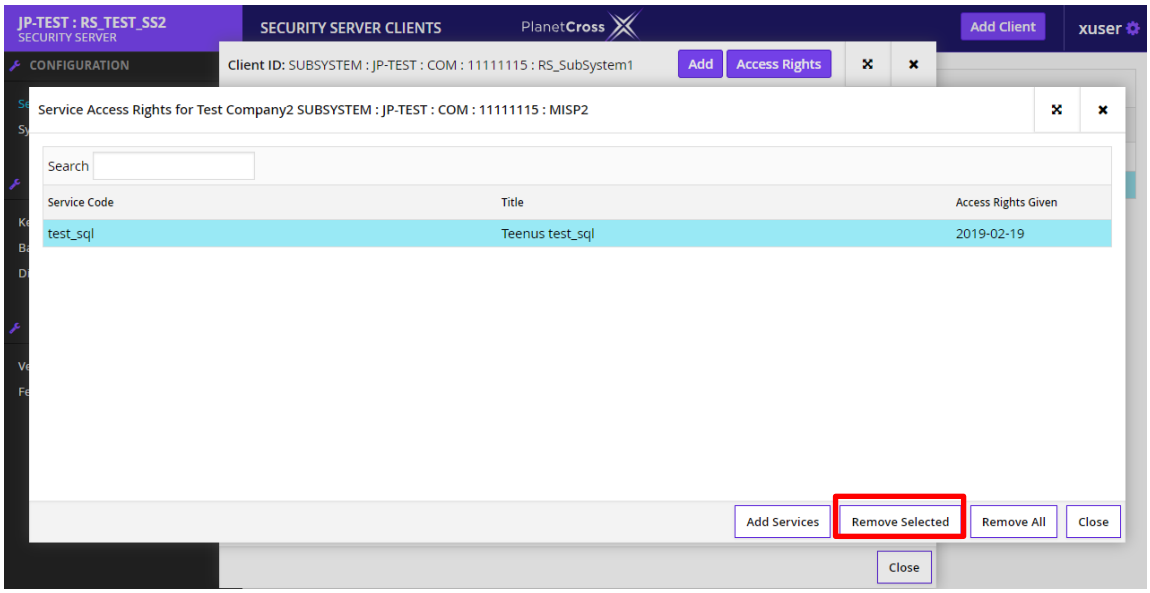
2. 表示されたウィンドウで、アクセス権を変更したいサブジェクト(サブシステム、ローカルまたはグローバルグループ)を見つけて選択し、[Access Rights]をクリックします。

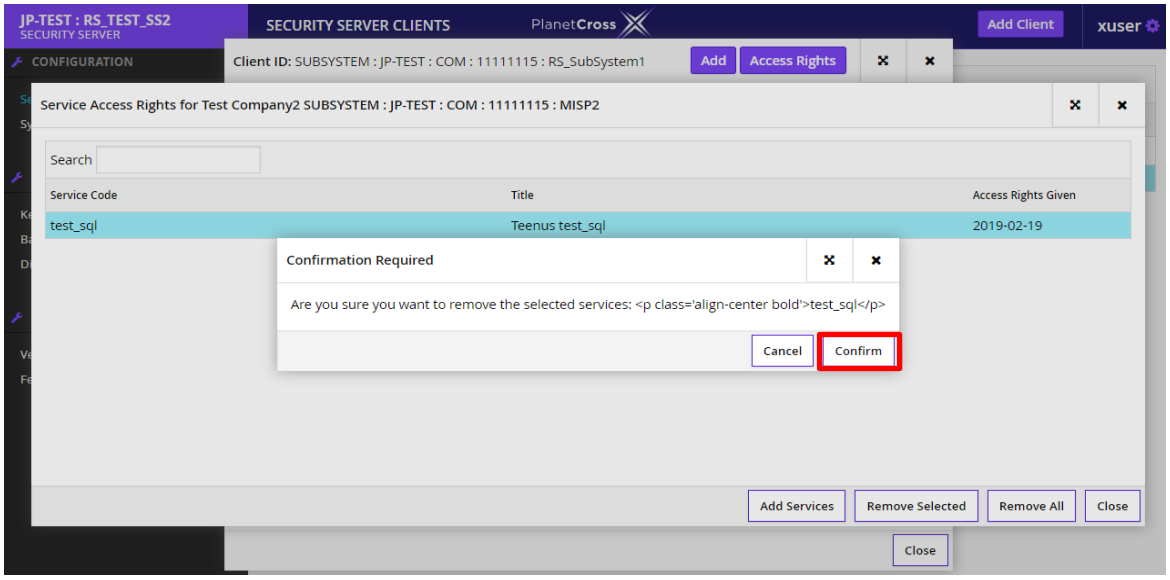


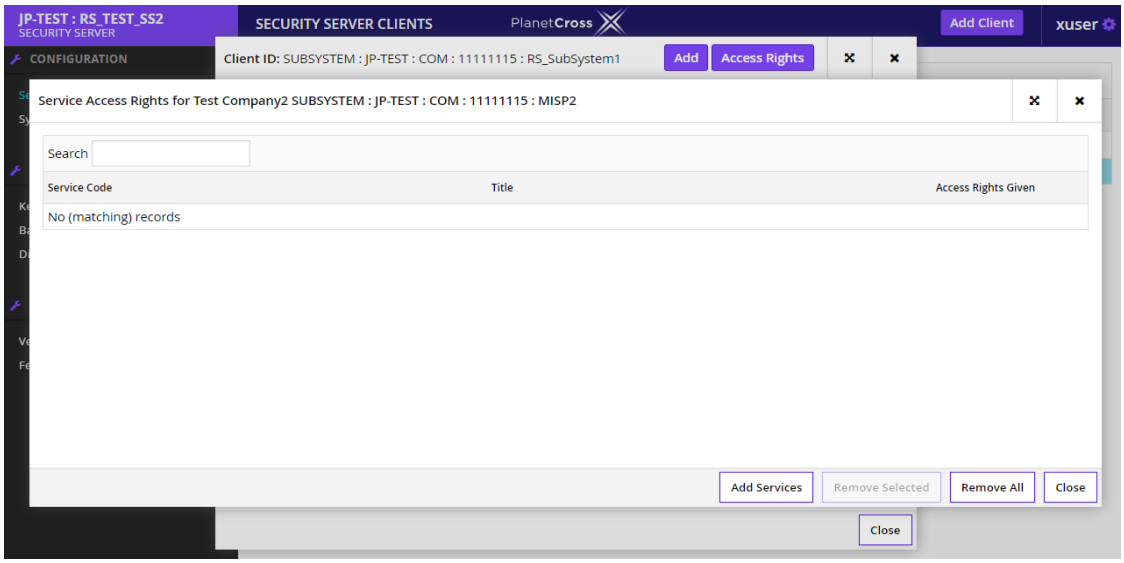
選択したサブジェクトに対して Security Server でオープンであるサービスのリストが表示されます。



- サービスクライアントからアクセス権を削除するためには、一覧から 1 つまたは複数のサービスを選択し、[Remove Selected]をクリックし、次に、[Confirm]をクリックします。







- サービスクライアントからすべてのアクセス権を削除するためには、[Remove All]をクリックし、次に[Confirm]をクリックします。
- サービスクライアントにアクセス権を追加するには、まず[Add Service]をクリックします。表示されたウィンドウで、サブジェクトに付与したいサービスを選択します(既に付与されているサービスはグレーで表示されます)。[Add Selected to ACL]をクリックします。検索で見つかったサービスをすべて追加するには、[Add All to ACL]をクリックします。

【注記】
ページを更新すると、サービスへアクセス権を持たないすべてのサービスクライアントがサービスクライアントの画面から削除されます。

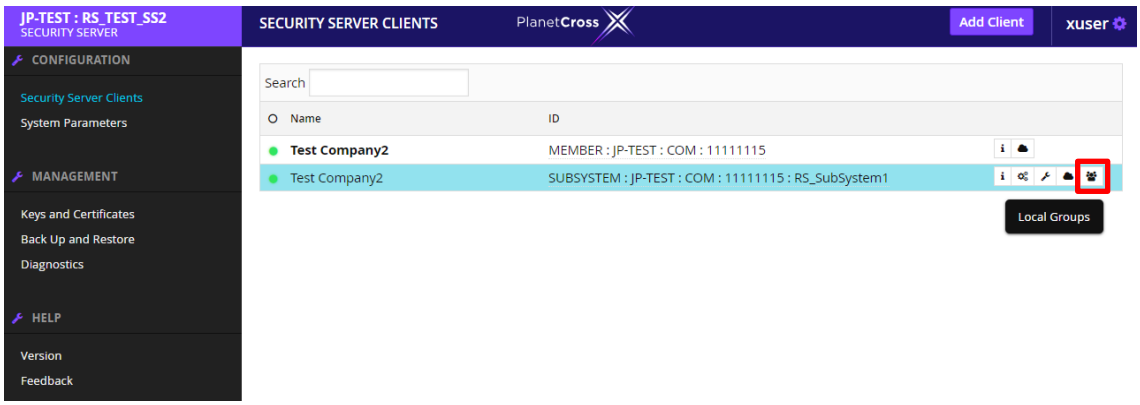
6.4 ローカルアクセス権グループ

同じサービスを使用する PlanetCross サブシステムグループに対するサービスアクセス権の管理を容易にするために、Security Server クライアント用ローカルアクセス権グループを作成することができます。
グループに付与されたアクセス権は、グループのすべてのメンバーに適用されます。ローカルグループはクライアントベースです。つまり、ローカルグループは、一台の Security Server の一つのクライアントのサービスアクセス権を管理するためにのみ使用できます。

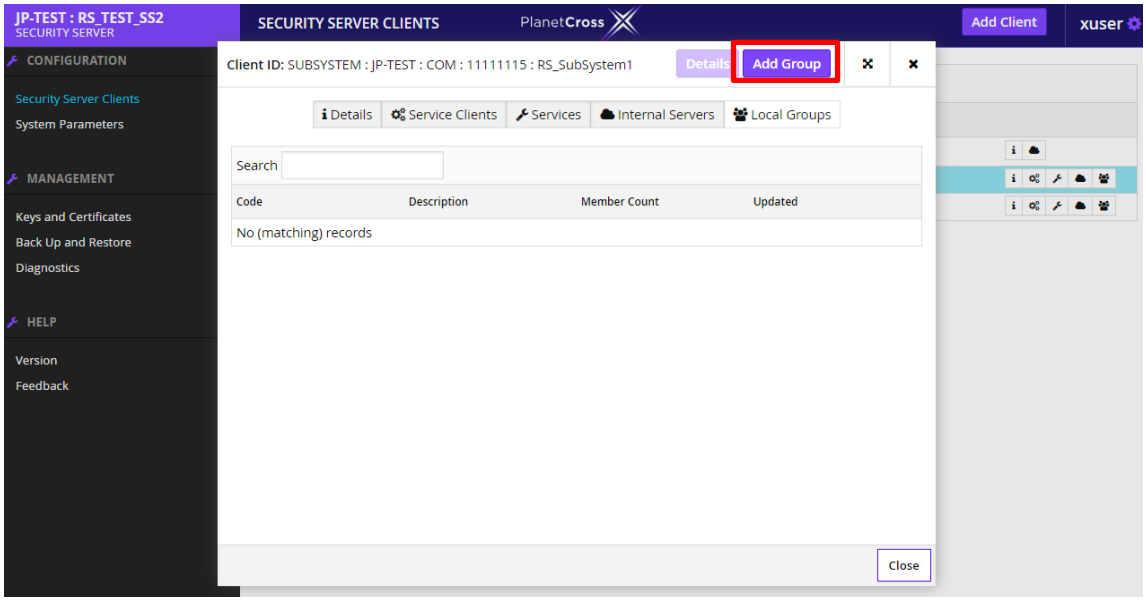
6.5 ローカルグループを追加する

Security Server クライアントのローカルグループを作成するためには、次の手順を実行します。
＜アクセス権: サービス管理者＞

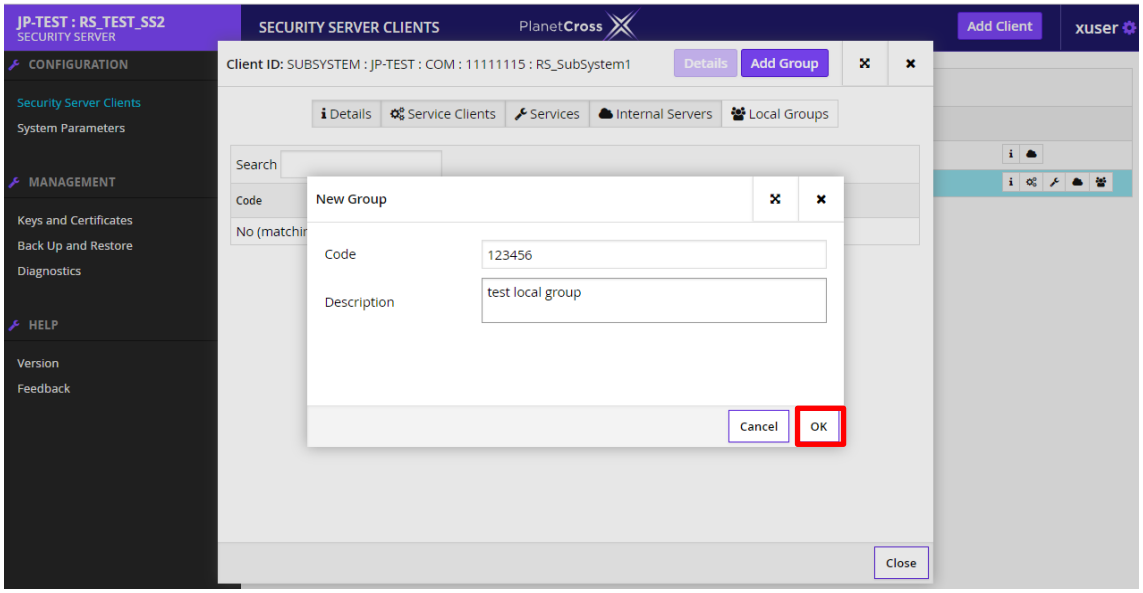
1. [Configuration]メニューで[Security Server Clients]を選択し、クライアントを選択して、その行のローカルグループアイコンをクリックします。
クライアントのローカルグループのリストが表示されます。

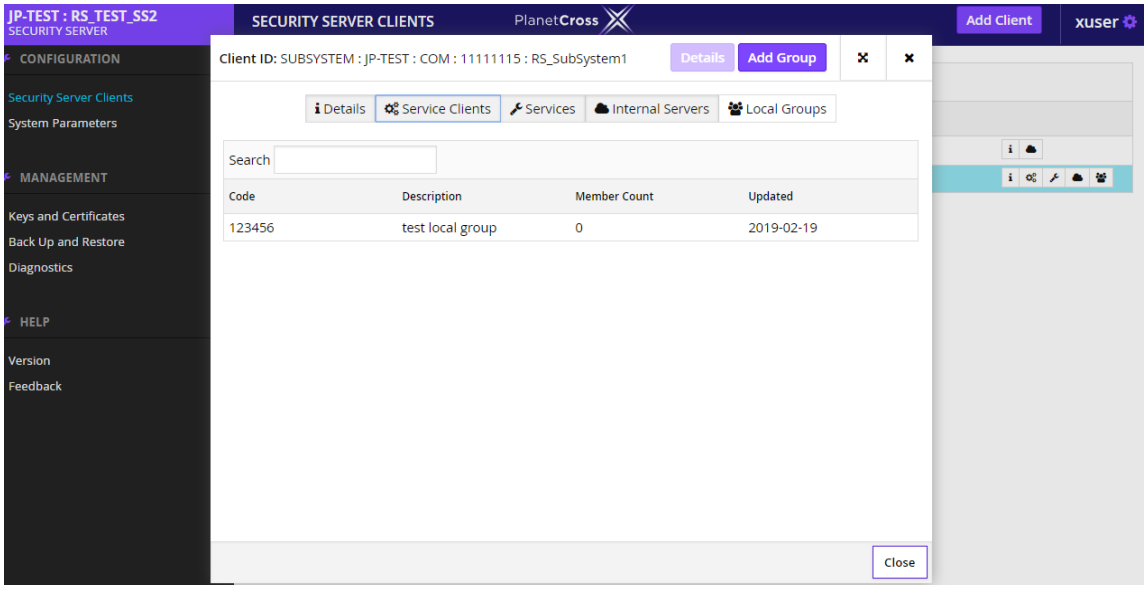


2. 新しいグループを作成するためには、[Add Group]をクリックします。



3. 表示されたウィンドウで、新しいグループのコードと説明を入力し、[OK]をクリックします。

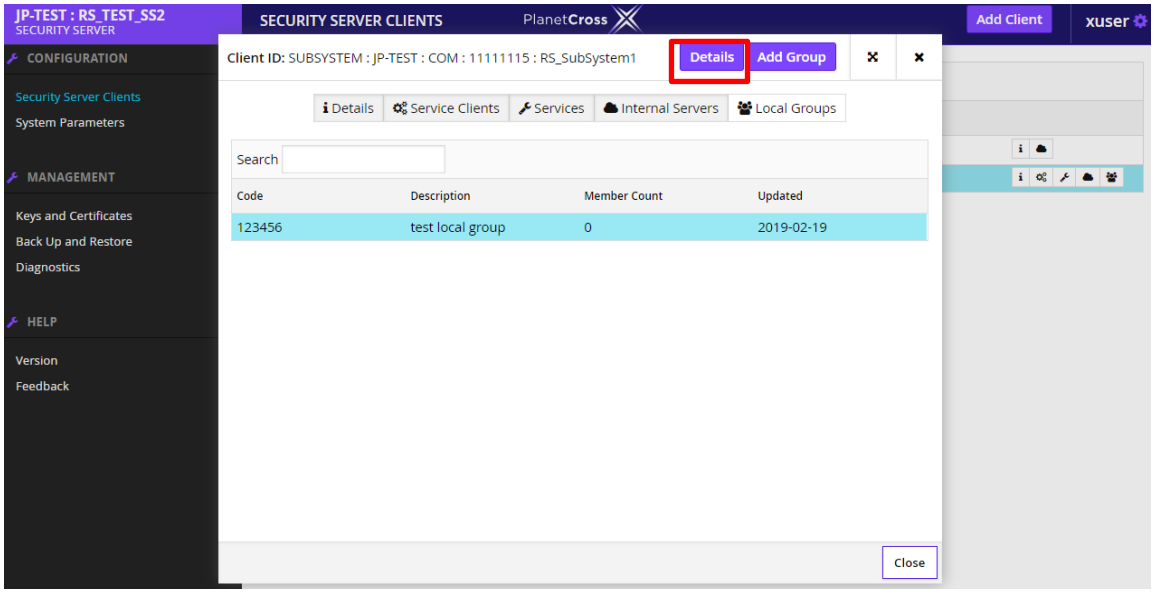




6.6 ローカルグループのメンバーの表示と変更

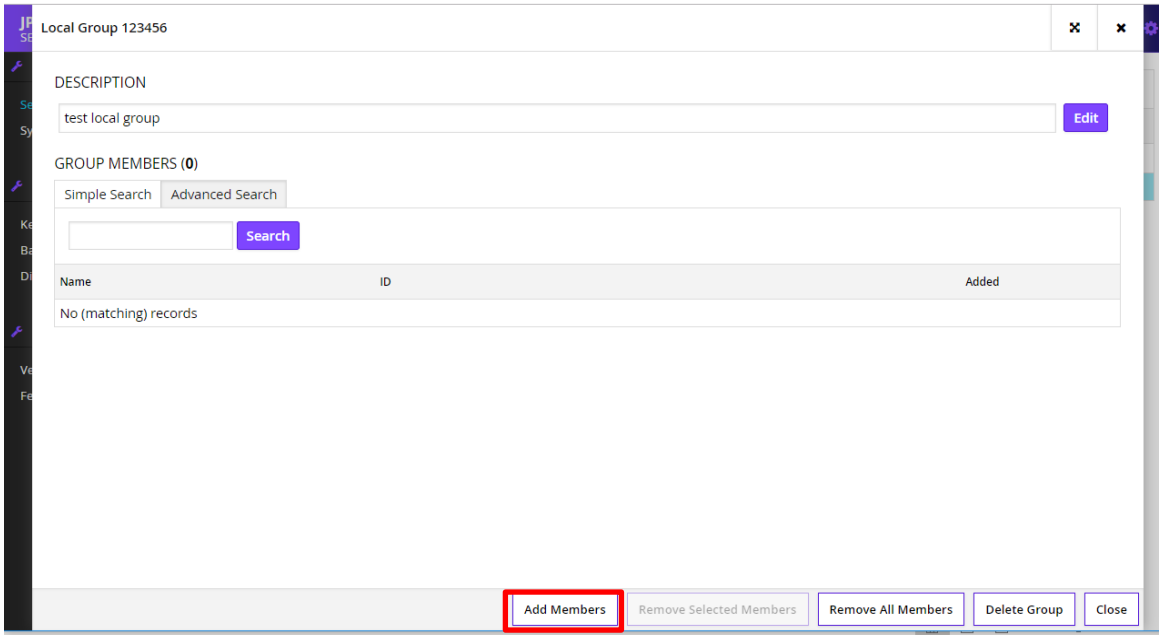
ローカルグループのメンバーを表示するためには、次の手順を実行します。
＜アクセス権: サービス管理者＞

1. [Configuration]メニューで[Security Server Clients]を選択し、クライアントを選択して、その行の[Local Groups]アイコンをクリックします。
2. 表示されたウィンドウで、メンバーを表示または変更したいグループを選択し、[Details]をクリックして詳細画面を開きます。

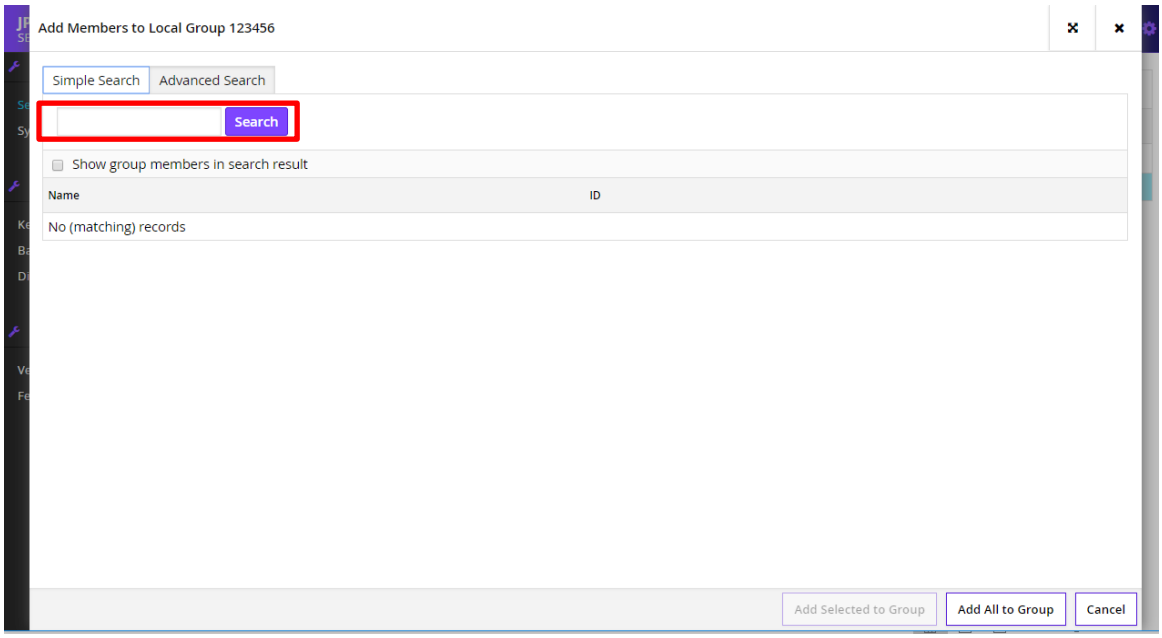


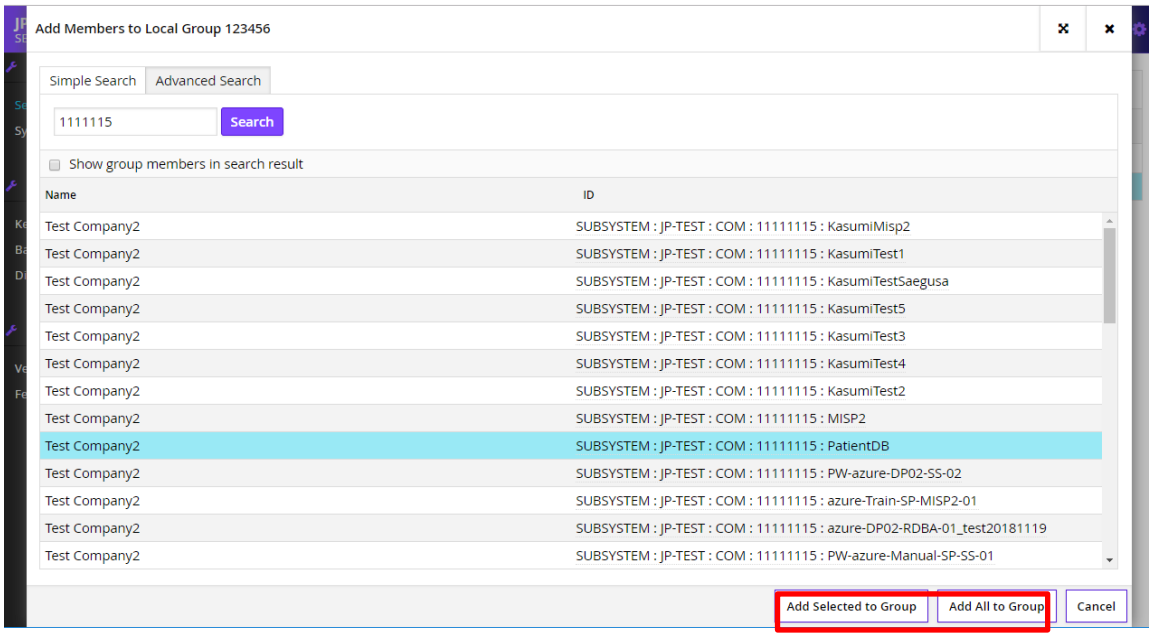
一つ以上のメンバーをローカルグループに追加するためには、グループの詳細画面で次の手順を実行します。

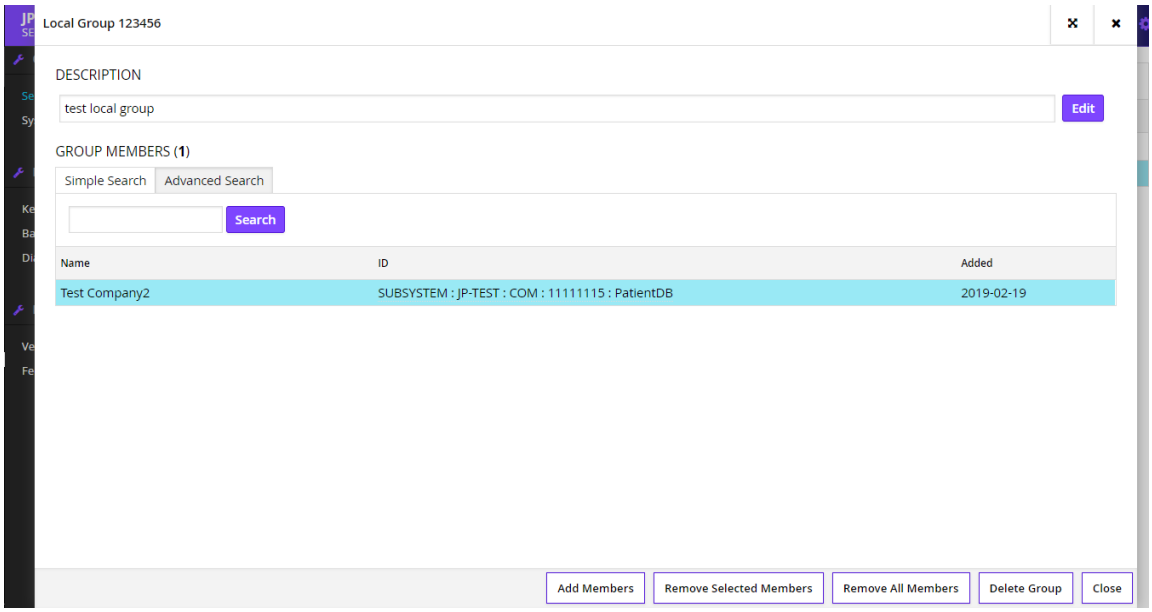
1. [Add Members]をクリックします。



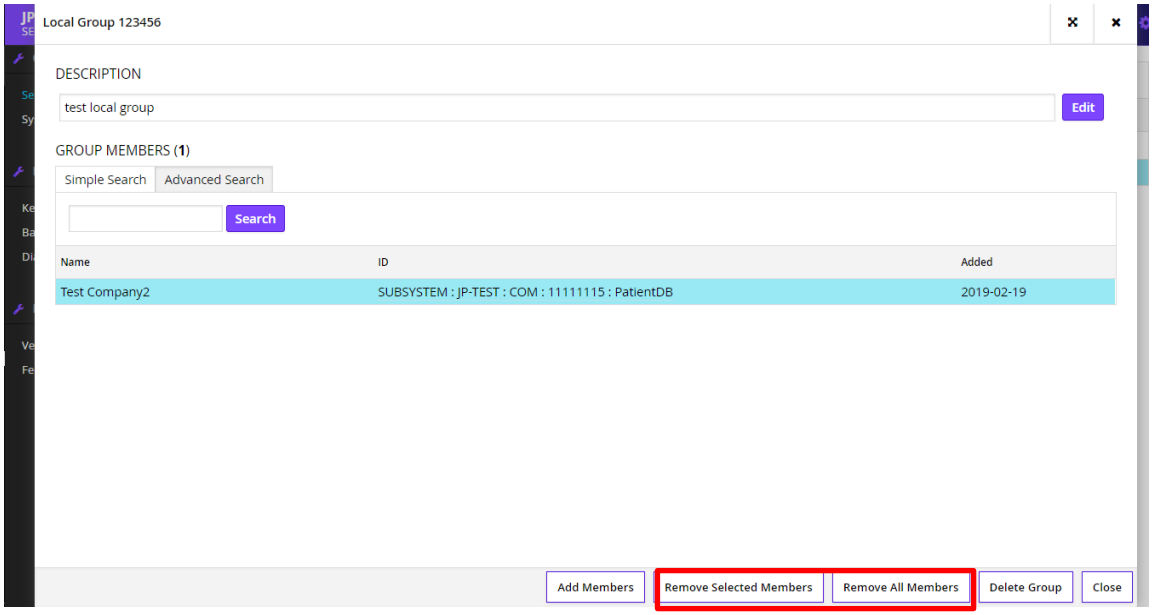
2. 表示されたウィンドウで、グループに追加したいサブシステムを探して、選択し、[Add Selected to Group]をクリックします。検索機能で発見したすべてのサブシステムをグループに追加するためには、[Add All to Group]をクリックします。

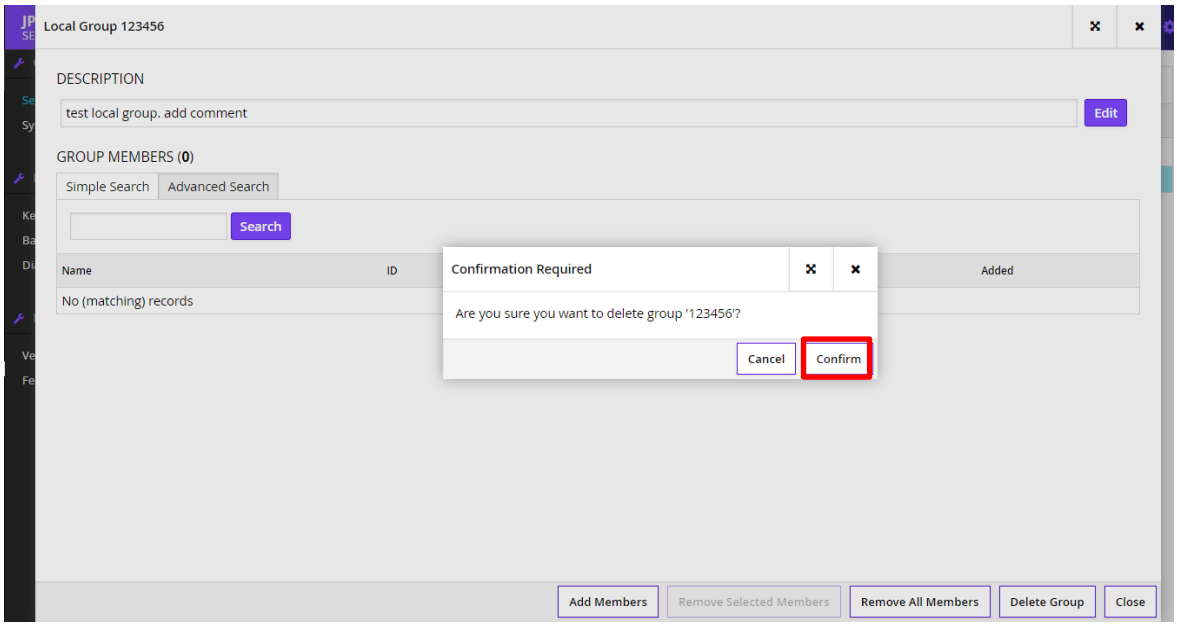


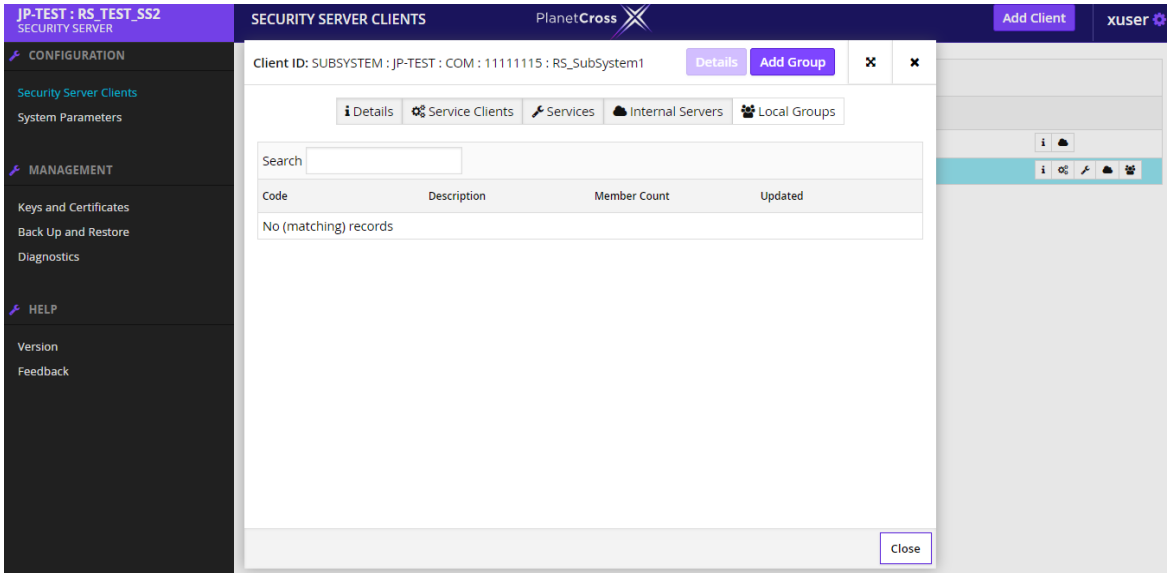




ローカルグループからメンバーを削除するには、グループの詳細画面で削除したいメンバーを選択し、[Remove Selected Members]をクリックします。グループからすべてのグループメンバーを削除するには、[Remove All Members]をクリックします。



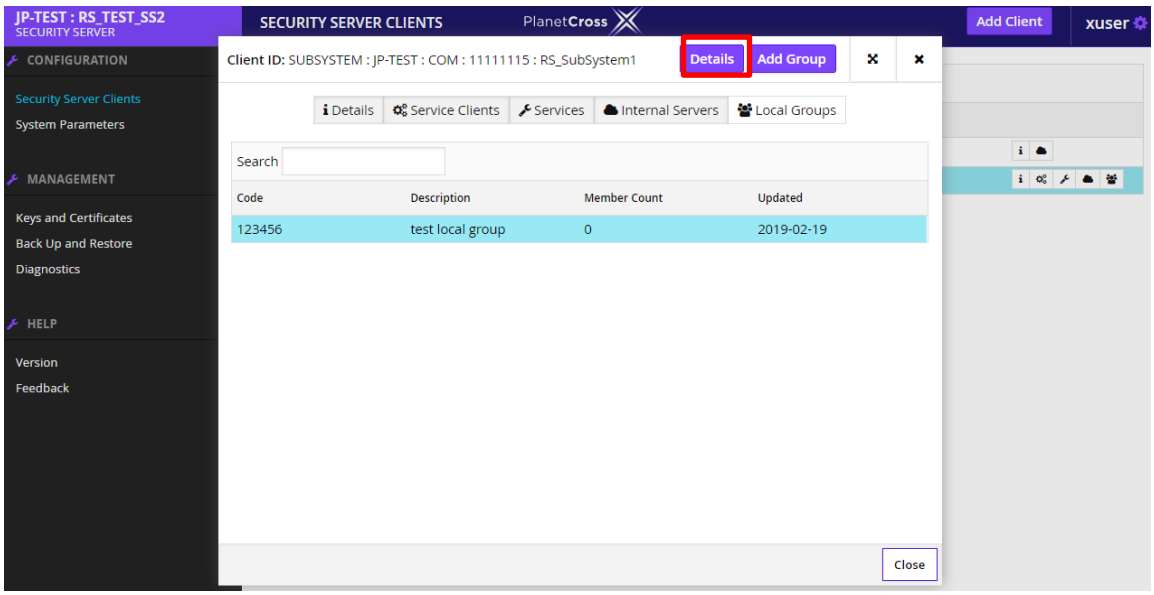




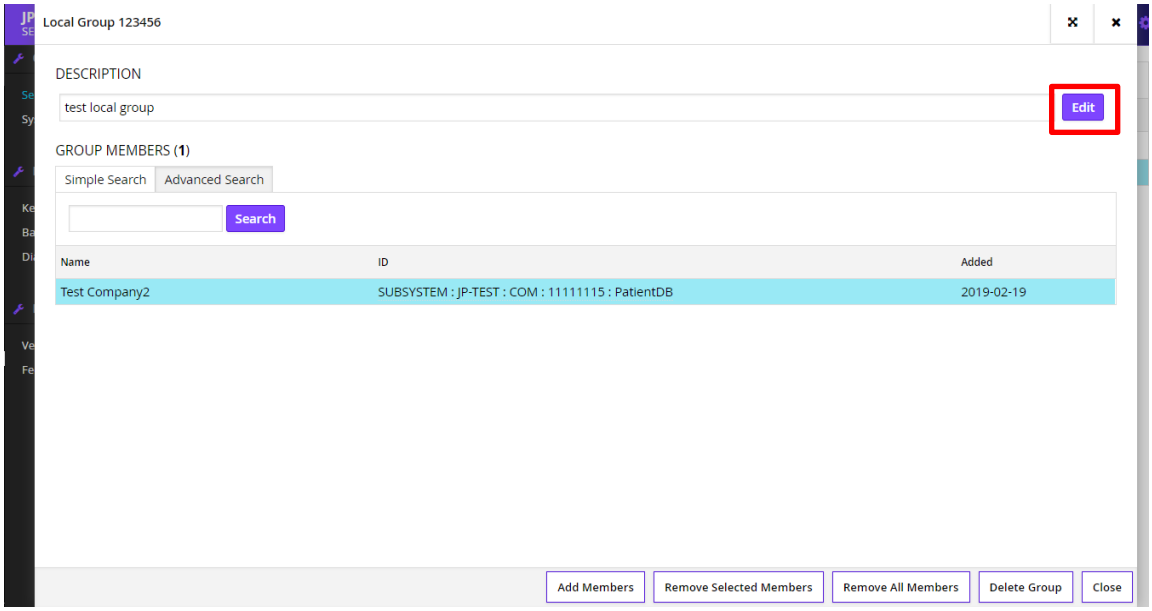
6.7 ローカルグループの説明変更

ローカルグループの説明を変更するためには、次の手順を実行します。
＜アクセス権: サービス管理者＞

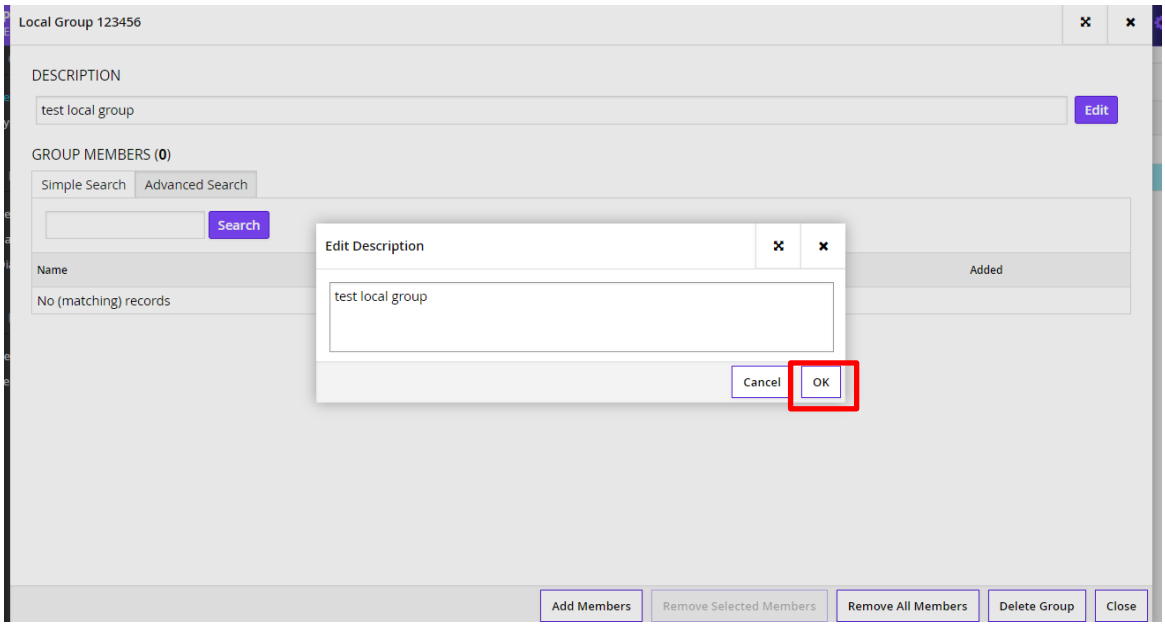
1. [Configuration]メニューで[Security Server Clients]を選択し、一覧からクライアントを選択して、その行の[Local Groups]アイコンをクリックします。
2. ローカルグループ一覧からグループを選択し、[Details]をクリックします。



3. グループ詳細画面で、[Edit]をクリックして、説明を変更します。



4. グループの説明を入力し、[OK]をクリックします。

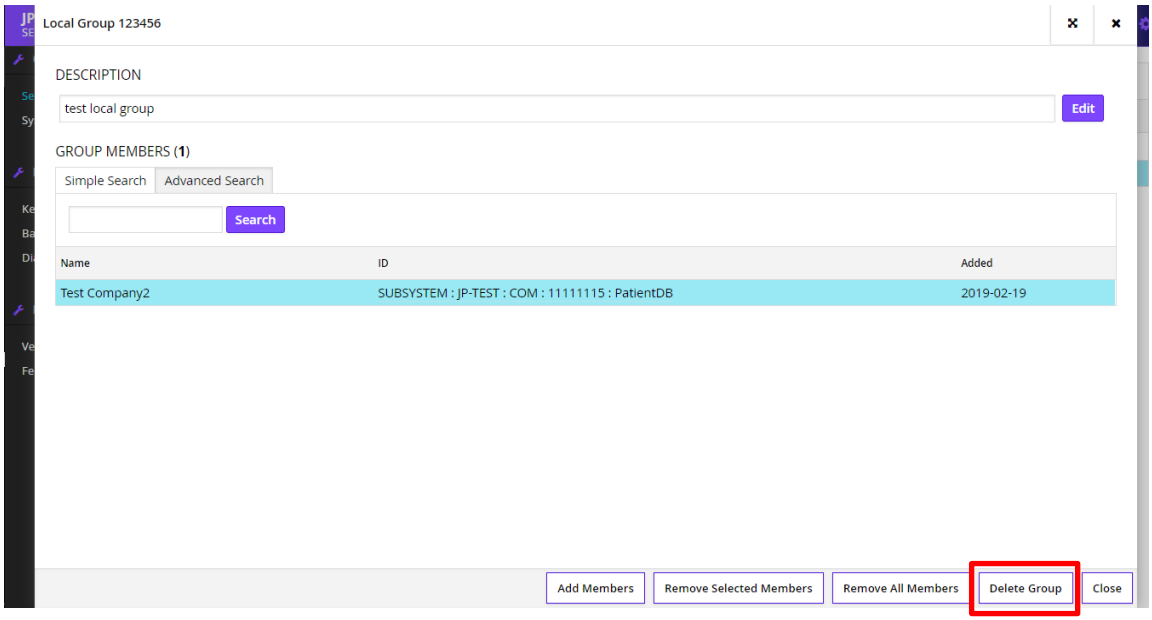


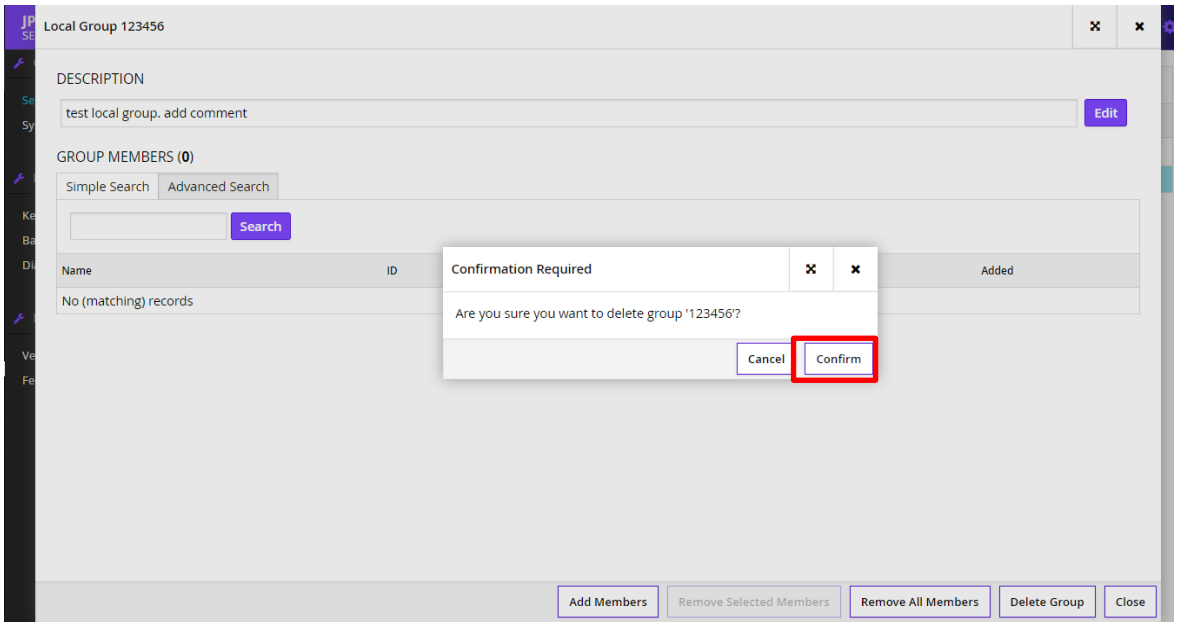
6.8 ローカルグループの削除

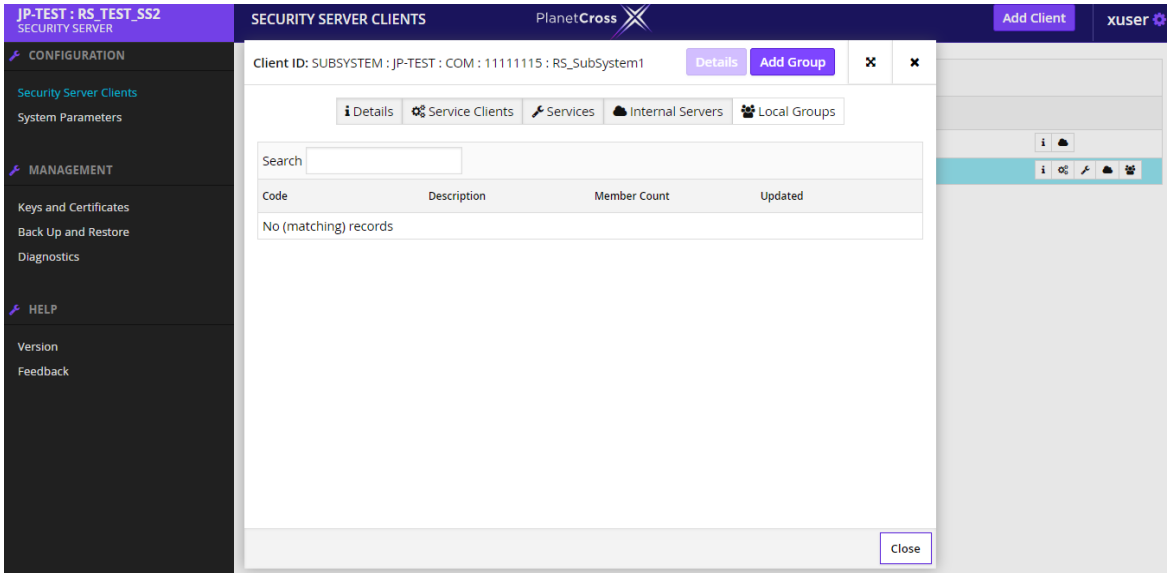
警告	ローカルグループを削除すると、グループメンバーシップを通じて付与されたすべてのグループメンバーアクセス権が取り消されます。

ローカルグループを削除するためには、次の手順を実行します。
＜アクセス権: サービス管理者＞

1. [Configuration]メニューで[Security Server Clients]を選択し、一覧からクライアントを選択して、その行の[Local Groups]アイコンをクリックします。
2. ローカルグループ一覧からグループを選択し、[Details]をクリックします。
3. グループ詳細画面で、[Delete Group]をクリックし、表示されたウィンドウで[Confirm]をクリックして、削除を確認します。







7. クライアント情報システムとの通信

Security Server は、HTTP、HTTPS、または HTTPS NOAUTH プロトコルのいずれかを通じて、サービスを提供および使用する情報システムサーバと通信できます。

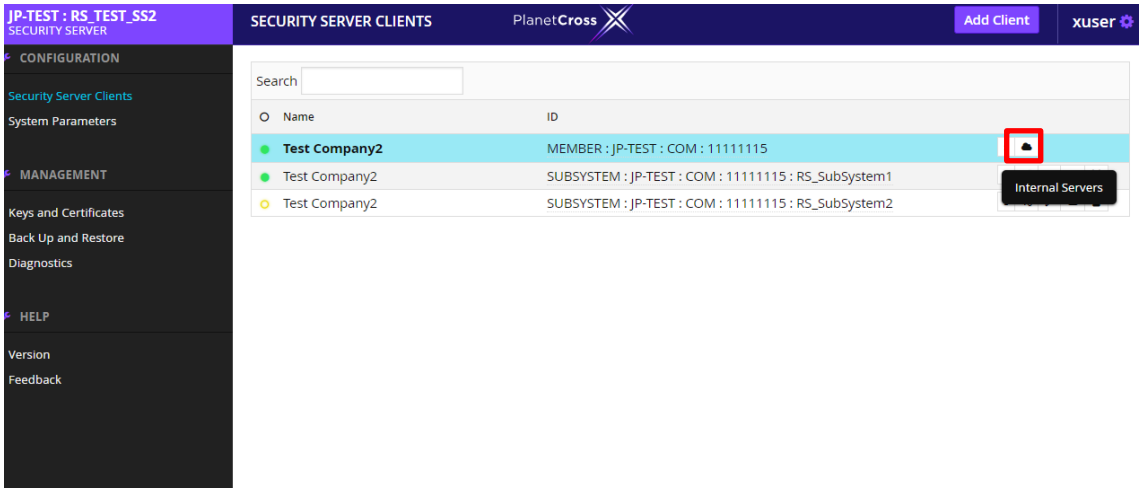
- 情報システムサーバと Security Server が他のコンピューターが接続されていないプライベートネットワークセグメントを介して通信する場合は、HTTP プロトコルを使用してください。さらに、情報システムサーバは対話的ログインを許可しないでください。
- 情報システムサーバと Security Server の間の通信に専用のネットワークセグメントを用意できない場合は、HTTPS プロトコルを使用してください。その場合、盗聴および傍受の可能性から通信を保護するために暗号方式が使用されます。HTTPS を使用する前には、情報システムサーバに対して内部 TLS 証明書を作成し、Security Server にロードする必要があります。
- Security Server によって情報システムの TLS 証明書の検証をスキップしたい場合は、HTTPS NOAUTH プロトコルを使用します。

【注記】
HTTP が選択されていますが、情報システムが HTTPS 上で Security Server に接続する場合、接続は承認されますが、クライアントの内部 TLS 証明書は検証されません(HTTPS NOAUTH と同じ動作)。

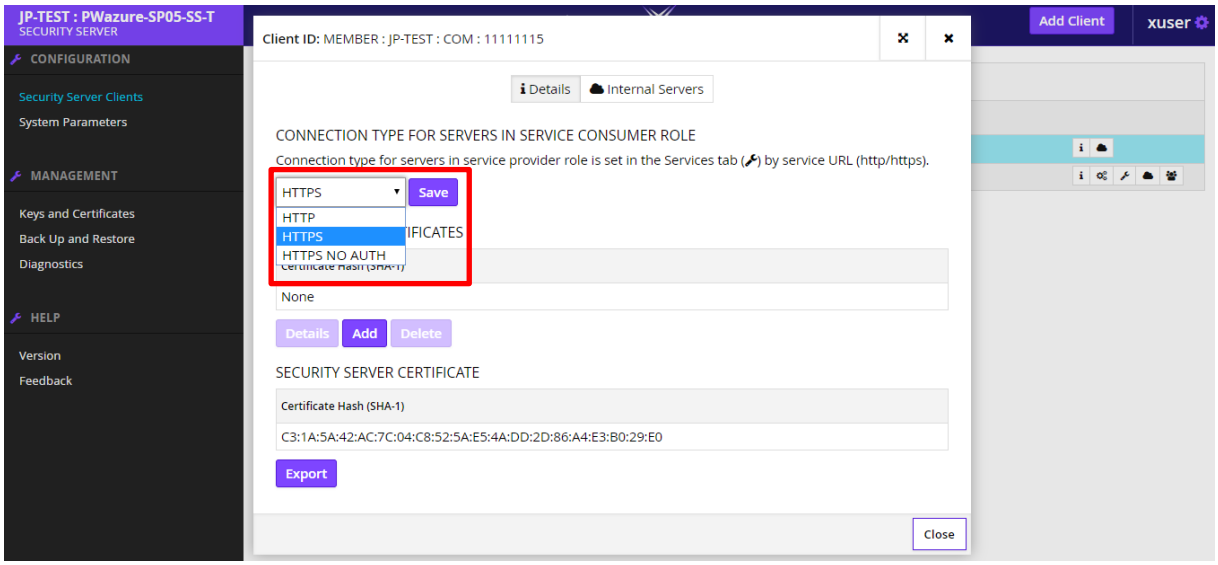
デフォルトでは、Security Server クライアントが、Security Server 所有者として運用モニタリングデータのリクエストを防止するために、Security Server の所有者の接続タイプは HTTPS に設定されています。

サービスコンシューマーの内部ネットワークサーバの接続方法を設定するには、次の手順を実行します。<アクセス権: サービス管理者>

1. [Configuration]メニューで[Security Server Clients]を選択し、一覧から Security Server の所有者またはクライアントを選択し、その行の[Internal Servers]アイコンをクリックします。



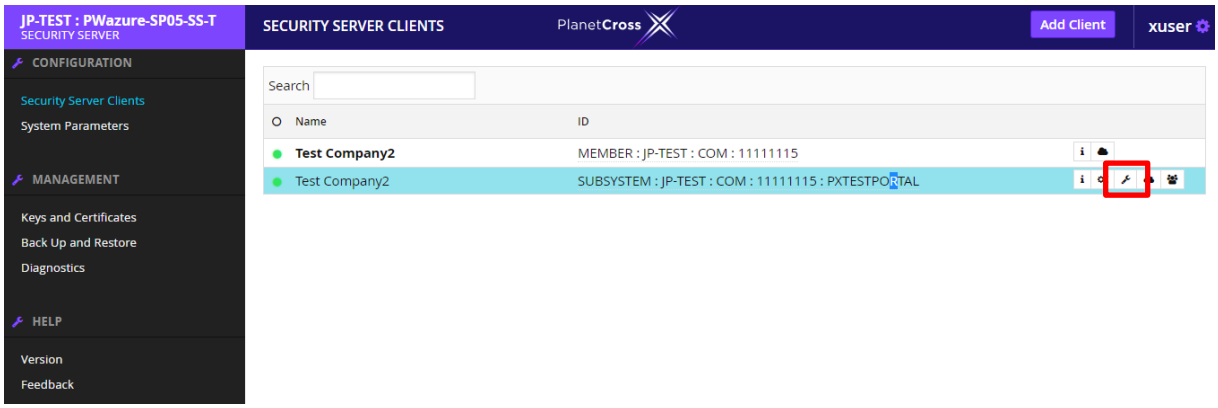
2. [Connection Type]のドロップダウンで接続方法を選択し、[Save]をクリックします。



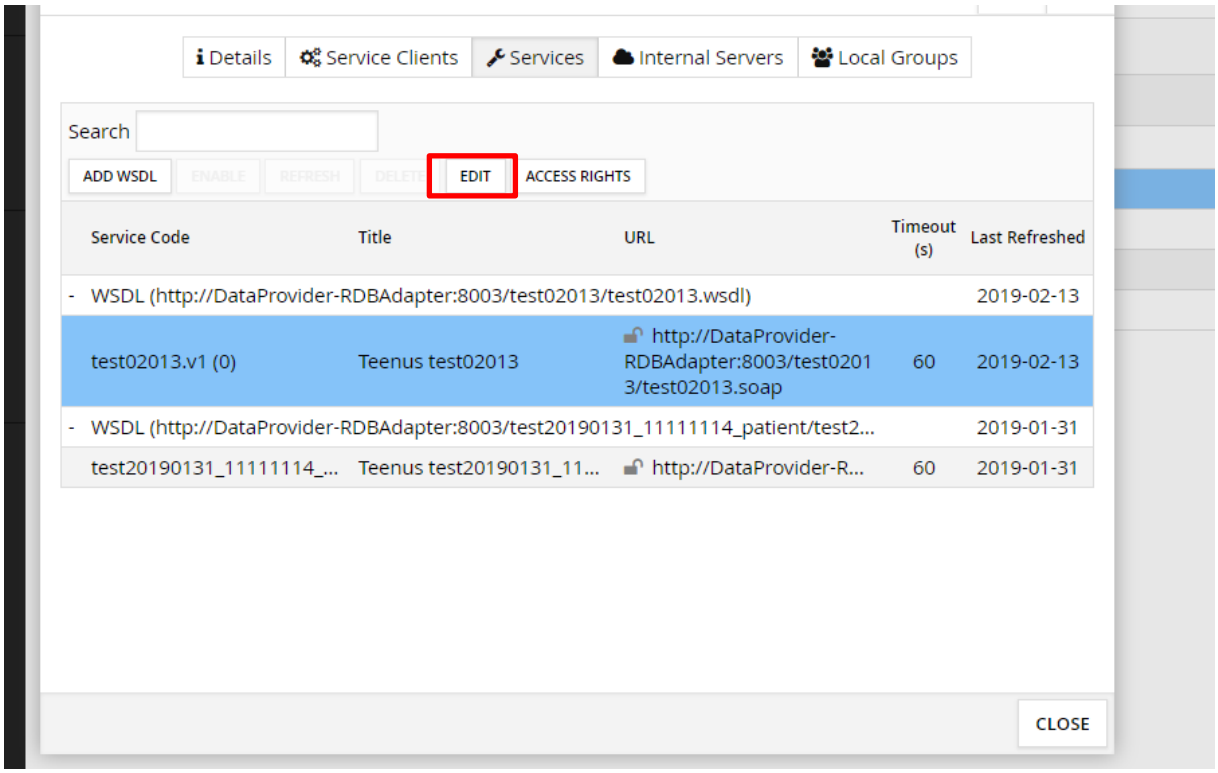
設定された接続方法により、情報システムのリクエスト URL は http://SECURITYSERVER/ または https://SECURITYSERVER/ です。リクエストをする際には、SECURITYSERVER というアドレスを Security Server の実際のアドレスに置き換える必要があります。

サービスプロバイダーの内部ネットワークサーバの接続方法は、URL によって決定されます。接続方法を変更するためには、次の手順を実行します。

1. [Configuration]メニューで[Security Server Clients]を選択し、一覧からクライアントを選択し、その行の[Services]アイコンをクリックします。



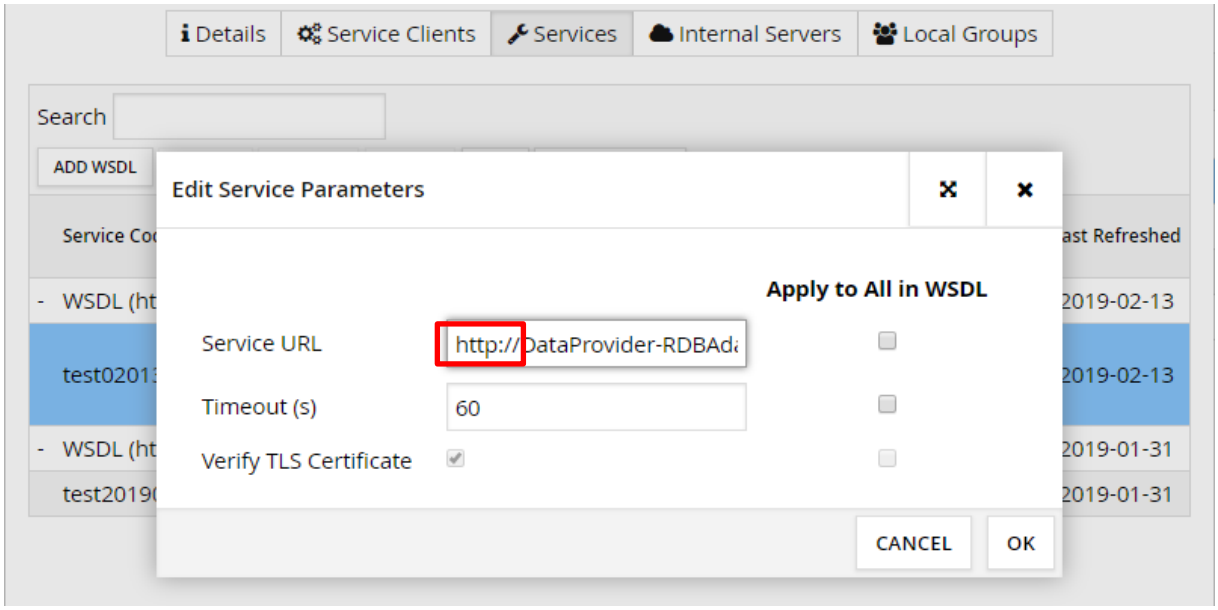
2. 一覧からサービスを選択し、[Edit]をクリックします。



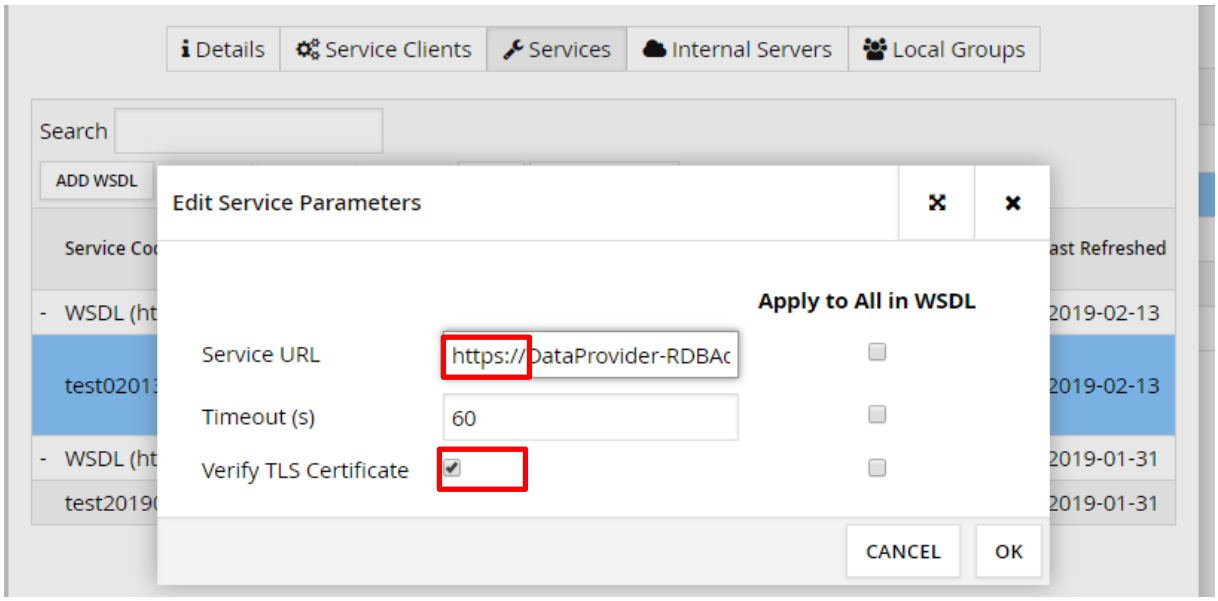
3. サービス URL のプロトコルを HTTP または HTTPS に変更します。

   HTTPS プロトコルが選択されている場合、必要に応じて[Verify TLS certificate]のチェックボックスを選択します。サービスパラメーターにより、内部ネットワークサーバとの接続は、次のプロトコルのいずれかを使用して作成されます。

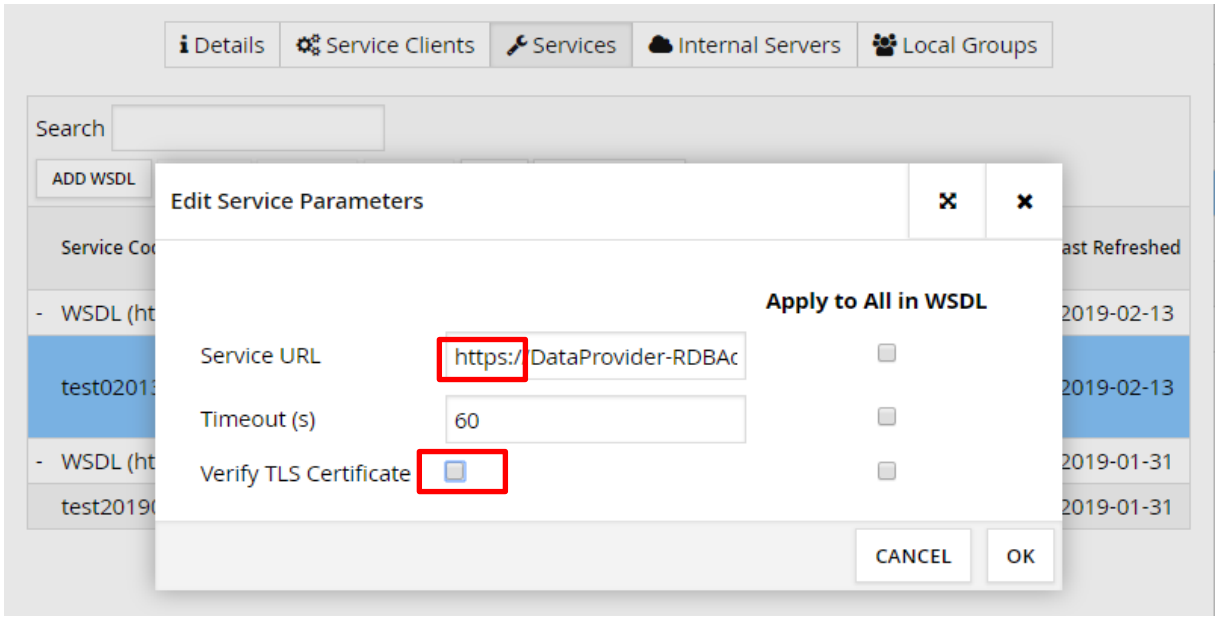
- **HTTP** - サービス/アダプタの URL は http://... で始まります。



- **HTTPS** - サービス/アダプタの URL は https://... で始まり、[Verify TLS certificate]チェックボックスが選択されています。



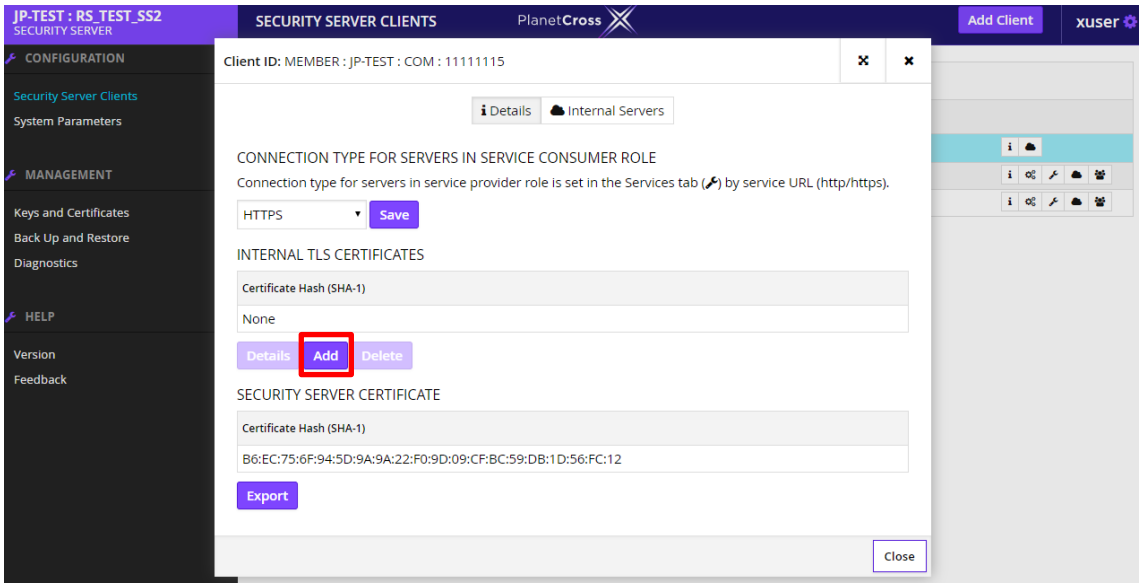
- **HTTPS NOAUTH** - サービス/アダプタの URL は https:// で始まり、[Verify TLS certificate]チェックボックスは選択されていません。



Security Server 所有者または Security Server クライアントが HTTPS 接続できるように、内部 TLS 証明書を追加するためには、次の手順を実行します。

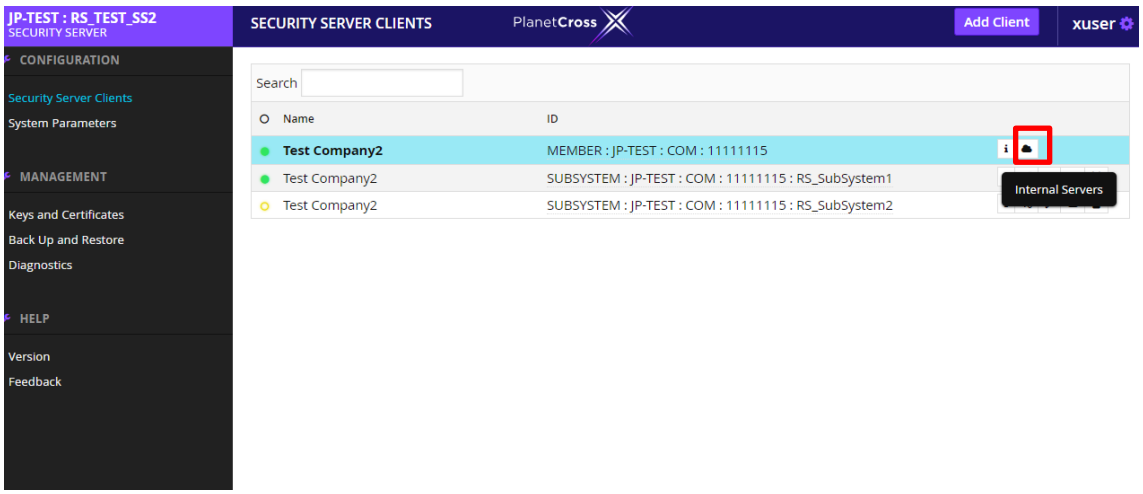
1. [Configuration]メニューで[Security Server Clients]を選択し、一覧から Security Server の所有者またはクライアントを選択し、その行の[Internal Servers]アイコンをクリックします。

2. 証明書を追加するには、[Internal TLS Certificates]セクションで、[Add]をクリックし、ローカルファイルシステムから証明書ファイルを選択して、[OK]をクリックします。
証明書フィンガープリントが「内部 TLS 証明書」一覧に表示されます。

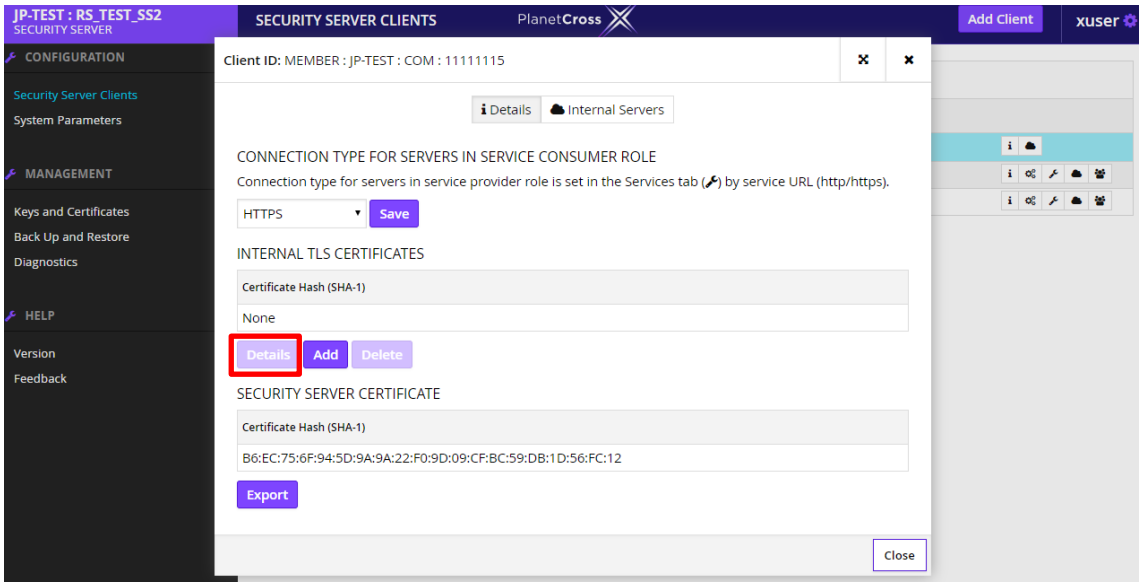


内部 TLS 証明書の詳細情報を表示するためには、次の手順を実行します。

1. [Configuration]メニューで[Security Server Clients]を選択し、一覧から Security Server の所有者またはクライアントを選択し、その行の[Internal Servers]アイコンをクリックします。

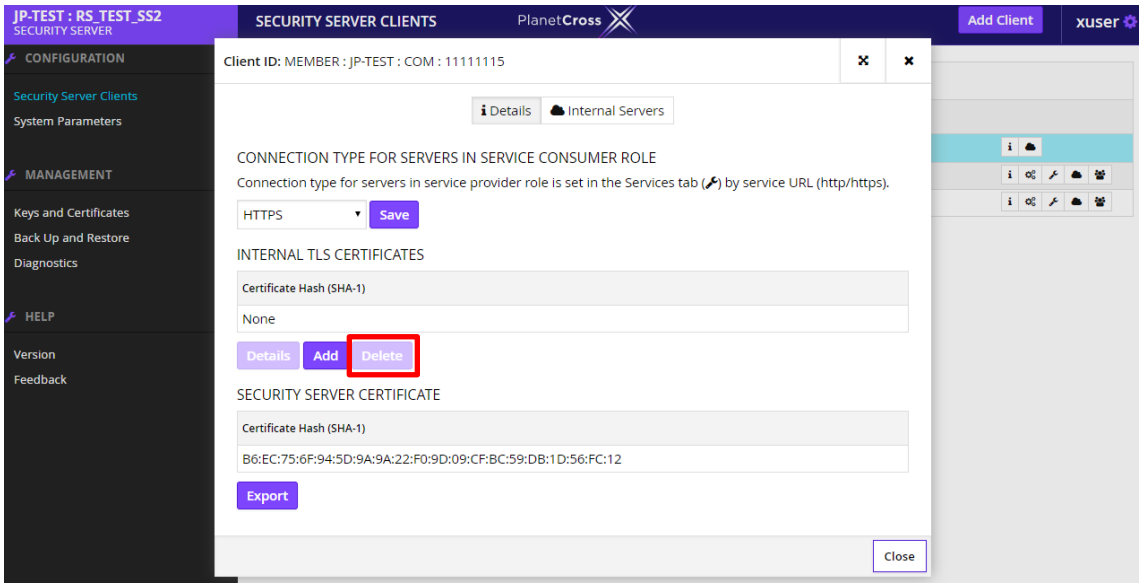


2. 「Internal TLS Certificates」一覧から証明書を選択し、[Details]をクリックします。



内部 TLS 証明書を削除するためには、次の手順を実行します。

1. [Configuration]メニューで[Security Server Clients]を選択し、一覧から Security Server の所有者またはクライアントを選択し、その行の[Internal Servers]アイコンをクリックします。
2. 「Internal TLS Certificates」一覧から証明書を選択し、[Delete]をクリックします。

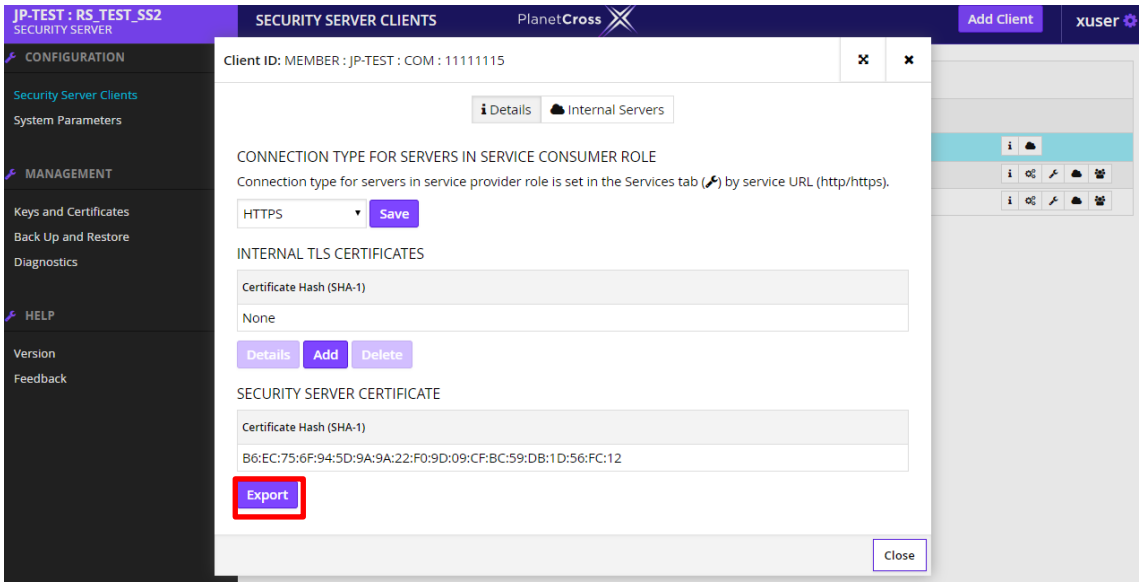


3. 表示されたウィンドウで[Confirm]をクリックし、削除を確認します。

Security Server の内部 TLS 証明書をエクスポートするためには、次の手順を実行します。

1. [Configuration]メニューで[Security Server Clients]を選択し、一覧から Security Server の所有者またはクライアントを選択し、その行の[InternalServers]アイコンをクリックします。

2. [Export]をクリックし、ファイルをローカルファイルシステムに保存します。



8. システムパラメーター

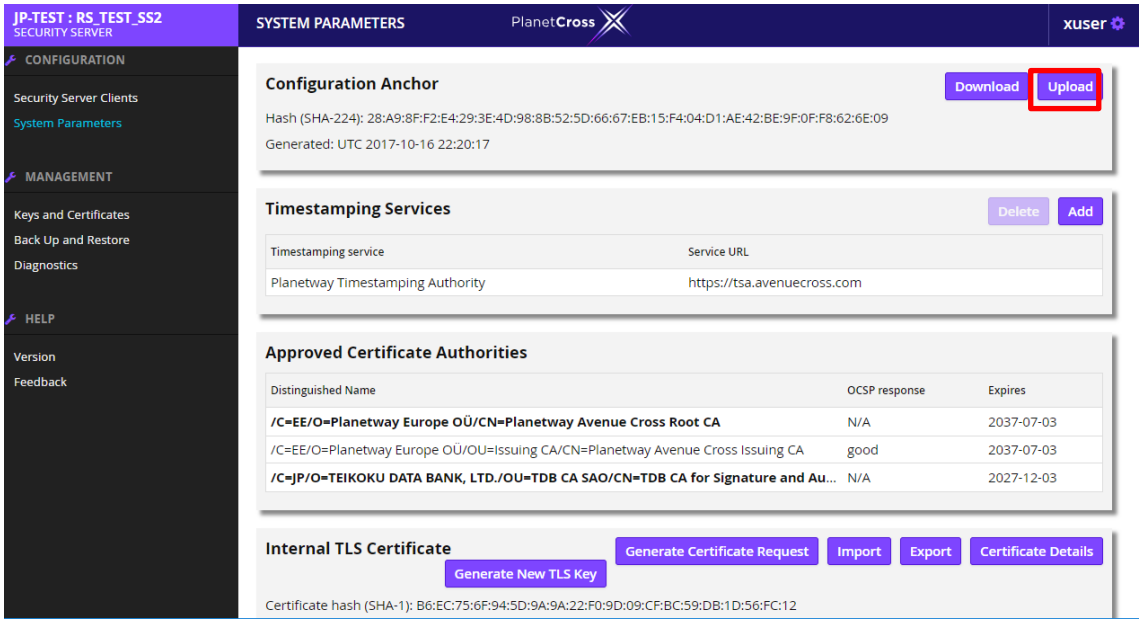
Security Server のシステムパラメーターは次のとおりです。

- コンフィギュレーションアンカーの情報 - コンフィギュレーションアンカーは、Central Server から署名された設定を定期的にダウンロードするため、およびダウンロードされた設定の署名を検証するためのデータを含みます。
- タイムスタンプサービス情報 - タイムスタンプは、PlanetCross を介して交換されるメッセージの証拠能力を担保するために使用されます。
- 内部 TLS 鍵と証明書 - 内部 TLS 証明書は、クライアントのサーバーに対して HTTPS 接続が選択されている場合、Security Server クライアントの情報システムとの TLS 接続を確立するために使用されます。

8.1 コンフィギュレーションアンカーの管理

コンフィギュレーションアンカーをアップロードするためには、次の手順を実行します。
＜アクセス権：コンフィギュレーションアンカーのアップロード: セキュリティ担当者＞
＜アクセス権：コンフィギュレーションアンカーのダウンロード: セキュリティ管理者、システム管理者＞

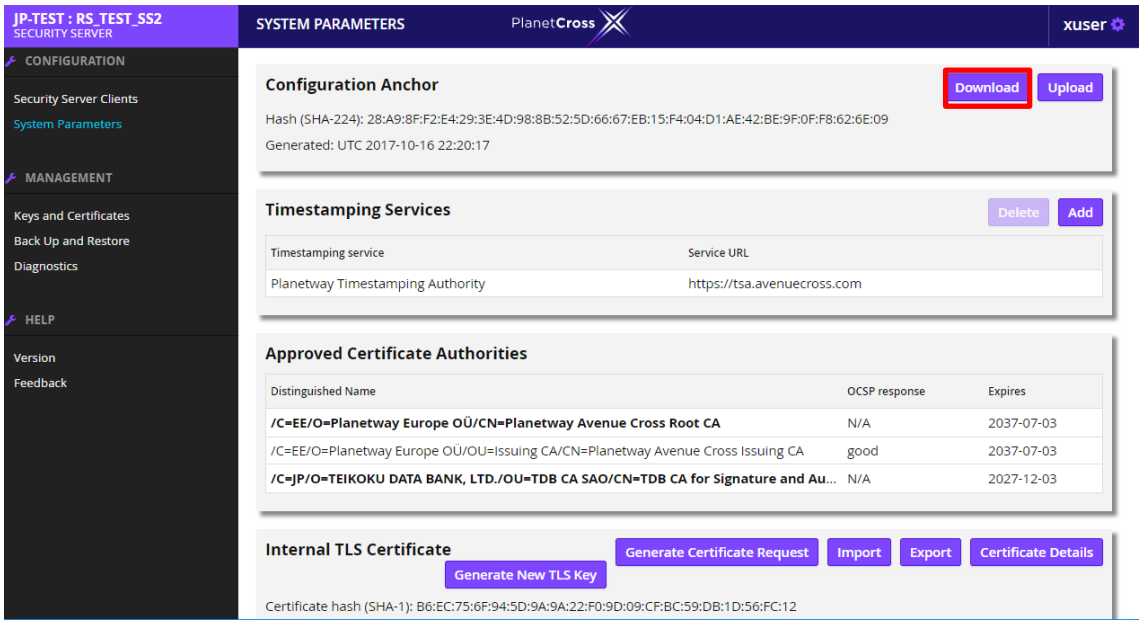
1. [Configuration]メニューで、[System Parameters]を選択します。
   システムパラメーター画面が表示されます。
2. [Configuration Anchor]セクションで、[Upload]をクリックします。



3. ローカルファイルシステムからアンカーファイルを探し、[Upload]をクリックします。
4. アップロードされたアンカーファイルのハッシュ値と、PlanetCross 監督機関によって発行された現在有効なアンカーのハッシュ値を比較することによって、アップロードしているアンカーファイルの有効性を確認します。
   ハッシュ値が一致する場合は、[Confirm]をクリックし、アップロードを確認します。

コンフィギュレーションアンカーをダウンロードするためには、次の手順を実行します。

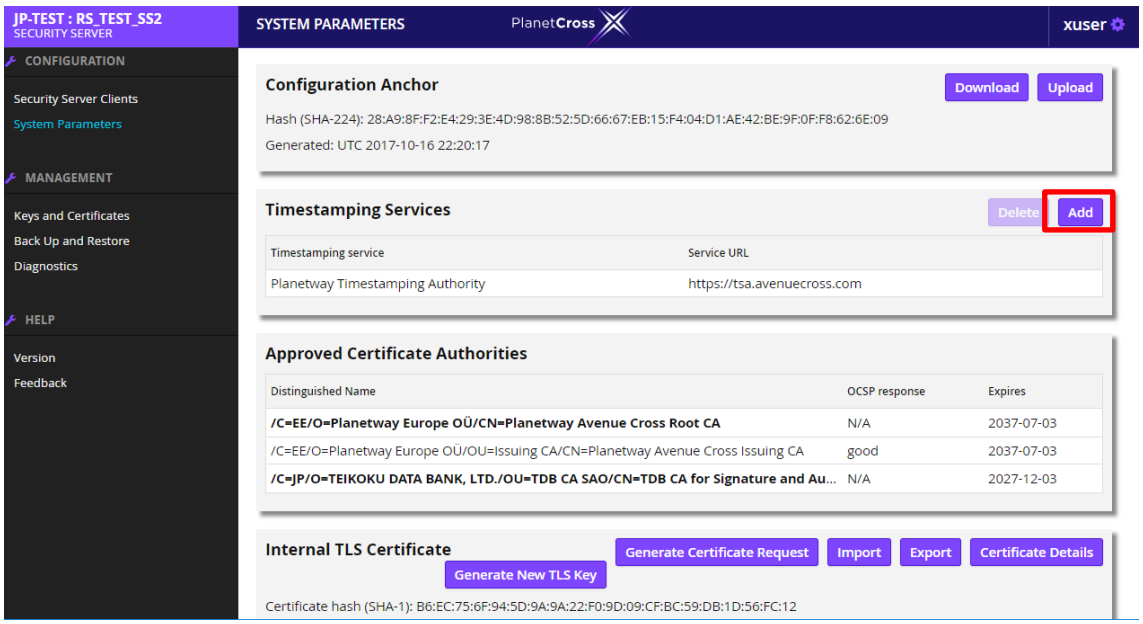
1. [Configuration]メニューで、[System Parameters]を選択します。
   システムパラメーター画面が表示されます。
2. [Configuration Anchor]セクションで、[Download]をクリックし、ファイルを保存します。



8.2 タイムスタンプサービスの管理

タイムスタンプサービスを追加するためには、次の手順を実行します。
＜アクセス権: セキュリティ担当者＞

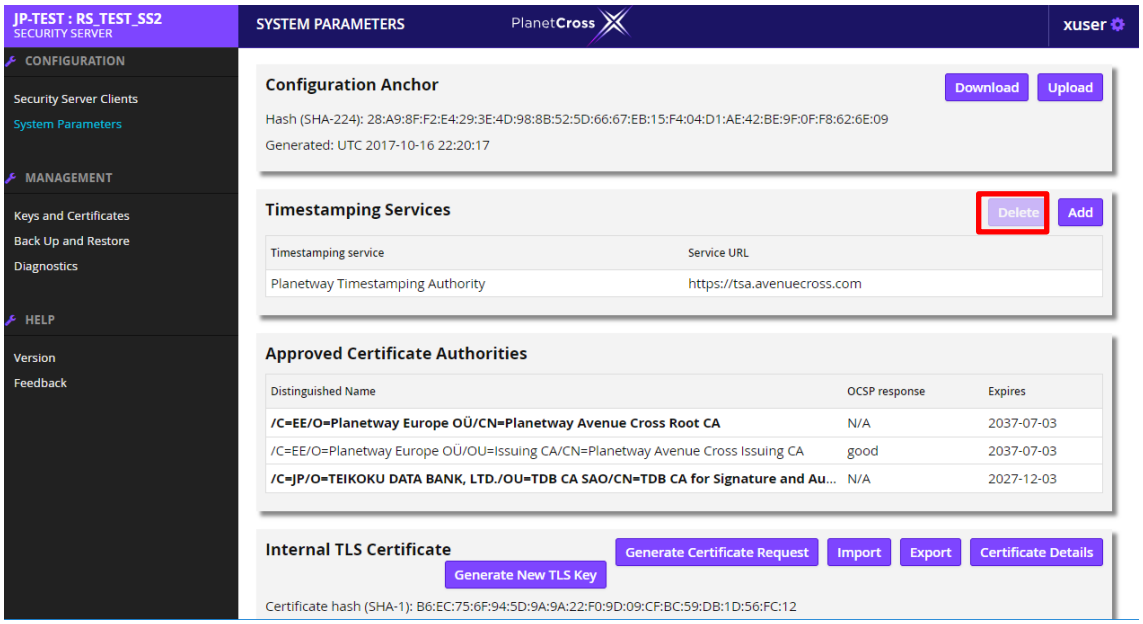
1. [Configuration]メニューで、[System Parameters]を選択します。
   システムパラメーター画面が表示されます。
2. [Timestamping Services]セクションで、[Add]をクリックします。



3. 表示されたウィンドウで、サービスを選択し、[OK]をクリックします。

タイムスタンプサービスを削除するためには、次の手順を実行します。

1. [Configuration]メニューで、[System Parameters]を選択します。
   システムパラメーター画面が表示されます。
2. [Timestamping Services]セクションで、削除するサービスを選択し、[Delete]をクリックします。

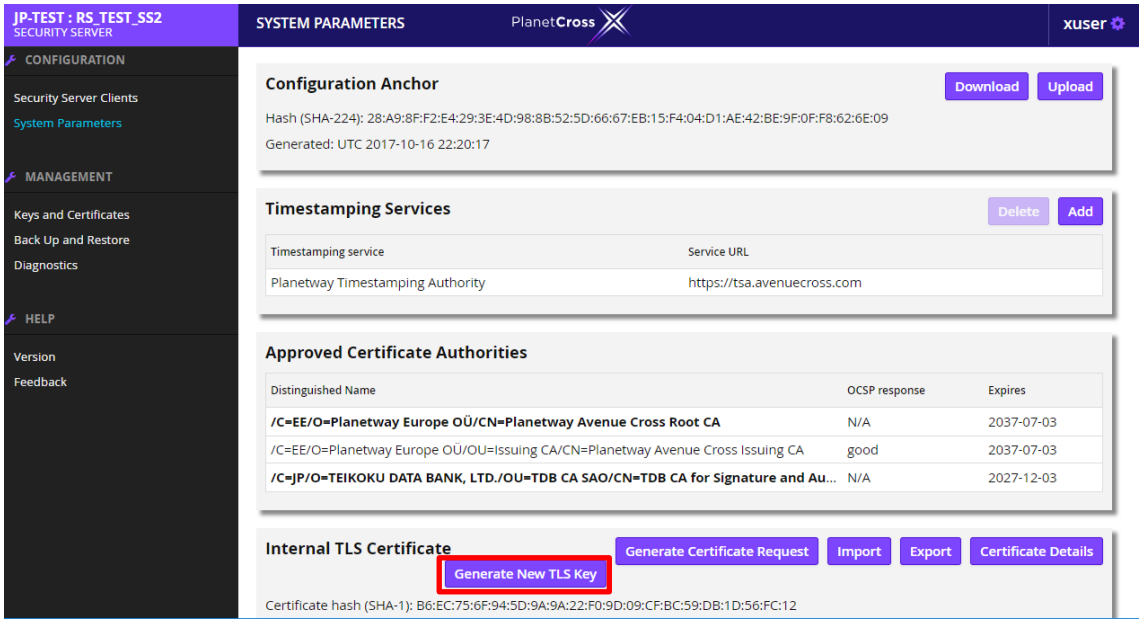


【注記】
複数のタイムスタンプサービスが設定されている場合、Security Server は、一覧の最上位のサービスからタイムスタンプを取得しようとします。それに失敗した場合は、次のサービスに移動します。

8.3 内部 TLS 鍵と証明書の変更

Security Server の内部 TLS 鍵と証明書を変更するためには、次の手順を実行します。
＜アクセス権: セキュリティ担当者、システム管理者＞

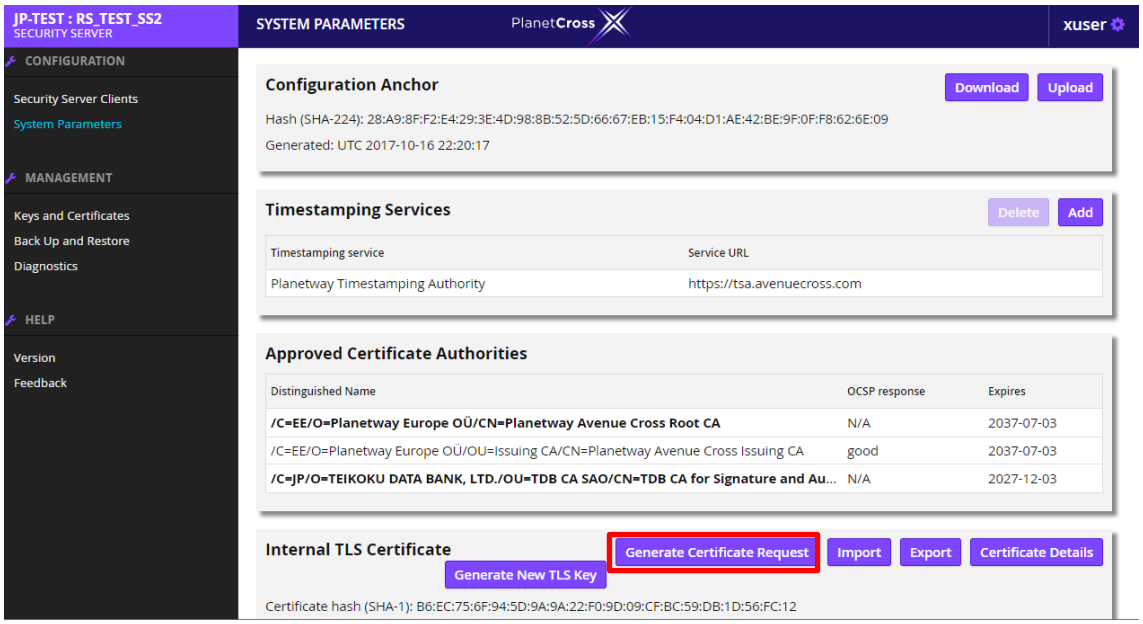
1. [Configuration]メニューで、[System Parameters]を選択します。
   システムパラメーター画面が表示されます。
2. [Internal TLS Certificate]セクションで、[Generate New TLS Key]をクリックし、表示されたウィンドウで[Confirm]をクリックします。



Security Server は、クライアント情報システムとの通信に使用する鍵および自己署名証明書を作成します。Security Server の証明書フィンガープリントも変更します。Security Server のドメイン名は、証明書の Common Name フィールドに、内部 IP アドレスは subjectAltName 拡張フィールドに保存されます。

新しい証明書リクエストを作成するためには、次の手順を実行します。

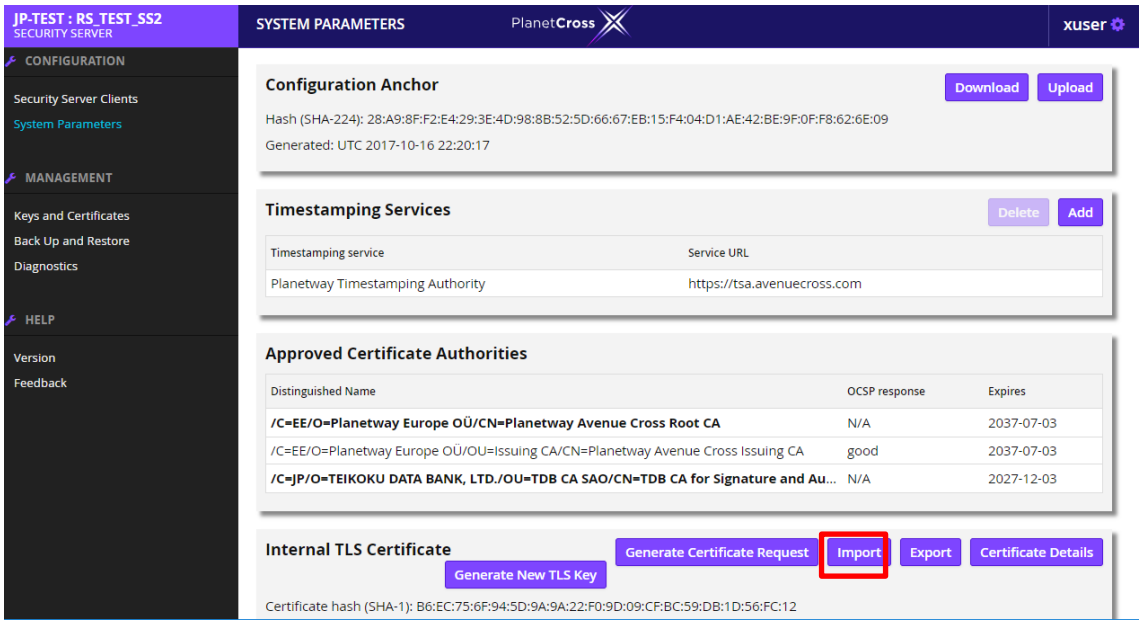
1. [Configuration]メニューで、[System Parameters]を選択します。
   システムパラメーター画面が表示されます。
2. [Internal TLS Certificate]セクションで、[Generate Certificate Request]をクリックし、識別名を入力し、証明書リクエストファイルをローカルファイルシステムに保存します。



Security Server は、現在の鍵および提供された識別名を使用して証明書リクエストを作成します。

新しい TLS 証明書をインポートするためには、次の手順を実行します。

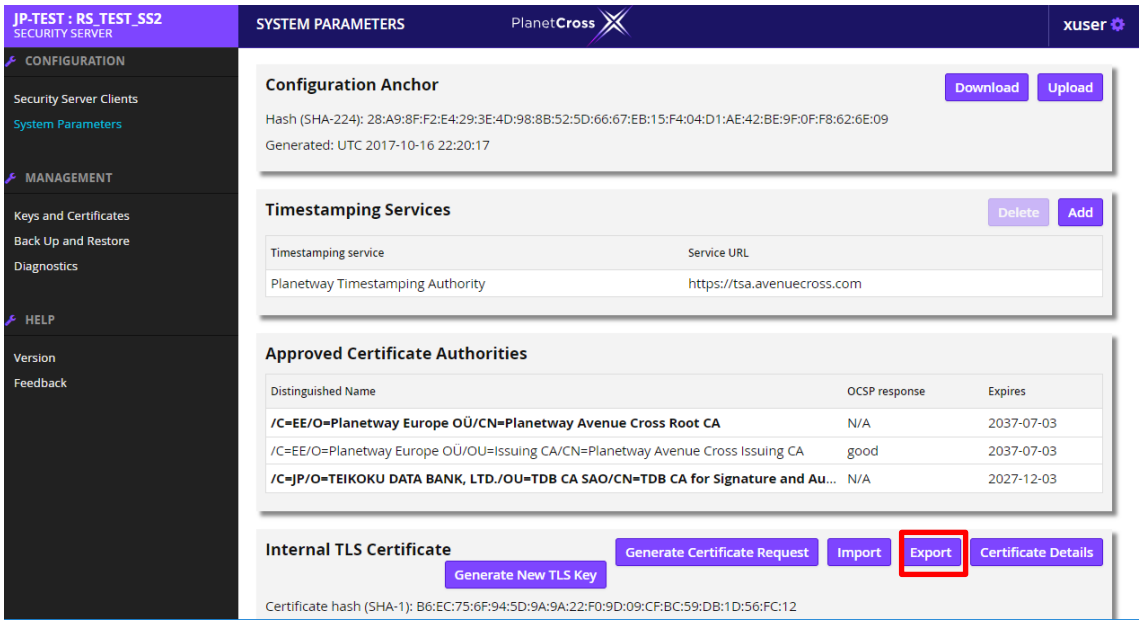
1. [Configuration]メニューで、[System Parameters]を選択します。
   システムパラメーター画面が表示されます。
2. [Internal TLS Certificate]セクションで、[Import]をクリックし、インポートするファイルを指定します。



【注記】
インポートする証明書は、PEM 形式でなければなりません。新しい TLS 証明書をインポートすると xroad-proxy は再起動し、Security Server からのサービスの提供に影響を与えることにご注意ください。

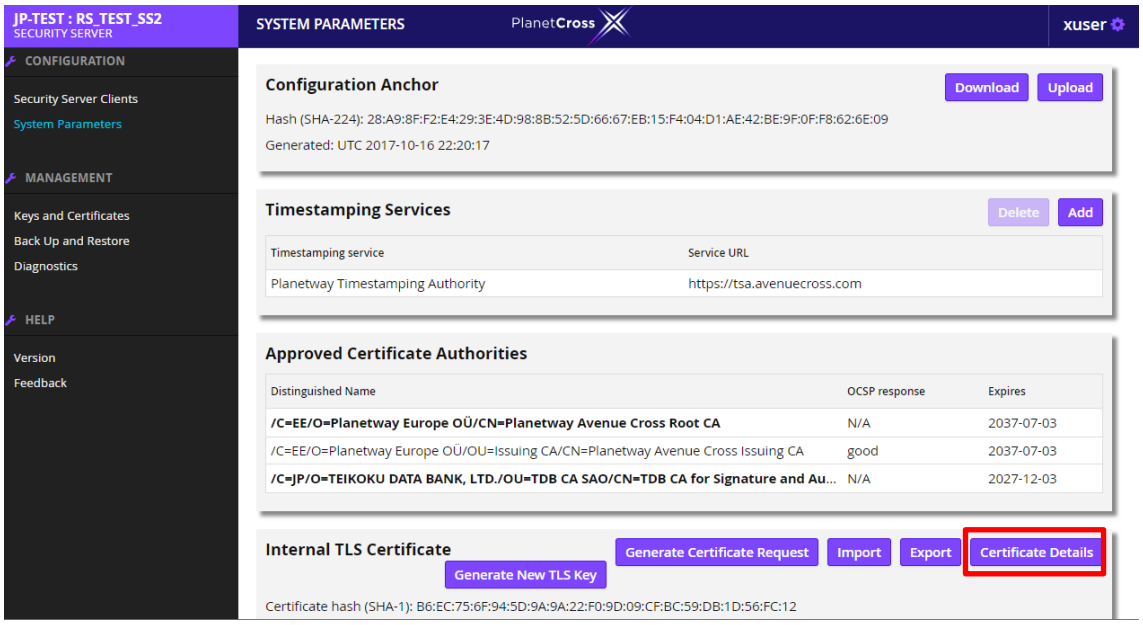
Security Server の内部 TLS 証明書をエクスポートするためには、次の手順を実行します。

1. [Configuration]メニューで、[System Parameters]を選択します。
   システムパラメーター画面が表示されます。
2. [Internal TLS Certificate]セクションで、[Export]をクリックし、ファイルをローカルファイルシステムに保存します。



Security Server の内部 TLS 証明書の詳細情報を表示するには、次の手順を実行します。

1. [Configuration]メニューで、[System Parameters]を選択します。
   システムパラメーター画面が表示されます。
2. [Internal TLS Certificate]セクションで、[Certificate Details]をクリックします。



9. メッセージログ

メッセージログの目的は、第三者へ通常のリクエストとレスポンスメッセージの受信を証明する手段を提供することです。Security Server の間で交換されるメッセージは署名され、暗号化されます。全通常リクエストとレスポンス毎に、Security Server は署名とタイムスタンプ済の完全なドキュメント(Associated Signature Container [ASiC])を作成します。

メッセージログデータは、メッセージ交換中に Security Server のデータベースに格納されます。設定により、交換されたメッセージの署名のタイムスタンプ発行は、メッセージ交換プロセスと同期的に行われるか、あるいは PlanetCross 監督機関によって設定された期間内に非同期に行われます。

同期的にタイムスタンプを行う場合、タイムスタンプ発行はメッセージ交換プロセスの不可欠な部分です(リクエストに対して 1 つのタイムスタンプが発行され、レスポンスにも 1 つのタイムスタンプが発行されます)。タイムスタンプの発行が失敗すると、メッセージ交換も失敗し、Security Server はエラーメッセージでレスポンスします。

非同期にタイムスタンプを行う場合、前回の定期的なタイムスタンプ発行以降のすべての(最大値は設定で決定されるメッセージログは単一のタイムスタンプ(バッチ)が発行されます。デフォルトでは、Security Server はパフォーマンスと可用性を高めるために非同期タイムスタンプを使用します。

Security Server は、メッセージログデータから定期的に署名付き(およびタイムスタンプ付き)ドキュメントを作成し、それらをローカルファイルシステムにアーカイブします。アーカイブファイルは、1 つ以上の署名付きドキュメントと、追加の完全性検証のための連携情報ファイルを含む ZIP コンテナです。

9.1 メッセージログの設定の変更

コンフィギュレーシパラメーターは、INI ファイル¥ [INI]に定義されています。各セクションは、特定の Security Server コンポーネントのパラメーターを含みます。デフォルトのメッセージログ設定は、ファイルにあります。

```
/etc/xroad/conf.d/addons/message-log.ini
```

デフォルト値をオーバーライドするためには、以下のファイルを作成または編集します。

```
/etc/xroad/conf.d/local.ini
```

ファイルに[message-log]セクションを作成します(存在しない場合)。セクションの開始点の下に、パラメーター値を一行に 1 つずつリストします。

たとえば、archive-path と archive-max-filesize を設定するためには、以下の行を設定ファイルに追加する必要があります。

```
[message-log]
archive-path=/my/arhcive/path/
archive-max-filesize=67108864
```


9.1.1 共通パラメーター

1. hash-algo-id - メッセージログのハッシュに使用されるハッシュアルゴリズムです。SHA-256、SHA-384、SHA-512 を選択できます。デフォルトは SHA-512 です。

9.1.2 タイムスタンプパラメーター

1. timestamp-immediately - true に設定する場合、タイムスタンプ発行はメッセージ交換と同期的に行われます。つまり、リクエストに対して 1 つのタイムスタンプが発行され、レスポンスに対してもう 1 つ発行されます。これは、メッセージのロギング中にタイムスタンプを保証するためのセキュリティポリシーですが、タイムスタンプが失敗すれば、メッセージ交換も失敗し、Security Server への負荷が増加するとともに、タイムスタンプサービスへの負荷も増加します。デフォルトでは、パフォーマンスと可用性を向上させるために、このパラメーター値は false になっています。パラメーター値が false になっている場合、タイムスタンプは定期的なバックグラウンドプロセスとして行われる(期間は PlanetCross 監督機関によって決定され、グローバルコンフィギュレーションを介して Security Server に伝播されます)。決定された期間内に保存された署名に(parameter timestamp-records-limit を参照)は、1 つのバッチでタイムスタンプが発行されます。
2. timestamp-records-limit - 一つのバッチでタイムスタンプできる署名されたメッセージの最大数です。このパラメーターのデフォルト値を変更するときは、メッセージ交換負荷(1 分あたりのメッセージ数)と Security Server のタイムスタンプ間隔を考慮する必要があります。正当な理由がなければ、このパラメーターを変更しないでください。デフォルトは 10000 です。
3. acceptable-timestamp-failure-period - Security Server 間のメッセージ交換が停止する前に、非同期的タイムスタンプの失敗が許可される時間を秒単位で示します。このチェックを無効にするためには 0 に設定します。デフォルトは 14400 です。

9.1.3 アーカイブパラメーター

1. **keep-records-for** - タイムスタンプとアーカイブされたレコードをデータベースに保存する日数です。デフォルトは 30 です。
2. **archive-max-filesize** - アーカイブファイルの最大バイトサイズです。最大値に達すると、ファイルのローテーションがトリガーされます。デフォルトは 33554432 (32 MB)です。
3. **archive-interval** - タイムスタンプ付きレコードをアーカイブするための Cron 式[CRON]としての時間間隔です。デフォルトは 0 0 0/6 1/1 *? *(6 時間ごとにアーカイブします)。
4. **archive-path** - タイムスタンプ付きログレコードがアーカイブされるディレクトリです。デフォルトは /var/lib/xroad/ です。
5. **clean-interval** - データベースからアーカイブされたレコードをクリーニングするための Cron 式[CRON]としての時間間隔。デフォルトは 0 0 0/12 1/1 *? * (12 時間ごとにクリーニングする)です。
6. **archive-transfer-command** - (定期的な)アーカイブ処理の後に実行されるコマンドです。この設定を使用して、Security Server からアーカイブファイルを自動的に転送するための外部スクリプトを設定することができます。デフォルトでは動作なしです。

システムの負荷とリソースの状況により、古いデータベースレコードの削除間隔を変更する必要がある場合があります。

keep-records-for-days というパラメーターは、たとえば、クリーンアップが発生する前にディスクがいっぱいになる場合、または 7 日間のデフォルト期間が短すぎる場合などに調整します。

clean-interval (Cron 式[CRON])というパラメーターは、システムがクリーンアップを実行する必要性を確認する頻度を定義します。デフォルトの期間である 12 時間が長すぎたり短すぎたりする場合は、必要に応じて調整します。

9.2 メッセージログの取得レベルとサイズの設定

9.2.1 メッセージログの取得レベルの設定

メッセージログには、デフォルト設定では SOAP メッセージのボディ部も含みます。Security Server を通るリクエスト、レスポンスに個人情報など Security Server のメッセージログに保存するべきでない情報がある場合には、Security Server 単位、サブシステム単位でボディ部をログに含める/含めないを切り替えることができます。
詳しくは X-Road: System Parameters User Guide を参照してください。

例えば、SOAP メッセージのボディ部を保持しない設定するためには/etc/xroad/conf.d/local.ini ファイルを編集し、以下を追記します。

```
[message-log]
soap-body-logging = false
```

9.2.2 メッセージログのサイズの設定

メッセージログをファイルシステムに保存する際に必要とするファイルサイズについて以下に見積方法を示します。

それぞれの SOAP リクエストは 9.5 kB のメタデータ(SOAP ネームスペース定義、ヘッダー、署名)を含みます。レスポンスメッセージは 11.2 kB のメタデータを含みます。さらに、1 分に一度 Security Server は前回タイムスタンプ付加を行った以降に処理したメッセージについて、バッチタイムスタンプを付加し、3.6 kB/分のメタデータを付加します。メッセージログの容量は以下のように表すことができます。

- 3.6kB + N * (21kB + R + A) = S
- N = 1 分あたりのリクエスト数
- R = リクエストのペイロードのサイズ (kB)
- A = レスポンスのペイロードのサイズ (kB)
- S = 1 分あたりのディスクの使用量 (kB / min)

9.3 Security Server からのアーカイブファイルの転送

ハードディスクの空き容量を節約するために、定期的にアーカイブファイルを Security Server から(手動または自動で)外部のロケーションに転送することを推奨します。

アーカイブファイル(ZIP コンテナー)は、設定パラメーター archive-path で指定されたディレクトリにあります。ファイル名は mlog-XYZ.zip の形式です。X は最初のメッセージログレコードのタイムスタンプ(UTC time in the format YYYYMMDDHHmmss)、Y は最後のメッセージログレコードのタイムスタンプ 、Z は 10 文字の長さの英数字のランダムです。次はアーカイブファイル名の実例です。

mlog-20150504152559-20150504152559-a7JS05XAJC.zip

メッセージログパッケージは、アーカイブファイルを転送するためのヘルパースクリプト /usr/share/xroad/scripts/archive-http-transporter.sh を提供します。このスクリプトはアーカイブファイルをアーカイブサーバへ転送するために HTTP / HTTPS プロトコル(POST 方法、フォーム名はファイル)を使用します。

スクリプトの使用法:

オプション	説明
-d, --dir DIR	アーカイブディレクトリ。デフォルトは /var/lib/xroad
-r, --remove	正常にアーカイブディレクトリから移動したファイルを削除します。
-k, --key KEY	PEM 形式の秘密鍵ファイル名。TLS 用。デフォルトは /etc/xroad/ssl/internal.key
-c, --cert CERT	PEM 形式のクライアント証明書ファイル。TLS 用。デフォルトは /etc/xroad/ssl/internal.crt
-cacert FILE	ピアを確認するための CA 証明書ファイル。TLS 用。このファイルは複数の CA 証明書を含む場合がある 証明書は PEM 形式でなければなりません。
-h, --help	このヘルプテキスト。

アーカイブサーバが HTTP ステータスコード 200 を返すと、アーカイブファイルは正常に転送されています。

転送スクリプトを設定するためには、設定パラメーターの archive-transfer-command をオーバーライドします(/etc/xroad/conf.d/local.ini ファイルを作成または編集する)。たとえば:

```
[message-log]
archive-transfer-command=/usr/share/xroad/scripts/archive-http-transporter.
sh -r http://my-archiving-server/cgi-bin/upload
```

メッセージログパッケージには、テストおよび開発するためにデモアーカイブサーバ用 CGI スクリプト/usr/share/doc/xroad-addon-messagelog/archive-server/demo-upload.pl を含みます。

9.4 リモートデータベースの使用

メッセージログデータベースは、Security Server の外部に置くことができます。次のガイドでは、メッセージログのためにリモートデータベーススキーマを設定および作成する方法について説明します。Security Server からデータベースへのアクセスが設定されていることを前提としています。

1. リモートデータベースホストにデータベースユーザーを作成します。

```
postgres@db_host:~$ createuser -P messagelog_user
Enter password for new role: <messagelog_password>
Enter it again: <messagelog_password>
```


2. リモートデータベースホストでメッセージログ、ユーザーが所有するデータベースを作成します。

```
postgres@db_host:~$ createdb messagelog_dbname -O messagelog_user -E
UTF-8
```

3. Security Server からリモートデータベースへの接続を確認します。

```
user@security_server:~$ psql -h db_host -U messagelog_user
messagelog_dbname
Password for user messagelog_user: <messagelog_password>
psql (9.3.9)
SSL connection (cipher: DHE-RSA-AES256-GCM-SHA384, bits: 256)
Type "help" for help.
messagelog_dbname=>
```

4. 設定のために xroad-proxy サービスを停止します。

```
root@security_server:~ # service xroad-proxy stop
```

5. /etc/xroad/db.properties で、暗号化された接続を実現するためにデータベース接続パラメーターを設定します。

```
messagelog.hibernate.jdbc.use_streams_for_binary = true
messagelog.hibernate.dialect =
ee.ria.xroad.common.db.CustomPostgreSQLDialect
messagelog.hibernate.connection.driver_class = org.postgresql.Driver
messagelog.hibernate.connection.url =
jdbc:postgresql://db_host:5432/messagelog_dbname?
ssl=true&sslfactory=org.postgresql.ssl.NonValidatingFactory
messagelog.hibernate.connection.username = messagelog_user
messagelog.hibernate.connection.password = messagelog_password
```

6. メッセージログアドオンパッケージの再インストールによって、データベーススキーマを作成します(xroad-proxy サービスも開始します)。

```
root@security_server:~ # apt-get install –reinstall
xroad-addon-messagelog
```


10. 監査ログ

Security Server は監査ログを保持します。監査ログイベントは、ユーザーがシステムの状態または設定を変更する時にユーザーインターフェイスによって作成されます。ユーザーのアクションは、結果が成功か失敗かに関係なく記録されます。監査ログイベントの完全なリストは、[SPEC-AL]に記述されています。

ユーザーインターフェイスを介して実行されていないシステム状態や設定を変更するアクションはログに記録されていません(たとえば、PlanetCross ソフトウェアのインストレーションとアップグレード、ユーザーの作成とアクセス権の付与、設定ファイルの変更など)。

監査ログレコードは以下を含みます。

- ユーザーアクションの説明
- イベントの日時
- アクションを実行しているユーザーのユーザー名
- イベントに関連するデータ

たとえば、新しいクライアントを Security Server に登録すると、次のログレコードが作成されます。

```
2015-07-03T10:21:59+03:00 my-security-server-host INFO [X-Road Proxy UI]
2015-07-03 10:21:59+0300 - {"event":"Register client", "user":"admin1",
"data":{"clientIdentifier":{"xRoadInstance":"EE", "memberClass":"COM",
"memberCode":"member1"},"clientStatus":"registration in progress"}}
```

イベントは、マシンの処理能力を確保するために、JSON [JSON]形式で表示されます。イベントフィールドは、イベントの説明を表し、ユーザーフィールドは、実行者のユーザー名を表し、データフィールドは、イベントに関連するデータを表します。失敗したアクションイベントレコードは、追加としてエラーメッセージの理由のフィールドを含みます。たとえば:

```
2015-07-03T11:55:39+03:00 my-security-server-host INFO [X-Road Proxy UI]
2015-07-03 11:55:39+0300 - {"event":"Log in to token failed", "user":"admin1",
"reason":"PIN incorrect", "data":{"tokenId":"0", "tokenSerialNumber":null,
"tokenFriendlyName":"softToken-0"}}
```

デフォルトでは、監査ログはファイルにあります。

/var/log/xroad/audit.log

10.1 監査ログの設定の変更

PlanetCross ソフトウェアは、UDP インターフェイス(デフォルトポートは 514)を使用して監査ログを syslog (rsyslog)に書き込みます。該当する設定は以下のファイルにあります。

```
/etc/rsyslog.d/90-udp.conf
```

監査ログレコードは、レベル INFO およびファシリティ LOCAL0 で書き込まれます。デフォルトでは、そのレベルとファシリティのログレコードは PlanetCross 監査ログファイルに保存されます。

```
/var/log/xroad/audit.log
```

デフォルトの動作は、rsyslog 設定ファイルを編集することで変更できます。

```
/etc/rsyslog.d/40-xroad.conf
```

設定ファイルの変更を追加するために rsyslog サービスを再起動します。

```
$ sudo systemctl rsyslog restart
```

監査ログは、logrotate によって毎月ローテーションされます。監査ログのローテーションを設定するためには、logrotate 設定ファイルを編集します。

```
/etc/logrotate.d/xroad-proxy
```

10.2 監査ログのアーカイブ

ハードディスクスペースを節約し、Security Server のクラッシュ中に、監査ログレコードが失われないようにするためには、監査ログファイルを定期的に外部ストレージまたはログサーバにアーカイブすることを推奨します。

PlanetCross ソフトウェアは、監査ログをアーカイブするために特別なツールを提供しません。

rsyslog は、監査ログを外部ロケーションにリダイレクトするように設定できます。

付録 A. サブシステム命名のベストプラクティス

本付録は、PlanetCross のサブシステムの名前付けガイドラインです。

A.1 サブシステムとは

PlanetCross のメンバーは、PlanetCross サービスを提供またはそれを利用するために、情報システムを Security Server にサブシステムとして登録する必要があります。

サブシステムとは、

アクセス権の付与は PlanetCross メンバーのサブシステムに対して行われるのであって、企業としての PlanetCross メンバーに対してではありません。サブシステムにより提供されるサービスとサブシステムへのアクセス権は、そのメンバーのその他サブシステムにより提供されるサービスからは独立しています。

A.2 サブシステム命名ガイドライン

同じメンバーの各サブシステムには、以下のガイドラインに従ってユニークな名前を付ける必要があります。

PlanetCross のサブシステムを定義するために、下記事項の扱い方や考え方に関して、どのようにその企業が(サービスを提供するための、あるいは利用するための)情報システムを分析し分類するかを最初に考慮します。

- 同じ法的根拠上で動作しているシステム
- 同レベルのセキュリティアクセスを備えるシステム
- 同じ技術的な仕組み上で動作しているシステム(すべて外部にホストされているなど)

次の特徴を持つ名前を選択します。

- 読みやすい
- 提供されるサービスまたは利用されるサービスを意味している、あるいは関連している
- 明確である
- 首尾一貫している
- スケーラブルである
- 柔軟である

A.3 サブシステム名に使用可能な文字

- 小文字アルファベット
- サブシステム名のキーエレメントを区別したり、切り離したりする必要がある場合は区切り文字 — (ダッシュ)も使用可能

付録 B. CRON を使用した設定の定期的なバックアップ

Security Server 設定のバックアップは、以下のスクリプトおよび cron ジョブを使用して、毎日行うことができます。

ログを別の場所に自動的に転送するには、rsync を使用します。rsync の自動転送をセットアップするには、下記の手順を参照してください。

下記の手順の以下の文字列は、それぞれの環境に応じて置き換えてください。

- [SERVER_CODE] - 各自の Security Server コードに置き換えます(Security Server の UI を開いたときに左上隅に表示されます)。
- [XROAD_BACKUP_STORAGE_SERVER_IP_OR_HOSTNAME] - バックアップストレージサーバーの IP アドレスまたはホスト名に置き換えます。

B.1 バックアップスクリプト

端末からバックアップスクリプトを実行するには、xroad ユーザーで以下のコマンドを発行してください。

```
$ /usr/share/xroad/scripts/backup_xroad_proxy_configuration.sh -s
[SERVER_CODE] -f /var/lib/xroad/backup/conf_backup_`hostname`_`date
+¥%Y¥%m¥%d-¥%H¥%M¥%S`.tar
```

このスクリプトの出力は以下のようになります。

```
...

Backup file saved to
/var/lib/xroad/backup/conf_backup_xrd-ss-01.test.avenuecross.com_20181023-1
41110.tar
```

B.2 Cron の設定

バックアップを定期的に実行するには、上記のスクリプトを使用して自動バックアップを行うよう Cron を設定する必要があります。

端末で xroad ユーザーで crontab -e を実行した後、Cron の設定を行います。

```
$ su - xroad
$ crontab -e
```

以下は、バックアップを実行するための Cron の設定例です。

Cron の設定に以下を追加します。

```
0 0 * * * /usr/share/xroad/scripts/backup_xroad_proxy_configuration.sh -s
[SERVER_CODE] -f /var/lib/xroad/backup/conf_backup_`hostname`_`date
+¥%Y¥%m¥%d-¥%H¥%M¥%S`.tar > /dev/null 2>>
/var/log/xroad/auto_backup_warnings.log
```

この設定では、毎日 00:00 にバックアップが実行され、バックアップファイルが /var/lib/xroad/backup に保存されます。

また、すべての警告が/var/log/xroad/auto_backup_warnings.log に出力されます。

B.3 リモートバックアップストレージサーバーへの RSYNC

バックアップストレージサーバーと Security Server、またはクラスター化された Security Server を使用している場合はすべての Security Server ノードで行う操作を下記に示します。

設定が完了すると、バックアップストレージサーバーのバックアップは以下のような構造になります。

```
Backups
└ [SERVER_CODE]
    └ YEAR
        └ MONTH
            └ HOSTNAME
                ├ conf_backup_xrd-ss-01.test.avenuecross.com_20181023-143201.tar
                └ conf_backup_xrd-ss-01.test.avenuecross.com_20181023-143301.tar
```

B.3.1 バックアップストレージサーバーの設定

バックアップストレージサーバーで、新しい ssh ユーザーを作成します。

```
$ sudo adduser --system --shell /bin/bash xroad-backups
```

.ssh フォルダと authorized keys ファイルを作成します。

```
$ sudo mkdir -m 750 -p /home/xroad-backups/.ssh && sudo touch
/home/xroad-backups/.ssh/authorized_keys
```

バックアップファイルと Security Server コードを転送するフォルダを作成して、xroad-backups ユーザーがアクセスできるよう許可します。

```
$ sudo mkdir -m 750 -p /home/xroad-backups/backups/[SERVER_CODE]/ && chown
xroad-backups -R /home/xroad-backups/
```


B.3.2 Security Server の設定

注) 以下のコマンドは root 権限で実行してください。

Security Server またはすべての Security Server ノードで、xroad ユーザー用にパスフレーズなしで ssh キー(ssh-keygen)を作成します(存在しない場合)。

```
$ su - xroad -c '/usr/bin/ssh-keygen -b 4096'
```

このキーおよび公開キーは以下のフォルダに格納されます。

```
/var/lib/xroad/.ssh/id_rsa
/var/lib/xroad/.ssh/id_rsa.pub
```

バックアップストレージサーバーマシンの/home/xroad-backups/.ssh/authorized_keys に公開キーを追加します。

Security Server から、ホストキーを受け入れ、ssh を使用してバックアップストレージサーバーマシンに接続します。

```
$ sudo ssh-keyscan -H [XROAD_BACKUP_STORAGE_SERVER_IP_OR_HOSTNAME] >
/var/lib/xroad/.ssh/known_hosts
```

```
$ su - xroad -c "ssh
xroad-backups@[XROAD_BACKUP_STORAGE_SERVER_IP_OR_HOSTNAME]"
```

Security Server で、xroad ユーザーで crontab を編集します。

```
$ su – xroad
$ crontab -e
```

crontab 設定に以下を追加します。

```
10 0 * * * /usr/bin/rsync -azq --timeout=10 --remove-source-files --log-file
'/var/log/xroad/backup-transferring.log' --include '*.tar' --exclude
'.*'--exclude '*' --rsync-path 'mkdir -p
/home/xroad-backups/backups/[SERVER_CODE]/`date +¥%Y`/`date
+¥%m`/`hostname`/ && rsync' /var/lib/xroad/backup/
xroad-backups@[XROAD_BACKUP_STORAGE_SERVER_IP_OR_HOSTNAME]:/home/xroad-back
ups/backups/[SERVER_CODE]/`date +¥%Y`/`date +¥%m`/`hostname`/
```

ログが正常に転送されるまでエラーが発生しないか監視します。

```
$ tail -f /var/log/xroad/backup-transferring.log
```


付録 C. メッセージログのアーカイブ設定

メッセージログの目的は、Security Server を通したリクエストとレスポンスを受け付けたことを第三者に証明する手段を提供することです。全てのリクエストとレスポンスについて、Security Server は署名とタイムスタンプを付加したドキュメント(Associated SignatureContainer ASiC)を生成します。

メッセージログはメッセージの交換時には Security Server のデータベースに保存します。

Security Server は定期的に、データベースからタイムスタンプの付加が完了したメッセージログを取り出し、ローカルファイルシステムにアーカイブファイルとして保存します。アーカイブファイルは 1 つ以上の署名済、タイムスタンプ済ドキュメントと完全性の検証のためのメタデータを含みます。

C.1 メッセージログの設定ファイル

メッセージログの設定ファイルはデフォルトでは以下の ini ファイルにあります。

```
/etc/xroad/conf.d/addons/message-log.ini
```

デフォルト設定を上書きするためには、以下のファイルを作成するか編集してください。

```
/etc/xroad/conf.d/local.ini
```

上記ファイル内になければ [message-log] section を作成しその下にパラメーターを 1 行ずつ書いてください。

C.2 パラメーター一覧

以下に主要なパラメーターを抜粋します。

- keep-records-for - データベースにメッセージログを保持する期間です。単位は 日。デフォルトは 30 です。
- archive-max-filesize - アーカイブファイルの最大サイズ。単位は Byte。最大サイズを超えると次のファイルに書きます。デフォルトでは 32MB です。
- archive-interval - メッセージログをアーカイブするインターバルです。デフォルトでは "0 0 0/6 1/1 * ? *" です。
- archive-path - メッセージログをアーカイブする先のディレクトリです。デフォルトでは /var/lib/xroad/ です。
- clean-interval - データベースからアーカイブされたメッセージログを消去するインターバルです。デフォルトでは「0 0 0/12 1/1 * ? *」です。
- archive-transfer-command - 定期的なアーカイブ後に実行されるコマンドです。外部スクリプトを起動しファイルを転送することができます。デフォルトでは「なし」です。

C.3 メッセージログのアーカイブファイルの転送設定

ディスクの使用量を減らし障害時の影響を抑えるため、アーカイブファイルを定期的に Security Server から外部に転送することを推奨します。

上記の archive-transfer-command を設定することで自動的にアーカイブファイルを転送することができます。ここでは rsync を使用した方法について案内します。

以下の文字列は環境に応じて変更してください。

[SS_OR_SS_CLUSTER_FQDN] - Security Server の FQDN、または Security Server クラスターの FQDN に変更してください。

[XROAD_ARCHIVE_SERVER_IP_OR_HOSTNAME] - アーカイブ先のサーバーの IP またはホスト名に変更してください。

アーカイブ先のサーバーと Security Server では以下の手順を実行します。手順の完了後には、アーカイブ先サーバーの以下のようなディレクトリ階層にファイルを保存します。Security Server が 1 台構成の場合と、クラスター構成の場合を上下に分けて表示しています。

```
mlogs
├── [SS_FQDN]
    └── YEAR
        └── MONTH
            ├── [SS_FQDN]
            └── ├── mlog-20181009200637-20181009200637-qbZAuY32az.zip
                └── ...
└── [SS_CLUSTER_FQDN]
    └── YEAR
        └── MONTH
            ├── [CLUSTER_NODE_1]
            │   ├── mlog-20181009193003-20181009193003-475iIYTxSM.zip
            │   └── ...
            └── [CLUSTER_NODE_2]
                ├── mlog-20181009185003-20181009185003-kQ5FqMZWnb.zip
                └── ...
```

C.3.1 アーカイブ先サーバーの設定

xroad-archive ユーザーを作成します。

```
$ sudo adduser --system --shell /bin/bash xroad-archive
```

.ssh ディレクトリと authorized_keys ファイルを作成します。

```
$ sudo mkdir -m 755 -p /home/xroad-archive/.ssh && sudo touch
/home/xroad-archive/.ssh/authorized_keys
```

ファイルを保存するディレクトリを作成し、xroad-archive ユーザーに書き込み権限を与えます。

```
$ sudo mkdir -m 755 -p /home/xroad-archive/[SS_OR_SS_CLUSTER_FQDN]/ && chown
xroad-archive /home/xroad-archive/[SS_OR_SS_CLUSTER_FQDN]/
```

C.3.2 Security Server の設定

まだ存在していなければ、xroad UNIX ユーザーの SSH キーをパスフレーズ無しで作成してください。クラスター構成の場合には、Slave ノードには SSH キーは既に存在するはずです。

```
$ su - xroad -c '/usr/bin/ssh-keygen -b 4096'
```

秘密鍵と公開鍵は以下に生成されます。

```
/var/lib/xroad/.ssh/id_rsa
/var/lib/xroad/.ssh/id_rsa.pub
```

公開鍵をアーカイブ先サーバーの/home/xroad-archive/.ssh/authorized_keys に配置してください。

Security Server からアーカイブ先サーバーに SSH 接続し、アーカイブ先サーバーの公開鍵を受け入れます。

```
$ su - xroad -c "ssh xroad-archive@[XROAD_ARCHIVE_SERVER_IP_OR_HOSTNAME]
```

/etc/xroad/conf.d/local.ini 設定ファイルを開き、[message-log]セクションを編集します。

```
[message-log]
archive-transfer-command=/usr/bin/rsync -azq
--timeout=10 --remove-source-files
--log-file '/var/log/xroad/mlog-archiving.log' --include '*.zip' --exclude
'.*' --exclude '*' --rsync-path 'mkdir -p
/home/xroad-archive/mlogs/[SS_OR_SS_CLUSTER_FQDN]/`date +%Y`/`date
+%m`/`hostname`/ && rsync' /var/lib/xroad/
xroad-archive@[XROAD_ARCHIVE_SERVER_IP_OR_HOSTNAME]:/home/xroad-archive/mlo
gs/[SS_OR_SS_CLUSTER_FQDN]/`date +%Y`/`date +%m`/`hostname`/
```

xroad-proxy service を再起動します。

```
$ sudo systemctl restart xroad-proxy
```

エラーの記録がログに表れないか確認します。

```
$ sudo tail -f /var/log/xroad/mlog-archiving.log
```


C.4 本番環境のメッセージログのアーカイブ設定

メッセージログの耐障害性が重要となる場合には、メッセージログを Security Server に蓄積する期間を最小にするべきです。以下にそのための設定例を記載します。本書の「9.1 メッセージログの設定の変更」を参考にして、設定ファイル/etc/xroad/conf.d/local.ini を編集してください。

- keep-records-for=0 (0 day)
- archive-max-filesize=104857600000 (100 MB)
- archive-interval=0 0/1 * 1/1 * ? * (毎分アーカイブを行う)
- clean-interval=0 0/5 * 1/1 * ? * (5 分おきにアーカイブされたメッセージログをデータベースから消去する)

付録 D. 大容量クエリーのための設定

Security Server で大容量クエリー（WSDL サイズが 100MB 以上）を扱う場合、以下の設定を組み合わせて設定することで処理可能なクエリーサイズを拡張できます。

D.1 SWAP の有効化

OS の SWAP を有効化することで処理可能なクエリーサイズを拡張できます。以下は 1 GB のファイルを SWAP 領域として使用する設定例です。

```
$ sudo swapon -show
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.7G     0  1.7G   0% /dev
tmpfs           345M   36M  309M  11% /run
/dev/sda1        30G  4.0G   26G  14% /
tmpfs           1.7G  8.0K  1.7G   1% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           1.7G     0  1.7G   0% /sys/fs/cgroup
/dev/sdb1        50G   52M   47G   1% /mnt
tmpfs           345M     0  345M   0% /run/user/115
tmpfs           345M     0  345M   0% /run/user/1000

$ sudo fallocate -l 1G /swapfile
$ sudo chmod 600 /swapfile
$ ls -l /swapfile
-rw------- 1 root root 1073741824 Mar 26 07:20 /swapfile

$ sudo mkswap /swapfile
$ sudo swapon /swapfile
$ echo '/swapfile none swap sw 0 0' | sudo tee -a /etc/fstab
$ tail -n 1 /etc/fstab
/swapfile none swap sw 0 0

$ sudo swapon -show
NAME      TYPE  SIZE USED PRIO
/swapfile file 1024M 524K   -2
```

D.2 proxy Xmx の変更

ヒープ Xmx の確保領域を大きくすることで、処理可能なクエリーサイズを拡張できます。以下の設定では、Xmx に 1536MB 割り当てる例を示します。

```
$ sudo vi /etc/xroad/services/local.conf
```

以下を追記してください。-Xmx の後の値を環境に応じて修正してください。

```
PROXY_PARAMS=" -Xms100m -Xmx1536m -XX:MaxMetaspaceSize=80m ¥
-Djavax.net.ssl.sessionCacheSize=10000 ¥
-Dlogback.configurationFile=/etc/xroad/conf.d/proxy-logback.xml ¥
```

```
-Dxroad.proxy.clientHandlers=${CLIENT_HANDLERS#?} ¥
-Dxroad.proxy.serverServiceHandlers=${SERVICE_HANDLERS#?}"
```

設定後に、Security Server の全てのサービスを再起動してください。

D.3 SOAP ボディロギングの無効化

メッセージログに対して、SOAP のボディ部分をロギングしないように設定することで、処理可能なクエリーサイズを拡張できます。以下のファイルを修正してください。

```
$ sudo vi /etc/xroad/conf.d/local.ini
```

以下を追記してください。

```
[message-log]
soap-body-logging = false
```

設定後に、Security Server のサービス全てを再起動してください。

D.4 SOAP ボディロギングの制限値の変更

メッセージログに対して、SOAP のボディ部分をロギングするサイズの上限を大きくすることで、処理可能なクエリーサイズを拡張できます。以下のファイルを修正してください。

```
$ sudo vi /etc/xroad/conf.d/addons/message-log.ini
```

archive-max-file-size パラメーターを変更してください。Byte 単位で記載する必要があります。（default 32MB）

```
archive-max-filesize=33554432
```

設定後に、Security Server のサービス全てを再起動してください。

D.5 設定の組み合わせと効果の例

メモリーサイズ 4GB の例を以下に示します。N0.1 の設定例では WSDL サイズが最大 252MB の取り扱いが可能なことを示しています。

NO	設定条件				インプットデータ		変換データ
	SWAP の有効化	Xmx の変更	SOAP ボディロギングの無効化	SOAP ボディロギングの制限値変更	レコード数	合計レコードサイズ	WSDL サイズ
1	Yes(8G)	Yes(1.5G)	Yes	Yes(256MB)	390,000	190.8 MB	252MB
2	Yes(8G)	Yes(1.5G)	-	Yes(256MB)	300,000	146.8 MB	193MB
3	Yes(8G)	Yes(1.5G)	-	-	265,000	129.6 MB	171MB

改訂履歴

バージョン	日付	変更履歴
第 1 版	2019 年 2 月 28 日	初版発行
第 1.1 版	2019 年 3 月 29 日	文書内の表現を全体的に更新
		11 章、12 章を追加
		付録として、サブシステム命名のベストプラクティス、CRON を使用した Security Server 設定の定期的なバックアップ、メッセージログのアーカイブ設定、大容量クエリーのための設定を追加
第 1.2 版	2019 年 8 月 1 日	７章のアクセス権から「登録担当者」を削除
第 1.3 版	2020 年 2 月 5 日	商標についての記載を追加。フッターを更新