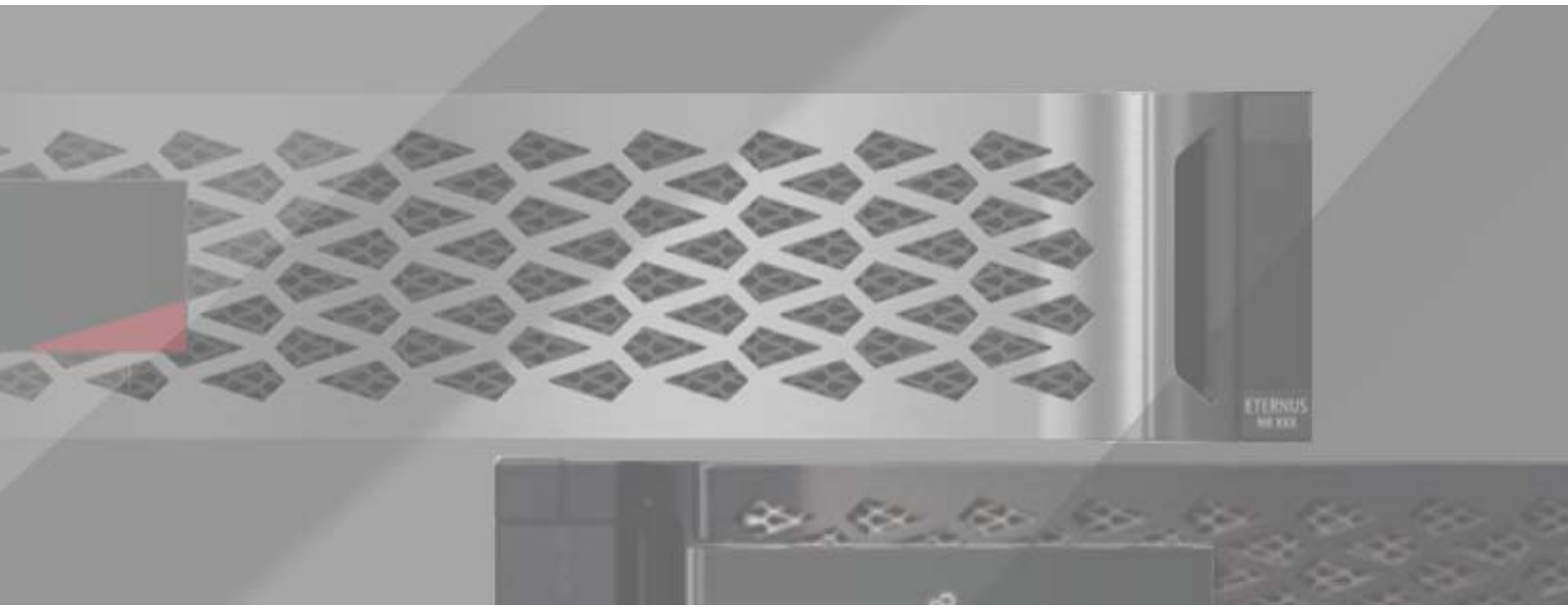
P3AG-6052-01Z0

FUJITSU Storage
ETERNUS AB series オールフラッシュアレイ ,
ETERNUS HB series ハイブリッドアレイ

# SANtricity 管理セキュリティ



機能の詳細と設定ガイド

FUJITSU

# 目次

# 図目次

# 表目次

# はじめに

FUJITSU Storage ETERNUS AB/HB series ストレージシステムは、SANtricity OS 11.60 で導入され、その後の SANtricity OS のリリースで強化された管理セキュリティ機能のコレクションを通じて、複数のユーザーにセキュアなロールベースのアクセス制御および監査可能な管理インターフェースを提供します。このレポートでは、ETERNUS AB2100/AB5100/AB6100 および ETERNUS HB1000/HB2000/HB5000 ストレージシステムの SANtricity System Manager セキュリティ機能について詳しく説明します。このレポートでは、SANtricity OS 11.60 で導入された管理セキュリティの更新についても説明します。



初版
2021 年 6 月

## 登録商標

本製品に関連する他社商標については、以下のサイトを参照してください。
https://www.fujitsu.com/jp/products/computing/storage/trademark/

本書では、本文中の ™、® などの記号は省略しています。

## 本書の読み方

### 対象読者

本書は、ETERNUS AB/HB の設定、運用管理を行うシステム管理者、または保守を行うフィールドエンジニアを対象としています。必要に応じてお読みください。

### 関連マニュアル

ETERNUS AB/HB に関連する最新の情報は、以下のサイトで公開されています。
https://www.fujitsu.com/jp/products/computing/storage/manual/

# 本書の表記について

## ■ 本文中の記号

本文中では、以下の記号を使用しています。

| | |
|---|---|
| 注 意 | お使いになるときに注意していただきたいことを記述しています。必ずお読みください。 |
| 備 考 | 本文を補足する内容や、参考情報を記述しています。 |

# 第 1 章
# SANtricity セキュリティー機能

ETERNUS AB2100/AB5100/AB6100 および ETERNUS HB1000/HB2000/HB5000 用の SANtricity OS ソフトウェアは、個々のシステムの安全な Web ベースのストレージ管理をサポートします。このアレイ・レベルの管理セキュリティに加えて、富士通は、SANtricity Unified Manager および SANtricity Web Services Proxy (WSP) におけるエンタープライズ･レベルのセキュアな管理をサポートしており、数百のシステムをセキュアに一元管理することができます。

組み込み型の Web サービス管理インフラストラクチャ、つまり SANtricity Unified Manager と SANtricity WSP を使用することにより、管理者は、ETERNUS AB/HB series コントローラ管理ポートおよび WSP Web サーバへの IP アクセスが可能なネットワーク・ブラウザ・クライアントからストレージシステムを管理できます。Web ベースのストレージ管理では、管理対象デバイスがプライベートおよびパブリック･ネットワークに公開されるため､ETERNUS AB/HB seriesのシステムとSANtricity WSP は、トランスポート・レイヤ・プロトコル、アクセス方式、アクセス制御などのさまざまなレベルで適切なセキュリティ・スキームをサポートし、認証と承認の側面を備えています。

SANtricity OS では、SANtricity System Manager GUI、セキュア CLI ( セキュア SMcli)、および API アクセス方式を使用してストレージのセットアップと管理機能を個々のシステム上でセキュアに実行するために、マルチユーザー管理という概念が導入されました。SANtricity WSP と SANtricity Unified Manager も同じレベルのセキュリティを提供します。

記憶域またはシステムの管理機能を実行するユーザーは、まず、ローカルで、または Lightweight Directory Access Protocol (LDAP) を使用するディレクトリサーバーで認証されます。認証が成功すると､割り当てられたロール ( ロールによるアクセス制御 [RBAC]) に従って管理タスクを実行できます。LDAP を使用する場合､ユーザーのロールはディレクトリサーバ内のユーザーのグループ設定に基づきます。ローカルユーザーの場合、アクセスロールは管理アクセス許可ワークフローの一部としてハードコードされ、パスワードは admin ユーザーによって管理されます。

SANtricity System Manager、SANtricity WSP、および Unified Manager を使用すると、システムと WSP でサポートされている複数のクライアント / サーバー関係間に信頼証明書 (Web サーバと CA ルート証明書または中間証明書 ) を設定する必要があるため、セキュリティがさらに強化されます。

- SANtricity WSP および SANtricity Unified Manager
- LDAPS サーバ
- Key Management Interoperability Protocol (KMIP) 準拠の外部暗号鍵管理サーバ
- ETERNUS AB/HB series システムでは、アクティブな操作に対するユーザー資格証明 ( ユーザー ID とパスワード ) が、安全な接続を使用して、ブラウザに直接、またはリストされている他の方法で、常に信頼できるエンティティに転送されるように、いずれかの方法で管理されます。

組み込みの監査ログをログサーバーにストリーミングすることで、アレイ上のイベントを追跡し、要件に合わせてログのレベルを調整できます。

最後に、Security Assertion Markup Language (SAML) 2.0 を使用した多要素認証を使用して、個別システムの管理インターフェースを保護できます｡SANtricity WSPおよびSANtricity Unified Manager は SAML をサポートしていないため、SAML を使用してシステムを検出および管理することはできません。ディレクトリサービスの代わりに多要素認証を使用する場合、ストレージアレイの管理には

SANtricity System Manager GUI のみを使用できます。すべての API アクセスを含むその他のすべての管理インターフェースが無効になります。
これらの管理セキュリティ機能は、SANtricity OS 11.60 以降を実行しているストレージシステムで使用できます。

# 第 2 章
# RBAC およびディレクトリサービス

さまざまな権限レベルを持つ複数のユーザーをサポートするため、富士通は、SANtricity OS 11.60 以降 (SANtricity WSP および SANtricity Unified Manager にも拡張 ) を実行するストレージシステムに組み込み型のディレクトリサービス統合および RBAC を導入しました。この実装は、SANtricity System Manager GUI および WSP API に適用されます。

RBAC スキームは、システム管理タスクを実行するための特定の権限セットを、システム定義のロールに関連付けます。これらのタスクを実行するユーザーは、適切なシステム定義のロールにマップされます。ユーザーが認証されると、関連付けられた認証が適用され、そのユーザーは管理アプリケーションまたは API へのアクセス権を持つ特定の権限を持つことができます。

ユーザーは、組み込みのロールを使用して定義され、Linux の 389 Directory Server または Windows の Active Directory (AD) といった、LDAP を使用するディレクトリサーバーのメンバーになることが可能です。

**注 意**

ローカルシステム上のユーザーロールには、変更できないユーザーアカウントと関連するロールの固定セットがあります。

新しい管理セキュリティ機能には、従来の SYMbol API インターフェースと HTTPS API インターフェースを切り替える構成オプションも含まれています (SYMbol は、ETERNUS AB/HB series ストレージシステムを管理するための Open Network Computing RPC インターフェースです )。SYMbol インターフェースを無効にすると、非セキュア・アクセス方式を使用するアレイへのアクセスがブロックされます。セキュリティ機能を有効にすると、HTTPS を使用している Web Services API が基盤となるインフラストラクチャ要素として機能し、ディレクトリサービスと RBAC を使用してシームレスなシステム構成オプションを提供します。

アレイ監査ログは、System Manager GUI、SMcli、Web Services API、およびサポートシェルを通じて、ストレージアレイ上でのユーザーのアクティビティを記録します。

**注 意**

従来の SYMbol アクセス方式によるアクティビティは、監査ログには記録されません。

図 2.1 は、ETERNUS AB/HB series システム、管理クライアント、ディレクトリサーバ間の論理接続関係を示しています。

図 2.1　ディレクトリサーバと RBAC を統合した ETERNUS AB/HB series の管理セキュリティ機能

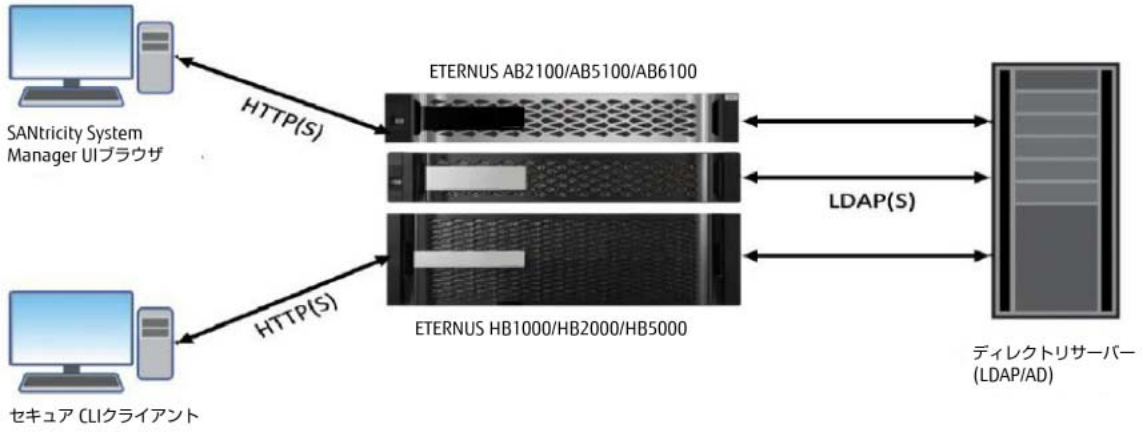
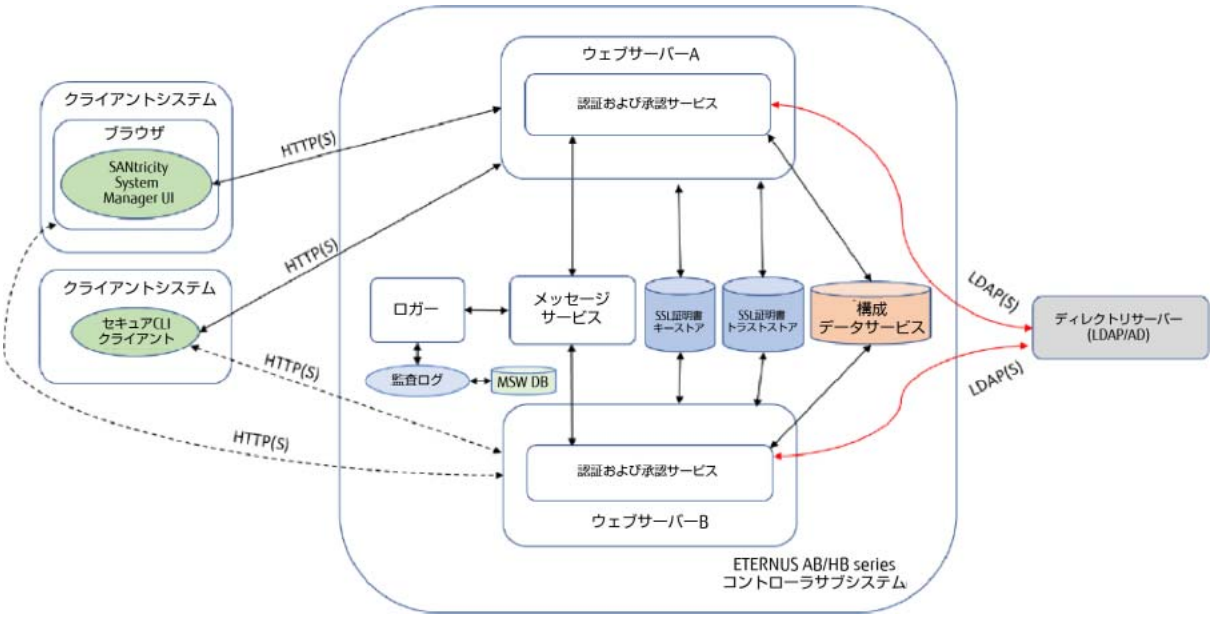



図 2.2 は、ETERNUS AB/HB series コントローラにおける認証ワークフローの論理的な内訳を示しています。

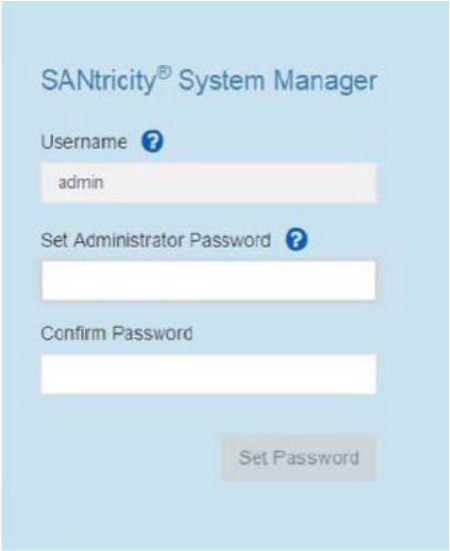
図 2.2　ETERNUS AB/HB series 管理セキュリティ機能の技術コンポーネント



# 2.1　ローカルユーザーパスワード

ストレージアレイをインストールし、SANtricity System Manager GUI を初めて開くと、ローカル管理者パスワードの設定を求めるプロンプトが表示されます。わかりやすくするために、Username フィールドはデフォルトで Admin に設定されていますが、図 2.3 に示すように、ユーザーはパスワードを入力して有効にする必要があります。また、SANtricity System Manager は、SYMbol API パスワードを admin アカウントと同じパスワードに設定します。パスワードは、ソルト化かつ SHA-256 ハッシュ化されて保存されます。

図 2.3　初期電源投入時の管理者ローカルパスワードの設定




SANtricity WSP および SANtricity Unified Manager では、工場出荷時のデフォルト・パスワードとして管理者アカウントが設定されています (user=admin/password=admin)。管理者が初めてログインするときは、管理者パスワードを変更できます。

admin ユーザーは、各ローカルユーザーのパスワードを設定できます。図 2.4 は、パスワードが設定されている SANtricity Unified Manager のスクリーン・ショットです。図 2.5 は、SANtricity System Manager からの同じビューを示しています。ほかのローカルユーザーアカウントのパスワードが設定されていない場合、これらのローカルユーザーアカウントにログインしようとするユーザーはアクセスを拒否されます。他のローカルユーザーアカウントを使用する予定がない場合は、他のユーザーアカウントパスワードを設定しなくてもストレージアレイは機能します。

**注 意**

admin ユーザーは、root admin ロールを持ち、ローカルユーザーのパスワードを設定または変更する権限を持つ唯一のユーザーです。

# 2.2　組み込みのロールとローカルユーザーアカウント

新しいセキュリティモデルは、RBAC の実装を強制します。これは、すべてのユーザーに一連の権限が割り当てられており、管理対象アレイのセットアップおよび管理機能に対して行う権限が定義されていることを意味します。つまり、ユーザーは 1 つ以上のシステム定義のロールに事前に割り当てられており、特定のロールによって委任された一連の許可された操作にアクセスできます。ロールオブジェクトは、よく使用される LDAP 属性を組み込んで、LDAP アクセス可能なユーザーおよびグループディレクトリからこの情報を簡単に取得できるように定義されています。

この機能には、次のロールが実装されています。

- monitor
  このロールは、すべてのストレージアレイプロパティへの読み取り専用アクセス権を付与します。このユーザーはセキュリティ構成を表示できません。

  **注 意**

  ストレージアレイにログインするには、すべてのユーザーに monitor ロールが必要です。その他のロールは、認証後にユーザーが実行できる操作を定義します。

- root admin
  これは、ユーザーがローカルユーザーのパスワードを変更し、アレイでサポートされているコマンドを実行できる唯一のロールです。monitor のロールと組み合わせると、root admin のロールによって、アレイ上のすべての機能にアクセスできます。

  **注 意**

  root admin ユーザー名は「root」ではなく「admin」です。その他のユーザー名は、security、storage、support、および monitor です。

- security admin
  このロールでは、監査ログの表示、安全な syslog サーバの設定、LDAP/LDAPS サーバ接続の設定、証明書の管理など、アレイのセキュリティ構成を変更できます。このロールには、プールやボリュームの作成 / 削除などのストレージアレイプロパティへの書き込みアクセス権はありませんが、読み取りアクセス権はあります。また、アレイへの SYMbol アクセスを有効 / 無効にする権限も持っています。
- storage admin
  このロールは、ストレージアレイプロパティに対する完全な読み取り / 書き込みアクセス権を持ちますが、セキュリティ構成機能を実行するためのアクセス権は持ちません。
- support admin
  このロールは、アレイ上のすべてのハードウェアリソース、障害データ、MEL/ 監査ログ、および CFW アップグレードにアクセスできます。
- rw
  これは、読み取り / 書き込み権限を持つ従来の WSP アカウントです。新世代のストレージシステムではサポートされていません。
- ro
  これは、読み取り専用のアクセス許可を持つ従来の WSP アカウントです。新世代のストレージシステムではサポートされていません。

図 2.4 と図 2.5 は、SANtricity Unified Manager および SANtricity System Manager GUI のユーザーアカウントとマップされたロールを示しています。
SANtricity Unified Manager で個々のユーザーアカウントを表示するには、[Access Management] タブに直接移動します。SANtricity System Manager を使用して個々のシステムのアカウントを表示するには、[Settings] に移動して [Access Management] タイルを開き、[Local User Roles] タブをクリックします。

図 2.4　SANtricity Unified Manager ローカルアカウントのパスワード管理

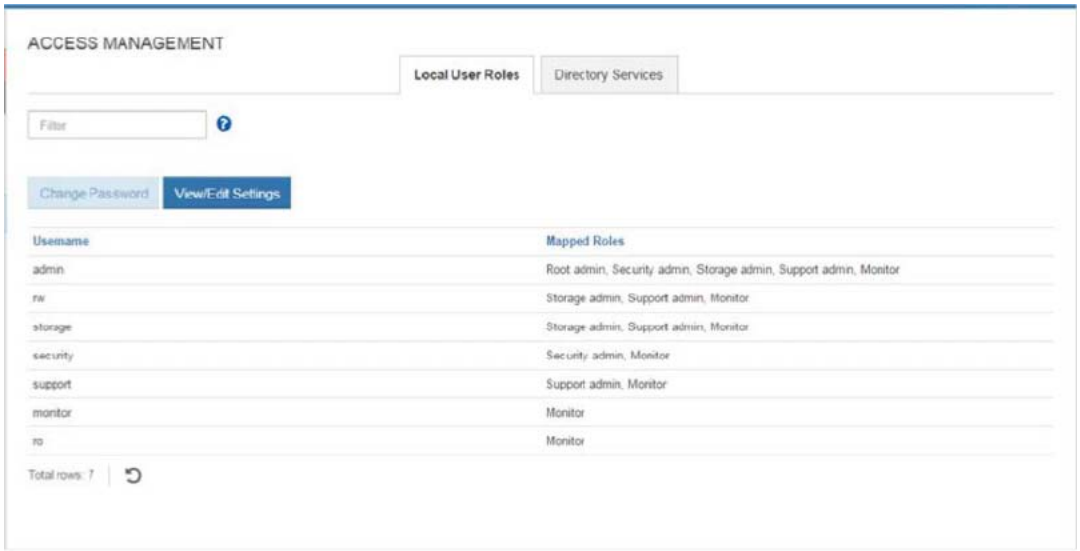
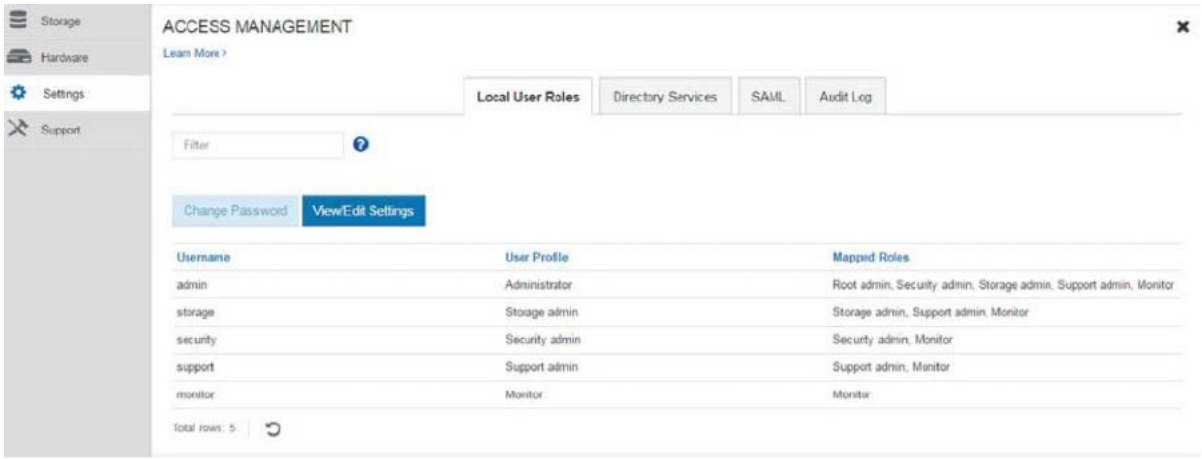



図 2.5　SANtricity System Manager アクセス管理 ( ローカルユーザーのロール ) 設定




ロールの割り当てに基づいて特定のストレージ管理機能にアクセスする権限を持つローカルユーザーまたはディレクトリユーザーは、ユーザー・インターフェース (System Manager GUI、セキュア SMcli、または REST API) の選択を通じて、許可された一連の操作を実行できます。

ユーザーがアレイを管理するために必要な最低限の権限セットは、monitor のロールに割り当てられます。アレイを管理する必要があるすべてのユーザーには、少なくとも monitor のロールが割り当てられている必要があります。ディレクトリサーバー内の特定のグループにロールを割り当てると、monitor のロールが自動的に割り当てられます。その他のアクセス許可レベルは、admin または security ユーザーが追加できます。

この機能は、定義された一連のローカルユーザーアカウントをサポートします。管理者は、定義済みのアカウント以外に新しいローカルユーザーアカウントをアレイに追加することはできません。また、定義済みのローカルユーザーアカウントを変更することもできません。

## 2.3　LDAP ユーザーおよびグループアカウントのマッピング

LDAP は、IP ネットワークを介して分散ディレクトリ情報サービスにアクセスし、保守するための、オープンでベンダーに依存しない業界標準のアプリケーション・プロトコルです。LDAP の一般的な使用によって、ユーザー名とパスワードを保管する中心的な場所が提供され、さまざまなアプリケーションやサービスを LDAP サーバーに接続してユーザーを検証できます。LDAP の詳細については、Wikipedia の LDAP のトピックを参照してください。

SANtricity OS が LDAP を介してユーザーを検証するには、Microsoft AD、Linux 389、またはその他のディレクトリサーバーで認証するように構成する必要があります。構成スキームを使用すると、ディレクトリサーバー構成の複数のインスタンスで複数の LDAP ドメインをサポートできます。各 LDAP ドメインには、LDAP サーバーの DNS ドメインと一致すると想定される名前がありますが、必須ではありません。Secure Sockets Layer (SSL) を使用して LDAP 用の証明書をセットアップするには、「5.2 SANtricity System Manager コントローラの証明書管理」(P.50) を参照してください。

ドメインには、ASCII 文字のみを含む有効な DNS 名であれば、任意の名前を付けることができます。表 2.1 は、ドメイン名に加えて、ディレクトリサーバー構成の一部としてサポートされる属性を示しています。

表 2.1　LDAP 構成パラメーター

| 名称 | 説明 |
|---|---|
| ドメイン名 | 有効な DNS 名で、a から z までの ASCII 文字 ( 大文字と小文字を区別しない )、0 から 9 までの数字、およびハイフン (-) のみを含み、ハイフンで始まらないもの。RFC 3629 および 4514 によると、識別名に関連付けられた文字列表現の ASN.1 から UTF-8 でエンコードされた Unicode 表現への変換が許可されています。 |
| LDAP URL | 次の形式で LDAP サーバーにアクセスするための URL。<br>`ldap[s]://host:port` |
| ユーザーバインド属性 ( フィルターベース ) | ユーザーを認証するために attribute=%s の形式でユーザー ID がバインドされる属性。%s はユーザー名に置き換えられます。これにより、柔軟性が大幅に向上します。 |
| 検索ベース | ユーザーを検索する LDAP コンテキスト。通常は次の形式です。<br>`CN=Users, DC=cpoc, DC=local` |
| グループ属性 | グループからロールへのマッピングを検索するユーザーのグループ属性のリスト。 |
| グループからロールへのマッピング | ロールに一致するユーザーのグループ属性に一致する正規表現パターンのリスト。 |
| バインドアカウントユーザー ID | LDAP サーバーに対する検索クエリやグループの範囲内での検索には、読み取り専用のユーザーアカウントが必要です。 |
| バインドアカウントパスワード | LDAP サーバーに対する検索照会やグループの範囲内での検索のための読み取り専用アカウントに関連付けられたパスワード。 |

図 2.6 はディレクトリサーバーセットアップウィザードを示し、図 2.7 は「Role Mapping」タブを示しています。このタブでは、ディレクトリサービスサーバーで定義されたユーザーとグループに、アレイに対するアクセス権限が割り当てられます。

**注 意**

図には SANtricity System Manager のスクリーンショットが示されていますが、SANtricity Unified Manager は同じセットアップウィザードをディレクトリサーバーに使用します。

図 2.6　SANtricity System Manager ディレクトリサーバー構成設定

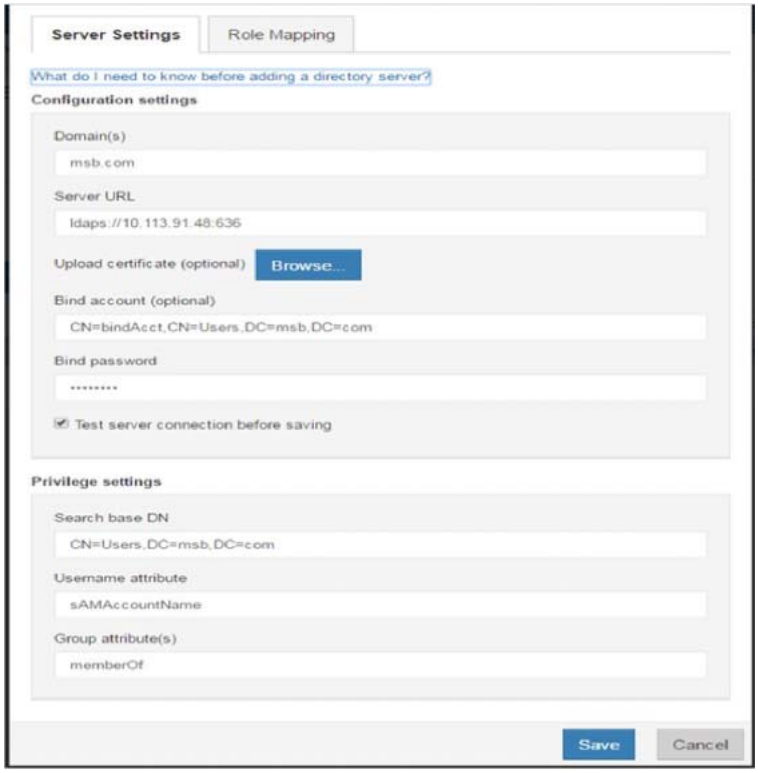
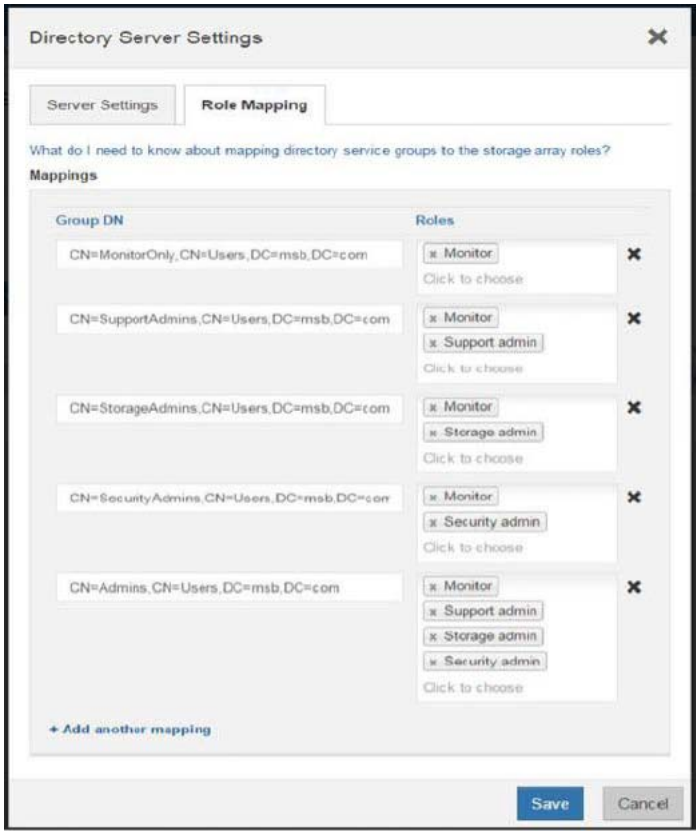


図 2.7　SANtricity System Manager ディレクトリサーバーのロールマッピング設定




ディレクトリユーザーがログインしようとすると、ユーザー ID とユーザーが指定したドメインが検索範囲を決定する基準になります。
ユーザー ID の形式は、次のいずれかになります。

- 標準メールアドレスパターン : user@domainname
- ドメイン名 \user。ここで、ドメイン名は LDAP 構成内のドメインに関連付けられた名前です。
- local

このフォーマットは、特定のユーザーを検証するためにどのユーザー・ベースを使用するかを明確に識別し、認証要求を転送するためにどのドメインを使用するかを決定するために必要です。ディレクトリサーバー内にグループを作成し、そこにユーザー名を入れる必要があります。

**注 意**

ディレクトリ内のユーザー名の自動検索はサポートされていません。

local というドメイン名は、ローカルユーザーアカウントデータベースを参照するために予約されています。ディレクトリサービスが設定されていない場合、ユーザー ID はローカルユーザーアカウントデータベースと照合されます。ディレクトリサービスが構成されると、user@local という形式のユーザー ID によって、ローカルユーザーアカウントデータベースに対する検証が開始されます。

2019 年 8 月 (2020 年 3 月更新 )、Microsoft はセキュリティアドバイザリ (ADV190023) を公開し、ユーザーが LDAP チャネルバインディングと LDAP 署名を有効にできるようにしました。Microsoft は、LDAP チャネルバインディングと LDAP 署名の現在のデフォルト設定が Active Directory ドメインコン

トローラ上に存在することを認めています。LDAP チャネルバインディングと LDAP 署名を強化することなく、Active Directory ドメインコントローラと LDAP クライアントとの通信が可能になっています。

**注 意**

SANtricity OS は LDAP チャネルバインディングと LDAP 署名の両方をサポートしていないため、今後のリリースで SANtricity OS が LDAP の 2 つの機能をサポートするまでは、LDAP の代わりに LDAP over SSL/TLS (LDAPS) を実装して LDAP 環境を強化することを強くお薦めします。

Microsoft は 2020 年 3 月 10 日のアップデートで、次の 2 つの変更を加えました。

- 変更 1:
  Microsoft では、LDAP 署名グループポリシーを手動で [Require Signing] に設定し、ディレクトリサービスのイベントログで LDAP 署名の失敗を監視することを推奨しています。LDAP 署名ポリシー設定とレジストリ設定の間のマッピングは次のとおりです。
  - ポリシー設定 : "Domain controller: LDAP server signing requirements"
  - レジストリ設定 : LDAPServerIntegrity
  - データ型 : DWORD
  - レジストリパス :
    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters

| グループポリシーの見出し | レジストリ設定 |
|---|---|
| Off | 0 |
| None | 1 ( デフォルト ) |
| Require Signing | 2 |

**注 意**

富士通では、ユーザーが LDAPS 用に構成されていない限り、今後のリリースで LDAP 署名をサポートするまで、このレジストリ設定を「0」(Off) または「1」(None) のいずれかに設定することを推奨しています。

- 変更 2:
  Microsoft は新しいドメインコントローラを追加しました。LDAP サーバーチャネルバインドトークン要件グループポリシー。サポートされているデバイス上で LDAP チャネルバインディングを構成します。LDAP チャネルバインディングポリシー設定とレジストリ設定の間のマッピングは次のとおりです。
  - ポリシー設定 : "Domain controller: LDAP server channel binding token requirements"
  - レジストリ設定 : LdapEnforceChannelBinding
  - データ型 : DWORD
  - レジストリパス :
    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters

| グループポリシーの見出し | レジストリ設定 |
|---|---|
| Never | 0 |
| When Supported | 1 ( デフォルト ) |
| Always | 2 |

**注 意**

今後のリリースで LDAP チャネルバインディングがサポートされるまで、このレジストリ設定を「0」(Never) または「1」(When Supported) のいずれかに設定することを推奨します。

# 第 3 章
# セキュア SMcli

セキュア SMcli を使用すると、SMcli クライアントはセキュアな HTTPS チャネルを介してストレージアレイとやり取りできます。従来の SMcli 文法とコマンドセマンティクスを使用し、安全なプロトコルでストレージシステムと相互運用できる HTTPS シンクライアントを提供します。

クライアントが配列に対して構文解析ロジックを提供しコマンドを実行する代わりに、セキュア SMcli はコマンド処理の大部分が行われるストレージアレイと対話する軽量ラッパーを提供します。

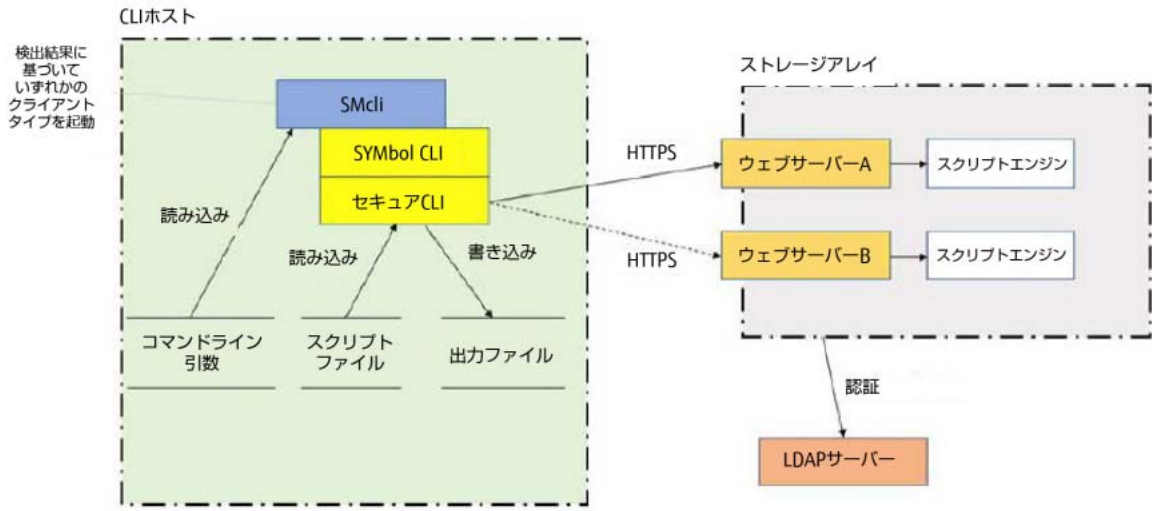
System Manager を介してセキュア SMcli パッケージをダウンロードできます。入手先は図 3.1 に示すように、Settings > System > Add-ons セクションの下にあります。

図 3.1　System Manager から SMcli をダウンロードする場所

# 3.1　セキュア SMcli 論理アーキテクチャ

セキュア SMcli がストレージシステムと直接やり取りする場合、アレイ・インターフェースの設定に応じて、従来の SYMbol インターフェースまたは HTTPS プロトコルを使用してストレージシステムと通信できます。図 3.2 は、SANtricity System Manager が管理する ETERNUS AB/HB series アレイへの SMcli ホストからの論理接続を示しています。

図 3.2　ストレージアレイに対して動作するセキュア SMcli の技術コンポーネント




**注 意**

デフォルトでは、ストレージシステムのレガシー SYMbol インターフェースは出荷時からアクティブになっています。アレイをセキュリティー保護されたインターフェースに変更するには、適切な CA ルート証明書、中間証明書、および署名付きサーバー証明書を両方のストレージアレイコントローラにインストールする必要があります。また、SANtricity System Manager GUI を使用して、アレイ管理インターフェースをセキュア・モードに変更する必要があります。図 3.3 および図 3.4 に示すように、GUI では Settings > System > Additional Settings の順に移動し、Change Management Interface を選択します。

図 3.3　管理インターフェースのセキュリティモードを変更するためのナビゲーション

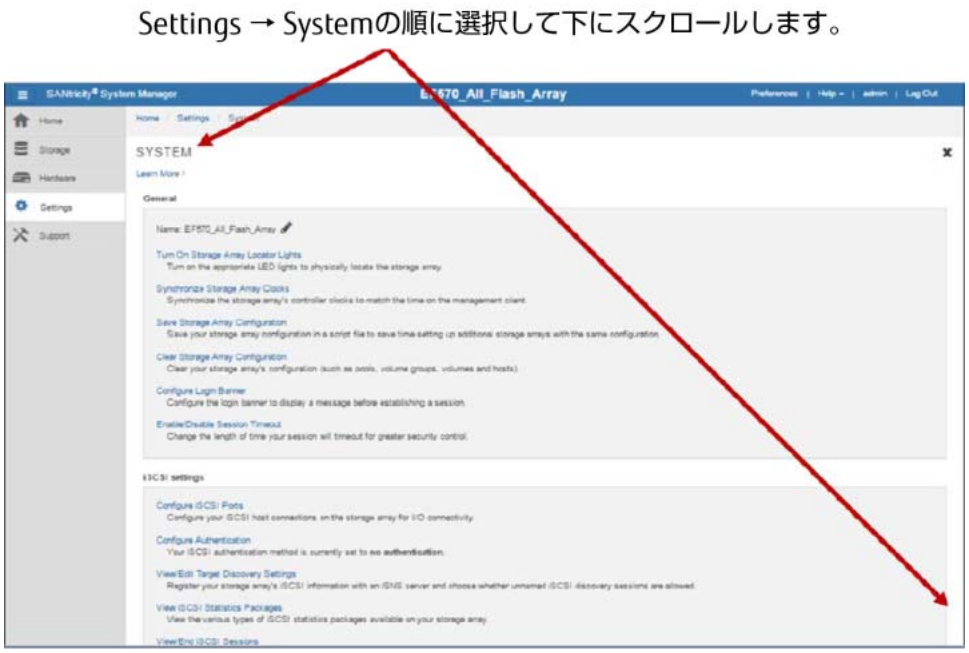
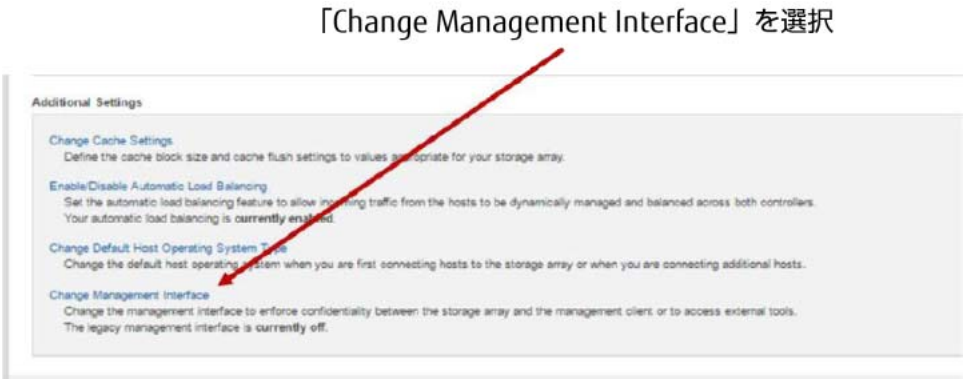



図 3.4　SANtricity System Manager GUI を使用した管理インターフェース・モードの変更




**注 意**

セキュリティー保護された通信を有効にするためのアレイ管理インターフェースの構成方法については、「第 5 章 証明書の管理」(P.28) を参照してください。

# 3.2　セキュア SMcli コマンドのフォーマット

セキュア SMcli 接続を確立するために、ユーザーは、特定のコマンドまたはセッションのコマンドラインでユーザー名とパスワードの両方を呼び出します。たとえば、セキュア SMcli を使用してストレージアレイの名前を変更するには、アレイ管理ポートに IP アクセスできる管理ステーションからコマンド・プロンプトを開きます。セキュア SMcli は、一方または両方のコントローラの SMcli コマンド文字列で指定されたホスト名または IP アドレスに基づいて、コントローラ A またはコントローラ B への管理パスを使用します。

**注 意**

SMcli をレガシー・モードまたはセキュア・モードで使用するには、管理ステーションに SANtricity System Manager 11.60 以降をインストールする必要があります。Windows の場合、インストール・ディレクトリは通常、C:\Program Files\SystemManager\client です。

SMcli.exe ファイルを含む Windows ディレクトリが表示されたら、セキュリティで保護されたコマンドまたはセキュリティで保護されていないコマンドを実行してストレージアレイ名を変更できます。

```
C:\Program Files\SystemManager\client>SMcli <Array management IP> -u <root admin or
storage admin username> -p <password> -c "set storageArray userLabel=\"EF570_All_-
Flash_Array\""; Performing syntax check...

Syntax check complete.

Executing script...

Script execution complete. SMcli completed successfully.

C:\Program Files\SystemManager\client>
```

**注 意**

Windows SMcli では、新しいアレイ名の前後にバックスラッシュを使用します。Linux ベースのコマンドラインを使用する場合は、スラッシュは必要ありません。

SMcli コマンド文字列における -u <username> の使用は、セキュリティで保護された接続が使用可能な場合に HTTPS を使用することを示します。セキュリティで保護された接続が使用できない場合、SMcli は SYMbol を代わりに使用します。アレイの管理インターフェースが secure に設定されている場合、アレイは有効なユーザー名とパスワードを含む SMcli コマンドのみを受け入れます。表 3.1 は、さまざまなアレイ・モデルおよびセキュリティ・モードとのコマンドラインのやり取りを示しています。

表 3.1　SMcli コマンドで -u <username> を使用した場合の接続動作

| コマンド構文 | ETERNUS AB2100/AB5100/AB6100 および ETERNUS HB1000/HB2000/HB5000; Legacy SYMbol- On | ETERNUS AB2100/AB5100/AB6100 および ETERNUS HB1000/HB2000/HB5000; HTTPS - On |
|---|---|---|
| ...> SMcli <IP Address> -u <username> -p <Password> -c <"command=\"argument\">"; | SMcli は、システムに対してレガシー SYMbol 接続を使用します。 | SMcli は、システムへのセキュアな HTTPS 接続を使用します。 |
| ...> SMcli <IP Address> -p <Password> -c <"command=\"argument\">"; | SMcli は、システムに対してレガシー SYMbol 接続を使用します。 | コマンドが失敗し、ネットワークエラーが検出されました。 |

-p|-P パラメータを使用すると、次を使用できます。

- -p "password"
- -P <file-name> | -

-p 形式を使用する場合、パスワードはクリア・テキストでコマンドラインに直接指定します。これは既存の動作と一致します。-P <file-name> 形式では、パスワードをファイルから読み取ることができます。-P を指定すると、標準入力からパスワードを読み取ることができます。

ユーザー名は -u <user-name> で指定します。ユーザー名は、次のいずれかの形式で指定できます。

- user-name@domain-name
  @ 記号の後のユーザーの資格情報を解決するために使用するドメイン名を指定します。
- domain-name\user-name
  \ の前にドメイン名を指定します。これは Microsoft Active Directory スタイルの慣習的な名前付けです。
- user-name
  ユーザー名だけを指定できます。ユーザー名がローカルアカウント名のいずれかと一致する場合は、それが使用されます。それ以外の場合は、デフォルトのディレクトリサービスドメイン名を使用してログインが試みられます。両方が失敗すると、ログインは失敗します。

ストレージシステムに対してセキュア SMcli コマンドを実行するための前提条件として、HTTPS でログインする必要があります。ユーザーは認証され、認証の許可はローカルアカウント情報またはディレクトリサーバーから取得されます。どちらの場合も、ログインしているユーザーには一連のロールがあります。

すべての SMcli コマンドには、これらのコマンドの実行を許可される一連のロールがあります。アレイに対する受信 SMcli 要求により、コマンドの実行前にロールチェックが実行されます。ユーザーにコマンドを実行するための十分なアクセス許可がない場合は、エラーが返され、コマンドの実行が終了します。SMcli からロールへのマッピングは設定されており、ユーザーは変更できません。

最後に、CA 署名証明書をアレイにインストールする前にセキュア SMcli コマンドを実行する場合は、コマンド文字列の IP アドレスの後に -k オプションを指定します。これにより、SMcli は HTTPS 接続のセットアップの一部として証明書をチェックしないようになります。これは、HTTPS を使用してブラウザに接続し、接続がセキュリティで保護されていないというセキュリティ警告を受け入れる場合と同じ条件です。
これは、コントローラに CA 署名証明書ではなく自己署名証明書が残っている場合です。

# 第 4 章
# 監査ログ

SANtricity OS には、監査証跡ログを通じてユーザー・アクティビティーを追跡する機能があります。セキュリティイベントが発生するセキュリティで保護されたアクセス方法のいずれかを使用してユーザーが操作またはコマンドを開始すると、エントリがログに記録されます。ログイン、認証、および認証アクティビティーを試みるユーザーも、セキュリティー・イベントを構成します。

監査ログの範囲は、ユーザーがアクセスできるすべてのセキュアなアクセスインターフェース(System Manager GUI、セキュア SMcli、シェルインターフェースのサポート、Web Services API) に拡張されますが、SYMbol API を使用してアクティビティのログを作成することはありません。ストレージシステムでディレクトリサービス認証が設定されている場合は、このインターフェースを介したユーザーアクセスを無効にできます。

表 4.1 は、さまざまなアクセス方式にわたる監査ログのスコープを示しています。

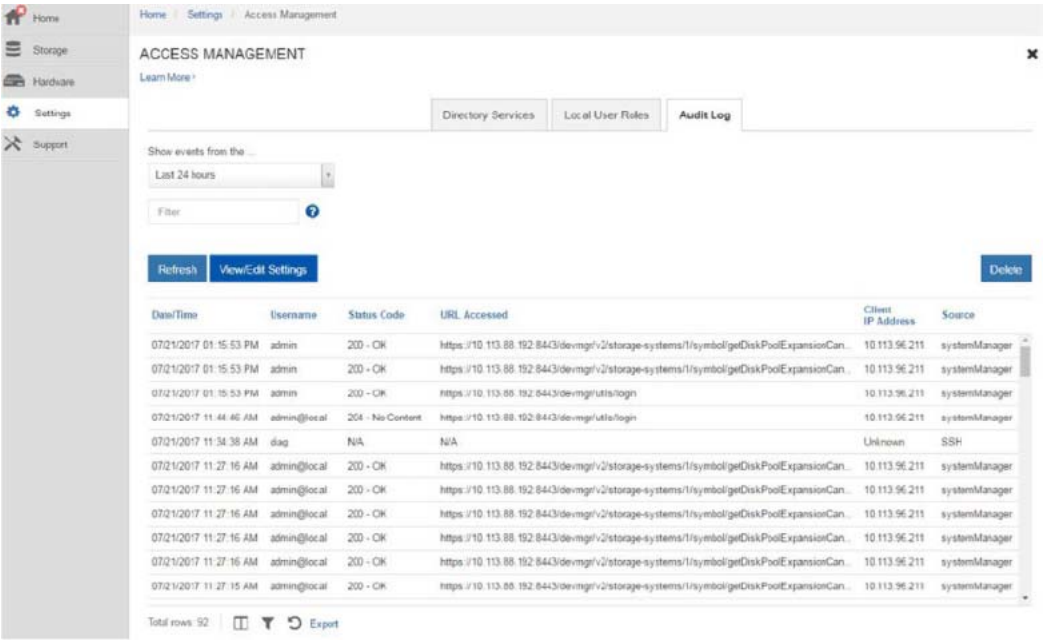
表 4.1　監査ログの範囲

| 管理アクセス・インターフェース | 監査ログの範囲 |
|---|---|
| System Manager GUI | ログインとログアウト、セッションの確立と終了、呼び出されたアクションと要求、およびそれぞれの結果を含むすべてのユーザー・アクティビティー。 |
| セキュアSMcli | ログインとログアウト、セッションの確立と終了、呼び出された要求とエンドポイント、SMcli コマンド、コマンド・コンテキスト、およびそれぞれの結果を含むすべてのユーザー・アクティビティ。 |
| Web Services API | ログインとログアウト、セッションの確立と終了、呼び出されたアクションと要求、およびそれぞれの結果を含むすべてのユーザー・アクティビティー。 |
| シェルインターフェースのサポート | SSH セッションの確立と終了、ユーザーのログインとログアウトのアクティビティ。<br>このアクセス方式では、ユーザーが開始したアクションとコマンドのタイプ、およびそれぞれの結果は追跡されません。 |

ログは、ストレージシステムの不揮発性記憶領域に保存され、両方のコントローラからアクセスできます。セキュリティ管理権限を持つユーザーは、任意のアクセス方法を使用してログを表示および取得したり、CSV ファイル形式にエクスポートしたりできます。

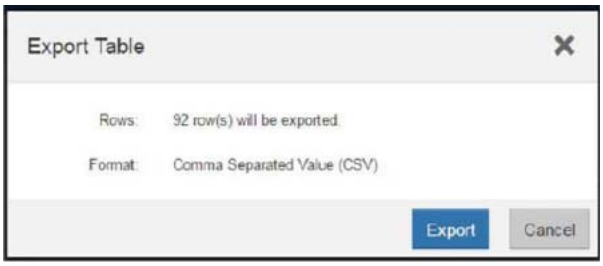
図 4.1 は、SANtricity System Manager の Settings > Access Management > Audit Log の下にある監査ログを示しています。

図 4.1　監査ログを表示するための SANtricity System Manager ページ




ファイルのエクスポート操作では、System Manager GUI、セキュア SMcli、または API アクセス方式による、タイムスタンプ範囲またはレコード ID 範囲要求を使用した監査ログレコードのエクスポートがサポートされます。図 4.2 に、エクスポートテーブルダイアログボックスを示します。

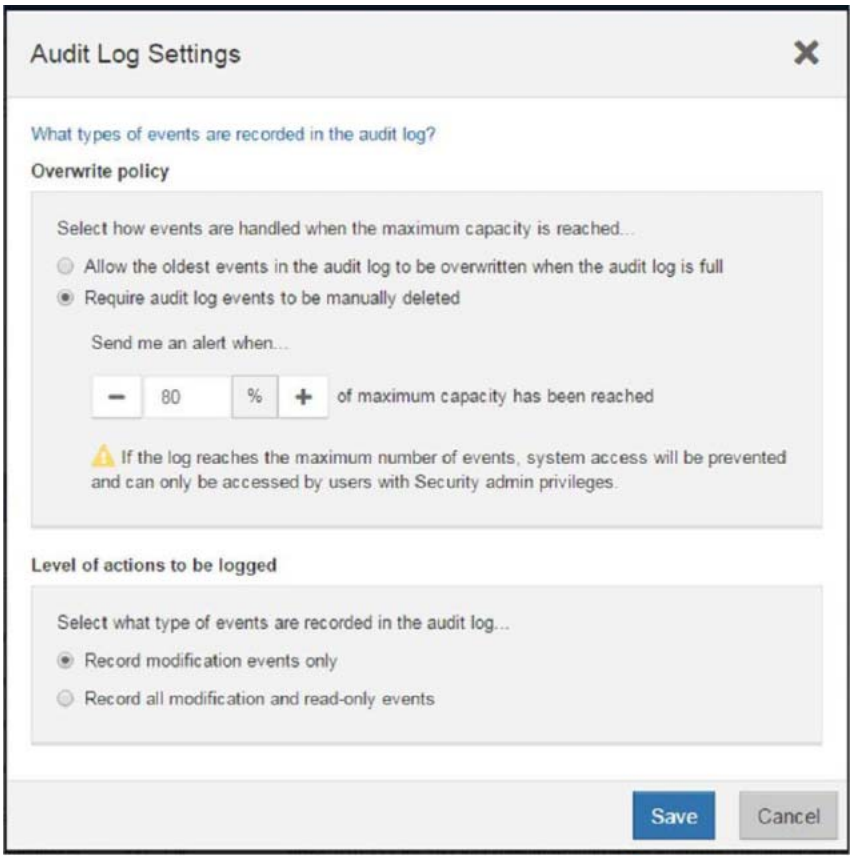
図 4.2　監査ログをエクスポートする SANtricity System Manager ダイアログボックス




監査ログは、この機能をサポートするアレイのライフサイクルを通じて、ユーザーの操作を継続的に記録することを目的としています。したがって、ログ・ファイル・サイズが特定の基準に達したときの制御アクションに関して、ファイル・サイズまたはログ・エントリー・レコードの数に基づいて、適切なルール・セットを定義する必要があります。

図 4.3 は、監査ログ設定が管理されるページを示しています。

図 4.3　監査ログ設定を構成するための SANtricity System Manager ページ



# 第 5 章
# 証明書の管理

暗号技術では、証明機関 (CA) はデジタル証明書を発行するエンティティです。デジタル証明書は、証明書の名前付きサブジェクトによって公開鍵の所有権を証明します。この認証は、認証された公開鍵に対応する秘密鍵について作成された署名またはアサーションに依存することを他の人に許可します。CA は、証明書の所有者と証明書を信頼する側の両方から信頼される、信頼された第三者として機能します。これらの証明書の形式は、International Telecommunications Union's Standardization (ITU-T) X.509 国際標準によって指定されています。

認証局の一般的な使用方法は、World Wide Web の安全なブラウズ・プロトコルである HTTPS で使用される証明書に署名することです。以下のワークフローについては、このセクションの後半で説明します。

- WSP API エンドポイントを使用した WSP 証明書
- SANtricity Unified Manager を使用した WSP 証明書

SANtricity System Manager には、証明書管理機能が導入されおり、次のことが可能です。

- ストレージシステムの各コントローラでの CA 証明書のサポート
- LDAPS またはその他のサーバー証明書を信頼する
- 組み込み鍵管理サーバー証明書をサポートする

SANtricity WSP は証明書管理をサポートし、Web Services Proxy ソフトウェアを実行するサーバと、プロキシによって管理および監視されるサポート対象のストレージシステムとの間の安全な通信を提供します。

どのインターフェースを使用するかは、セキュリティの必要性と特定の機能を使用する必要性によって決まります。表 5.1 に、その決定に役立つ考慮事項を示します。

表 5.1　さまざまな管理クライアントでサポートされている管理機能

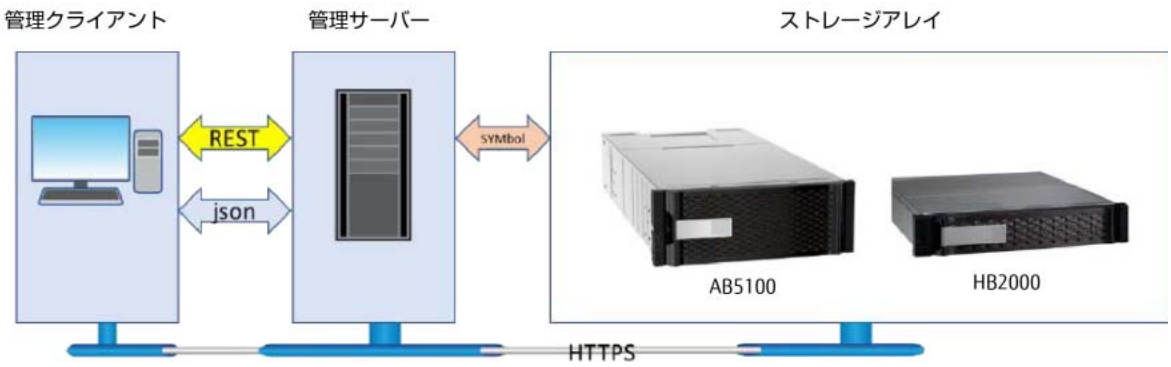
| 管理クライアント | ミラーリング機能 | SMcli | スクリプトエディタ (Script Editor) | あるシステムから他のシステムへの設定のインポート |
|---|---|---|---|---|
| SANtricity Web Services Proxy および Unified Manager | ミラーリングは、ETERNUS AB/HB series システムでのみサポート | サポートされていません | サポートされていません | 共通の設定 ( アラート、ASUP、ストレージ構成など ) を使用する新しいシステムの導入を自動化する新機能 |

# 5.1　Web Services Proxy の証明書管理

富士通 Web サービスは、次の 3 つの分野で使用されています。Web Services Proxy は、SANtricity ソフトウェアがインストールされているサーバーに常駐します。Web Services Proxy は、リモートミラーリング構成を容易にするために、同じサーバ上で実行されている SANtricity System Manager のみが代替アレイと通信するために使用する制限付きプロキシです。

Web Services Proxy に加えて、スタンドアロンの富士通 SANtricity WSP を Windows または Linux サーバにインストールできます。このプロキシは、ETERNUS AB/HB series のシステムを構成、管理、および監視するための Web Services API を提供します。プロキシは、ストレージシステム用に定義されたサービスにアクセスするために、REST スタイルのインターフェースのコレクションへのアクセスを提供します。図 5.1 は、クライアント・マシン、サーバーで実行されている Web Services Proxy、および ETERNUS AB/HB series システム間の通信のハイレベルな概要を示しています。

図 5.1　管理クライアントとサーバにインストールされた Web Services Proxy 間の通信



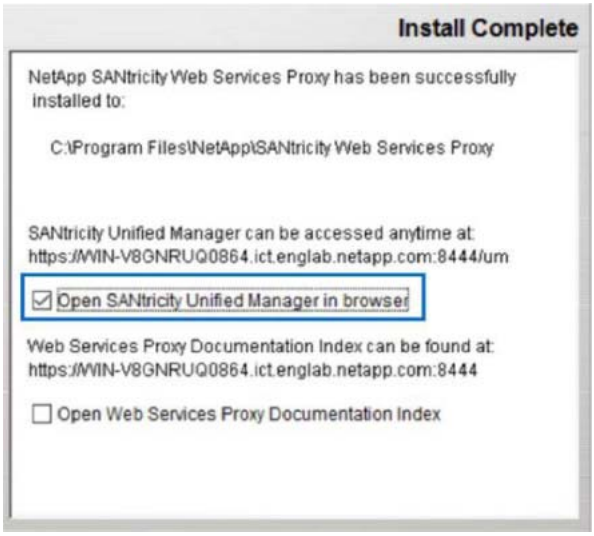

3 番目の Web サービス実装は、アレイ・コントローラに組み込まれている SANtricity System Manager Web Service です。同様に、クライアントは標準的な HTTPS メカニズムを介して Web サービスにアクセスします。Web サービスがストレージシステムへのデータ収集または構成変更要求の実行によってクライアント要求を満たすと、Web サービス・モジュールはストレージシステムに SYMbol 要求を発行します。

## 5.1.1　SANtricity Unified Manager を使用した WSP 証明書の管理

SANtricity WSP には、SANtricity Unified Manager が含まれています。組み込み機能の 1 つに、Unified Manager GUI から WSP セキュリティ証明書を管理する機能があります。次の手順は、WSP 証明書の管理に必要なワークフローを示しています。最初の手順は、WSP サーバーがシステムからの着信クライアント要求の認証に使用する CA ルート証明書と中間証明書を WSP にインポートすることです。

**手順 ▶▶▶**

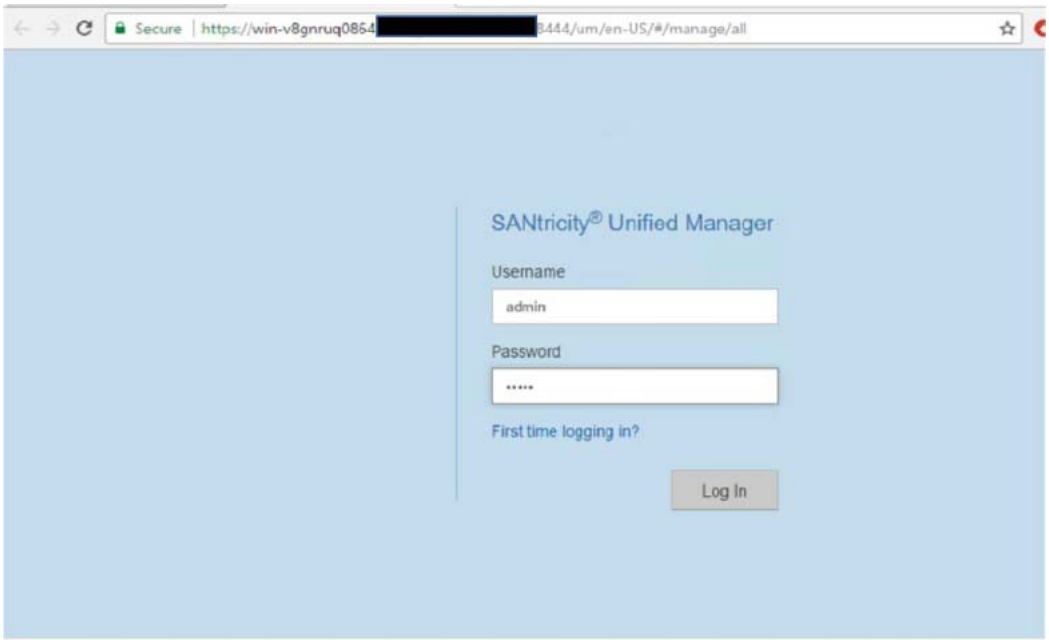
1. WSP インストールウィザードからまたは https://<WSP Server FQDN>:<Secure Port #>/um に移動して、SANtricity Unified Manager を開きます。



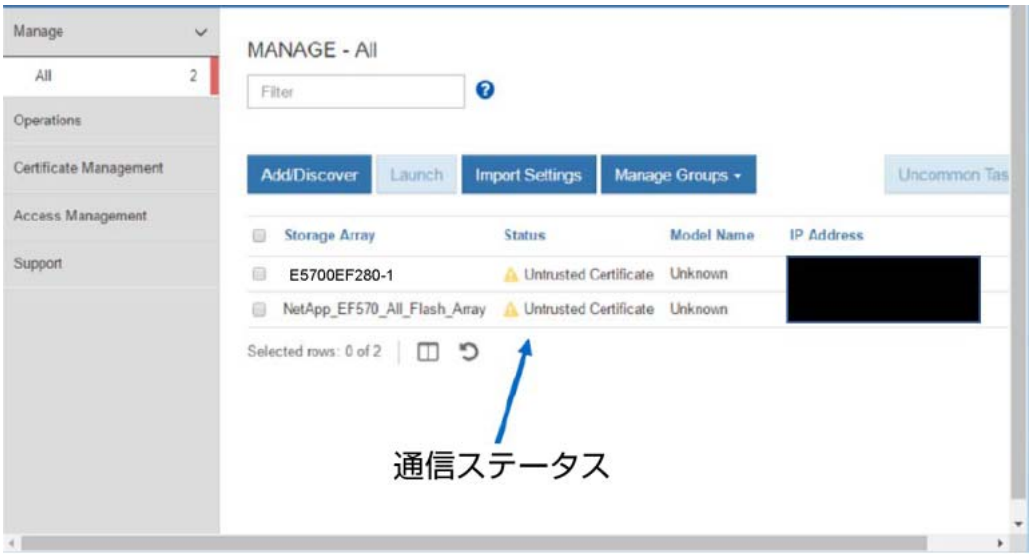
**2** user=admin、password=admin としてログインします。

**注 意**

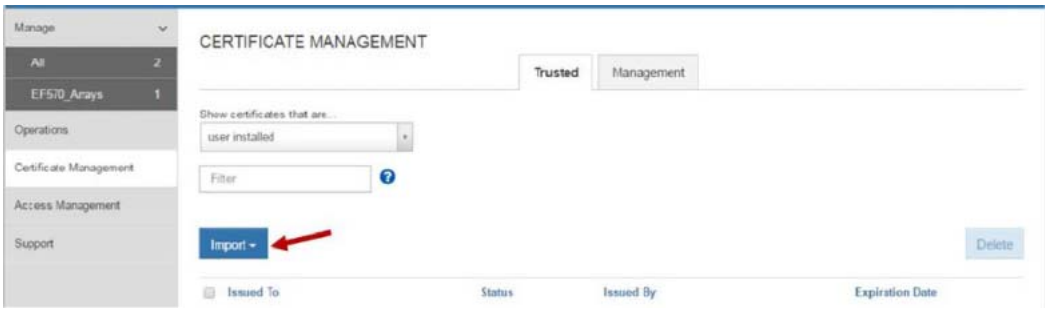
デフォルトの admin アカウントのパスワードを変更した場合は、その新しいパスワードでログインします。



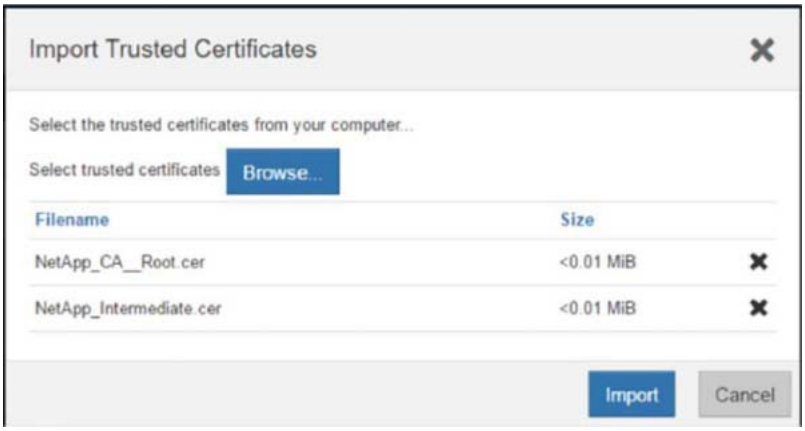

検出されたシステムは、各アレイとの通信ステータスを含むランディング・ページに表示されます。



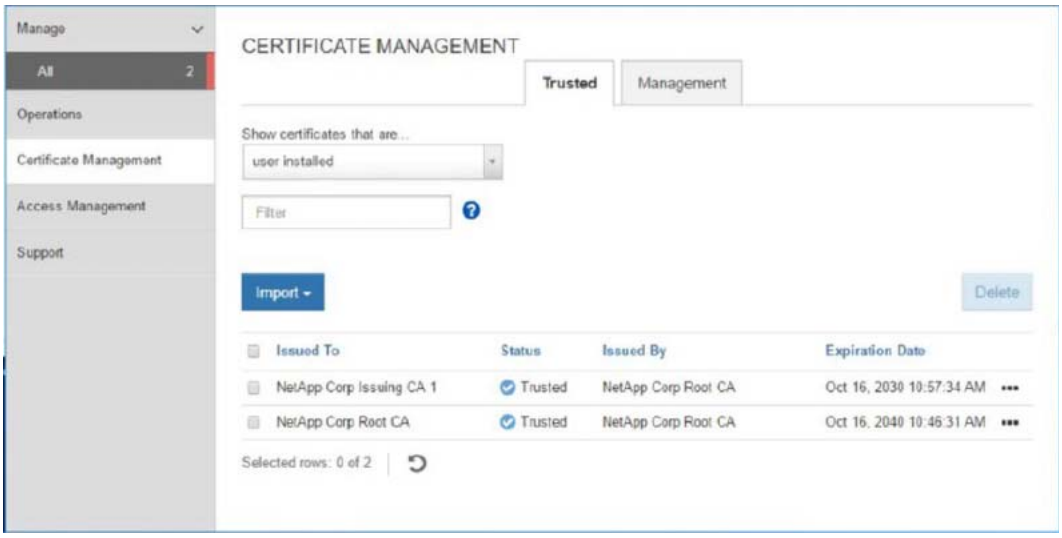
**3** Certificate Management タブに移動し、Import を選択します。



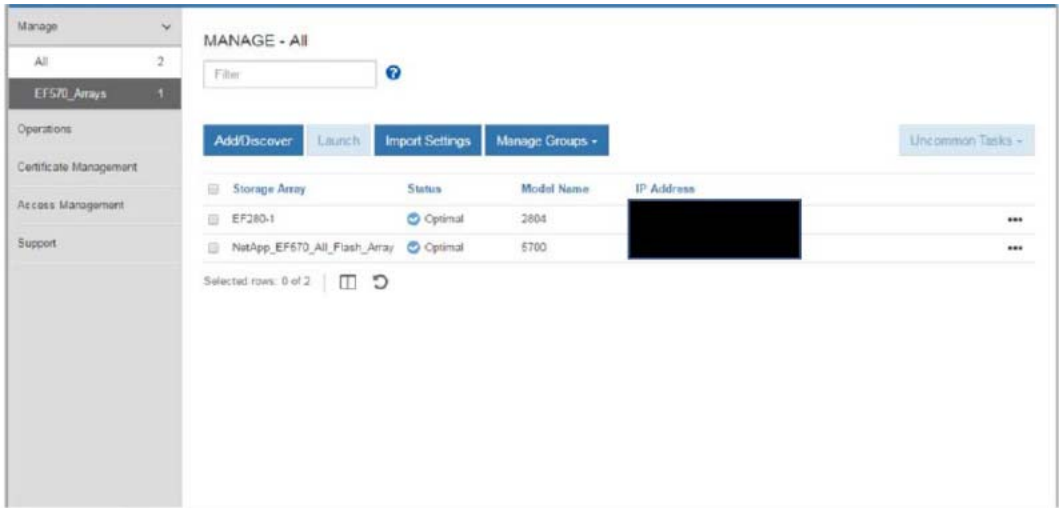

**4** Certificates ウィザードのプロンプトが表示されたら、CA ルート証明書ファイルと中間証明書ファイルを参照し、インポートするファイルを選択します。
Ctrl キーを使用して複数のファイルを選択します。




新しくインポートされた証明書が、Certificate Management ペインに表示されます。



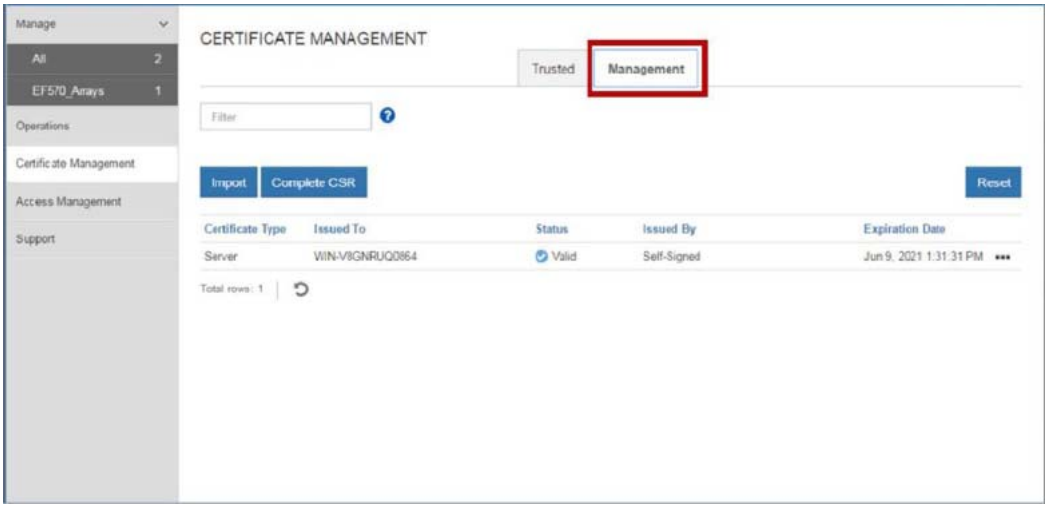

これにより、CA 証明書がインストールされているシステムでの証明書の問題が解決されます。



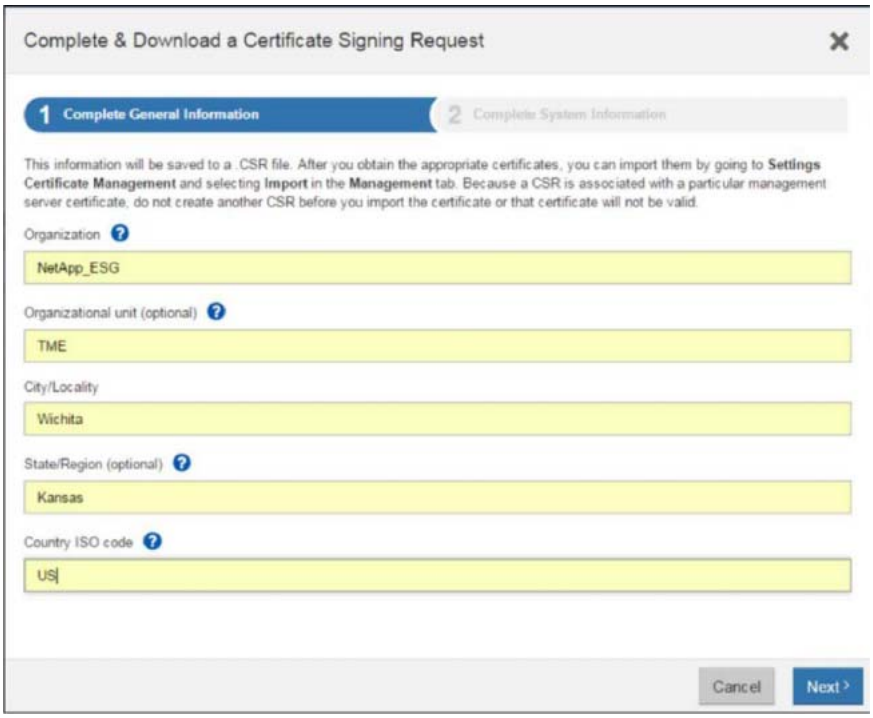

新しい SANtricity WSP Web サーバー証明書 (WSP に接続するクライアントに WSP が提示するサーバ証明書 ) を生成してインストールするには、CSR を生成し、その CSR ファイルを CA 機関に送信する必要があります。新しい証明書を受け取ったら、前の手順と同様の方法でインポートします。

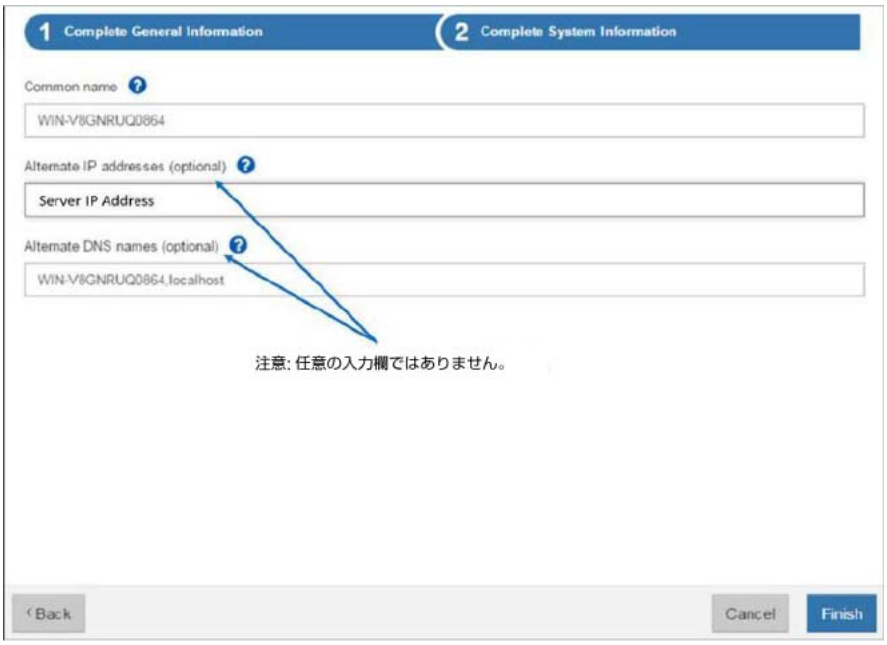
**5** 「Certificate Management」タブにナビゲートし、「Management」をクリックして「Reset」を実行し、Web サーバー上で新しい自己署名証明書を再生成します。

ブラウザが更新されると、ブラウザが宛先サイトへのアクセスをブロックし、サイトが HTTP Strict Transport Security を使用していることを報告する場合があります。この状態は、自己署名証明書に切り替えたときに発生します。宛先へのアクセスをブロックしている状態をクリアするには、ブラウザから参照データをクリアする必要があります。



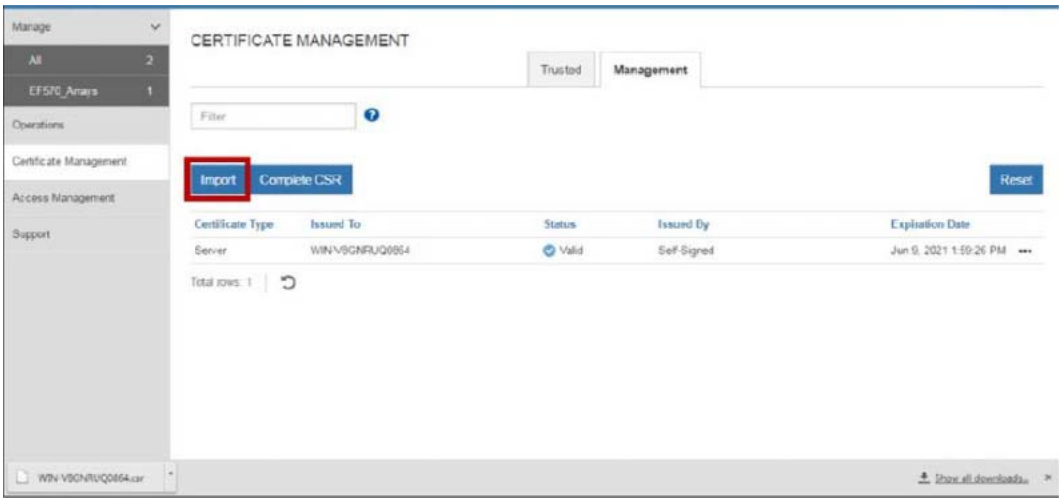
**6** Complete CSR タブを選択し、ウィザードに従って CSR を完了します。



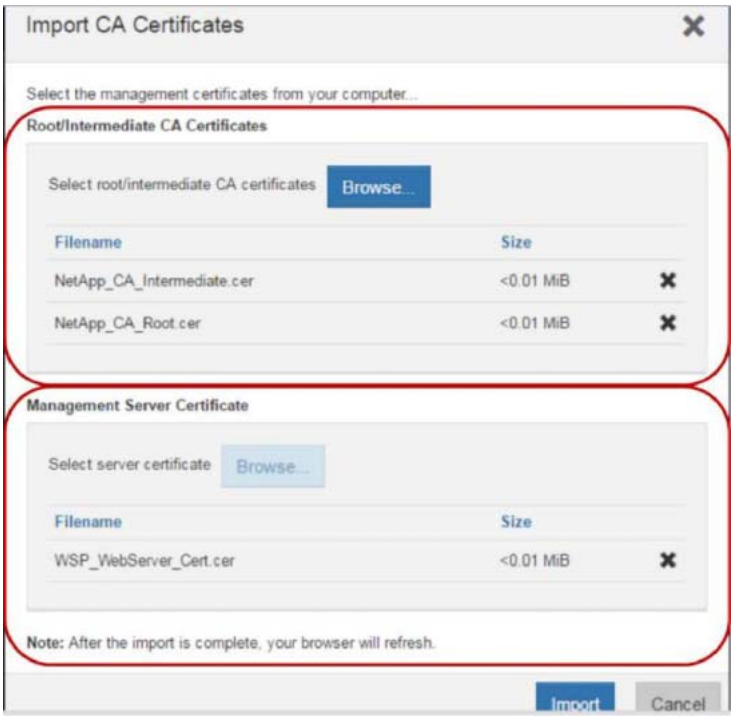




**7** Finish をクリックし、CSR ファイルをダウンロードして、CSR ファイルを CA 機関に送信し、新しい Web サーバー証明書 ( これは通常、ルート証明書と中間証明書を持つ証明書チェーンにあります ) を要求します。

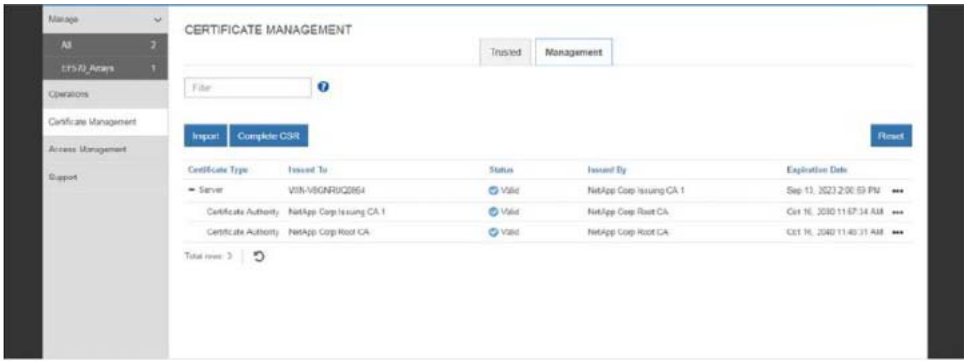
**8** Import ウィザードを使用して、新しい証明書をインポートします。




**9** インポートするルート証明書と中間証明書、および新しい Web サーバー証明書を選択します。



**10** Web サーバをインポートした後、再起動すると、ブラウザウィンドウがリセットされ、ブラウザセッションはセキュリティで保護されます。新しいブラウザセッションを開始します。



## 5.1.2　Web Services REST API へのアクセス

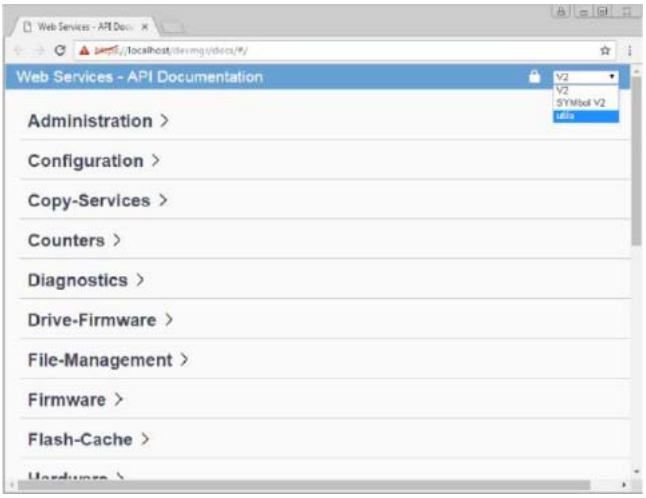
プロキシがインストールされているホストで Web ブラウザを使用して REST API にアクセスするには、以下に進みます。

https://localhost/devmgr/docs/#/

REST API に初めてアクセスする場合は、各タイプのブラウザに次の情報が表示されます。

- Chrome に「この接続ではプライバシーが保護されません」と表示されます。「詳細設定」をクリックして Web サイトに進みます。
- Internet Explorer で、「この Web サイトのセキュリティ証明書には問題があります」と表示されます。「このサイトの閲覧を続行する（推奨されません）」をクリックして、Web サイトに進みます。
- Firefox で「安全な接続ができませんでした」と表示されます。「詳細」ボタンをクリックし、証明書の例外を追加して Web サイトに進みます。

図 5.2　Web Services Proxy のセキュリティ証明書が機能せず、接続がセキュアでない




サポートされているブラウザを使用して https://<Web_Proxy_host_server_FQDN_or_IP>:<secure port ID>/devmgr/docs/#/ にアクセスし、リモートから Web Services Proxy にアクセスすることもできます。

**注 意**

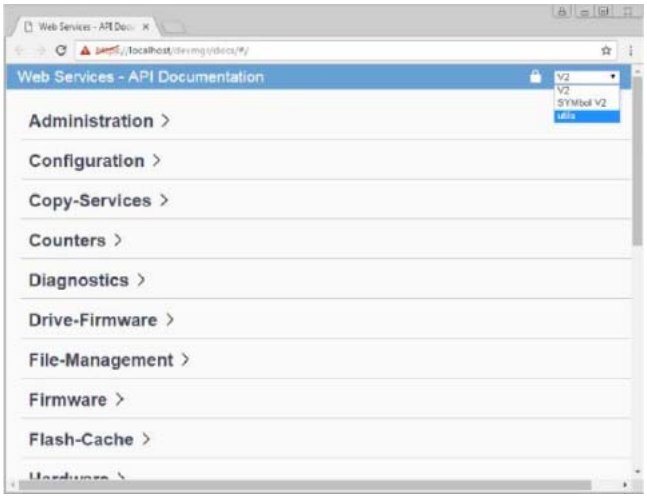
デフォルトのセキュア・ポートは 8443 ですが、SANtricity WSP がインストールされているサーバーによっては、プロキシーが別のポート番号に切り替わる場合があります。その結果、このアプリケーションのポートが環境によって異なる場合があります。

## 5.1.3　管理者としての Web Services Proxy へのログイン

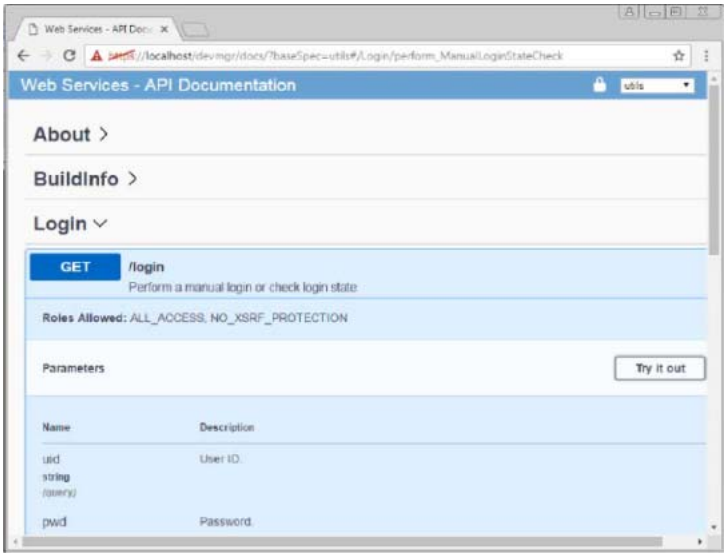
セキュリティ管理者ロールに関連付けられたアクセス権を含め、ターゲット Web サーバーにログインできることを確認するには、次の手順に従います。

**手順 ▶▶▶**

1. ドロップダウンメニューから「Utils」を選択して、「Utilities」ページにアクセスします。



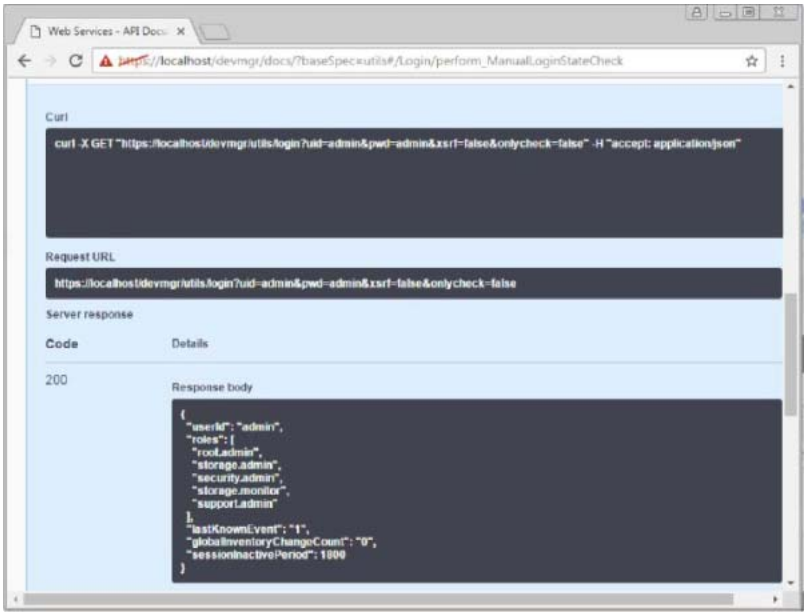

2. Login コマンドを展開し、Get:/ login コマンドを選択します。



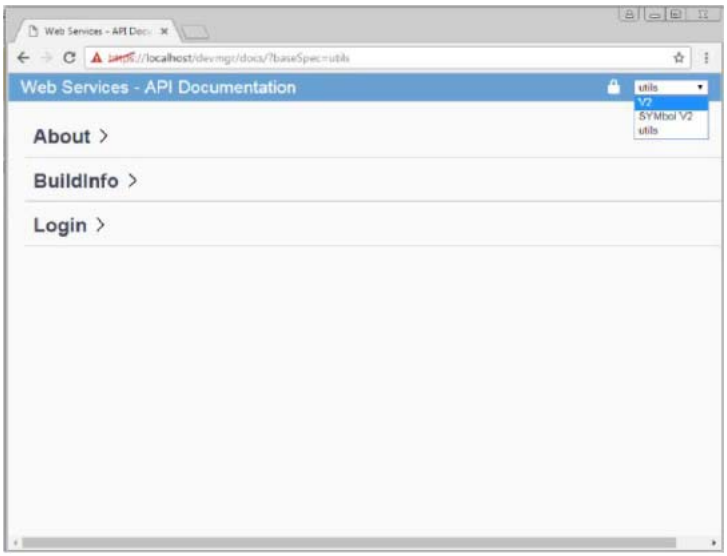
**3** Try It Out をクリックし、ユーザー ID とパスワードを user=admin/ password=admin に編集して、Execute をクリックします。

**注 意**

Responses セクションには、コマンドセットが表示され、関連する情報の返答を含むコマンドの状態が示されます。この例では、admin ユーザーに割り当てられたロールが一覧表示されます。




**4** ドロップダウンメニューから V2 を選択して V2 ページに戻り、CA 証明書を生成およびインストールする手順を実行します。

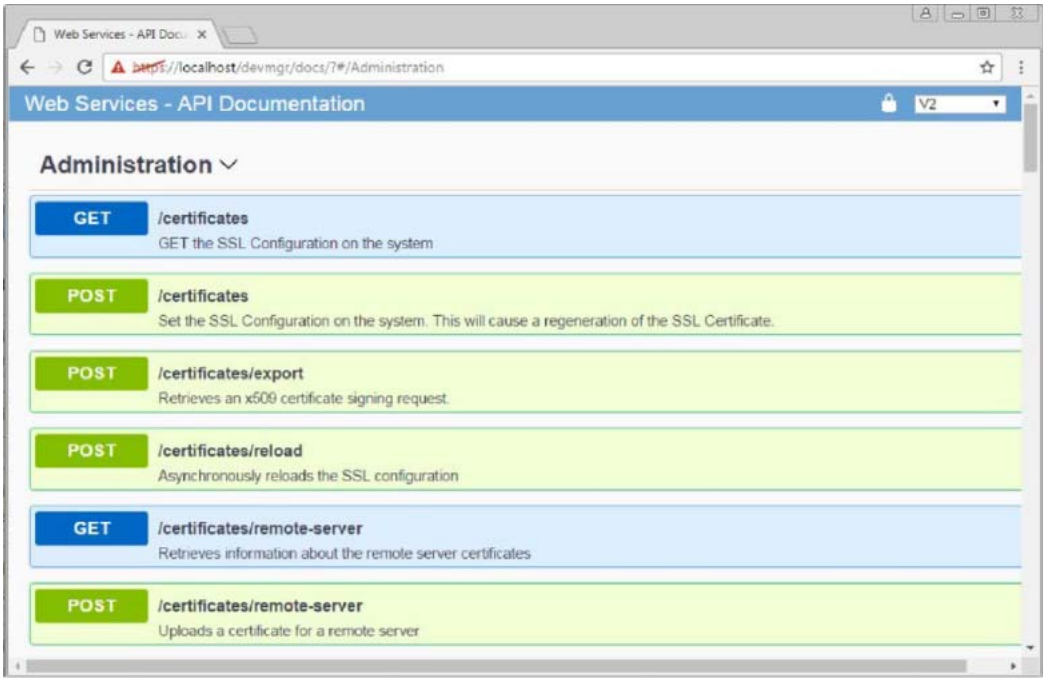


## 5.1.4　WSP を使用した Web Services Proxy セキュリティ証明書のインストール

以下の手順は、Web Services Proxy で使用可能なエンドポイントの例に基づいています。

**手順 ▶▶▶**

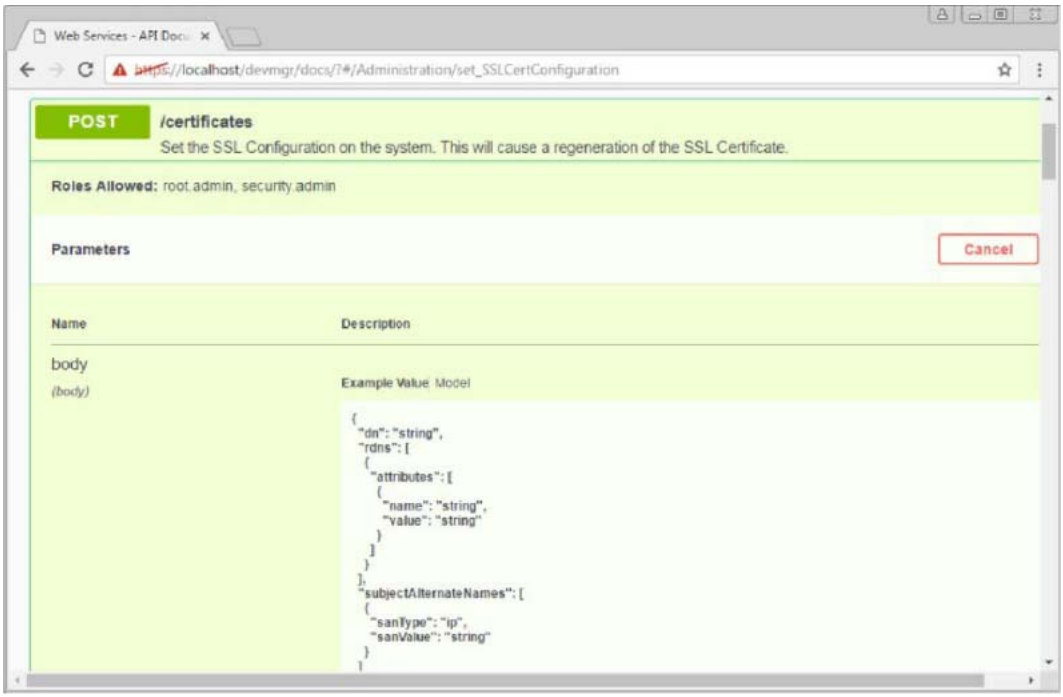
1 「Administration」行を展開し、/certificates エンドポイントまでスクロールします。



**2** POST:/certificates を選択し、Try It Out をクリックします。

**注 意**

この手順により、Web サーバーは自己署名証明書を再生成し、いくつかのフィールドに情報を入力して、CSR の生成に使用する共通名、組織、組織単位、代替 ID、およびその他の情報を定義できます。



**3** Example の値のペインで必要な情報を追加して、有効な CA 証明書を生成し、コマンドを実行します。

**注 意**

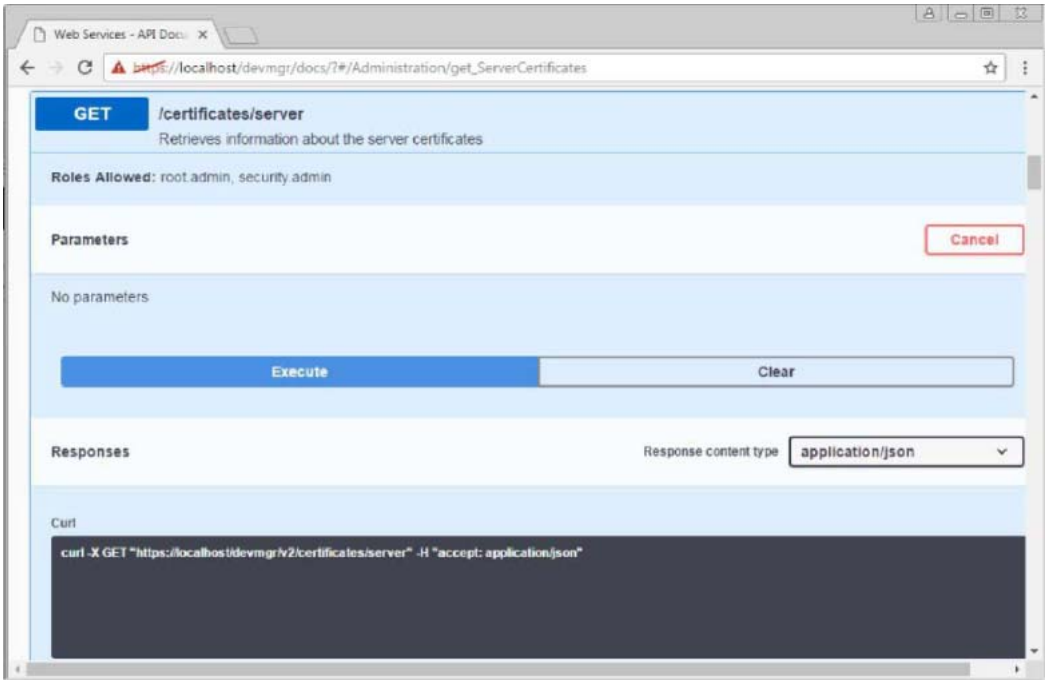
有効な DN 属性を見つけるには、https://www.ietf.org/rfc/rfc2253.txt を参照してください。この例は、米国を拠点とするお客様を対象としています。

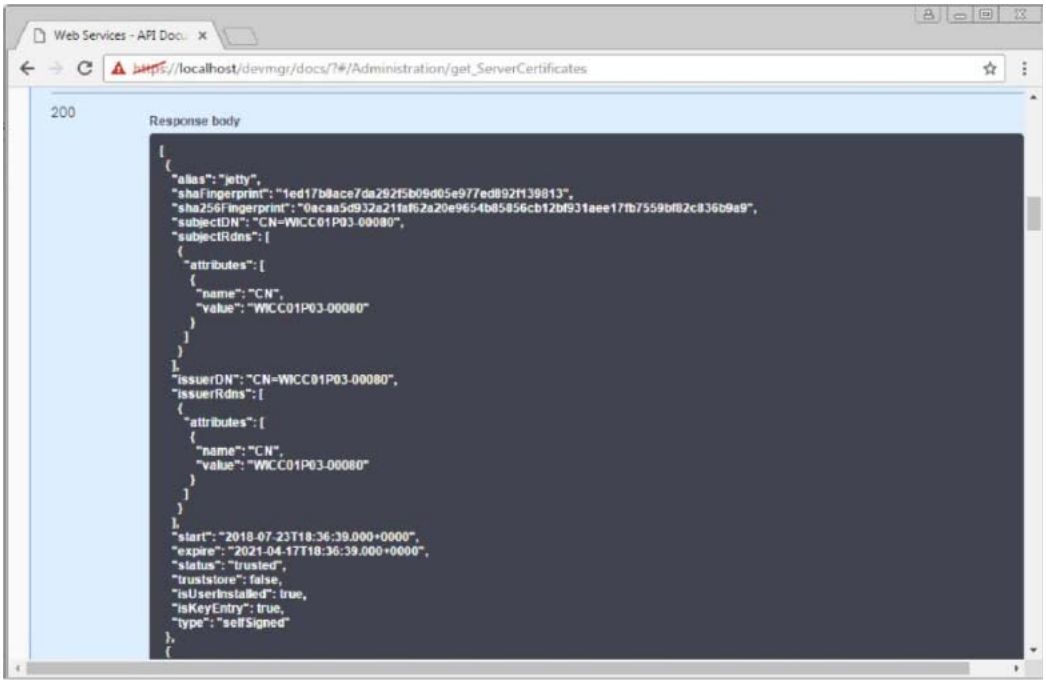
```
{
  "dn": "CN=Enter_server_FQDN,O=Company_Name,OU=Organization_Unit,L=Loca-
tion,ST=State,C=US","rdns": [
   {
     "attributes": [
       {
         "name": "CN",
         "value": "Enter_server_FQDN"
       },
       {
         "name": "O",
         "value": "Enter_Company_Name"
       },
       {
         "name": "OU",
         "value": "Enter_Origanization_Unit"
       },
       {
         "name": "L",
         "value": "Enter_Location"
       },
       {
         "name": "ST",
         "value": "Enter_State"
       },
       {
         "name": "C",
         "value": "US"
       }
      ]
     }
    ],
    "subjectAlternateNames": [
      {
       "sanType": "dns",
       "sanValue": "Enter_server_FQDN"
     },
     {
       "sanType": "ip",
       "sanValue": "Enter_server_IP"
     }
    ]
}
```

**注 意**

POST:/certificates または POST:/certificates/reset を再度呼び出さないでください。呼び出してしまうと、CSR を再生成する必要があります。POST:/certificates または POST:/certificates/reset を呼び出すと、新しい秘密鍵を持つ新しい自己署名証明書が生成されます。サーバー上の秘密鍵が最後にリセットされる前に生成された CSR を送信すると、新しいセキュリティ証明書は機能しません。新しい CSR を生成し、新しい CA 証明書を要求する必要があります。

**4** GET:/certificates/server エンドポイントを実行して、現在の証明書ステータスが、POST:/certificates コマンドから追加された情報を持つ自己署名証明書であることを確認します。

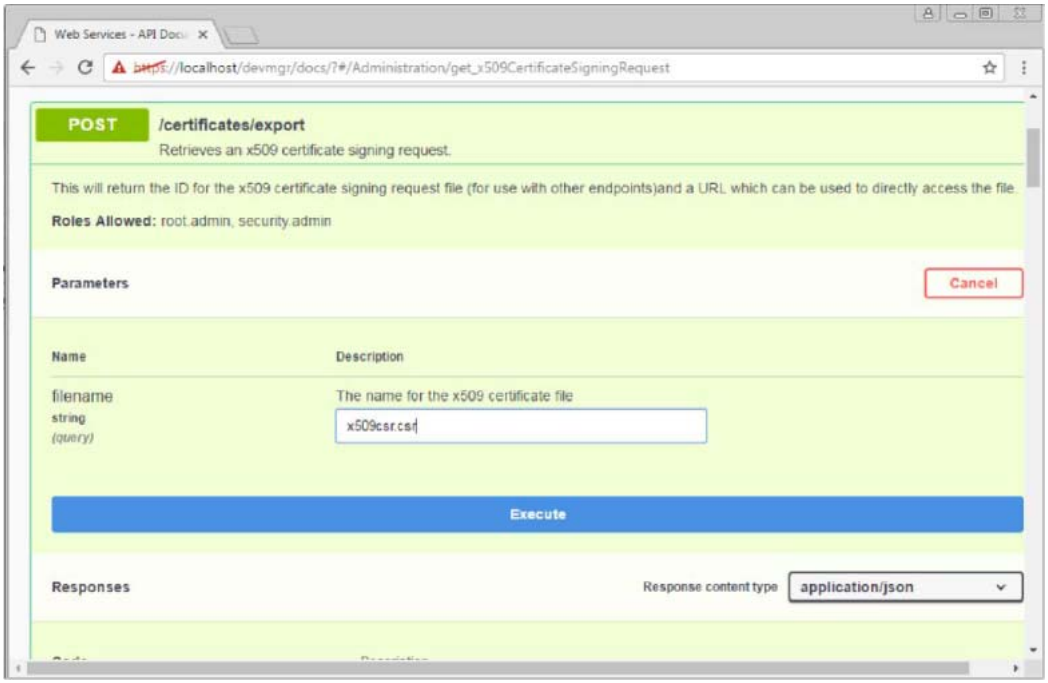




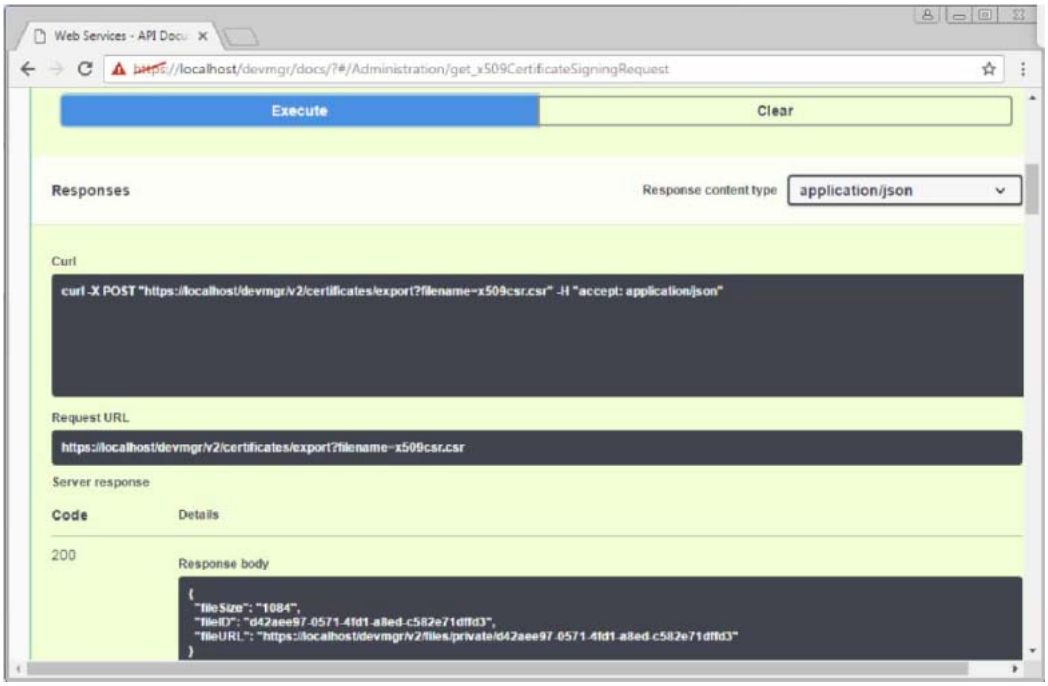

注 意

サーバー証明書 ( 別名 jetty で表される ) は、この時点でも自己署名されています。

**5** POST:/certificates/export エンドポイントを展開し、Try It Out をクリックし、CSR ファイルのファイル名を入力して、Execute をクリックします。



**6** ファイルの URL をコピーして新しいブラウザタブに貼り付け、CSR ファイルをダウンロードします。




**7** CSR を有効な CA に送信し、新しい Web サーバー証明書チェーンを要求します。

**8** CA が新しい証明書チェーンを発行するときは、証明書マネージャーツールを使用して、ルート、中間、および Web サーバー証明書を分割します。

**9** 個々の証明書ファイルが使用可能になったら、Web Services Proxy サーバーにインポートします。

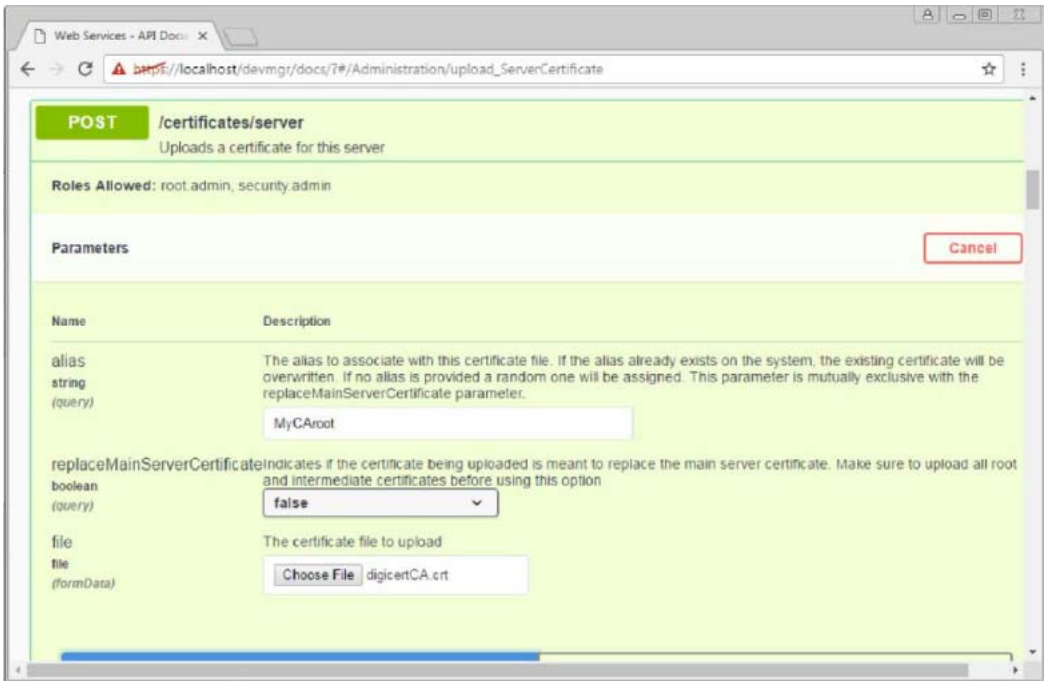
**9-1** POST:/sslconfig/server endpoint を展開し、Try It Out をクリックします。

**9-2** 別名フィールドに CA ルート証明書の名前を入力します。

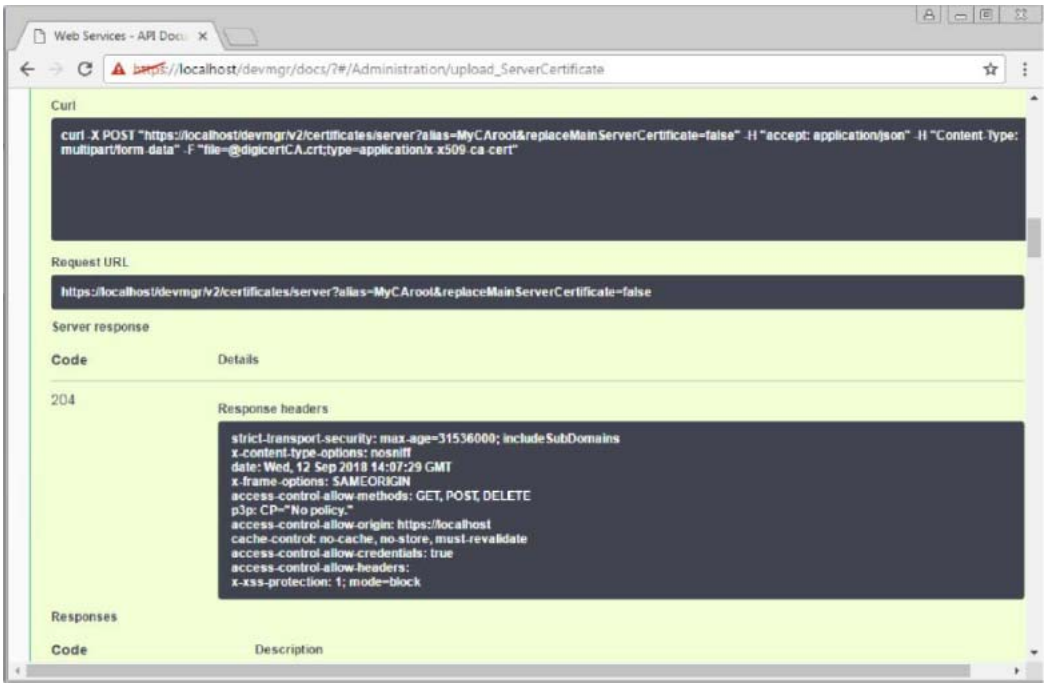
**9-3** replaceMainServerCertificate フィールドで false を選択します。

**9-4** 新しい CA ルート証明書を参照して選択します。

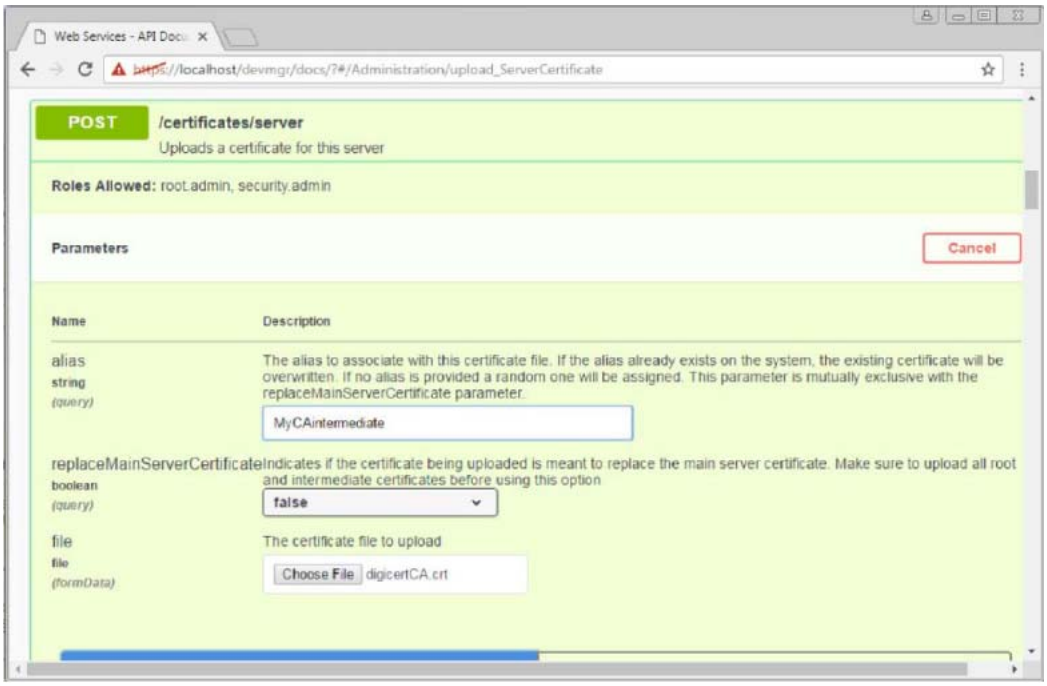
**9-5**　Execute をクリックします。



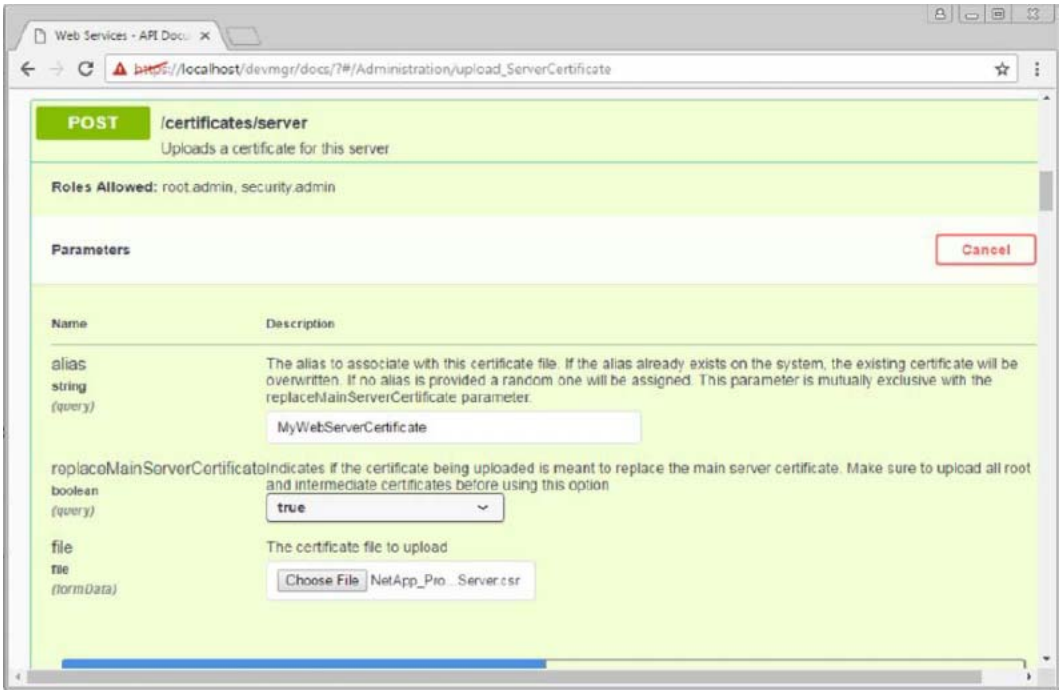

**9-6**　証明書のアップロードが成功したことを確認します。



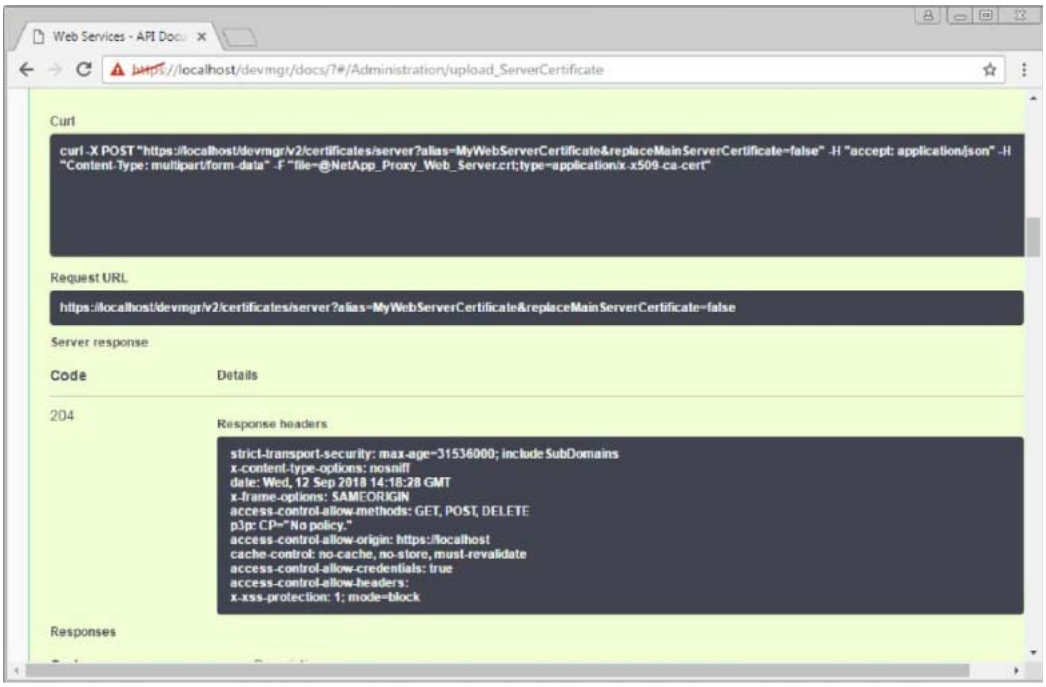
**9-7** CA 中間証明書について、CA 証明書のアップロード手順を繰り返します。




**9-8** 新しい Web サーバのセキュリティ証明書ファイルに対して、証明書のアップロード手順を繰り返します。replaceMainServerCertificate ドロップダウンメニューから True を選択します。

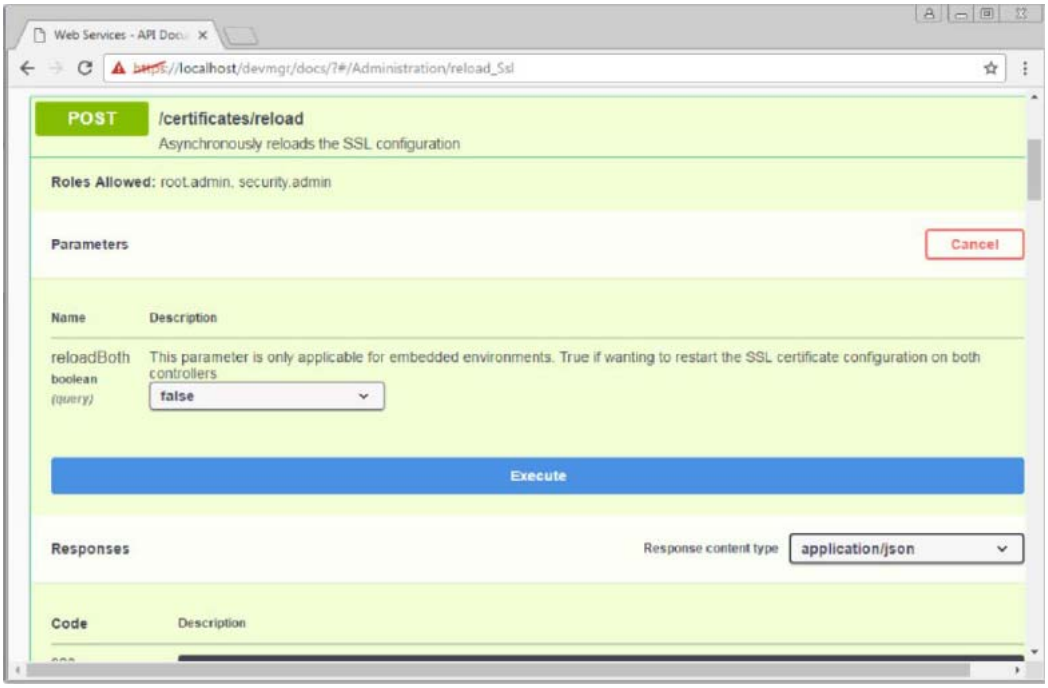


**9-9** Web サーバのセキュリティ証明書が正常にインポートされたことを確認します。




**9-10** 新しいルート、中間、および Web サーバー証明書がキーストアで使用可能になったことを確認するには、GET:/certificates/server を実行します。

**10** POST:/certificates/reload エンドポイントを選択して展開し、Try It Out をクリックします。両方のコントローラを再起動するかどうかを確認するメッセージが表示されたら、False を選択します。(True は、デュアルアレイコントローラの場合にのみ適用されます。) [Execute] をクリックします。



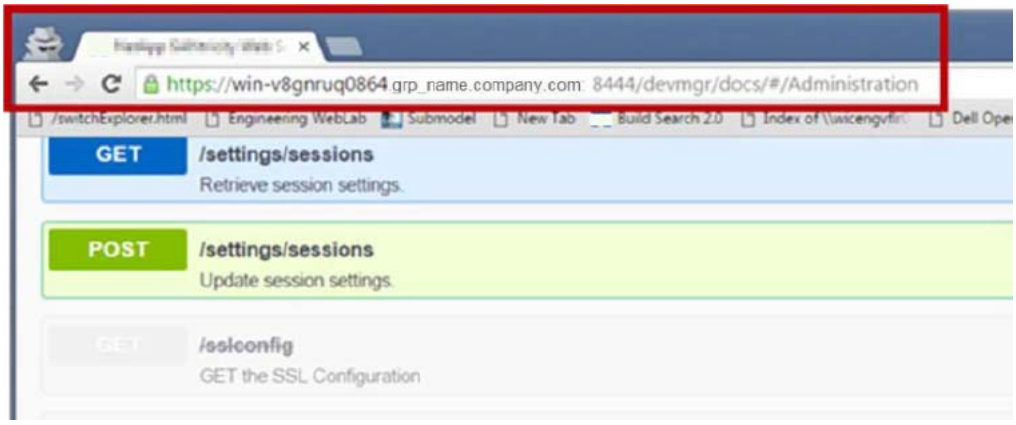
**注 意**

通常、/certificates/reload エンドポイントは、成功した http 202 応答を返します。ただし、Web サーバーのトラストストアとキーストアの証明書をリロードすると、API プロセスと Web サーバーの証明書リロードプロセスの間に競合状態が発生します。まれに、Web サーバーの証明書のリロードが API の処理を上回ることがあります。この場合、リロードは正常に完了したにもかかわらず、失敗したように見えます。この場合は、次の手順に進みます。リロードが実際に失敗した場合、次の手順は成功しません。

**11** Web Services Proxy への現在のブラウザ・セッションを閉じ、新しいブラウザ・セッションを開き、Web Services Proxy への新しいセキュアなブラウザ接続を確立できることを確認します。

**注 意**

匿名またはプライベートブラウジングセッションを使用すると、以前のブラウジングセッションで保存されたデータを使用せずに、サーバーへの接続を開くことができます。



# 5.2　SANtricity System Manager コントローラの証明書管理

管理者が SANtricity System Manager を使用してアレイに初めて証明書を設定する場合、コントローラ上の Web サーバーは両方ともデフォルトの自己署名証明書を持つため、デフォルトのステータスは相互を信頼しないことになります。

SANtricity System Manager が物理的にアクセスする必要があるのは、2 つのコントローラのうちの 1 つだけなので、Settings > Certificates に初めて移動すると、他のコントローラの自己署名証明書を受け入れるかどうかを尋ねるダイアログボックスが開きます。

**注 意**

OpenSSL などの外部ツールを使用して Certificate Signing Request (CSR) を生成できるようになりました。また、署名済み証明書とともに秘密鍵ファイルもインポートする必要があります。

図 5.3 は、HTTPS 接続が安全でないデフォルトのコントローラ Web サーバー証明書ステータスを示しています。

図 5.3　証明書を管理するための SANtricity System Manager のナビゲーション

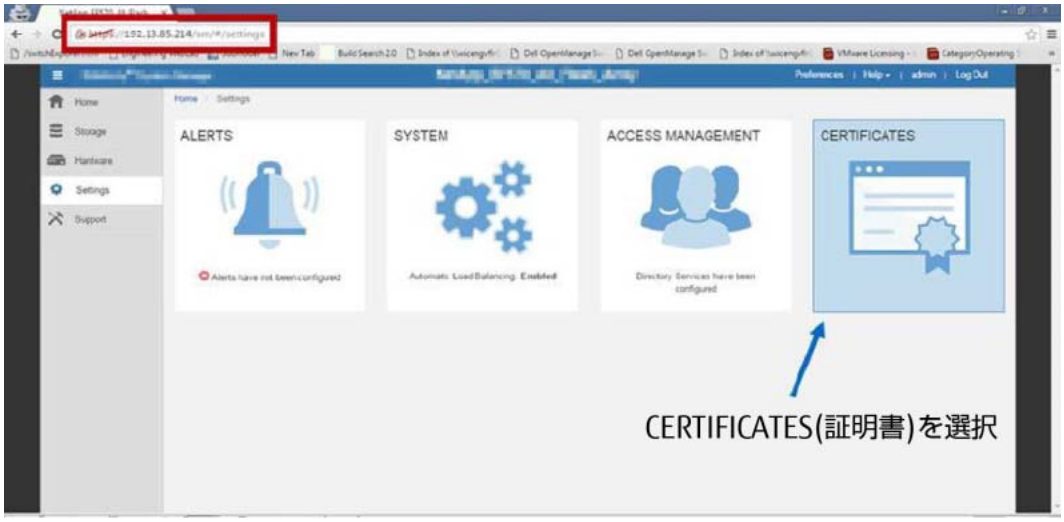
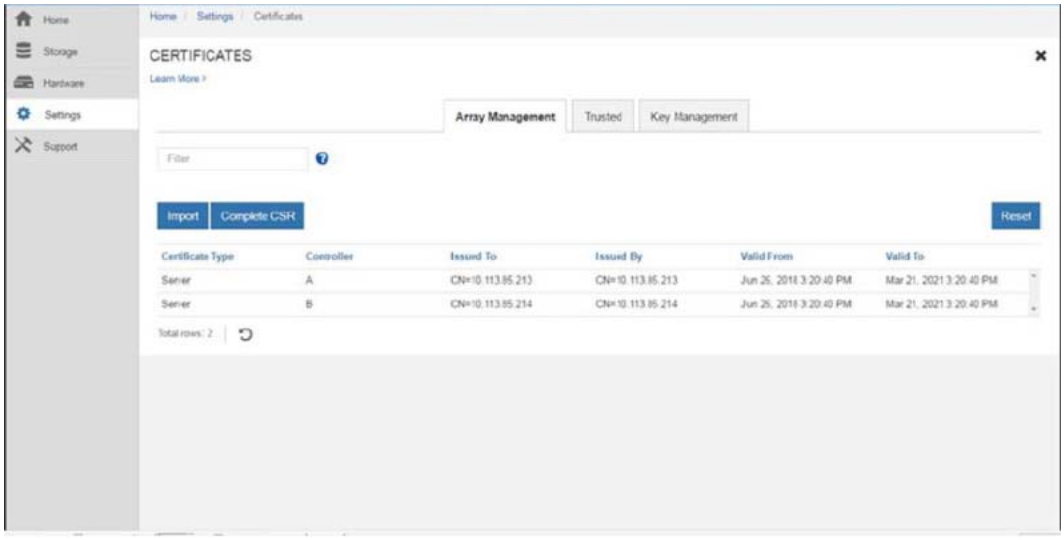



図 5.4 は、代替コントローラの自己署名証明書を受け入れるように求められるダイアログボックスを示しています。

図 5.4　ユーザーが自己署名証明書を受け入れることができるダイアログボックス

代替コントローラの自己署名証明書を受け入れて、コントローラ証明書を管理します。証明書を受け入れると、図 5.5 に示すように [Certificates] ウィンドウが表示されます。

図 5.5　代替コントローラの自己署名証明書が受け入れられた後のデフォルトのコントローラ証明書ステータス




以下の手順では、SANtricity System Manager GUI コントローラの CSR プロセスについて説明します。

## 手順 ▶▶▶

**1**　Certificates ペインで Reset コマンドを実行して、コントローラの自己署名証明書をリセットおよび再生成します。
このコマンドは、アレイのインストール後、プロセスをクリーンな状態で再起動します。

**注 意**

ブラウザが更新されると、ブラウザが宛先サイトへのアクセスをブロックし、サイトが HTTP Strict Transport Security を使用していることを報告する場合があります。この状態は自己署名証明書に戻したときに発生します。宛先へのアクセスをブロックしている状態をクリアするには、ブラウザのキャッシュデータをブラウザからクリアする必要があります。

**2**　アレイの管理ネットワーク内のサーバのコマンド・プロンプトから nslookup コマンドを実行して、コントローラの FQDN を取得します。

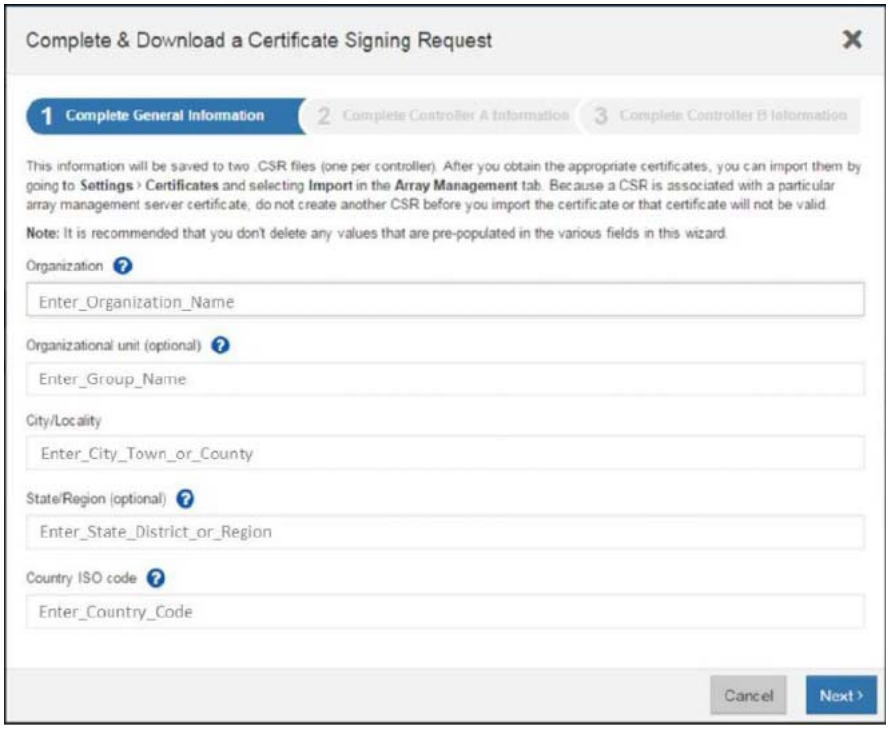
```
C:\Users\admin>nslookup 192.13.85.213
Server: DNS1.location.group.company.com
Address: 192.11.102.130

Name:    ICTM0904C1-A.group.company.com
Address: 192.13.85.213

C:\Users\admin>nslookup 192.13.85.214
Server: DNS1.location.group.company.com
Address: 192.11.102.130

Name:    ICTM0904C1-B.group.company.com
Address: 192.13.85.214
```

**注 意**

DNS サーバーを使用していない場合は、nslookup の手順を省略できます。代わりに、CSR フォームの共通名として自動設定されたプライマリコントローラの IP アドレスを使用し、代替 IP アドレスとして同じ自動設定された IP アドレスを使用します。コンマ区切り一覧を使用して代替 IP アドレスを追加できますが、CA 署名証明書をインポートして正常に動作させるには、最初の代替 IP アドレスが共通名 IP と一致している必要があります。

**3** 両方のコントローラの新しい証明書要求を生成するには、「Complete CSR」タブを選択します。

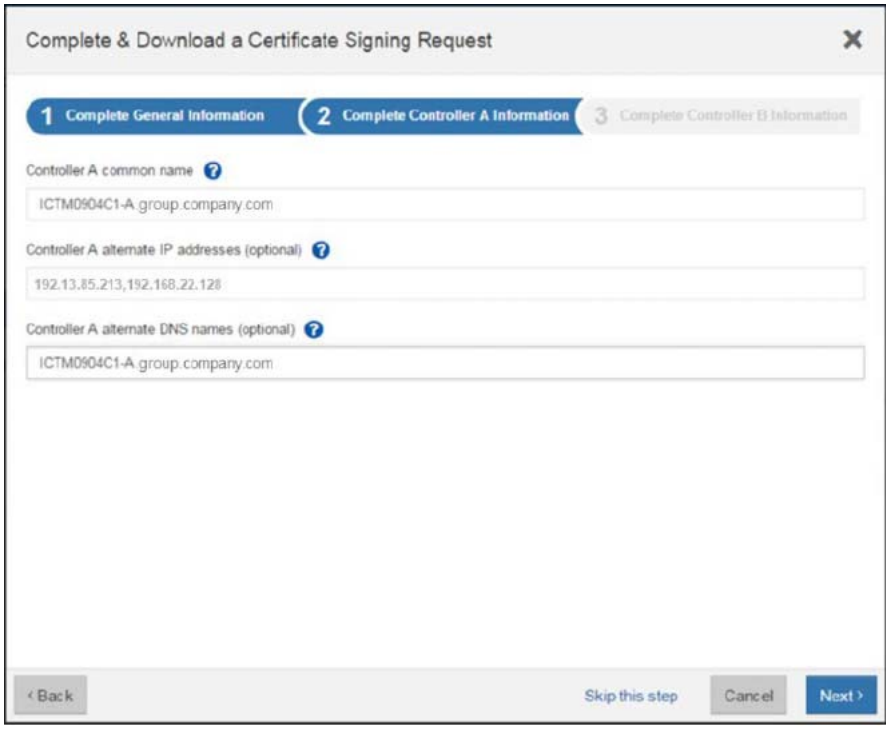
**3-1** 組織および所在地を識別する情報を入力します。



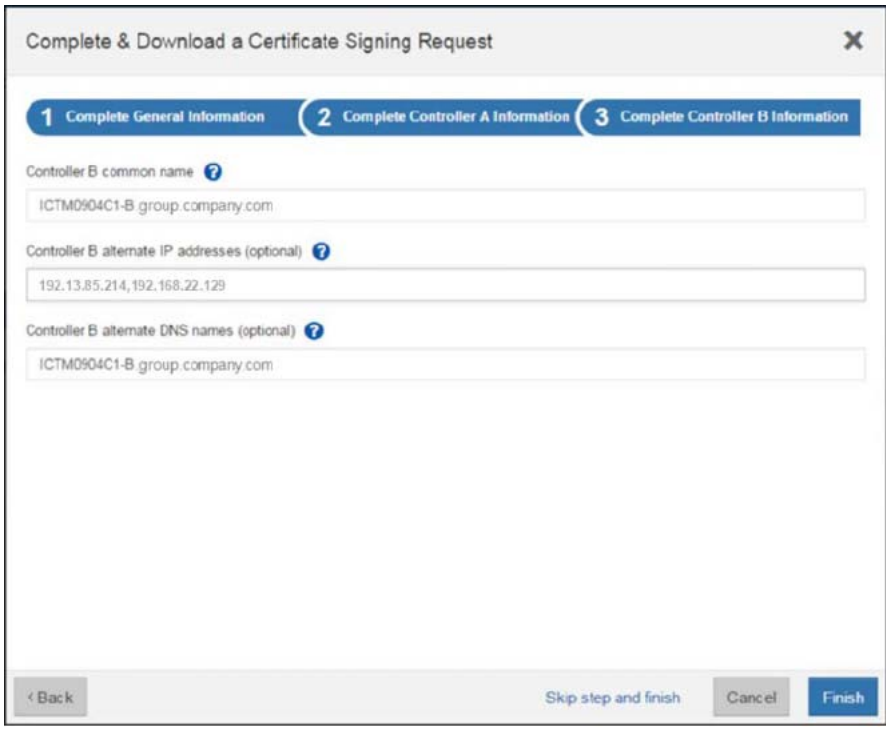
**3-2** コントローラ A の情報を変更または入力するには、コントローラ A の FQDN を使用します。

**注 意**

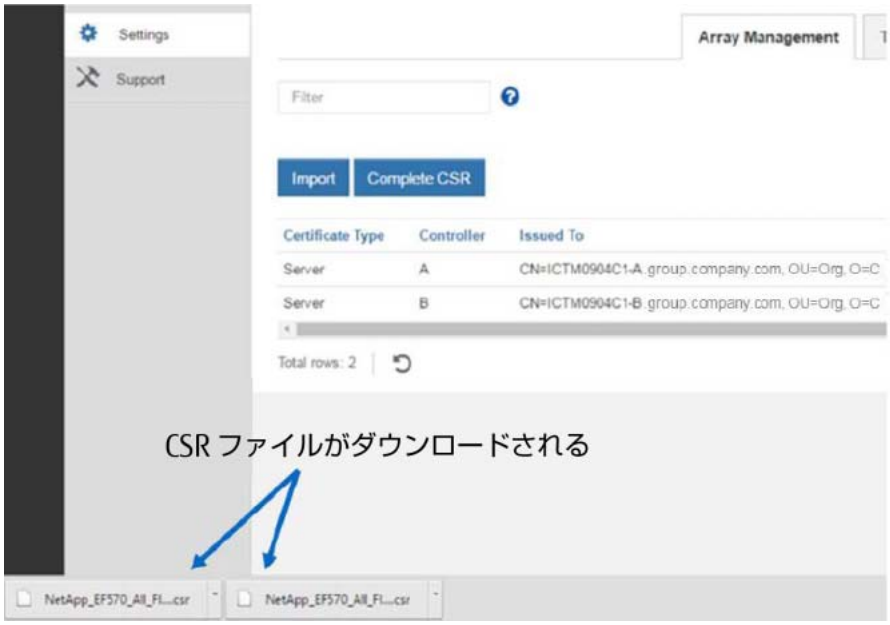
DNS を使用しない場合は、自動設定された共通名や代替 IP アドレスを変更しないでください。コンマ区切りの一覧に代替 IP アドレスを追加できますが、共通名 IP と最初の代替 IP アドレスは完全に一致する必要があります。



**3-3** コントローラ B の情報を変更または入力するには、コントローラ B の FQDN を使用します。




**3-4** Finish をクリックして、コントローラ A 用とコントローラ B 用の 2 つの CSR ファイルを生成します。



**4** CSR ファイルを CA に送信し、1 つ以上の新しい署名済みセキュリティ証明書 ( たとえば、Verisign や DigiCert) を要求し、PEM 形式の署名済み証明書を要求します。

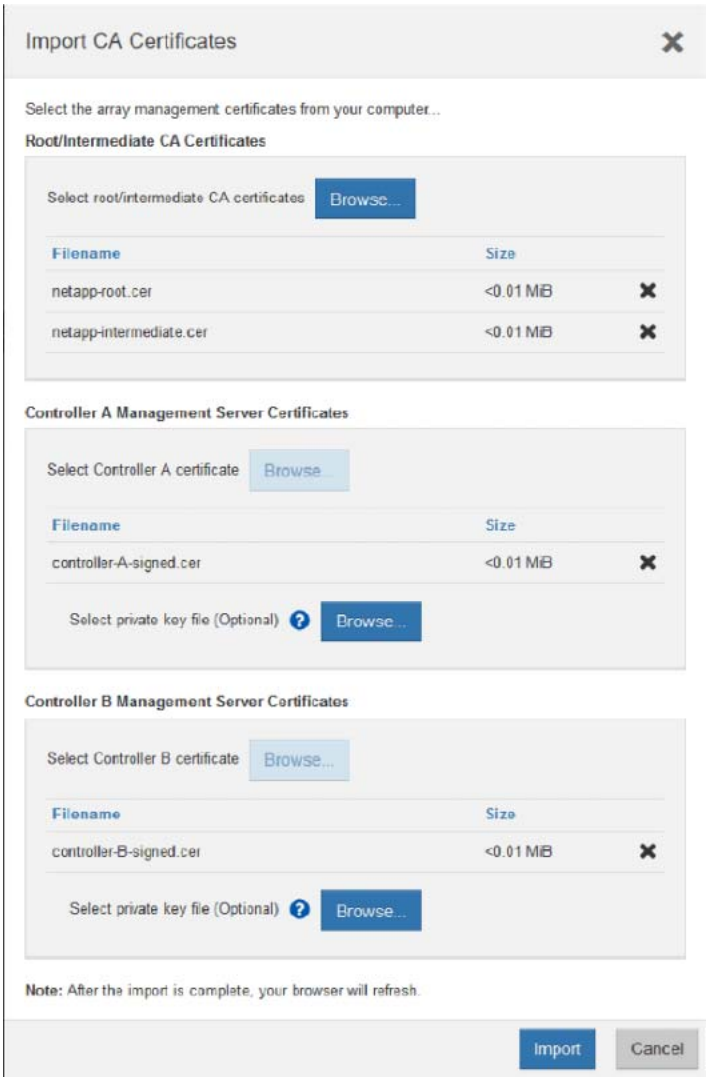
注 意

- ETERNUS AB/HB series システムでは、署名付き証明書に PEM 形式 (Base 64 ASCII エンコーディング ) が必要です。PEM 形式には、次のファイルタイプ .pem、.crt、.cer、および .key が含まれます。
- CSR ファイルを CA に送信した後は、別の CSR ファイルを再生成しないでください。CSR を生成するたびに、秘密鍵と公開鍵のペアが作成されます。公開鍵は CSR の一部ですが、秘密鍵はシステムのキーストアに保持されます。署名付き証明書を受け取ってインポートすると、システムは秘密鍵と公開鍵の両方が元のペアであることを確認します。キーが一致しない場合、署名された証明書は機能しないため、CA に対して新しい証明書を要求する必要があります。

**5** CA から証明書ファイルを受け取ったら、SANtricity System Manager Import Certificates ウィザードを使用してインポートする必要があります。これらのファイルには、ルート証明書、1 つ以上の中間証明書、およびサーバー証明書が含まれます。

注 意

- 証明書が個別に提供されない場合 ( ルート証明書、中間証明書、およびセキュリティ証明書 )、Windows 証明書マネージャツールを使用してチェーンを分割する必要があります。証明書チェーンを分割する場合は、必ず base-64 エンコーディングを使用してください。
- CA がチェーン化された証明書ファイル ( たとえば、a .p7b ファイル ) を提供した場合は、チェーン化されたファイルを個別のファイル、つまりルート証明書、1 つ以上の中間証明書、およびコントローラを識別するサーバー証明書にアンパックする必要があります。Windows の certmgr ユーティリティーを使用して、ファイルをアンパックできます ( 右クリックして All Tasks > Export を選択します )。Base-64 エンコーディングをお勧めします。エクスポートが完了すると、チェーン内の証明書ファイルごとに CER ファイルが表示されます。




**6** Settings > Certificates を選択します。

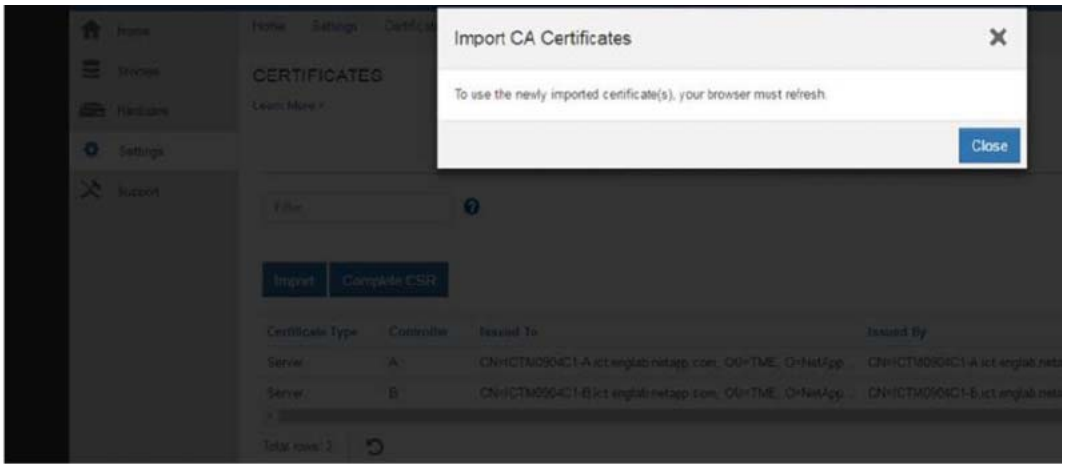
**7** [Array Management] タブで、[Import] を選択します。証明書ファイルをインポートするためのダイアログボックスが開きます。

**8** [Browse] ボタンをクリックして、最初にルートおよび中間証明書ファイルを選択し、次にコントローラの各サーバー証明書を選択します。

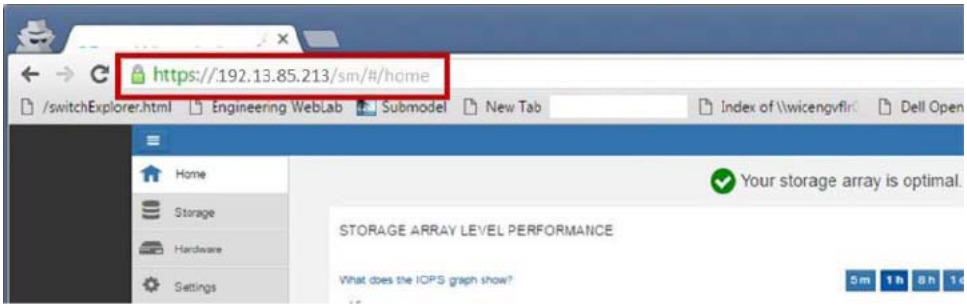
ルートファイルと中間ファイルは、両方のコントローラで同じです。サーバー証明書だけが各コントローラで一意です。外部ツールから CSR を生成した場合は、CSR とともに作成された秘密鍵ファイルもインポートする必要があります。

**9** ファイル名はダイアログボックスに表示されます。[Import] をクリックします。

**10** ファイルがアップロードされ、検証されます。CA ルート証明書と中間証明書はすべてのインターフェースで同じであり、各コントローラの署名済みセキュリティ証明書を検証するためにアップロードする必要があります。
セッションは自動的に終了します。証明書を有効にするには、再度ログインする必要があります。再度ログインすると、新しい CA 署名証明書がセッションに使用されます。インポート処理が完了すると、ブラウザセッションを更新するためのメッセージがブラウザに表示されます。




**11** ブラウザセッションを閉じて新しい SANtricity System Manager セッションを開始すると、セキュリティで保護されたブラウザ接続であることが示されます。



# 5.3　LDAPS サーバーの証明書管理

デフォルトでは、クライアントとサーバーアプリケーション間の LDAP 通信は暗号化されません。つまり、ネットワーク監視デバイスまたはソフトウェアを使用して、LDAP クライアントとディレクトリサーバ間の通信を表示できます。この状況は、資格情報 ( ユーザー名とパスワード ) が暗号化されずにネットワーク上で渡されるため、LDAP 単純バインドが使用される場合に特に問題になります。これはすぐに資格情報の侵害につながる可能性があります。

LDAP over Secure Sockets Layer (SSL) および Transport Layer Security (TLS)、別名 LDAPS を有効にする理由は次のとおりです。

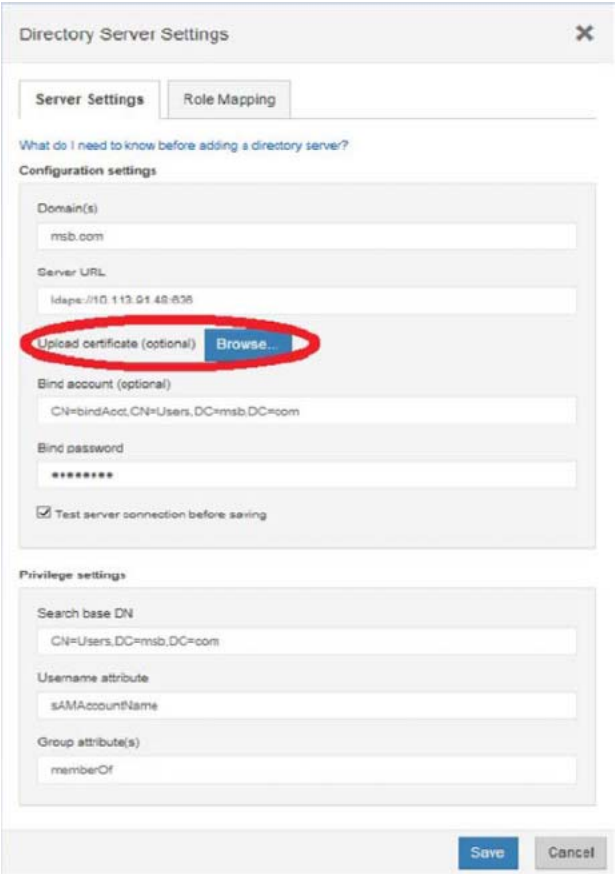
- 一部の Windows アプリケーションは、単純バインドによって Active Directory ドメインサービス (AD DS) で認証します。単純バインドではユーザーの資格情報が平文で公開されるため、Kerberos を使用することをお勧めします。単純バインドが必要な場合、SSL/TLS を使用して認証セッションを暗号化することを強く推奨します。
- LDAP 上でのプロキシバインドの使用またはパスワード変更 (LDAPS が必要 ) 。
- LDAP サーバーと統合されている一部のアプリケーション (Active Directory および Active Directory ドメインコントローラなど ) では、暗号化された通信が必要です。Windows ネットワークで LDAP 通信を暗号化するには、LDAP over SSL/TLS (LDAP) を有効にします。

LDAPS がサポートされており、図 5.7 に示すように、SANtricity System Manager GUI を使用して構成できます。便宜上、ディレクトリサーバー構成ウィザードでは、LDAPS サーバーの CA 署名付き証明書に一致する CA ルート証明書と中間証明書をアレイトラストストアにアップロードできます。これは、セキュア SMcli を使用して行うこともできます。

**注 意**

ほとんどの場合、ルート証明書のみをアレイトラストストアにアップロードする必要がありますが、LDAPS サーバーのルート証明書と中間証明書の両方をアレイトラストストアに置く必要がある場合もあります。

図 5.6　LDAP サーバの CA ルート証明書をアレイトラストストアにアップロードするオプション




# 5.4　組み込み外部鍵管理サーバーの証明書管理

Gemalto SafeNet KeySecure Enterprise Encryption Key Management などの中央鍵管理プラットフォームを使用して FDE セキュリティキーを管理でき、フルディスク暗号化 (FDE) 機能が強化されています。このプラットフォームは Key Management Interface Protocol (KMIP) 規格に準拠しています。この機能は、SANtricity OS 11.60 以降を実行するすべてのストレージシステムで使用できます。

外部鍵管理機能を有効にするプロセスで、管理者はアレイに一連の証明書をインストールする必要があります。これらの証明書は、ストレージシステムと鍵管理サーバー間の安全な接続と認証の両方を確立するために使用されます。SANtricity System Manager は、管理者がインターフェースを使用して、ストレージシステムコントローラに対する証明書署名要求 (CSR) を生成し、ストレージシステムの署名付きクライアント証明書と EKMS サーバの SSL 証明書の両方をインストールするプロセスを提供します。この処理は、SMcli を使用して実行することもできます。

**注 意**

以下のステップは、Gemalto Key Management Server に適しています。他の Key Management Server 製品には、他のシーケンスが必要な場合があります。

## 5.4.1　外部鍵管理を有効にする手順

外部鍵管理サーバ (EKMS) 自体で実行する必要のある設定手順がいくつかあります。このガイドでは、これらの手順について詳しく説明するのではなく、EKMS から取得した成果物について説明します。

**手順 ▶▶▶**

1. EKMS サーバーのセットアップ中に、クライアント要求に使用する認証のタイプを選択できます。最もセキュアなタイプとして SSL session and username を選択することをお勧めします。
   この構成ステップでは、クライアントの証明書のどのフィールドをユーザー名として使用するかを選択できます。これにより、認証を提供するためにクライアント証明書にユーザー名を渡すことができます。
2. SANtricity System Manager を使用して、新しい CSR を生成します。CSR 要求ダイアログで、ステップ 1 で指定したのと同じフィールドにユーザー名を指定します。
   「図 5.8　証明書署名要求ダイアログ」(P.61) を参照してください。
3. CSR 情報を EKMS サーバーに送信し、証明書署名プロセスを実行します。
   新しいクライアント証明書を生成し、ローカルシステムにダウンロードする必要があります。
4. SANtricity System Manager を使用して、EKMS サーバーへの接続を構成します。
   この手順では、EKMS サーバの IP アドレスまたはホスト・アドレスとポート番号を指定し、ストレージアレイクライアント証明書をインポートする必要があります。ストレージアレイが EKMS サーバを信頼できるように、EKMS サーバ証明書もインポートする必要があります。EKMS サーバの中間証明書またはルート証明書もインポートできます。「図 5.9　鍵管理サーバーへの接続」(P.62) を参照してください。
5. 次の手順では、オプションでバックアップキーを取得し、接続設定を終了します。
   [Create backup key] チェックボックスをオフにすると、バックアップキーはダウンロードされません。
6. [Finish] ボタンをクリックして、Create External Security Key ワークフローを完了します。

◀◀◀

図 5.7 は、外部鍵管理サーバー証明書が管理される SANtricity System Manager のオープン証明書タイルを示しています。

図 5.7　SANtricity System Manager で CSR を完了し、ストレージシステムの署名付きクライアント証明書および EKMS サーバーの SSL 証明書をインポートするためのオプション


図 5.8　証明書署名要求ダイアログ

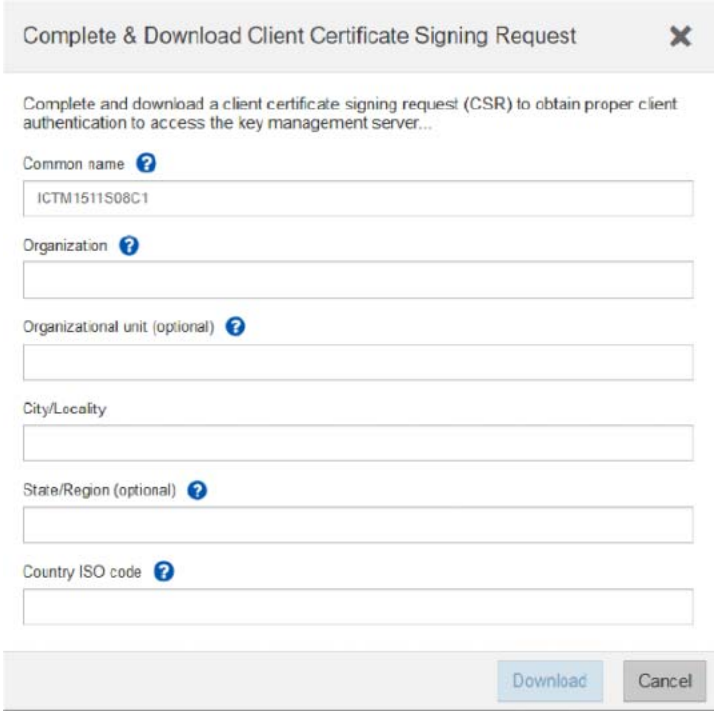


図 5.9　鍵管理サーバーへの接続

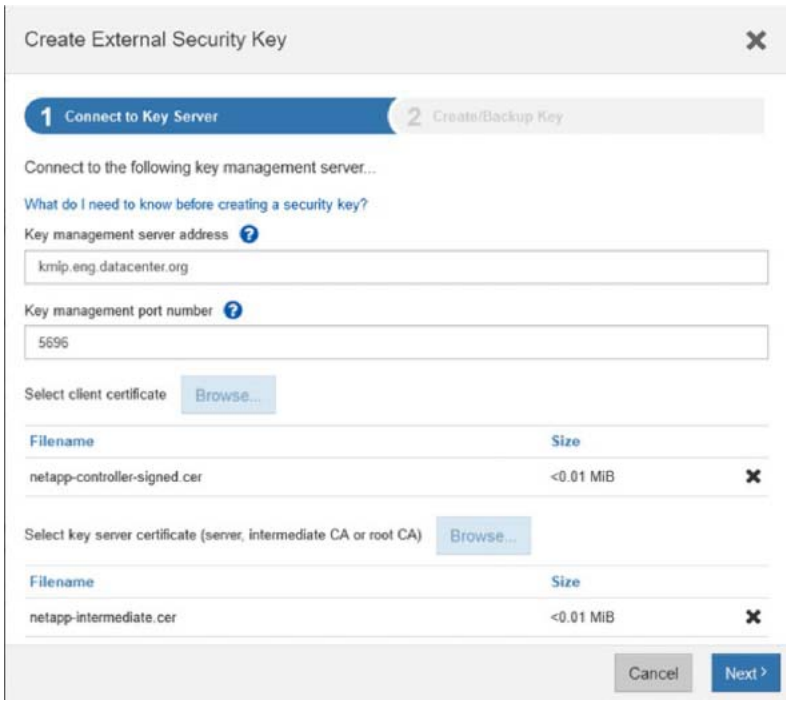
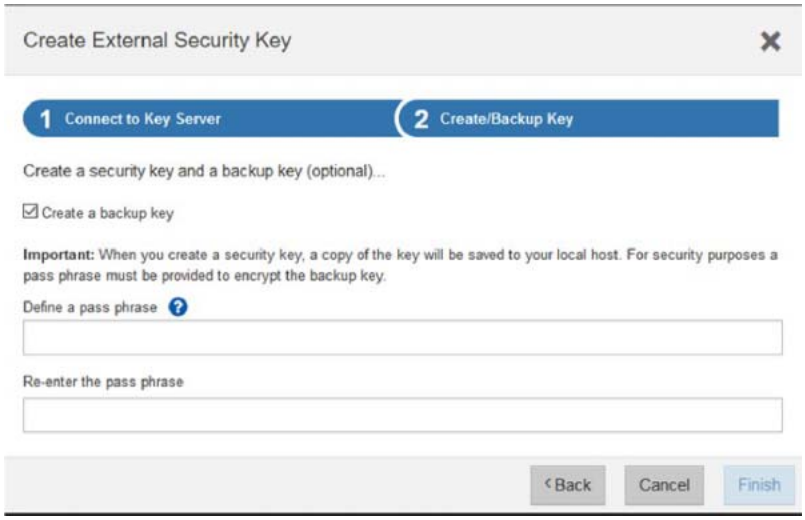



図 5.10　オプションのバックアップキーの作成



# 第 6 章

# SAML 2.0 および MFA (SANtricity OS の場合 )

Security Assertion Markup Language (SAML) は、複数のシステム間で安全に認証要求とユーザー・データを送信するための業界標準です。この標準では、多くのアプリケーションが 1 つのサービスを使用して、すべてのユーザー認証とセッション管理を管理できます。

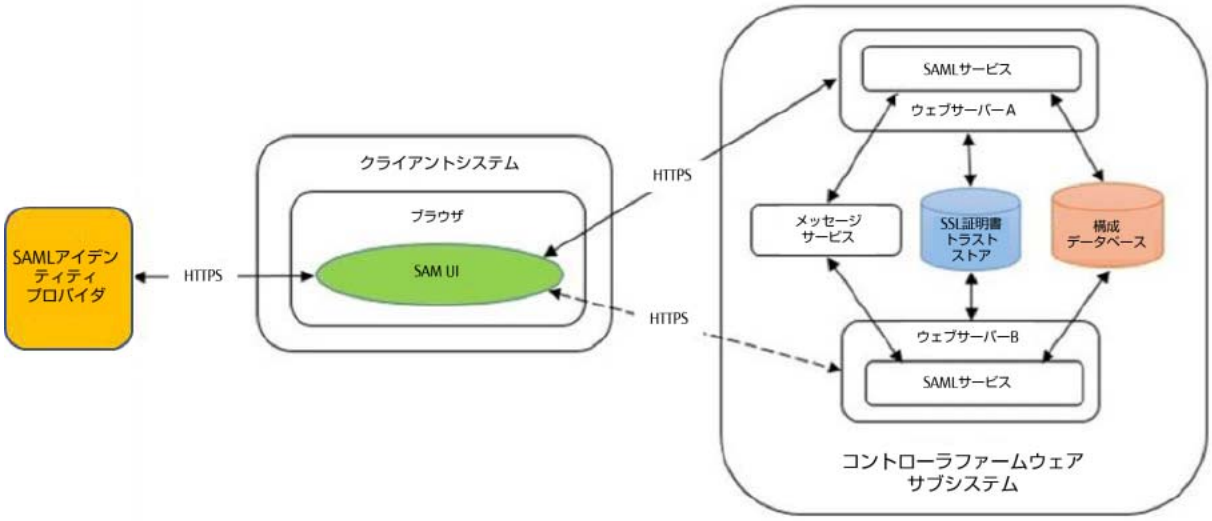
多要素認証 (MFA) では、認証に成功するために、ユーザーが本人であることの証明として 2 つ以上の項目を提供する必要があります。認証に必要な項目で典型的なものは知識 ( パスワードなどユーザーが記憶しているもの )、所有物 ( コード変更をする機械などユーザーが所持しているもの )、または個人のもの ( 指紋などの生体認証をはじめとするユーザーに固有のもの ) の内の、少なくとも二種類です。必要なエビデンスの具体的なタイプは、エンドユーザー組織のセキュリティチームが設定します。

SAML を ETERNUS AB/HB series 製品に統合すると、複数の形式の認証でユーザーを認証し、認証の成功または失敗を SANtricity System Manager アプリケーションに報告できる外部システムと通信できます。外部システムは、単一要素認証、2 要素認証、または多要素認証を使用するように構成できます。外部システムは、他のアプリケーションとのシングル・サインオン機能をサポートする機能も提供します。

## 6.1 MFA アーキテクチャの概要

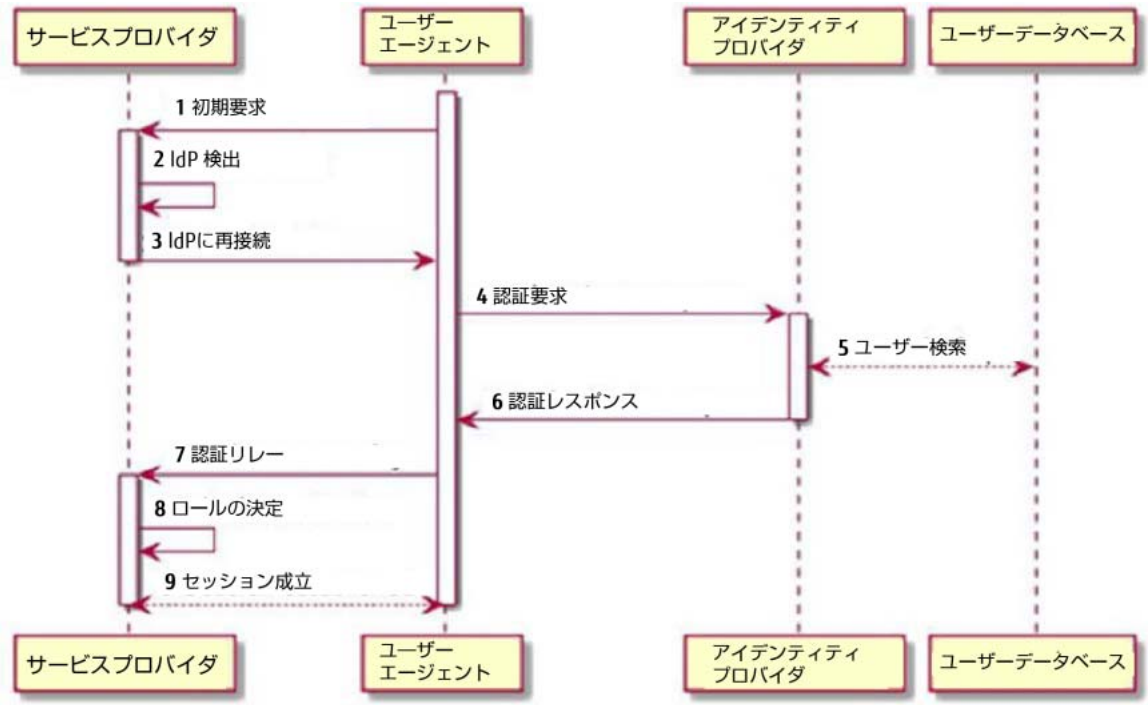
SAML は、ETERNUS AB/HB series 製品に標準のバージョン 2.0 を使用して統合されており、富士通は、Shibboleth と Microsoft ADFS をアイデンティティプロバイダ (IdP) として公式にサポートしています。図 6.1 は、SAML 統合を実現するために使用されるすべてのコンポーネントのハイレベルな概要を示しています。認証サーバとの通信はユーザーの Web ブラウザを通じて行われるため、SANtricity System Manager アプリケーションが直接接続することはありません。SAML により、SANtricity System Manager はユーザーの Web ブラウザを経由して HTTP リダイレクションを使用し、機密情報をアイデンティティプロバイダに渡すことができます。すべての情報は、アイデンティティプロバイダが提供する証明書を使用して署名および暗号化されます。これにより、ETERNUS AB/HB series 製品では、Shibboleth や Microsoft ADFS などのサードパーティ製 IdP で認証されたユーザーによる管理が可能になります。SANtricity System Manager を構成すると、適切なロールで承認を行い、IdP を使用して認証されたユーザーに固有の識別名または ID を関連付けることができます。

図 6.1　SAML の ETERNUS AB/HB series 製品への統合



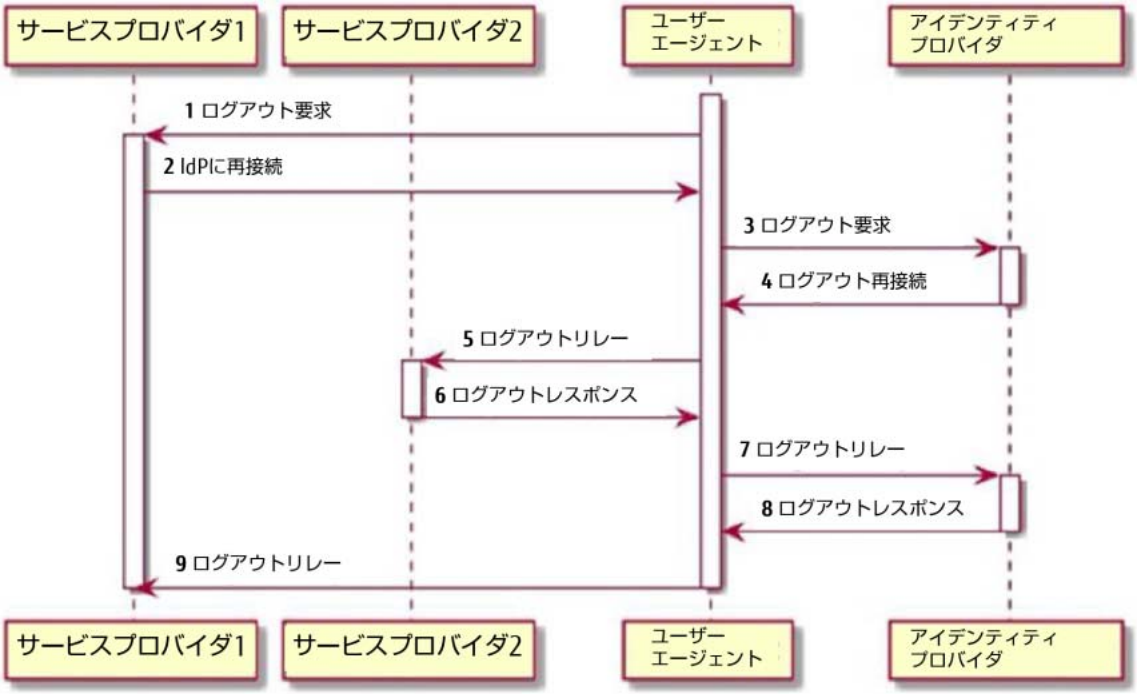

SAML が ETERNUS AB/HB series システムで構成された後、SANtricity System Manager へのログインは、構成された IdP からのみ可能です。ユーザーが SANtricity System Manager にアクセスしようとすると、デフォルトの SANtricity System Manager ログイン・ページではなく、IdP のログイン・ページに転送されます。認証情報を入力すると、ユーザーは認証されたセッションとともに SANtricity System Manager に送り返され、ユーザーに関連付けられた属性に基づいて認証されます。図 6.2 は、ETERNUS AB/HB series システムのさまざまなコンポーネントでのログイン要求の流れを示しています。サービス・プロバイダは ETERNUS AB/HB series 製品を表します。ユーザーエージェントは、ユーザーの Web ブラウザを表します。アイデンティティプロバイダは、認証を管理するサード・パーティのサービス (Microsoft ADFS や Shibboleth など ) を表します。ユーザー・データベースは LDAP などのバックエンド・ユーザー管理アプリケーションです。

図 6.2　SAML を使用したログイン要求の概要




アイデンティティプロバイダは、認証されたユーザーに関連付けられたすべてのセッションを管理するため、ユーザーをシステムからログアウトする要求を発行する場合があります。IdP は、図 6.3 に示すように、サポートするすべてのアプリケーションに対して単一のログアウト要求を発行することによって、このタスクを実行します。SANtricity System Manager アプリケーションはこの要求を受信し、ログアウト要求に関連するすべてのセッションを無効にします。

図 6.3　SAML を使用した IdP 起動ログアウトの概要



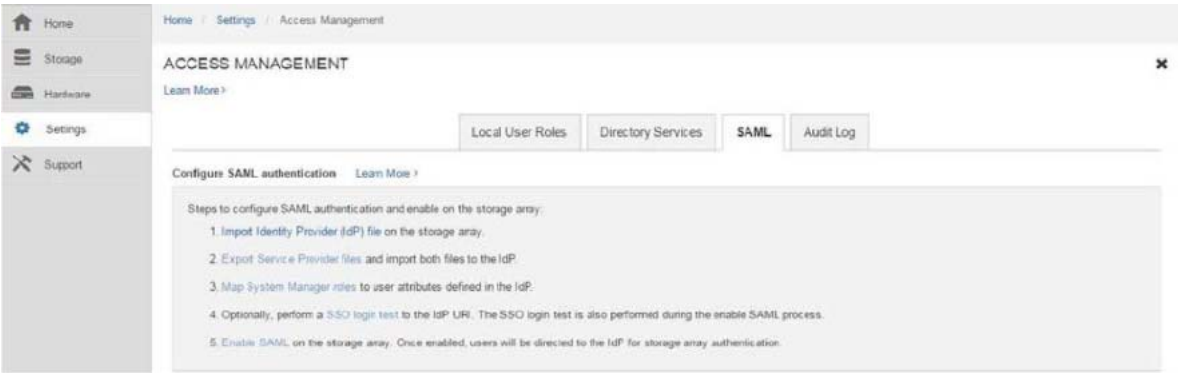
# 6.2　SAML の構成

サード・パーティのアイデンティティプロバイダと連携するように SANtricity System Manager を構成するには、SANtricity System Manager と IdP サーバーの両方で、いくつかの手順を実行する必要があります。図 6.4 に示すように SAML タブは SANtricity System Manager の Settings > Access Management タイルにあります。このタブでは、IdP の設定でユーザーを認証できます。SAML 構成が完了して検証されると、有効にできます。SAML が使用可能になっている場合、SAML は、SANtricity System Manager にアクセスするユーザーの認証に使用される唯一の方法です。他の形式の管理は、認証できないために機能しなくなりました。これには、SANtricity、SMcli クライアント、ソフトウェア開発キットクライアント、UTM を使用したインバンド管理、HTTP 基本認証を使用した REST API クライアント、および標準ログインエンドポイントを使用した REST API クライアントが含まれます。

**注 意**

お客様は、SAML を有効にする前に、構成が十分にテストされていることを十分に確認する必要があります。ハードウェアに物理的にアクセスしないと無効にできません。SAML を使用不可にするには、ストレージシステム上のコントローラへのシリアル・シェル・アクセスが必要であり、手順についてテクニカル・サポート・エンジニアに連絡する必要があります。

図 6.4　構成が存在しない場合の SANtricity System Manager の「SAML」タブ




SANtricity System Manager は、メタデータ・ファイルを交換することによって、アイデンティティプロバイダとの信頼関係を確立します。お客様は、アイデンティティプロバイダのメタデータ・ファイルをエクスポートし、Access Management の「SAML」タブにある「Import Identity Provider file」リンクを使用して SANtricity System Manager にインポートする必要があります。このプロセスでは、IdP を SANtricity System Manager に登録して、アプリケーションがユーザーを認証用に送信する場所を認識できるようにします。

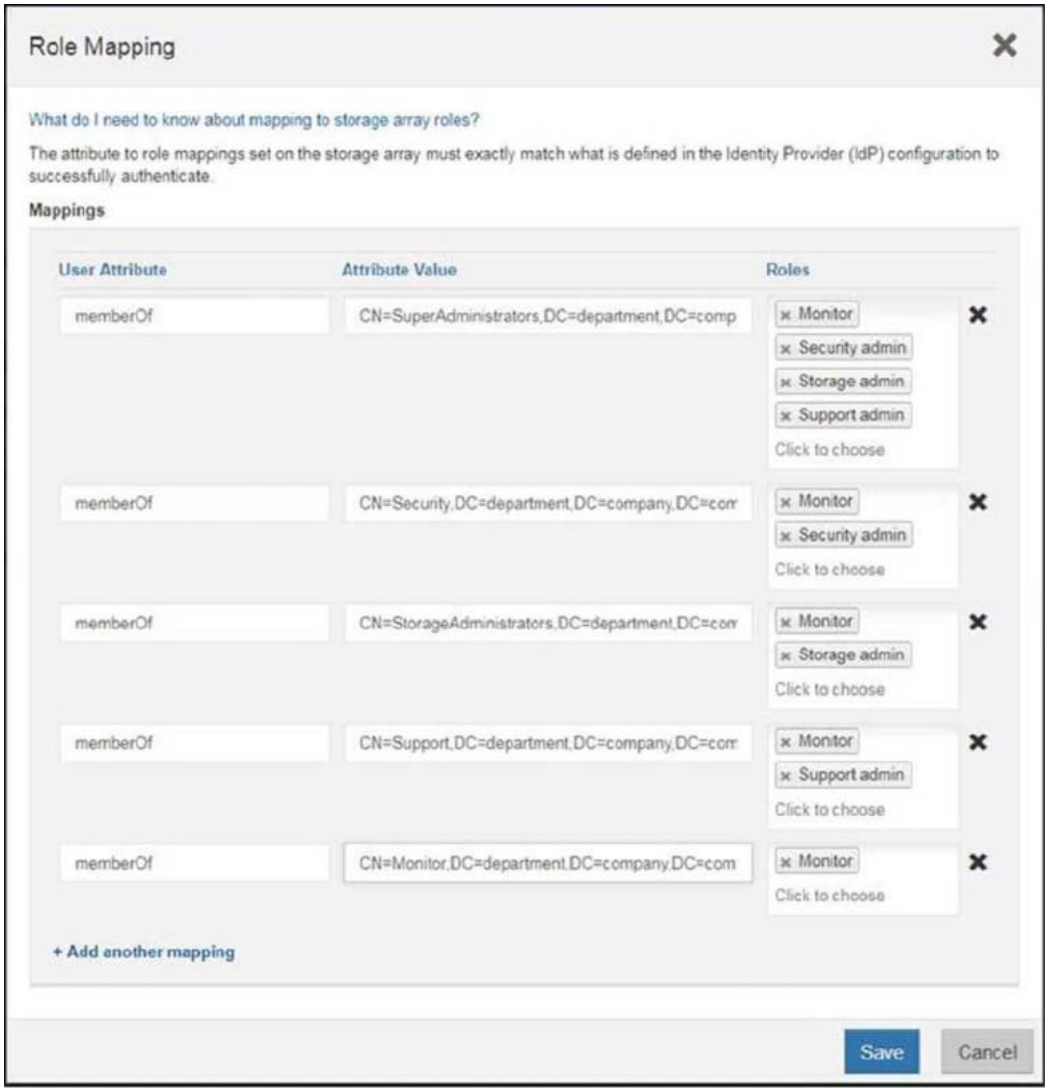
次に、Access Management の「SAML」タブにある「Export Service Provider Files」リンクを使用して、ストレージシステムのすべてのコントローラから SANtricity System Manager メタデータ・ファイルをエクスポートする必要があります。これらのファイルは IdP に送信され、IdP からの認証を使用するサービスプロバイダとして ETERNUS AB/HB series システムを登録します。

SANtricity System Managerがユーザーにさまざまなロールを適切に許可できるように、アイデンティティプロバイダは属性を提供する必要があります。Microsoft ADFS では、LDAP 属性を、認証要求で返すことができる要求ルールにマッピングすることによって、これを実現しています。Shibboleth では、さまざまな構成 XML ファイルを使用して、各アイデンティティプロバイダに対する認証要求とと

もに返される属性をマッピングします。認証中に SANtricity System Manager に戻される属性のセットアップ方法については、これらの製品の公式資料を参照してください。IdP で属性を構成した後、Access Management の「SAML」タブにある「Map System Manager Roles」リンクを使用して、これらの属性を SANtricity System Manager のさまざまなロールに割り当てます。

図 6.5 に示すように、ユーザーに SANtricity System Manager へのアクセスを許可するため、その組み合わせに一致させたいロールのユーザー属性と属性値を入力します。これにより、SANtricity System Managerは、ユーザーがIdPを介して認証された後に、そのユーザーにロールを正しくマップできます。

図 6.5　SANtricity System Manager でロールを構成する一般的な方法




IdP は、ユーザー属性に加えて、ランダムに生成された ID を使用せずにユーザーを一意に識別するために、SANtricity System Manager の有効な NameID を送り返す必要があります。これは必須ではありませんが、監査ログを使用してユーザーアクティビティをより適切に報告できます。Shibboleth と Microsoft ADFS は、さまざまな構成オプションとともに NameID を返すことをサポートしています。SANtricity System Manager に送信される NameID を構成するには、IdP の資料を参照してください。

この時点で、SANtricity System Manager は、構成済みのアイデンティティプロバイダを使用してログインをテストできる状態になっています。これは、Access Management の「SAML」タブの「SSO

Login Test」リンクを使用して行います。このテストでは、ユーザーを IdP のログインページにリダイレクトして、設定されているすべての設定を使用してユーザーが正しく認証および承認されていることを確認します。この検査はいくつかの理由で失敗することがありますが、最も一般的な原因は、認証されたユーザーのロールが正しくマップされていないことです。
ロールのマッピングが有効でもログインテストを正常に完了できない場合は、表 6.1 を参照して、IdP 構成で発生する可能性のあるその他の問題を確認してください。

表 6.1　一般的な構成の問題

| 設定ミスの問題 | 説明 |
|---|---|
| ストレージシステムのクロックとアイデンティティプロバイダのクロックが同期していません | SAML は、古いデータを使用する攻撃を防ぐために、期限切れのタイムスタンプを使用します。ストレージシステムクロックと IdP クロックの間隔が 5 分を超えると、SANtricity System Manager の SAML 認証が失敗します。 |
| 期限切れの IdP 証明書 | IdP 証明書の期限が切れていると、SANtricity System Manager 内のすべての SAML 認証が失敗します。この場合、お客様は富士通 のテクニカルサポートエンジニアの支援を受けて SAML を無効にし、ストレージシステムにシリアル接続して、メタデータに埋め込まれた有効な x 509 証明書を持つ IdP メタデータ・ファイルを再インポートする必要があります。 |
| ロールをマップできません | SSO ログイン・テストは、適切なロールをマップできなかったというエラーで継続的に失敗します。これは、属性をロールにマップするようにアイデンティティプロバイダまたは SANtricity System Manager が正しく構成されていないために発生します。また、テストを成功させるにはセキュリティ管理者とストレージ監視者のロールが必要であるために発生することもあります。認証中に SANtricity System Manager に戻される属性のセットアップ方法については、これらの製品の公式資料を参照してください。 |
| ユーザー名は、数字と文字の長い読み取り不能なリストとして報告される | アイデンティティプロバイダに構成済みの NameID がないため、ランダムに生成された ID を持つユーザーが SANtricity System Manager で識別されます。SANtricity System Manager に送信される NameID を構成するには、IdP の資料を参照してください。 |

テストが正常に完了したら、「Enable SAML」リンクを使用できます。SAML が使用可能になった後、SAML は、SANtricity System Manager へのアクセスのためにユーザーを認証するために使用される唯一の方法です。他の形式の管理は、認証できないために機能しなくなりました。これには、SANtricity、Unified Manager、SMcli クライアント、ソフトウェア開発者キットクライアント、UTM を使用したインバンド管理、HTTP 基本認証を使用した REST API クライアント、および標準ログインエンドポイントを使用した REST API クライアントが含まれます。

# 第 7 章
# まとめ

富士通は、ストレージ管理のセキュリティと保存されているデータのセキュリティを重要視しています。増え続ける悪意のあるインサイダー活動による脅威に対処するために、RBAC、ディレクトリサービスのサポート、セキュア SMcli、証明書管理、監査ログ、SAML 2.0 を使用した IdP との多要素認証などの新機能を SANtricity OS 11.60 以降に実装しました。これらの機能拡張は、お客様がデータを保護するのに役立ちます。複数のインターフェース・オプションとセキュリティ構成の選択肢により、管理セキュリティの強化がすべての新しいストレージシステムの重要な要件となっているエンタープライズ環境において、ETERNUS AB/HB series のシステムを容易に導入できます。

# 付録 A
# よくある質問

この付録では、SANtricity Management セキュリティ機能のルールと機能に関する一般的な質問に回答します。

## A.1 LDAP、RBAC、および証明書

この節では、LDAP、RBAC、および証明書に関するよくある質問について説明します。

### ■ SYMbol API が無効になっていて、ユーザーが LDP パスワード ( またはアクセス ) を失った場合はどうなりますか。

回答 :
ユーザーは、ローカルアカウントを使用してストレージシステムにログインするか、シリアル・シェルにアクセスして、SYMbol アクセスを手動で再度有効にしたり、LDAP 認証を無効にしたりできます。シリアル・シェルを使用する必要がある場合は、富士通サポートにお問い合わせください。

### ■ 証明書の形式を指定してください。

回答 :
PEM (Base-64 エンコード ) 形式でなければなりません。

### ■ SANtricity System Manager にタイルがないのはなぜですか。

回答 :
タイルが存在しない場合は、ユーザーの現在のロールではアクセスできない REST API エンドポイントに関連付けられます。

### ■ SANtricity System Manager 全体で一部の入力、ボタン、およびその他の要素が使用不可になっているのはなぜですか。

回答 :
選択したオブジェクトまたは特定のコンテキストでオプションがサポートされていない場合、適用できない場合、または有効でない場合は、要素を無効にできます。さらに、ユーザーの現在のロールではアクセスできないダイアログボックスや REST API エンドポイントに関連付けられている要素は無効にすることができます。

## ■ 一部のストレージシステムやミラーグループが [Create Mirror Group] および [Create Mirrored Pair] ダイアログボックスに表示されないのはなぜですか。

回答 :
リモートストレージシステムのリストは、ストレージシステムが現在のストレージシステムと互換性のある非同期ミラーリングまたは同期ミラーリングのどちらであるかに基づいてフィルタリングされます。SYMbol を無効にできるようになりましたが、SANtricity System Manager で Create Mirror Group ワークフローと Create Mirrored Pair ワークフローを有効にするには、両方のストレージシステムで SYMbol を有効にする必要があります。[Create Mirror Group] ダイアログボックスと [Create Mirrored Pair] ダイアログボックスのリモートストレージシステムの一覧、および [Create Mirrored Pair] ダイアログボックスのミラーグループは、そのリモートストレージシステムで SYMbol が有効になっているかどうかに基づいてフィルタされます。

## ■ 有効な LDAP ユーザー名とパスワードが認証されないのはなぜですか。

回答 :
LDAP 構成が正しく構成されていない可能性があります。使用した設定を再度確認し、問題が解決しない場合は、エラーメッセージが Web サーバーのデバッグログに記録されていないかどうかを確認します。

または、ブラウザで <array_ip>/devmgr/v2/storage-systems/1/ldap/test を実行し、その組み込みシステムで構成されているドメインに関する問題を出力します。

## ■ SANtricity System Manager を実行している組み込みシステムに定義されているローカルユーザーアカウントは何ですか。

回答 :
admin@local、storage@local、monitor@local、support@local、security@local です。

## ■ デフォルトの admin パスワードは何ですか。

回答 :
デフォルトの admin パスワードは、常にストレージアレイパスワードです。

## ■ ログイン時に 403 応答が返されるのはなぜですか。

回答 :
監査ログがいっぱいの場合、試行回数が多すぎるか、権限が不十分なため、ログインがロックアウトされます。過度のログイン失敗の場合は 10 分待つか、セキュリティ管理者権限でログインして監査ログを消去します。

## ■ ログイン以外の要求に対して 403 応答が返されるのはなぜですか。

回答 :
認証されたユーザーがその要求に対する適切なアクセス権を持っていないか、XSRF トークンが無効であるか、監査ログがいっぱいでアクセスが制限されています。

## ■ SANtricity System Manager をアクティブに使用していたときにログアウトしたのはなぜですか。

回答 :
別のユーザーがセキュリティ関連の構成を変更したため、他のすべてのユーザーがログアウトされました。

## ■ LDAP ドメイン名として local を指定できないのはなぜですか。

回答 :
Rest API は "local" をシステムのローカルアカウントに使用するために予約しています。

## ■ 署名済みサーバー証明書をインポートすると、ルート証明書と中間証明書がキーストアから削除されるのはなぜですか。

回答 :
署名されたサーバー証明書がインポートされると、キーストアは削除され、署名された証明書チェーンの検証に必要なルート証明書と中間証明書だけが残ります。

# A.2 ETERNUS AB/HB series 上の SAML 2.0

この項では、ETERNUS AB/HB series の SAML 2.0 に関する質問について説明します。

## ETERNUS AB/HB series がサポートするアイデンティティプロバイダを教えてください。

回答 :
ETERNUS AB/HB series は、ADFS 3.0 および Shibboleth IdP をサポートしています。

## SANtricity System Manager で SSO テストがタイムアウトになるのはなぜですか。

回答 :
SANtricity System Manager は、ダイアログボックスを使用して SSO テストを実行します。ブラウザが SANtricity System Manager のダイアログボックスをブロックしていないことを確認します。

## ストレージシステムをアクティブに管理しているときに SANtricity System Manager からログアウトしたのはなぜですか。

回答 :
IdPは、ユーザーのセッションが無効になる時間を指定します。この時間に達すると、SANtricity System Manager はユーザーをログアウトし、再認証を要求します。また、SAML の構成を変更すると、すべてのユーザーがログアウトされます。

## ストレージシステム構成をクリアした場合、アイデンティティプロバイダを再構成する必要がありますか。

回答 :
はい。正しい証明書ファイルが設定されていることを確認するには、E-Series システムによって生成されたメタデータをコントローラから再エクスポートし、IdP にインポートする必要があります。

## SAML 機能の SANtricity System Manager でサポートされているブラウザは何ですか。

回答 :
Internet Explorer、Firefox、Chrome、および Safari です。現在、Edge ブラウザでは SAML 機能はサポートされていません。

FUJITSU Storage ETERNUS AB series オールフラッシュアレイ ,
ETERNUS HB series ハイブリッドアレイ
SANtricity 管理セキュリティ

P3AG-6052-01Z0

発行年月　2021 年 6 月
発行責任　富士通株式会社

FUJITSU