同意トークン

同意トークンは、ネットワーク管理者と Cisco Technical Assistance Centre（Cisco TAC）の相互の同意により、システムシェルにアクセスする組織のネットワーク管理者を認証するために使用されるセキュリティ機能です。

同意トークンの制約事項

- 同意トークンはデフォルトで有効であり、無効にすることはできません。
- デバイスからチャレンジが送信された後、30 分以内に応答を入力する必要があります。入力しないとチャレンジが期限切れになり、新しいチャレンジの要求が必要になります。
- 単一の応答は、対応するチャレンジに対して 1 回だけ有効です。
- ルートシェルアクセスの最大承認タイムアウトは 7 日間です。
- スイッチオーバーイベント後、既存の同意トークンベースの承認はすべて期限切れとして処理されます。その後、サービスアクセスの新しい認証シーケンスを再起動する必要があります。
- シスコのチャレンジ署名サーバー上の同意トークン応答生成にアクセスできるのは、シスコ認定担当者のみです。
- システムシェルアクセスのシナリオでは、承認タイムアウトが発生するか、または同意トークン終了承認コマンドによってシェル承認が明示的に終了されるまで、シェルを終了しても承認は終了しません。

システムシェルアクセスの目的を達成したら、同意トークン終了コマンドを明示的に発行することによって、システムシェルの承認を強制終了することを推奨します。

同意トークンに関する情報

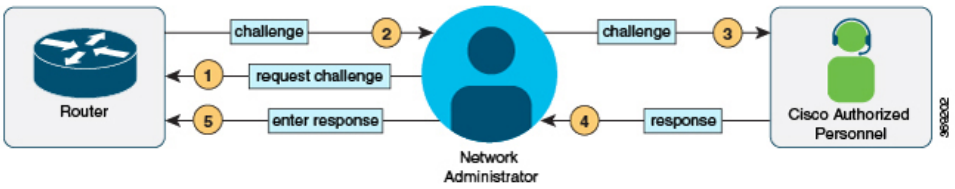
一部のデバッグシナリオでは、Cisco TAC エンジニアが特定のデバッグ情報を収集したり、実稼働システムでライブデバッグを実行する必要がある場合があります。このような場合、Cisco TACエンジニアは、デバイスのシステムシェルにアクセスするようユーザー（ネットワーク管理者）に依頼します。同意トークンは、システムシェルへの特権アクセス、制限アクセス、およびセキュアアクセスを提供する、ロック、ロック解除、および再ロックのメカニズムです。

システムシェルへのアクセスを要求する場合は、認証を受ける必要があります。最初にコマンドを実行し、デバイスの同意トークン機能を使用してチャレンジを生成する必要があります。デバイスは、固有のチャレンジを出力として生成します。このチャレンジ文字列をコピーし、電子メールまたはインスタントメッセージでシスコ認定担当者に送信する必要があります。

シスコ認定担当者は、一意のチャレンジ文字列を処理し、一意のレスポンスを生成します。シスコ認定担当者はこのレスポンス文字列をコピーし、電子メールまたはインスタントメッセージで送信します。

次に、このレスポンス文字列をデバイスに入力する必要があります。チャレンジ/レスポンスペアが一致すると、システムシェルへのアクセスが許可されます。一致しない場合は、エラーが表示され、認証プロセスを繰り返す必要があります。

システムシェルにアクセスしたら、Cisco TAC エンジニアが必要とするデバッグ情報を収集します。システムシェルへのアクセスが完了したら、セッションを終了し、デバッグプロセスを続行します。



システムシェルアクセスの同意トークン承認プロセス

ここでは、システムシェルにアクセスするための同意トークン承認のプロセスについて説明します。

手順の概要

1. 指定された期間、システムシェルへのアクセスを要求するチャレンジを生成します。
2. シスコ認定担当者にチャレンジ文字列を送信します。
3. デバイスにレスポンス文字列を入力します。

4. セッションを終了します。

手順の詳細

ステップ 1 指定された期間、システムシェルへのアクセスを要求するチャレンジを生成します。

例：

```
Device# request consent-token generate-challenge shell-access auth-timeout 900
zSSdrAAAAQEBAAQAAAABAgAEAAAAAAAMACH86csUhmDl0BAAQ0FvdJ7CxqRYUeoD7B4AwW7QUABAAAAG8GAAhDVEFfREVNTwcAGENUQV9ERU1PX0NUQV9TSUdOSU5HX0tFWQgAC0M5ODAwLUNMIUs5CQALOVpQUEVESE5KRkI=
Device#
*Jan 18 02:47:06.733: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (challenge generation attempt:
Shell access 0).
```

request consent-token generate-challenge shell-access *time-validity-slot* コマンドを使用して、チャレンジの要求を送信します。システムシェルへのアクセスを要求する期間（分単位）は、time-slot-period です。

この例の期間は、セッションの期限切れ後 900 分です。

デバイスは、固有のチャレンジを出力として生成します。このチャレンジは、base-64 形式の文字列です。

ステップ 2 シスコ認定担当者にチャレンジ文字列を送信します。

デバイスによって生成されたチャレンジ文字列を、電子メールまたはインスタントメッセージでシスコ認定担当者に送信します。

シスコ認定担当者は固有のチャレンジ文字列を処理し、レスポンスを生成します。レスポンスもまた、固有の base-64 文字列です。シスコ認定担当者はこのレスポンス文字列をコピーし、電子メールまたはインスタントメッセージで送信します。

ステップ 3 デバイスにレスポンス文字列を入力します。

例：

```
Device# request consent-token accept-response shell-access
[illegible]
% Consent token authorization success
*Jan 18 02:51:37.807: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (authentication success: Shell
access 0).

Device# request platform software system shell
Activity within this shell can jeopardize the functioning of the system.
Are you sure you want to continue? [y/n] y
Device#
*Jan 18 02:56:59.714: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (authorization for Shell access
0 will expire in 10 min).
```

request consent-token accept-response shell-access *response-string* コマンドを使用して、シスコ認定担当者から送信されたレスポンス文字列を入力します。

チャレンジ/レスポンスペアが一致すると、システムシェルへのアクセスが許可されます。チャレンジ/レスポンスペアが一致しない場合は、エラーが表示され、手順 1 ー 3 を繰り返す必要があります。

承認されると、要求されたタイムスロットのシステムシェルにアクセスできます。

承認セッションの残り時間が 10 分になると、デバイスはメッセージを送信します。

ステップ 4 セッションを終了します。

例：

```
Device# request consent-token terminate-auth
% Consent token authorization termination success

Device#
*Jan 18 23:33:02.937: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (terminate authentication: Shell
 access 0).
Device#
```

システムシェルへのアクセスが終了したら、**request consent-token terminate-auth** コマンドを使用してセッションを終了できます。このコマンドを使用して、承認タイムアウトの前にセッションを強制終了することもできます。要求したタイムスロットが期限切れになると、セッションも自動的に終了します。

開発キーとリリースキー

Cisco IOS XE セキュアブート機能により、シスコの署名付きソフトウェアのみが Cisco IOS XE プラットフォームにロードされます。開発キーインストール機能を導入する前に、Cisco IOS XE プラットフォームには開発公開キーとリリース公開キーが付属しています。これらのキーは、対応する秘密キーによって署名されたイメージを検証するために使用されます。開発キーのインストール機能をサポートするCisco IOS XEプラットフォームのサブセットは、開発公開キーのないリリース公開キーのみで出荷されます。この機能の変更により、イメージ検証用の開発公開キーがないため、開発秘密キーで署名されたイメージは起動しません。ただし、何らかの理由で、Cisco IOS XEデバイスがシスコに返送された場合、製品の返品および交換（RMA）担当者は、開発秘密キーで署名されたイメージをロードする必要があります。これには、RMA スペシャリストがデバイスに開発公開キーをインストールして、開発秘密キーで署名されたイメージの検証に合格することを確認する必要があります。Dev公開キーをインストールするには、次のセクションで説明するコマンドを使用します。

開発キーアクセスのための同意トークン認証プロセス

ここでは、開発キーにアクセスするための同意トークン承認のプロセスについて説明します。

手順の概要

1. 指定された期間の開発キーへのアクセスを要求するチャレンジを生成します。
2. シスコ認定担当者にチャレンジ文字列を送信します。
3. デバイスにレスポンス文字列を入力します。
4. セッションを終了します。

手順の詳細

ステップ 1 指定された期間の開発キーへのアクセスを要求するチャレンジを生成します。

例：

```
Device# request consent-token generate-challenge dev-key auth-timeout 900
zSSdrAAAAQEBAAQAAAABAgAEAAAAAAAMACH86csUhmDl0BAAQ0FvdJ7CxqRYUeoD7B4AwW7QUABAAAAG8GAAhDVEFfREVNTwcAGENUQV9ERU1PX0NUQV9TSUd0SU5HX0tFWQgAC0M5ODAwLUNMIUs5CQALOVpQUEVESE5KRkI=
Device#
*Jan 18 02:47:06.733: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (challenge generation attempt:
Dev key install).
```

request consent-token generate-challenge Dev-key *time-validity-slot* コマンドを使用して、チャレンジの要求を送信します。開発キーへのアクセスを要求する期間（分単位）は、time-slot-period です。

この例の期間は、セッションの期限切れ後 900 分です。

デバイスは、固有のチャレンジを出力として生成します。このチャレンジは、base-64 形式の文字列です。

（注） ゼロの認証タイムアウトは、永続的な開発公開キーのインストールを意味します。このような永続的なインストールは、セキュリティ上の理由から、シスコの内部デバイスにのみ許可されています。

ステップ 2 シスコ認定担当者にチャレンジ文字列を送信します。

デバイスによって生成されたチャレンジ文字列を、電子メールまたはインスタントメッセージでシスコ認定担当者に送信します。

シスコ認定担当者は固有のチャレンジ文字列を処理し、レスポンスを生成します。レスポンスもまた、固有の base-64 文字列です。シスコ認定担当者はこのレスポンス文字列をコピーし、電子メールまたはインスタントメッセージで送信します。

ステップ 3 デバイスにレスポンス文字列を入力します。

例：

```
Device# request consent-token accept-response dev-key
[illegible]
% Consent token authorization success
*Jan 18 02:51:37.807: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (authentication success: dev key
 access 0).
```

request consent-token accept-response dev-key *response-string* コマンドを使用して、シスコ認定担当者から送信されたレスポンス文字列を入力します。

チャレンジ/レスポンスペアが一致すると、開発公開キーがインストールされます。チャレンジ/レスポンスペアが一致しない場合は、エラーが表示され、手順 1 ー 3 を繰り返す必要があります。

承認セッションの残り時間が 10 分になると、デバイスはメッセージを送信します。

ステップ 4 セッションを終了します。

例：

```
Device# request consent-token terminate-auth
% Consent token authorization termination success
```

```
Device#
*Jan 18 23:33:02.937: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (terminate authentication: Dev
key install).
Device#
```

次に、システムが承認セッションの終了に失敗した場合の出力例を示します。

```
Router#request consent-token terminate-auth dev-key
% No in progress authorization, please generate challenge
Router#
```

開発キーへのアクセスが終了したら、**request consent-token terminate-auth** コマンドを使用してセッションを終了できます。このコマンドを使用して、承認タイムアウトの前にセッションを強制終了することもできます。要求したタイムスロットが期限切れになると、セッションも自動的に終了します。

インストール承認の検証

キーのインストールの承認を検証するには、**show platform software threat-token dev-key** コマンドを使用します。

```
Router#show platform software consent-token dev-key
Consent token statistics : dev-key
   Instance Id                      : 0
   Authorization remaining (minutes) : Permanent
   Challenge generation requests     : 1
   Challenge response timeouts       : 0
   Authentication success            : 1
   Authentication failure            : 0
   Authentication expiry             : 0
   Terminate authentication requests : 0
   Challenge generation errors       : 0
```

同意トークンの有効化または無効化

同意トークンをオンまたはオフにするには、次のデバッグコマンドを使用します。

- **debug platform software consent-token all**
- debug platform software consent-token errors

同意トークンの機能履歴と情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

リリース	機能情報
Cisco IOS XE Gibraltar 16.11.1	この機能が導入されました。
Cisco IOS XE Bengaluru 17.4.1	[開発キー（Dev Key）] および [リリースキー（Release Key）] オプションが導入されました。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。