Consent Token

Consent Token is a security feature that is used to authenticate the network administrator of an organization to access system shell with mutual consent from the network administrator and Cisco Technical Assistance Centre (Cisco TAC).

Restrictions for Consent Token

- Consent Token is enabled by default and cannot be disabled.
- After the challenge has been sent from the device, the response needs to be entered within 30 minutes. If it is not entered, the challenge expires and a new challenge must be requested.
- A single response is valid only for one time for a corresponding challenge.
- The maximum authorization timeout for root-shell access is seven days.
- After a switchover event, all the existing Consent Token based authorizations would be treated as expired. You must then restart a fresh authentication sequence for service access.
- Only Cisco authorized personnel have access to Consent Token response generation on Cisco's challenge signing server.
- In System Shell access scenario, exiting the shell does not terminate authorization until the authorization timeout occurs or the shell authorization is explicitly terminated by the consent token terminate authorization command.

  We recommend that you force terminate System Shell authorization by explicitly issuing the Consent Token terminate command once the purpose of System Shell access is complete.

Information About Consent Token

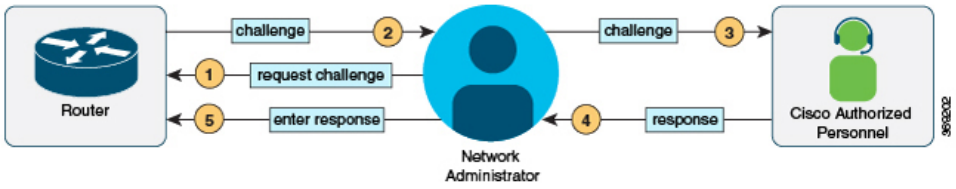
In some debugging scenarios, the Cisco TAC engineer may have to collect certain debug information or perform live debug on a production system. In such cases, the Cisco TAC engineer will ask you (the network administrator) to access system shell on your device. Consent Token is a lock, unlock and re-lock mechanism that provides you with privileged, restricted, and secure access to the system shell.

When you request access to system shell, you need to be authorized. You must first run the command to generate a challenge using the Consent Token feature on your device. The device generates a unique challenge as output. You must then copy this challenge string and send it to a Cisco Authorized Personnel through e-mail or Instant Message.

The Cisco Authorized Personnel processes the unique challenge string and generates a response that is unique. The Cisco Authorized Personnel copies this response string and sends it to you through e-mail or Instant Message.

You must then input this response string into your device. If the challenge-response pair match, you are authorized to access system shell. If not, an error is displayed and you are required to repeat the authentication process.

Once you gain access to system shell, collect the debug information required by the Cisco TAC engineer. After you are done accessing system shell, terminate the session and continue the debugging process.



Consent Token Authorization Process for System Shell Access

This section describes the process of Consent Token authorization to access system shell:

SUMMARY STEPS

1. Generate a challenge requesting for access to system shell for the specified time period.
2. Send the challenge string to a Cisco Authorized Personnel.
3. Input the response string onto your device.
4. Terminate the session.

DETAILED STEPS

Step 1 Generate a challenge requesting for access to system shell for the specified time period.

Example:

```
Device# request consent-token generate-challenge shell-access auth-timeout 900
zSSdrAAAQEBAQAAABgAEAAAAAAAACH86csUmDlOBAQOFvdTCxqFVUsDJB4AwWQAEAAAC8GAAhDVEFTEVNIwAGENUQV9ERUlPXNUQV9TSUDSU5HX0tEWQgACOM5ODAwLUNMUs5CQAlOVpQLEVESESRkI=
Device#
```

```
*Jan 18 02:47:06.733: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (challenge generation attempt:
Shell access 0).
```

Send a request for a challenge using the **request consent-token generate-challenge shell-access** *time-validity-slot* command. The duration in minutes for which you are requesting access to system shell is the time-slot-period.

In this example, the time period is 900 minutes after which the session expires.

The device generates a unique challenge as output. This challenge is a base-64 format string.

Step 2 Send the challenge string to a Cisco Authorized Personnel.

Send the challenge string generated by the device to a Cisco Authorized Personnel through e-mail or Instant Message.

The Cisco Authorized Personnel processes the unique challenge string and generates a response. The response is also a base-64 string that is unique. The Cisco Authorized Personnel copies this response string and sends it to you through e-mail or Instant Message.

Step 3 Input the response string onto your device.

Example:

```
Device# request consent-token accept-response shell-access
[redacted]
% 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).
```

Input the response string sent to you by the Cisco Authorized Personnel using the **request consent-token accept-response shell-access** *response-string* command.

If the challenge-response pair match, you are authorized to access system shell. If the challenge-response pair do not match, an error is displayed and you are required to repeat steps 1 to 3.

After you are authorized, you can access system shell for the requested time-slot.

The device sends a message when there is ten minutes remaining of the authorization session.

Step 4 Terminate the session.

Example:

```
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#
```

When you finish accessing system shell, you can end the session using the **request consent-token terminate-auth** command. You can also force terminate the session prior to the authorization timeout using this command. The session also gets terminated automatically when the requested time slot expires.

Dev Key and Release Key

The Cisco IOS XE secure boot functionality ensures that only Cisco signed software is loaded on a Cisco IOS XE platform. Before introducing the dev-key install functionality, Cisco IOS XE platforms are shipped with Dev Public Key and Release Public Key. These keys are used to validate the images signed by corresponding private keys. The subset of Cisco IOS XE platforms which support dev-key install functionality are shipped only with Release Public Key without a Dev Public Key. With this change in the functionality, an image that is signed with a Dev Private Key will not boot due to the absence of Dev Public Key for image verification. However, for some reason, if the Cisco IOS XE device is shipped back to Cisco, a Product Return and Replacement (RMA) specialist may need to load an image signed with Dev Private Key. This requires the RMA specialist to install a Dev Public Key on the device to ensure that the verification of the image signed with Dev Private key passes. To install the Dev Public Key, use the commands mentioned in the following section.

Consent Token Authorization Process for Dev Key Access

This section describes the process of Consent Token authorization to access dev-key:

SUMMARY STEPS

1. Generate a challenge requesting for access to dev-key for the specified time period.
2. Send the challenge string to a Cisco Authorized Personnel.
3. Input the response string onto your device.
4. Terminate the session.

DETAILED STEPS

Step 1 Generate a challenge requesting for access to dev-key for the specified time period.

Example:

```
Device# request consent-token generate-challenge dev-key auth-timeout 900
zSbzAAAQEBAQAAAAAgAEAAAAAAMACH86csUmDlOEAAQOFvd7CxqRUeD7B4AW7QAEAAAC8ZAAhDAEFEEMNwaGENUQ9ERUlPXNUQV9ISUdSUSHXOtHWQgAOM5ODAwIUNMU55CQALOVpQLEAESE5RkI=
Device#
*Jan 18 02:47:06.733: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (challenge generation attempt: Dev
 key install).
```

Send a request for a challenge using the **request consent-token generate-challenge Dev-key** *time-validity-slot* command. The duration in minutes for which you are requesting access to dev-key is the time-slot-period.

In this example, the time period is 900 minutes after which the session expires.

The device generates a unique challenge as output. This challenge is a base-64 format string.

Note Auth-timeout of zero signifies permanent Dev Public Key installation. Such permanent installation is only allowed on Cisco internal devices for security reasons.

Step 2 Send the challenge string to a Cisco Authorized Personnel.

Send the challenge string generated by the device to a Cisco Authorized Personnel through e-mail or Instant Message.

The Cisco Authorized Personnel processes the unique challenge string and generates a response. The response is also a base-64 string that is unique. The Cisco Authorized Personnel copies this response string and sends it to you through e-mail or Instant Message.

Step 3 Input the response string onto your device.

Example:

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

Input the response string sent to you by the Cisco Authorized Personnel using the **request consent-token accept-response dev-key** *response-string* command.

If the challenge-response pair match, a Dev Public Key is installed. If the challenge-response pair do not match, an error is displayed and you are required to repeat steps 1 to 3.

The device sends a message when there is ten minutes remaining of the authorization session.

Step 4 Terminate the session.

Example:

```
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#
```

This example displays the output when the system fails to terminate the authorization session.

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

When you finish accessing dev-key, you can end the session using the **request consent-token terminate-auth** command. You can also force terminate the session prior to the authorization timeout using this command. The session also gets terminated automatically when the requested time slot expires.

Validating the Installation Authorization

To validate the key installation authorization, use the **show platform software consent-token dev-key** command.

```
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
```

Enabling or Disabling Consent Token

To turn on or turn off the consent token, use the following debug commands:

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

Feature History and Information for Consent Token

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Release	Feature Information
Cisco IOS XE Gibraltar 16.11.1	This feature was introduced.
Cisco IOS XE Bengaluru 17.4.1	Dev Key and Release Key options were introduced.