



Consent Token

- [Restrictions for Consent Token, on page 1](#)
- [Information About Consent Token, on page 1](#)
- [Consent Token Authorization Process for System Shell Access, on page 2](#)

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

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).

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.

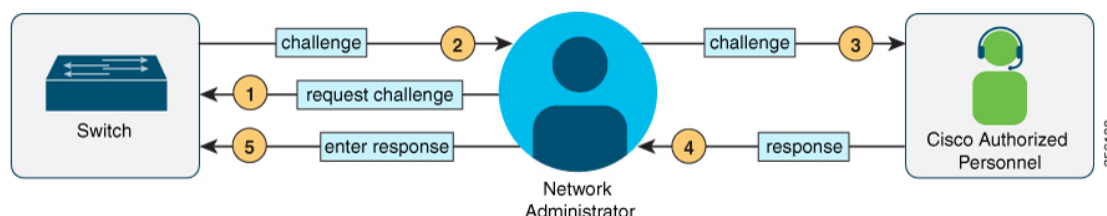
When you request access to system shell, you need to be authorized. You must first run the command to generate a challenge using the Consent Token feature on your device. The device generates a unique challenge as output. You must then copy this challenge string and send it to a Cisco Authorized Personnel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

Figure 1: Consent Token



Consent Token Authorization Process for System Shell Access

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

Procedure

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
zSSdrAAAAQEBAAQAAAABAgAEAAAAAMACH86csUhmDl0BAAQ0Fvd7CxqRYUeoD7B4AwW7QUABAAAAG8GAAhDVEff
REVNtWcAGENUQV9ERU1PX0NUQV9TSUdOSU5HX0tFWQgAC0M5ODAwLUNMLUs5CQALOVpQUEVESE5KRkI=
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
1R1y2AAUKFcAAAABAAABY1VDZ2d6MnkxL3JxTTJSSC9FZE5aW
nRSa1FteS9FOWZqF0N1Tk1LL3VoUwKt0FsOH15OW5vckQ4YVW0elpZZGYNClNqWHY0b1B4Q000UGs1M2ZEMUpcazBCUkYyM3FML1A2ckVjM3paR05wd
Hcvck95UVduYUVUfInA5bnhIZ09CNE0NCjBmVjh4b3I4TzE3aHNMaULJedQ3YVWtkde9xb0JhfmLzMWReFBVZE93QUkvZDVEBmo4UEtiR01VWUM5b3LZ
WQNCjFIRnJBhXczmpszTJHUnIxOWJUNkZLlWlpZ0ZmbENVRWw4K2xoaXgsS0ZtdDVPcdBYczVPSU43L0dSK1pGTncNcmYxTUtjaWlOWdhWTINLQ0Z
WNURHU3pIenFlUFBxZVNDU0xLNkhXUTFROTlFMXJVakdlZlNqTWxmnNFlySkJYL0wNCnpaTDVVRnVfdWpRWDDdUThtIdkVPM1E9PQ==
% 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.

