Token Authentication

The Token Authentication feature allows you to secure the authentication mechanism by protecting it with a temporary authentication access. This feature increases the security to the network by providing a time-bound access without revealing the password to the login user.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Token Authentication

- Ensure that AAA authentication is configured on the device. For more information, see the "Configuring Authentication" chapter in the *Authentication, Authorization, and Accounting Configuration Guide*.
- You must configure the user account using the **token** keyword before configuring the token authentication.

Restrictions for Token Authentication

- The Token Authentication feature requires the Connected Grid (CG) network management system (NMS) to generate the authentication token.

Information About Token Authentication

Token Authentication Overview

Token Authentication is a method to provide a device-bound and time-bound access to a Cisco IOS device that is offline and therefore not able to reach the AAA database for a proper authentication. The access is unauthenticated and should be used in caution, in particular the privilege level granted to the session.

Token authentication can configure the privilege level for the technician to grant access for any operation on the device. This feature is used to grant a technician access to the Cisco IOS device to perform simple device management such as statistics collection or even restarting an interface while the Cisco IOS device is in an error state and disconnected from the rest of the network.

The local technician accounts are authorized with a temporary time-bound authentication token without exposing the password. The token structure is encrypted and not visible to the technician. The technician uses this encrypted token as the password.

The generated token is encrypted with the token encryption key and provided to the technician. Once the temporary time-bound authentication token is used as the login credential, it is decrypted and verified by the local AAA database by using the token encryption key.

The network security is protected by ensuring that the technician is given access to the network after authenticating the technician's token credentials (shared by the Connected Grid [CG] network management system [NMS] and the device). In addition, this access is for a limited time period that is embedded inside the token structure. Beyond that specific time period in which the token is valid, the technician's session is disconnected and no future network session is allowed with the same token.

How to Configure Token Authentication

Configuring Token Authentication

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **username** *name* [**privilege** *level*] **token password** *encryption-type password*
4. **aaa new-model**
5. **aaa authentication login default** *method1* [*method2 ...*]
6. **aaa authentication token key** *string*
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**username** *name* [**privilege** *level*] **token password** *encryption-type password* **Example:** `Device(config)# username user1 privilege 1 token password 0 cisco123`	Establishes a username-based authentication system.
Step 4	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables authentication, authorization, and accounting (AAA) network security services.

	Command or Action	Purpose
Step 5	**aaa authentication login default** *method1* [*method2* ...] **Example:** `Device(config)# aaa authentication login default local`	Sets AAA authentication at login.
Step 6	**aaa authentication token key** *string* **Example:** `Device(config)# aaa authentication token key abcdefghcisco123`	Creates a token authentication key to provide temporary access to the network.
Step 7	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

Configuration Examples for Token Authentication

Example: Configuring Token Authentication Key

```
Device> enable
Device# configure terminal
Device(config)# username user1 privilege 1 token password 0 cisco123
Device(config)# aaa new-model
Device(config)# aaa authentication login default local
Device(config)# aaa authentication token key abcdefghcisco123
Device(config)# exit
```

Additional References for Token Authentication

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases

Related Topic	Document Title
Security commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z
AAA authentication	"Configuring Authentication" chapter in the *Authentication, Authorization, and Accounting Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Token Authentication

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.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Token Authentication

Feature Name	Releases	Feature Information
Token Authentication	15.4(1)T	The Token Authentication feature allows you to secure the authentication mechanism by protecting it with a temporary authentication access. This feature increases the security to the network by providing a time-bound access without revealing the password to the login user. The following command was introduced or modified: **aaa authentication token key**.