Secure Reversible Passwords for AAA

The Secure Reversible Passwords for AAA feature enables secure reversible encryption for authentication, authorization, and accounting (AAA) configurations using type 6 advanced encryption scheme (AES) passwords.

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 Secure Reversible Passwords for AAA

The following commands should be enabled for the type 6 password encryption:

- **password encryption aes**
- **key config-key password-encrypt** [*password*]
- **aaa new-model**

Information About Secure Reversible Passwords for AAA

Secure Reversible Passwords

Passwords in Cisco IOS configurations require a secure storage so that the key for the reversible encryption can be stored to ensure that authentication methods can access the user credentials whenever required.

Reversible encryption is the process by which a password is encrypted with a reversible, symmetric encryption algorithm. To check if the password entered by the user is valid, the password is decrypted and compared to the user-input password. To perform this encryption, the symmetric encryption algorithm requires a key.

The type 6 advanced encryption scheme (AES) encrypted passwords help to secure the reversible passwords for authentication, authorization, and accounting (AAA) features. This type 6 encryption key is stored in a private NVRAM and secured.

AAA network configurations use Lightweight Directory Access Protocol (LDAP), RADIUS, or TACACS+ server hosts. Use the **radius server host**, **tacacs-server host**, and **ldap server** commands to configure RADIUS, TACACS+, or LDAP host servers respectively.

Type 6 Encryption Configuration

The following commands have been updated with the type **6** keyword to enable secure reversible passwords to configure authentication, authorization, and accounting (AAA) features. For more information about the security commands, see the *Cisco IOS Security Command Reference*. For more information about AAA configuration, see the *Authentication, Authorization, and Accounting Configuration Guide*.

- **aaa configuration**
  - **aaa configuration** {**config-username username** *username* [**password** [**0** | **7**] *password*] | {**pool** | **route**} **username** *username* [**password** [**0** | **6** | **7**] *password*}
- **bind authenticate root-dn (config-ldap-server)**
  - **bind authenticate root-dn** *username* **password** {**0** *string* | **6** *string* | **7** *string*} *string*
- **client (config-locsvr-da-radius)**
  - **client** *ip-address* **server-key** [**0** | **6** | **7**] *word*
- **key (config-radius-server)**
  - **key** {**0** *string* | **6** *string* | **7** *string*} *string*
- **key (config-server-tacacs)**
  - **key** {**0** *string* | **6** *string* | **7** *string*} *string*
- **pac key (config-radius-server)**
  - **pac key** {**0** *string* | **6** *string* | **7** *string*} *string*
- **password (config-filter)**

  - **password** [**0** | **6** | **7**] *password*

- **server-private (RADIUS)**
  - **server-private** *ip-address* [**auth-port** *port-number* | **acct-port** *port-number*] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** [**0** | **6** | **7**] *string*]

- **server-private (TACACS+)**
  - **server-private** {*ip-address* | *name* | *ipv6-address*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **6** | **7**] *string*]

- **tacacs-server host**
  - **tacacs-server host** {*host-name* | *host-ip-address*} [**key** {**0** *string* | **6** *string* | **7** *string*} *string*] [[**nat**] [**port** [*integer*]] [**single-connection**] [**timeout** [*integer*]]]

- **tacacas-server key**
  - **tacacs-server key** {**0** *string* | **6** *string* | **7** *string*} *string*

Note We recommend to use type 6 to reduce the vulnerability of a malicious attack against password integrity. When the AAA commands that support type 6 are configured with either type 0 or type 7 encryption option, warning messages are displayed.

Additional References for Secure Reversible Passwords for AAA

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
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 configuration	*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 Secure Reversible Passwords for AAA

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 Secure Reversible Passwords for AAA

Feature Name	Releases	Feature Information
Secure Reversible Passwords for AAA	15.4(1)T	The Secure Reversible Passwords for AAA feature enables secure reversible encryption for authentication, authorization, and accounting (AAA) configurations using type 6 advanced encryption scheme (AES) passwords. The following commands were introduced or modified: **aaa configuration**, **bind authenticate root-dn (config-ldap-server)**, **client (config-locsvr-da-radius)**, **key (config-radius-server)**, **key (config-server-tacacs)**, **pac key (config-radius-server)**, **password (config-filter)**, **server-private (RADIUS)**, **server-private (TACACS+)**, **tacacs-server host**, and **tacacas-server key**.