TACACS+ Authentication

Avi Technical Reference (v17.1)

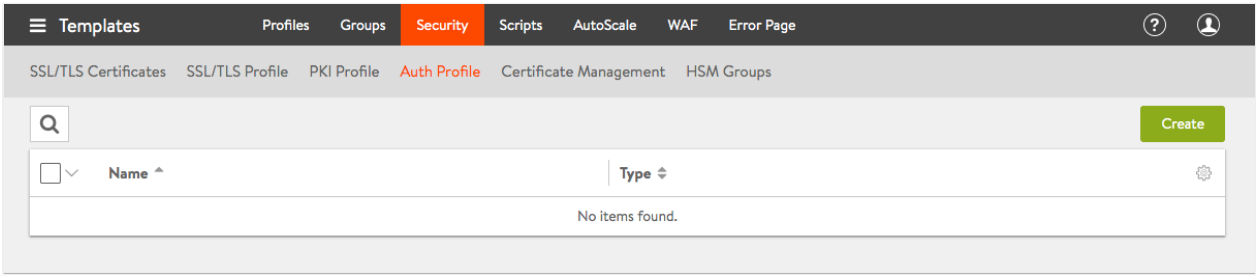
TACACS+ Authentication

view online

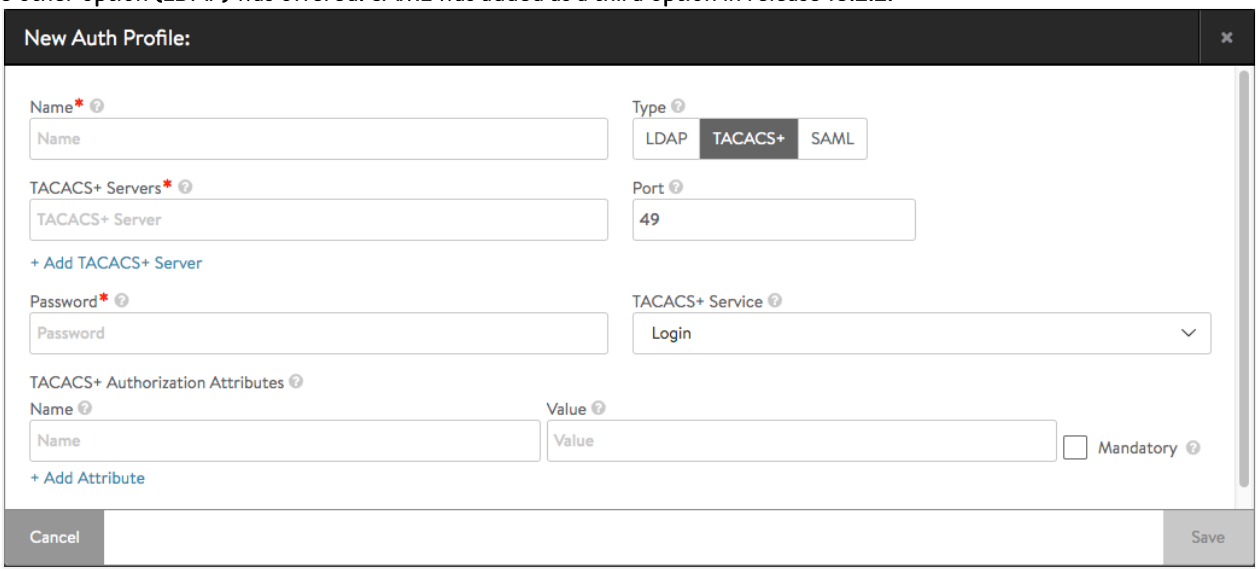
Avi Vantage supports authentication and authorization of Avi Vantage users with TACACS+. TACACS+ is an open standards protocol that handles authentication and accounting (the first two "A"s in "AAA").

TACACS+ AAA Settings

TACACS+ settings are specified in an Avi auth profile. To create one, navigagte to Templates > Security > Auth Profile. as shown below.

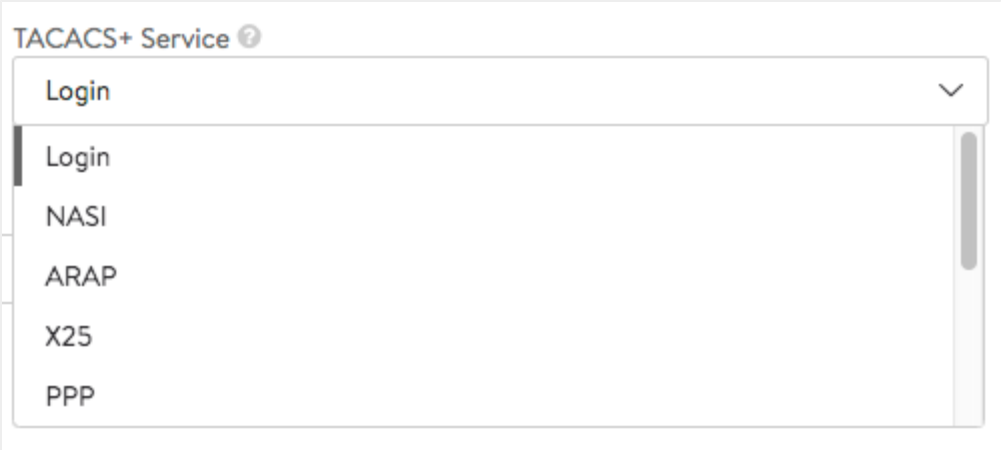


Click on Create to open up the auth profile editor, which is shown below. Notice that the Type chosen is TACACS+. Initially, one other option (LDAP) was offered. SAML was added as a third option in release 18.2.2.



Auth Profile Editor Fields

- TACACS+ Servers: TACACS+ server IP. Multiple servers can be specified. If the first server does not respond, Avi Vantage tries the next server. If that server also does not reply, the next server is tried, in round-robin fashion. Click on Add Item to add a server.
- Port: TACACS+ server port (default 49).
- Password: TACACS+ server shared secret.
- TACACS+ Service: TACACS+ service type, used in all authentication and authorization queries. The below illustrates the pulldown from which one of several services may be chosen.



- TACACS+ Authorization attributes: Set of attribute value pairs to identify the host. The TACACS+ server configures user-level authorization based on these attributes. Cisco Access Control Servers (ACSs) typically expect authorization attribute values for ?service? and ?protocol? to be populated in order to identify and authorize an Avi Vantage user. Authorization attributes from a TACACS+ server can be used to map Avi Vantage users to various roles and tenants. If the attribute is required, check the Mandatory box. Click on Add Attribute to add additional name-value pairs.

Authentication and Authorization Walkthrough

Authentication and authorization of an Avi Vantage user with TACACS+ takes place as follows:

1. AUTHEN START packet from Avi Vantage to TACACS+ server. Contains:
    - action=login
    - authen_type=ascii
    - service=
    - user=
    - remote_addr=
2. AUTHEN REPLY packet from TACACS+ server to Avi Vantage. Contains status of type GETPASS indicating that password needs to be supplied for the user message field with text ?Password.?
3. AUTHEN CONTINUE packet from Avi Vantage to TACACS+ server. Contains user message field with actual password from user.
4. AUTHEN REPLY packet from TACACS+ server to Avi Vantage. Contains:
    - SUCCESS status if password is valid and user is allowed
    - FAILED status
5. AUTHOR START packet from Avi Vantage to TACACS+ server. Contains:
    - Username of the user
    - Remote address of the user
    - Authorization attribute name, value and whether or not they are mandatory
    - An authorization attribute string ?abc=xyz? that indicates an attribute named ?abc? is mandatory and has value ?xyz?
    - An authorization attribute string ?abc*xyz? that indicates an attribute named ?abc? is optional and has value ?xyz?
6. AUTHOR REPLY packet from TACACS+ server to Avi Vantage. Contains one of the following:
    - PASS_ADD or PASS_REPL status, which authorizes the successfully authenticated user with attribute value pairs to be added or replaced.
    - FAIL status, indicating the user is not authorized.

Encryption

All TACACS+ packets are encrypted, whereas the 12-byte header is passed in the clear. Encryption is part of the TACACS+ standard and is compatible with all TACACS+ servers.

Error Handling

If an error is indicated in the Status field of any reply packet during this process, the user login is rejected and results in a failure.

Other Articles of Interest:

TACACS+ Configuration Examples