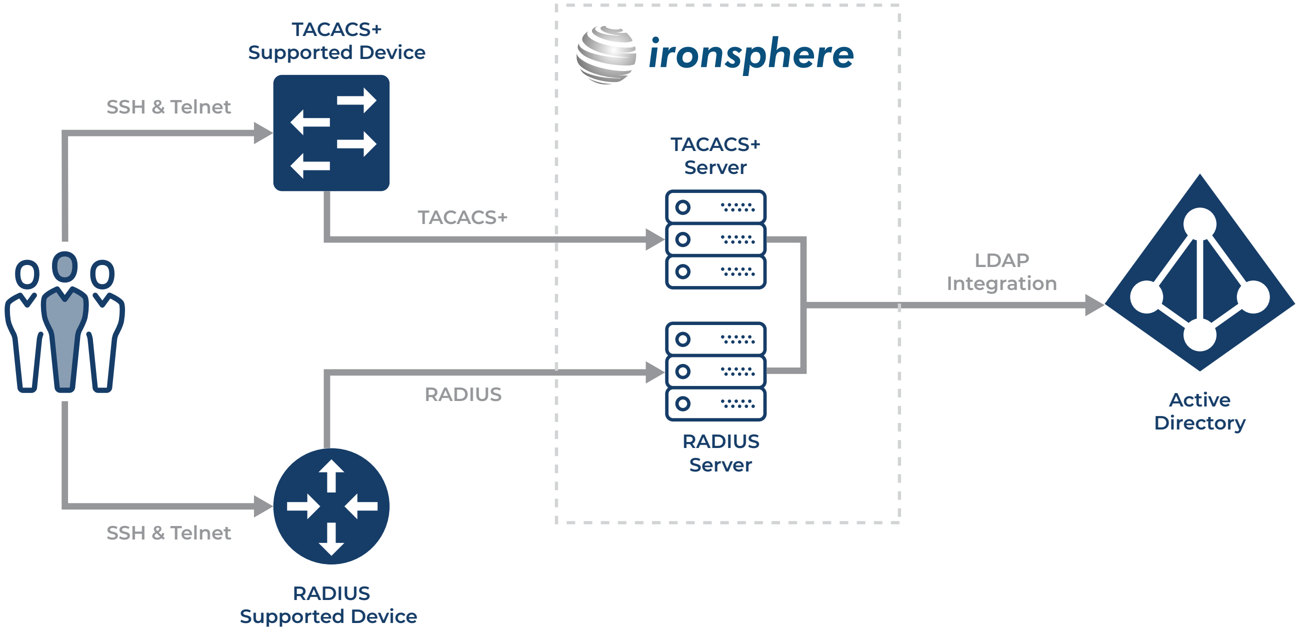
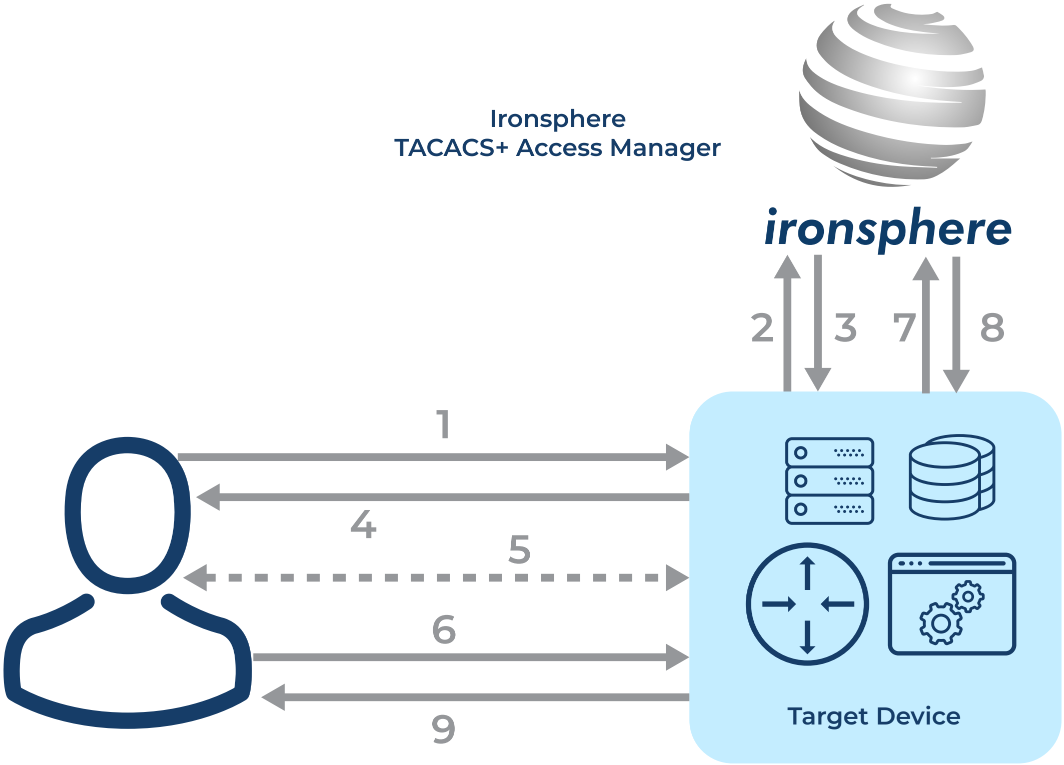
TACACS+ Access Manager

Cisco announced the end of life for its ACS (Access Control System) product and offered to migrate their customers from Cisco ACS to Cisco ISE (Identity Service Engine). However, Cisco ISE is originally designed for Network Access, not for Network Administration, and although it offers RADIUS/TACACS+ protocol support, it does NOT support any other Privileged Access Management features, such as RDP/HTTP/SFTP/SQL session management, Dynamic Password Controller, Application-to-Application Password Management or Multi-Factor Authentication. So, from a SecOps point of view, migrating from Cisco ACS to Cisco ISE means using it as a Network Access Management tool (wireless network access, bring your own devices, guest users, etc.).

Most of the time SecOps teams are not interested in Network Access, either because they already have a product for that purpose, or it is not under their scope. However, SecOps are very much interested in PAM tools.



How TACACS+ Access Manager Works



Authentication

Step 1: The user initiates a CLI session towards the target device. The user enters a username & password.

Step 2: The target device sends the username & password to the TACACS+ Access Manager.

Step 3: Successful response if the username & password are correct.

Step 4: The target device sends the response to the user.

Step 5: A CLI session between the user and the target device is established. The user can now enter commands for device administration purposes.

Administration

Step 6: The user enters a command on his CLI screen. It is sent to the target device.

Step 7: The target device sends the command to the TACACS+Access Manager.

Step 8: The TACACS+ Access Manager

» Checks whether the user has the right/privilege to run that command.

» Respond either accept or reject.

» Logs the command along with the response.

Step 9: If the TACACS+Access Manager responds with an accept message, the target device runs the command and sends the response to the user. If the response was a reject message, the target device sends a fail message to the user.

Benefits

- Full visibility, detailed audit logs. All commands, either failed or succeeded, are indisputably logged, creating a record of which user attempted to run which command on which device and when.
- "Separation of duties" and "least privilege" best practices are achieved, regardless of the role/profile capabilities of the device. Ironsphere's TACACS+ Access Manager enables any custom policies (allowed command sets, blocked command sets) to be defined and applied to any user group, ensuring that only the "required set of commands" can be executed by a user to fulfill his tasks, and no other command execution is allowed at all.
- Eliminates weak passwords and/or non-expiry passwords.
- Enables the definition of time-based access limitations. Based on time of day, day of the week, maintenance-window hours, etc.
- Disables inactive privileged accounts.
- Multi-tenant. On a single TACACS+ Access Manager instance, while keeping the governance of the entire network in place, each enterprise department/region can be assigned limited privileges to manage their own devices, isolated from the larger network.
- Auto lock user account when an employee terminates employment. Integration with enterprise Active Directory (or LDAP) is required.