ARMIS APEX SECURE CONFIGURATION GUIDE V1.1

Armis APEX

April 20, 2026

Document history

This table shows a history of recent updates to this documentation.

Date	Changes
April 20, 2026	• Added Pre-deployment and periodic review checklists. Doc version 1.1.
March 16, 2026	• Initial document. Doc version 1.0.

This secure configuration guide serves as a supplement to the Armis Partner Experience User Guides. It specifically identifies and addresses the requirements outlined in the FedRAMP Secure Configuration Guide to ensure the highest standards of cloud security, data integrity, and access control for the platform. For additional operational information, refer to the Apex Manage User Guide.

1 Overview

Armis Partner Experience (APEX) Manage is a portal where Armis partners and customers can view and manage multiple Armis APEX environments. The portal provides a unified management plane for analytics, tenant information, policy templates, and security settings.

Key functionalities controlled by top-level and privileged accounts include:

- **User Provisioning**—Defining APEX Manage admins and standard users.
- **Security Analytics**—Viewing dashboards with aggregated alerts and device information.
- **Operational Control**—Pushing and managing security policies across all tenants.
- **Compliance Monitoring**—Accessing audit logs for forensic and compliance review.
- **Access Control**—Configuring detailed roles and permissions.

1.1 Guide scope

This guide supplements the Armis APEX and Armis Centrix™ for VIPR User Guides by detailing the specific configurations required to meet FedRAMP security standards. It provides the controls necessary to maintain platform integrity and robust access management within federally regulated environments. For general operational workflows, refer to the standard product documentation.

Included are essential procedures for managing top-level administrative accounts, privileged settings, and enterprise-wide security configurations:

- **Administrative Account Lifecycle**—Instructions on how to securely access, configure, operate, and decommission top-level administrative accounts that control enterprise access to the entire cloud service offering.
- **Top-Level Security Settings**—Explanations of security-related settings that can be operated only by top-level administrative accounts and their security implications.
- **Privileged Account Settings**—Explanations of security-related settings that can be operated only by privileged accounts and their security implications.

2 Top-level administrative account management

Top-level administrators (those with the **Admin** role) possess complete control over the platform's security environment. The first user created in the system is automatically assigned this role, which contains full system access.

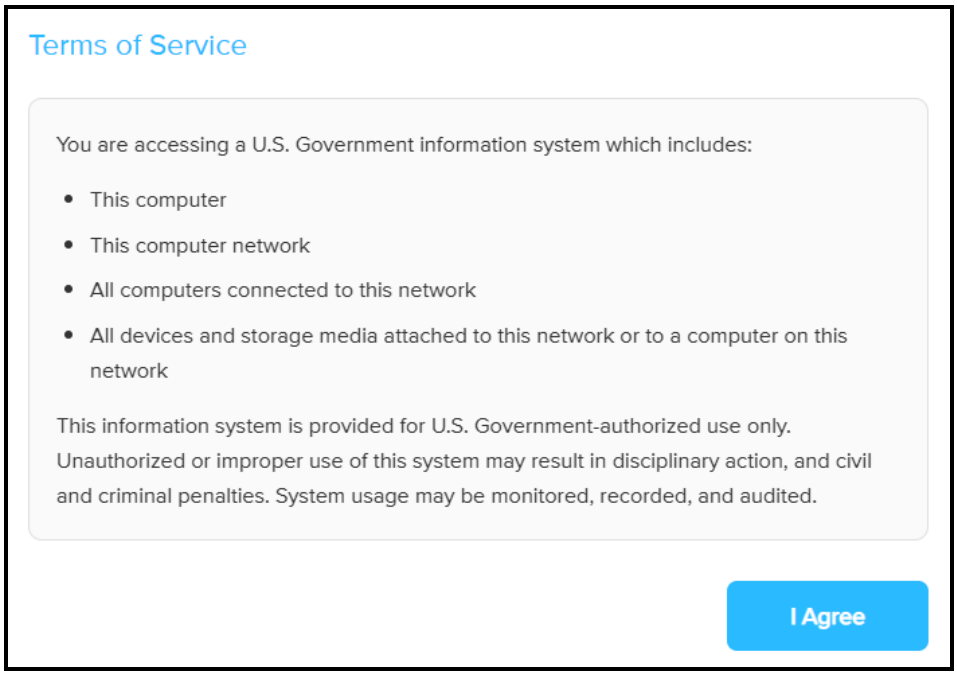
2.1 Federal security hardening

Administrative accounts in federal environments are subject to enhanced security controls to meet strict compliance requirements:

- **Inactivity Timeout**—Inactive sessions are strictly set to automatically timeout after 15 minutes, requiring a re-login.
- **Session Termination**—Sessions are decommissioned and terminated immediately when the user explicitly clicks Log Out, closes the web browser, or the inactivity timeout is reached.
- **Password Complexity**—Passwords must be at least 15 characters and cannot be "common" passwords.
- **Account Lockout**—Three unsuccessful login attempts result in a 15-minute lockout.

2.2 Session and login security

- **Login Banner**—By default, users must accept the **Terms of Service** below.
  - **Security Implication**—Establishes clear legal grounds regarding authorized use and active monitoring.



2.3 Creating a top-level Administrator

To create an Admin role:

1. Navigate to **Settings** > **Roles & Permissions**.
2. Click **Add role** to create a role:

- In the **Role Name** field, enter the name for the role.
- Apply full permissions in all categories: **Policy**, **Report**, **Dashboard Template**, **Tenant Template**, **Roles**, **Users**, **Tenant**, and **Settings**.

3. Click **Save**.

To create a User:

1. Navigate to **Settings** > **Users**.
2. Click **Add User**.
3. In the **Add User** page, configure the following:
   - **Firstname**—Enter the first name of the user.
   - **Lastname**—Enter the last name of the user.
   - **Email**—Enter the email address of the user.
   - **Phone Number** (optional)—Enter the phone number of the user.
   - **Roles**—Select the Custom or Admin role created in Creating a top-level Administrator from the drop-down list.
   - **By Tenants** (optional)—Select All Tenants from the drop-down list to grant comprehensive visibility.
   - **By Tags**—Select the relevant tags from the drop-down list.
4. Click **Add**.

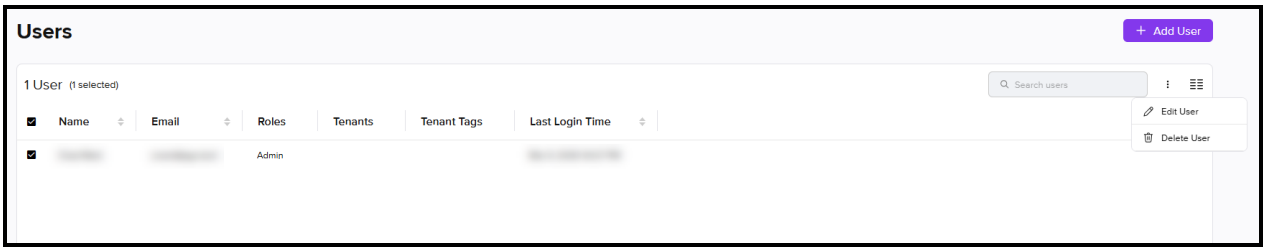
Security Implication—Explicit custom roles ensure administrative power is granted intentionally and follows the principle of documented authorization.

2.4 Removing an Admin User

Proper decommissioning of administrative accounts is critical to maintain data continuity and prevent unauthorized access.

To manually delete an admin user:

1. Navigate to **Settings** > **Users**.
2. Select the checkbox of the specific user.
3. Select the 3-dots menu, and click **Delete User**.



- **Ownership Transfer**—Upon deletion of a top-level administrator, ownership of all shared dashboards is automatically transferred to the remaining administrators to ensure data remains accessible.
- **Access Revocation**—Once the user is deleted, the user is immediately unable to access the system.

> **NOTE:** There is no user deactivation procedure. To restrict a user's access to the application, you must manually delete the user.

Security Implication—Automated ownership transfer and immediate session invalidation ensure security operations remain uninterrupted while preventing unauthorized access from decommissioned accounts.

3 Secure access and initial configuration

The web console is the primary interface for performing all tasks and managing the security posture of the environment.

3.1 Identity and access management

Establishing robust identity and access management (IAM) ensures that only authorized users can access the platform while maintaining strict control over administrative permissions and authentication protocols.

Mandatory Single Sign-On (SSO) Configuration—The first time you log in to APEX Manage, you must configure the **Login Management** page to establish secure access via an external Identity Provider (IdP) using SAML 2.0 or OpenID Connect (OIDC) by configuring the following:

Document history

Document history

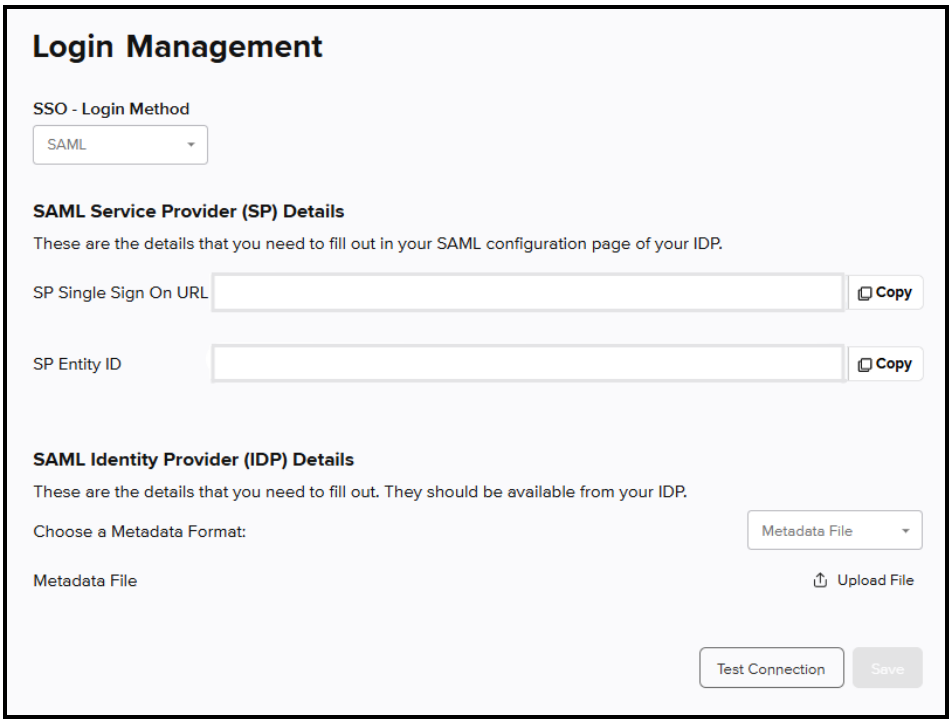
Document history

NOTE: Parameters such as SP Single Sign On URL and SP Entity ID are used in later steps for configuration inside the IDP.

3.1.1 SAML configuration

To configure SAML authentication between your Identity Provider and the Armis platform:

1. Navigate to **Settings** > **Login Management**.
2. In the **Login Management** page, configure the following:



   - **SSO - Login Method**—Select **SAML** from the dropdown menu.
3. In the **SAML Service Provider (SP) Details** section, the following details are required to configure your Identity Provider (IdP) to allow Armis APEX to send authentication requests:
   - **SSP Single Sign On URL**—The SAML identity provider's single-sign-on URL.
   - **SP Entity ID**—A URL or another unique identifier of the service provider (SP).
4. **SAML Identify Provider (IDP) Details** section, you must provide the SAML IDP URL that Armis uses to send authentication requests:

   NOTE: You can get this from your Identity Management provider. Refer to their documentation on where to find the value for this parameter.

   - **Choose a Metadata Format**—From the dropdown menu, select one of the following:
     - **Metadata File**—Select this option if you use an on-premises IDP, such as SiteMinder or Federated Active Directory, and you only have a metadata XML file.
     - **Metadata URL**—Select this option if you know the URL.

- **Metadata File**—Click **Upload File** to update the metadata file.

  > **NOTE:** This is only relevant if you selected **Metadata File** in **Choose a Metadata Format**.

- **Metadata URL**—Enter the URL into the text box.

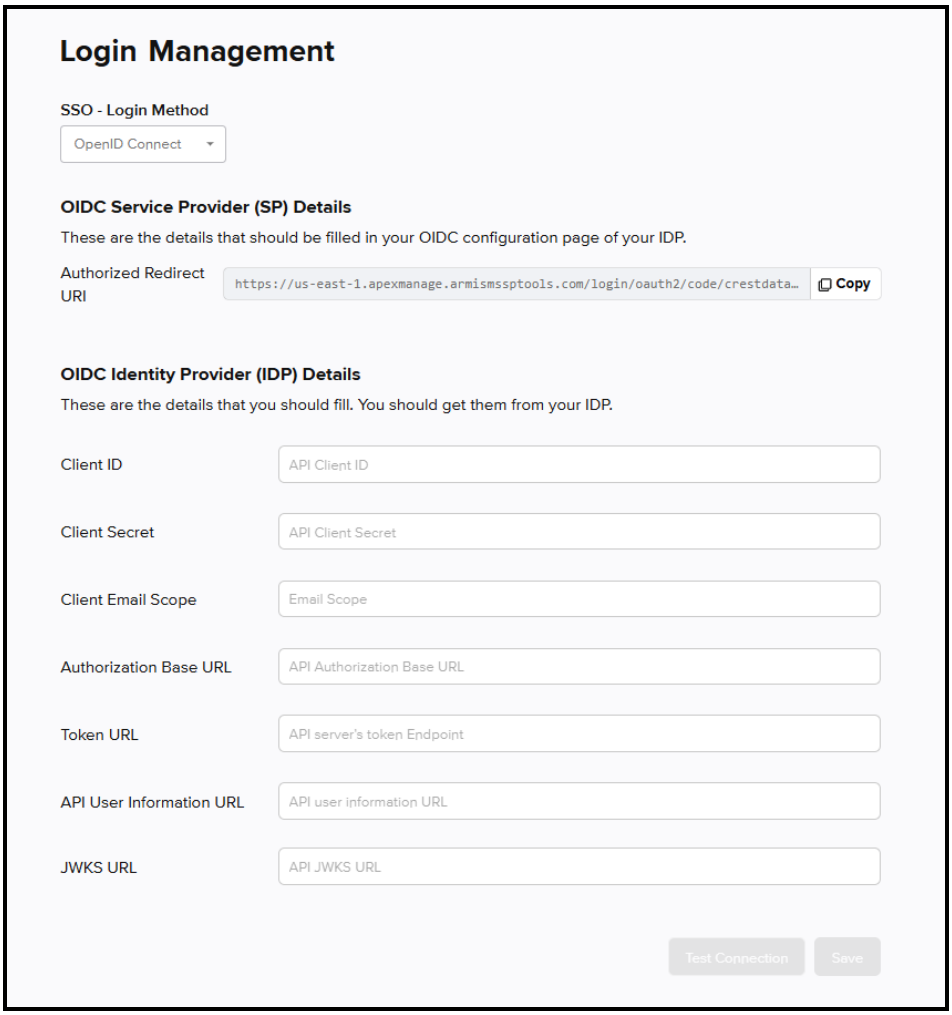
  > **NOTE:** This is only relevant if you selected **Metadata URL** in **Choose a Metadata Format**.

5. Click **Save**.
6. Click **Test Connection** to validate the configuration.

3.1.2 OpenID Connect configuration

To configure OpenID Connect authentication between your Identity Provider and the Armis platform:

1. Navigate to **Settings** > **Login Management**.
2. In the **Login Management** page, configure the following:



- **SSO - Login Method**—Select **OpenID Connect** from the dropdown menu.

3. In the **OIDC Identify Provider (IDP) Details** section, configure the following, provided by your IDP:
   - **Client ID**—The API client ID. E.g., `5545322...-mo53kjlqme2l71rc1.apps.googleusercontent.com`.
   - **Client Secret**—The API client secret.
   - **Client Email Scope**—The technical keyword used to request the user's email. E.g., email.
   - **Authorization Base URL**—The API authorization base URL. E.g., `https://accounts.google.com/o/oauth2/v2/auth`.
   - **Token URL**—The API server's token URL.
   - **API User Information URL**—The API user information URL. E.g., `https://openidconnect.googleapis.com/v1/userinfo`.
   - **JWKS URL**—The API JWKS URL. E.g., `https://www.googleapis.com/oauth2/v3/certs`.
4. Click **Save**.
5. Click **Test Connection** to validate the configuration.

3.1.3 Two-step verification

- Since most users log in to the application via SSO, MFA is handled by the identity provider itself.

4 SSO & SAML in Armis

This section provides the logic for how authentication works once configured:

- **Username-Only Prompt**—Users are no longer prompted for a password locally; they enter only their username and are redirected to their Identity Provider (IdP).
- **Access Criteria**—For successful entry, the user must exist in Armis APEX Manage, be a valid user in the IdP, and have a username that matches exactly between both systems.
- **Portal vs. Console Distinction**—Logging into the Armis APEX console is a separate process from the APEX Manage Portal (AMP); however, using the same IdP for both provides a seamless experience

5 Administrative role management

To ensure effective oversight and adherence to the Principle of Least Privilege, the platform provides granular visibility and lifecycle management tools for both predefined and custom administrative roles.

- **Audit Visibility**—Administrators can now click an expand button on any role to see its specific assigned permissions.
- **User Assignment Tracking**—The system now displays the total number of users assigned to each specific role.
- **Role Deletion**—To remove a custom role, it must be selected and then deleted by clicking **Delete Role**.

6 Restricted security settings

Certain high-impact settings are restricted to top-level administrative accounts due to their global security implications, ensuring that only the most trusted entities can alter the fundamental security posture of the platform.

6.1 Restricted administrative controls

Setting	Security Implication
User and Role Management	Controls system entry and internal permissions; improper settings can lead to unauthorized data access.
SSO Configuration	Defines the primary authentication gateway; errors can lock out legitimate users or permit unauthorized access.
Audit Log Monitoring	Provides the internal record of all system and user events; essential for detecting administrative abuse.
Audit Log Retention	Provides the necessary visibility to detect and investigate unauthorized administrative actions via 90-day log retention.
Overview Thresholds	Determines the sensitivity of the monitoring system; high thresholds for Alerts, Integrations, or Syncs may mask critical environment failures.

7 Privileged account security settings

Privileged accounts granted **Manage** permissions possess the authority to influence risk assessment and remediation workflows, necessitating strict adherence to the principle of least privilege.

- **Tenant Modification**—Users with edit tenant permission (**Settings** > **Roles & Permissions** > **Tenant** > **Manage** > **edit**) can change the secret key for tenants
  - **Security Implication**—Unauthorized edits can block the data inflow in the system.
- **Push Policy**—Privileged users with **Push** permission for **Policy** can push any policy in assigned tenant.

- **Security Implication**—Pushing the wrong policy to a tenant can create noisy alert or "alert fatigue" within that environment.

- **Login Management**—Users with **Login Management** permission can change the SSO configuration.
  - **Security Implication**—Misconfiguration can result in locking users out of the system, preventing access.

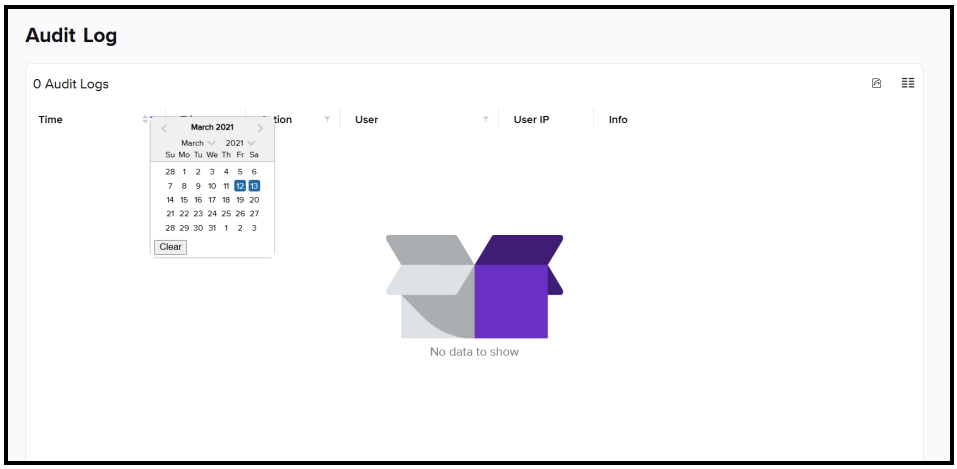
8 Continuous monitoring

Ongoing oversight through continuous monitoring ensures that all system activities are recorded and available for forensic review, meeting mandatory compliance standards for data retention and accountability. Internal audit logs are retained for 90 days to meet federal continuous monitoring requirements.

8.1 Audit Log exports

The platform maintains a comprehensive record of all administrative and user actions to support security audits and incident response.

- **Export Audit Log**—Users with the appropriate permissions can export audit logs in .xls or .csv formats.



- **Filters**—The interface provides granular filters (such as date range, user, or event type) to refine the exported data.

9 Pre-deployment and periodic review checklists

To ensure continuous compliance with FedRAMP Rev 5 requirements, use the following checklists to validate your security posture during initial deployment and ongoing operations. These checklists

help ensure that top-level administrative accounts and security-related settings are configured correctly and remain secure over time.

9.1 Pre-deployment checklist

Before deploying the Armis APEX environment, administrators must complete this checklist to verify that all enterprise-wide access controls and identity management settings are secure.

- **Top-level administrative accounts**—Verify that top-level Admin roles are restricted to authorized personnel only and follow the principle of least privilege.
- **SSO and MFA configuration**—Ensure Single Sign-On (SSO) and Multi-Factor Authentication (MFA) are fully configured, tested, and enforced via your external Identity Provider (IdP).
- **Secure defaults**—Confirm that all privileged accounts are initially provisioned with the recommended secure default settings.
- **Session security**—Validate that the inactivity timeout is successfully enforcing a 15-minute limit and that the federal login banner is properly displayed to all users.

9.2 Periodic review checklist

Regularly review the system configuration to prevent configuration drift and maintain a secure federal baseline.

- **Account audit (Quarterly)**—Review all users assigned the Admin role or any custom roles with Manage permissions. Delete any inactive accounts or users who no longer require enterprise-level access.
- **Role and permission review (Quarterly)**—Inspect custom administrative roles to ensure they still adhere to strict authorization needs.
- **SSO configuration check (Quarterly)**—Verify that the SSO configurations (SAML or OpenID Connect) remain active and have not been bypassed or misconfigured.
- **Audit log retention**—Export and check the internal audit logs periodically to confirm they are actively capturing system and user events for forensic review.
- **Privileged settings validation**—Check the restricted security settings to ensure no unauthorized changes have been made to user management, tenant modifications, or policy push permissions.