SaiFlow Secure Remote Access for Energy with Palo Alto Networks Idira and Prisma Access

Technology Partner Program: configuration guide

Author: SaiFlow

Revision history

DATE	CHANGE
8 September 2026	First version

Partner information

FIELD	DETAIL
Date	8 September 2026
Partner name	SaiFlow
Website	www.saiflow.com
Product name	Secure Remote Access for Energy
Partner contact	dor@saiflow.com
Support contact	support@saiflow.com

Product description

SaiFlow Secure Remote Access for Energy is a session brokering and access governance platform for energy OT sites and devices. Technicians, vendors, and support engineers use one console to request, scope, and launch a remote session into a specific site and asset. Operators use it to govern, supervise, and audit every session across a multivendor, global fleet.

SaiFlow scopes each request by site, device, and user role, then routes it to Palo Alto Networks Idira® for just-in-time approval, zero standing privileges, and full session recording. It carries the session over Palo Alto Networks Prisma Access, which decrypts, inspects, and re-encrypts every leg.

What SaiFlow adds is the set of processes and capabilities energy OT operations actually run on, rather than generic remote access:

- Site and asset registration.
- Per-session step-up authentication.
- Supervised sessions with live watch and operator termination.
- Read-only and full-control site operating modes.
- Northbound collection of logs, diagnostics, and backups.
- Southbound software and firmware distribution with malware scanning.
- Ticket linkage and session reporting.

Use cases for integration with Palo Alto Networks

Use case 1: secure just-in-time remote access

Challenge: External vendors and technicians require access to energy OT sites across global regions. These third-party users are often granted broad, persistent access with minimal visibility. Without the ability to scope, approve, and record each session, operators must choose between blocking essential work and accepting unaudited, standing access to critical sites.

Solution: SaiFlow brokers every remote access session, enforcing Idira Privileged Access Manager SaaS for just-in-time access, zero standing privileges, and full privileged session recording. Each session is encrypted from the technician’s browser to Prisma Access,

inspected there against ZTNA and threat prevention policies, and re-encrypted before reaching the site, so every leg remains protected and no traffic reaches the site network uninspected. Operators gain a single, auditable workflow for operational support, guided assistance, remote commissioning, and remote repair without granting persistent access to any individual site or device.

Use case 2: secure northbound and southbound file transfer

Challenge: Updating energy sites requires constant file exchanges, including OS, firmware, and diagnostic data updates. Traditional tools make it difficult to manage these exchanges securely at a global scale across diverse OT environments. Most of these tools cannot verify file integrity in transit or show which user or session initiated a specific transfer, creating significant security and compliance gaps.

Solution: Every file transfer moves through the same brokered session as interactive access, inheriting the same security controls. Prisma Access scans files for malware and enforces DLP policy before they reach or leave the site. Idira ties each transfer to the privileged session, user, and device, creating a complete audit trail of what moved and when. Southbound, operators can push OS updates, firmware, and configuration changes to site systems and OT/IoT devices with the same scanning and audit controls. Northbound, system data, logs, diagnostics, and monitoring data return through the same channel for centralized reporting. The result is a verifiable chain of custody without a separate file-transfer tool.

Integration benefits

- Reduce standing remote-access risk. Every session is just-in-time and task-scoped. Idira enforces zero standing privileges, so no one holds persistent access to a site or device between jobs.
- Replace VPNs and shared logins with one console. Request, scope, approve, launch, and review every session across a multivendor, global fleet in a single workflow.
- Inspect every leg of the connection. Prisma Access decrypts, inspects, and re-encrypts session traffic against SWG, FWaaS, CASB, ZTNA, and threat prevention policies, wherever the user connects from.

- Get energy OT workflows, not generic access. Site and asset registration, per-session step-up authentication, supervisor watch and termination, read-only and full-control site modes, ticket linkage, and session reporting are built in.
- One controlled path for interactive access and file transfer. Northbound collection and southbound software distribution ride the same brokered session and inherit the same scanning, DLP, and audit controls.
- Scale without truck rolls. No SaiFlow hardware at the site: each site needs only its existing IPSec/VPN gateway and is onboarded as a Prisma Access remote network from the SaiFlow console.
- Reuse existing identity. Technicians sign in with their existing corporate identity and MFA through the customer's IdP, federated into Idira. No separate accounts are created.
- Produce audit evidence automatically. Session recordings, per-user attribution, reason and ticket capture, and per-site session history are generated for every session.

Integration diagram

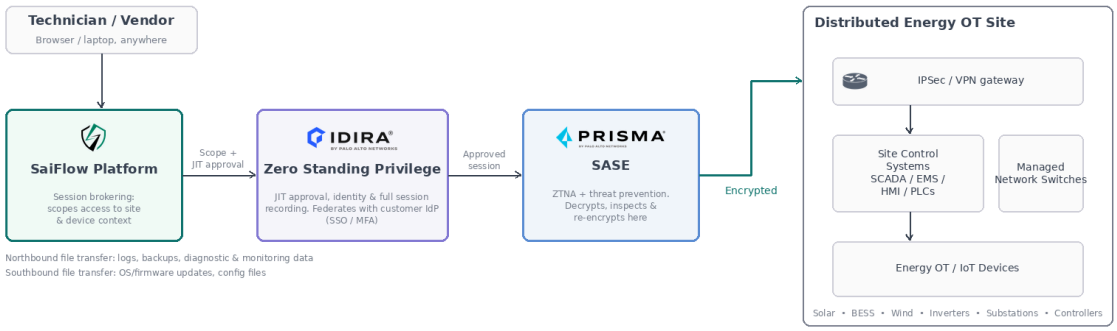

Figure 1: SaiFlow, Idira, and Prisma Access broker a scoped, inspected, and recorded session into a distributed energy OT site. A technician connects from any browser to the SaiFlow platform, which scopes the request and obtains just-in-time approval from Idira for zero standing privileges and full session recording, then carries the approved session over Prisma Access, which decrypts, inspects, and re-encrypts every leg before it reaches the site.

Data shared between the integrated products

Palo Alto Networks Prisma Access (via Strata Cloud Manager)

- **What data is shared:** SaiFlow writes site and network definitions: site name, region, remote network and service connection configuration, IPSec tunnel parameters, and asset network addresses. SaiFlow reads tunnel and session state, per-site throughput, and traffic and threat logs. No asset credentials cross this interface.
- **How the data is shared:** Over the Prisma Access configuration and logging APIs, using a customer-created service account with OAuth credentials (TSG service account ID and secret): Security Administrator and Network Administrator for configuration, and View Only Administrator on Strata Logging Service for telemetry.
- **What action is taken:** Registering a site in SaiFlow creates or updates its remote network, so the path to the site exists before any session is brokered. SaiFlow surfaces per-site tunnel status, active sessions, and throughput. All session traffic and file transfers then traverse Prisma Access, where SWG, FWaaS, CASB, ZTNA, DLP, and threat prevention policies are enforced.

Palo Alto Networks Idira

- **What data is shared:** SaiFlow provisions one Safe per site and multiple target accounts per asset (target address and platform), and binds Safe memberships to the customer's IdP groups as read-only or full-control permission sets. At connect time, SaiFlow sends the authenticated user, the requested asset and protocol, and the session context (access mode, reason, ticket). Idira returns session identifiers, session state, and recording references.
- **How the data is shared:** Over the Idira REST API, using a customer-created service account with OAuth credentials (OAuth confidential client, System Administrator role). Sessions are minted per user at connect time with a short-lived, single-use token bound to that identity. SaiFlow never handles the asset's credentials, only an opaque reference that Idira dereferences and injects.
- **What action is taken:** Idira applies just-in-time approval and zero standing privileges, injects the credential, brokers the session, and records it. SaiFlow renders the session in the browser, lets a supervisor watch or terminate it, and writes an audit record tying site, asset, user, access mode, reason, and ticket to the Idira session ID, so no privileged session is live without one. Recordings are linked back for playback and reporting.

Before you begin

Palo Alto Networks Prisma Access

- An administrator entitled to create a service account and grant it privileges.
- GlobalProtect installed and connected on the workstation running the setup wizard. The setup domain is reached over Prisma Access.

Palo Alto Networks Idira

- An administrator entitled to create a service account and grant it privileges.

Identity provider

- An identity provider for single sign-on, and the credentials to set up SAML 2.0/OIDC.

SaiFlow platform

- The setup domain provided to you by SaiFlow (for example, setup.app.saiflow.com).

Palo Alto Networks configuration

Configure Prisma Access

1. Log in to the Strata Cloud Manager (SCM) UI and create a service account with OAuth credentials.
2. Grant the service account at least the following permissions:
   - Strata Logging Service: View Only Administrator
   - Prisma Access & NGFW Configuration: Security Administrator, Network Administrator
3. Save the service account's credentials in a secure place.

Configure Idira

1. Create a service account with OAuth credentials through the Idira UI.
2. Make sure the **Is OAuth confidential client** checkbox is enabled.
3. Save the service account's credentials in a secure place.
4. Assign the **System Administrator** role to the service account.

Partner product configuration

Set up the SaiFlow platform with the setup wizard

1. Use GlobalProtect on your workstation to connect to the Prisma Access network. In your web browser, go to the setup domain provided to you (for example, setup.app.saiflow.com) and click **Begin**.
2. Add your IdP provider credentials for single sign-on.
3. Define the IdP group filter. Only the groups that match this regex pattern appear in SaiFlow, and those groups are used to assign access permissions for sites and assets. We recommend using a prefix to match only OT technician groups and their supervisors. You can change this setting later. Use the live preview to verify your pattern matches the intended groups.
4. Enter the Idira credentials for the service account you created in the Configure Idira step:
   - The Idira tenant domain (for example, acme.cyberark.cloud)
   - The service account username
   - The service account password
5. Click **Connect PAM**. SaiFlow tests the connection and verifies the service account has sufficient permissions by creating a temporary Idira Safe, which is deleted immediately afterward.
6. Enter the Prisma Access credentials for the service account you created in the Configure Prisma Access step:
   - The TSG service account ID
   - The TSG service account secret
7. Click **Connect Network**.

(Optional) Set up a test site and asset

This section is skippable. After the Idira and Prisma Access connectivity checks pass, you can go straight to the SaiFlow console.

This section lets you configure a test site and asset to verify data center to OT site connectivity. It launches a short-lived remote session to the asset you define. This asset carries on to the configured platform.

1. Configure the site details:
   - **Site name:** the display name of the site, shown across the SaiFlow platform. You can change this later.
   - **Location:** the Prisma Access region to assign this site to.
   - **Organization:** the organization to assign this site to.
   - **Operating mode:** controls how assets in this site are accessed (read-only or full-control).
2. Click **Create Site**.
3. Configure the test asset details:
   - **Asset name:** the asset display name.
   - **Protocol:** the connectivity method to the asset (SSH, RDP, VNC, or Citrix).
   - **Network identity:** the asset's IP address, reachable across the SASE.
   - **Gating group:** the groups that are allowed to connect to this asset.
4. Click **Create Asset**.
5. Click **Provision**.
6. Click **Launch test session** to remotely connect to the asset and verify connectivity from the technician to the asset.

If the session connects successfully, the integration is verified and complete. Click **Open the console** to go to the SaiFlow platform dashboard.

Tested versions

This integration was tested and validated with the following. All three are continuously delivered cloud services with no customer-managed version number.

PRODUCT	VERSION
Palo Alto Networks Prisma Access	Cloud-delivered, managed through Strata Cloud Manager
Palo Alto Networks Idira	Idira Privileged Access Manager SaaS
SaiFlow Secure Remote Access for Energy	SaaS, current release

Troubleshooting

> **Note:** Use cases that do not match the use cases documented in this configuration guide, or that use product versions other than those listed under Tested versions, are out of scope for the integration as documented here. Any additional use cases, or variation from those documented, are out of scope for this configuration guide. Unanticipated issues (for example, scalability, concurrent API session limits, interoperability, or other incompatibilities) can be encountered if out-of-scope use cases are deployed. After familiarizing yourself with the documented use cases, if you plan to deploy use cases that are out of scope, we highly recommend that the initial deployment be performed in a pilot or proof-of-concept environment before deployment in production.

Helpful resources

SaiFlow

- https://docs.saiflow.com/

Palo Alto Networks

- Palo Alto Networks TechDocs: https://docs.paloaltonetworks.com/

Contact information for support

For SaiFlow-specific issues:

- Email support@saiflow.com

For Palo Alto Networks-specific issues:

- Palo Alto Networks Live Community
- Palo Alto Networks Customer Support

Technical details

SaiFlow integrates with Prisma Access and Idira over their REST APIs.

Prisma Access

Configuration plane (Strata Cloud Manager)

- `POST /sse/config/v1/tags` : create tag
- `POST | PUT /sse/config/v1/addresses` : create/update address objects
- `POST | PUT /sse/config/v1/services` : create/update service objects (custom TCP ports)
- `POST | PUT /sse/config/v1/security-rules` : create/update security rules
- `POST /sse/config/v1/ike-gateways` : create IKE gateway (IKEv2, PSK)
- `POST /sse/config/v1/ipsec-tunnels` : create IPsec tunnel
- `POST | GET /sse/config/v1/remote-networks` : create/get/list remote networks
- `GET /sse/config/v1/bandwidth-allocations` : list SPN bandwidth allocations
- `GET /sse/config/v1/service-connections` : list service connections
- `POST /sse/config/v1/config-versions/candidate:push` : commit and push the folder's candidate config

Optional capabilities (feature-gated per deployment)

- `POST /insights/v3.0/resource/query/tunnel_status` : Insights API, tunnel-state dashboards (requires region header configuration)
- `POST /api/sase/v3.0/resource/query/logviewer/firewall_traffic` : log plane, incident evidence
- `POST /api/sase/v3.0/resource/query/logviewer/firewall_file_data` : log plane, incident evidence
- `GET /adem/telemetry/v2/measure/internet/metric` : ADEM telemetry, health-check series

Idira

Safes

- `GET /PasswordVault/API/Safes` : list Safes
- `GET /PasswordVault/API/Safes/{safeName}` : look up a Safe by name
- `POST /PasswordVault/API/Safes` : create Safe
- `GET /PasswordVault/API/Safes/{safeUrlId}/Members` : list Safe members

- `POST /PasswordVault/API/Safes/{safeUrlId}/Members/` : add Safe member
- `DELETE /PasswordVault/API/Safes/{safeUrlId}/Members/{memberName}/` : remove Safe member

Accounts

- `GET /PasswordVault/API/Accounts` : list/search accounts
- `POST /PasswordVault/API/Accounts` : create account
- `GET | PATCH /PasswordVault/API/Accounts/{id}` : get/update account
- `POST /PasswordVault/API/Accounts/{id}/Password/Retrieve` : retrieve account secret
- `POST /PasswordVault/API/Accounts/{id}/Password/Update` : change account password
- `GET /PasswordVault/API/Accounts/{id}/Activities` : account activity trail
- `POST /PasswordVault/API/Accounts/{id}/PSMConnect` : mint a privileged session (browser session or connection file)

Sessions and recordings

Requires the service user to hold the Privilege Cloud Auditors role (a literal Idira Privileged Access Manager SaaS role name).

- `GET /PasswordVault/API/LiveSessions` : list live sessions
- `GET /PasswordVault/API/LiveSessions/{id}/Monitor` : mint session-monitoring gateway details
- `POST /PasswordVault/API/LiveSessions/{guid}/Terminate` : terminate a live session
- `GET /PasswordVault/API/Recordings` (plus `/{id}` and `/{id}/activities`): list/get recordings and activity trails
- `POST /PasswordVault/API/Recordings/{id}/Play` : open recording playback

Identity

- `GET /PasswordVault/api/UsersGroupsQuery?isIdentity=true` : list identity directory groups, for Safe-member mapping

Platform provisioning

SaiFlow manages target platforms and connection components under `/PasswordVault/API/Platforms/*` and `/PasswordVault/api/ConnectionComponents/*`. The service user needs platform and connection-component management rights.
