Cisco SecureX Sign-On

This Privacy Data Sheet describes the processing of personal data (or personal identifiable information) by Cisco SecureX Sign-On ("SecureX Sign-On").

1. Overview of SecureX Sign-On

SecureX Sign-On is Cisco's secure identity solution used by various Cisco security and networking products. SecureX Sign-On is used as a single sign-on (SSO) across products, and operates as the native Identity Provider (IdP) or delegated IdP across selected Cisco products. It provides robust regulatory compliance, resilience, performance, and strong security through adaptive multi-factor authentication (MFA) powered by Cisco Duo ("Duo"). SecureX Sign-On is an optional feature. Customers have the option to use the single sign-on provider of their choice.

SecureX Sign-On also enables delegated authentication through Cisco.com and Microsoft Azure. If a customer uses delegated authentication through Microsoft Azure, the customer's Microsoft Azure administrator determines, through the Microsoft Azure configuration, whether all or only certain of the personal data listed below under "User Registration Information" is shared with SecureX Sign-On. Please refer to Microsoft's privacy policies for information regarding the processing of personal data by Microsoft Azure.

2. Personal Data Processing

For the customers who choose to use SecureX Sign-On, the tables below list the personal data used by this feature to carry out its function, and describes why Securex Sign-On processes that data. Note that all SecureX Sign-On accounts require MFA with Duo, and customers have the option to configure Google Authenticator (or any RFC 6238-compliant Time-based One-Time Password generator) as a backup MFA.

Please see the Duo privacy data sheet here for more information on Duo. Please see Google's privacy policies for information regarding the processing of personal data by Google.

Personal Data Category	Types of Personal Data	Purpose of Processing
User Registration Information	• Email address • Password • First Name • Last Name • Organization • Title • Business phone number	• Account creation • Identity Authentication
Host & Usage Information	• User name • User Activity (e.g. signed on or signed off specific app) • Geo Location (City, Country, Latitude, Longitude, Postal Code and State) • ISP and IP Address • Browser and OS • Timestamp of User activity • Logs including the above information	• Authentication • Audit Trail • Adaptive MFA

3. Cross-Border Transfers

SecureX Sign-On uses Okta Customer Identity services, which are hosted in Amazon Web Services (AWS) only in the United States. Therefore, there is a cross-border transfer of the personal data referenced in Section 2 for users located outside of the United States who elect to use SecureX Sign-On.

Cisco has invested in a number of transfer mechanisms to enable the lawful use of data across jurisdictions. In particular:

- Binding Corporate Rules
- EU-US Privacy Shield Framework
- Swiss-US Privacy Shield Framework
- APEC Cross Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses

4. Access Control

Personal Data Category	Who has access	Purpose of the access
User Registration Information	Customer	Users can modify personal information detailed in Section 2, as part of self-registration. Self-services password reset capabilities
	Cisco	Maintain audit trail, investigate security threats; troubleshooting
	Okta	Troubleshooting and support for solution problems; investigate security threats
Host & Usage Information	Cisco	Maintain audit trail, investigate security threats; troubleshooting
	Okta	Troubleshooting and support for solution problems; investigate security threats

5. Data Deletion & Retention

Personal Data Category	Deletion/Retention Policy
User Registration Information	Since SecureX Sign-On is used across various Cisco products, User Registration Information is maintained until Customer requests deletion via a Cisco TAC service request.
Host & Usage Information	Automatically deleted from the service databases on a rolling 3-month basis.

6. Personal Data Security

Personal Data Processed by SecureX Sign-On	Type of Encryption
User Registration Information	Data is encrypted in transit and at rest
Host & Usage Information	Data is encrypted in transit and at rest

7. Third Party Service Providers (Sub-processors)

Cisco partners with service providers who contract to provide the same level of data protection and information security that you can expect from Cisco. A current list of sub-processors for the service is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
Okta	• User Registration Information • Host & Usage Information	Okta Identity Cloud is hosted in AWS West, and makes use of servers and storage in AWS to implement Okta Identity Cloud	United States
SendGrid	• Username, First Name, Last Name and/or user ID (e.g. email address)	Email Notification	United States https://www.twilio.com/legal/privacy

8. Information Shared by Customer for Support

If a customer contacts the Cisco Technical Assistance Center (TAC) for problem diagnosis and resolution, Cisco TAC may receive and process personal data from the account information provided by customer. The Cisco TAC Service Delivery Privacy Data Sheet describes Cisco's processing of such data. Cisco does not process this data for any other purpose than to assist the customer to resolve issues. For more information, please refer to the TAC Support Essentials Privacy Data Sheet.

9. Information Security Incident Management

Breach and Incident Notification Processes
The Data Protection & Privacy team within Cisco's Security & Trust Organization coordinates the Data Incident Response Process and manages the enterprise-wide response to data-centric incidents. The Incident Commander directs and coordinates Cisco's response, leveraging diverse teams including the Cisco Product Security Incident Response Team (PSIRT), the Cisco Security Incident Response Team (CSIRT), and the Advanced Security Initiatives Group (ASIG).

PSIRT manages the receipt, investigation, and public reporting of security vulnerabilities related to Cisco products and networks. The team works with Customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security issues with Cisco products and networks. The Cisco Security Center details the process for reporting security incidents.

The Cisco Notification Service allows Customers to subscribe and receive important Cisco product and technology information, including Cisco security advisories for critical and high severity security vulnerabilities. This service allows Customers to choose the timing of notifications, and the notification delivery method (email message or RSS feed). The level of access is determined by the subscriber's relationship with Cisco. If you have questions or concerns about any product or security notifications, contact your Cisco sales representative.

10. Certifications and Compliance with Privacy Laws

The Security and Trust Organization and Cisco Legal provide risk and compliance management and consultation services to help drive security and regulatory compliance into the design of Cisco products and services. Cisco and its underlying processes are designed to meet Cisco's obligations under the EU General Data Protection Regulation and other privacy laws around the world.

See Section 3 above for the privacy transfer mechanisms leveraged by Cisco for the lawful use of data across jurisdictions. In addition to complying with our stringent internal standards, Cisco also maintains third-party validations to demonstrate our commitment to information security.

In addition, SecureX Sign-On and its 3rd party provider have implemented a compliance program built upon industry-standard certifications and authorizations. As the compliance and regulatory environment is always changing, a current list of Okta certifications can be found at https://www.okta.com/security.

11. General Information and GDPR FAQ

For more general information and FAQs related to Cisco's Security Compliance Program and Cisco's GDPR readiness please visit The Cisco Trust Center.

Cisco Privacy Data Sheets are reviewed and updated on an annual, or as needed, basis. For the most current version, please see https://www.cisco.com/c/en/us/about/trust-center/solutions-privacy-data-sheets.html.