Securden

Unified PAM

Product Deployment Checklist

S.No	Feature	Notes
Backend Database		
1	Decide if you are going to use the PostgreSQL database bundled with the product or MS SQL server as the backend database.	Both databases are scalable and work well. However, you need to make the choice at the time of moving to production as data migration is not supported if you wish to change later.
Mandatory Settings		
2	Installation Encryption Key	When you apply the registered license key, you will be prompted to move the installation encryption key to a location other than the installation folder. This is to ensure that the encrypted data and the encryption key are not kept together. Follow the instructions on the interface to complete this step.
3	Mail Server Settings	Securden sends various email notifications to the admins/users and to facilitate that SMTP server details are to be configured. Navigate to **Admin >> General >> Mail Server Settings** in the GUI to perform this step.
4	Proxy Server Settings	If your organization makes use of a proxy server to regulate internet traffic, configure the proxy server details here to facilitate Securden to connect to the internet. Navigate to **Admin >> General >> Proxy Server Settings** in the GUI to perform this step. Internet connectivity is required if you want to run the report that checks breached passwords.

5	Server Connectivity Settings	This setting is to specify how to connect to the Securden web interface from client machines and the name with which the client machines identify the Securden server host. Navigate to **Admin >> General >> Securden Server Connectivity** in the GUI to perform this step.
User Onboarding and Management		
6	Integration with Directories	You can integrate with Active Directory /Azure AD / LDAP and import the required users and/or groups. You can keep the user database in synchronization with the respective directories and also leverage the authentication mechanism for allowing access to users. Navigate to **Users >> Add** section to do this.
7	Assign Roles to Users	After importing users, assign roles to them. You may make use of any of the predefined user roles or create custom roles as required. Use the 'Edit' icon next to the respective users to assign the role. You may create custom roles from **Admin >> Customization >> Custom Roles**. In addition, decide if you want to have super administrator role. If yes, you can also decide how many super admins you would like to have. The recommended approach is to create one or two super administrators and then completely turn off further creation. This can be done from **Admin >> Customization >> Configurations**.
8	Delete the default Securden Administrator account	By default, Securden comes with the administrator role as a locally created account. Delete that account. You may create another local account to serve emergency access scenarios such as active directory domain is down etc.

9	Enforce Two Factor Authentication	For enhanced security, you can enforce a second layer of authentication for your users to access their Securden accounts. Users will have to authenticate through two successive stages. It is strongly recommended to activate Two Factor Authentication (2FA). You can do this from **Admin >> Authentication >> Two Factor Authentication**.
10	Explore SSO	Securden integrates with various SAML-compatible federated identity management solutions such as Okta, G Suite, Microsoft ADFS, OneLogin, PingIdentity, Azure AD SSO, and others for Single Sign On. Securden serves as the SAML Service Provider (SP) and it integrates with SAML Identity Providers (IdP). If you are using any SSO solution already, you may integrate that with Securden (**Admin >> Integrations >> SAML SSO**).
Privileged Account Management, Remote Session Management		
11	Create Password Policies	Security best practices recommend usage of strong, unique passwords for every account. Password policy in Securden helps you define the strength, complexity requirements, periodicity for password resets and other conditions. Wherever automation is possible, Securden password generator will automatically assign unique passwords as per the policy defined. Navigate to **Admin >> Account Management >> Password Policy** in the GUI to create password policies. After creating a policy that suits your requirements, you can set that policy as the default policy for your organization from **Admin >> Account Management >> Password Policy >> Set As Default Policy** section in the GUI.

12	Create Account Types	Account types help identify and classify the accounts being added in Securden. Proper classification comes in handy to carry out various operations such as sharing, reporting etc. Super Administrators, Administrators, and Account Managers have the privilege to add custom types, edit and delete existing ones. When creating your own account types, you can define the fields needed for that type, decide if certain fields should be marked as 'mandatory', if any field to hold default values and so on. **Navigate to Admin >> Account Management >> Account Types** to create new account types and to manage existing ones.
13	Decide about allowing Personal accounts management	Securden allows classifying the accounts into 'work' and 'personal' categories. Work accounts belong to the organization and can be shared with others. 'Personal' accounts are purely personal to the user who is adding them and can't be shared with others. Even super administrators can't view them. If you don't want to allow managing personal passwords, you can disable this from **Admin >> Customization >> Configurations**.
14	Accounts Discovery	You can discover the computers (Windows, Mac, and Linux), databases, and SSH devices in your network and the accounts that are part of those computers/ devices. (**Accounts >> Add >> Discover Accounts**).
15	Import Account from CSV, XLSX, or KeePass	If you have your passwords in CSV or XLSX files, you may import them to Securden. Navigate to **Accounts >> Add >> Import from File** to perform this.

16	Manual Addition of Accounts	On an ongoing basis, you can add accounts manually too. You can make use of this provision to add website accounts and others that are not discoverable. Navigate to **Accounts >> Add >> Add Accounts Manually** in the GUI to perform this step.
17	Add SSH Keys	In addition to storing passwords, you can also store and manage SSH keys. The provision to manage SSH keys helps you store the keys securely, track their usage, and associate them with required Unix devices for authentication and remote access.
18	Create Folders	You can organize the accounts in Securden by grouping them as folders for easy and efficient management. At any point in time, a specific account could remain a member of one folder only. That means the same account cannot become a member of multiple folders. You can recreate your organization's hierarchy in the form of folders and multiple levels of subfolders.
19	Share Accounts and Folders	You can organize the accounts in Securden by grouping them as folders for easy and efficient management. At any point in time, a specific account could remain a member of one folder only. That means the same account cannot become a member of multiple folders. You can recreate your organization's hierarchy in the form of folders and multiple levels of subfolders.
20	Remote Connection Options	Securden allows users to launch RDP, SSH, SQL and other connections and supports launching web-based connections and using native applications. If you want to launch remote connections to multiple computers and IT assets, you may add the required IT resources from **Admin >> Remote Connections**

		and Session Recordings >> Assets for Remote Connections. After adding the IT assets, you need to pick specific assets for associating them with specific users/user groups and accounts/folders in Securden. This can be done from **Admin >> Remote Connections and Session Recordings >> Domain Account - Assets Association**.
21	Custom Application Launcher	In addition to the default modes of launching web-based connections and through native clients, you can define custom application launchers to supply credentials and automatically launch any application, including thick application clients. Basically, you will be creating a profile for each such application capturing the input fields as found in the target application. The profile will have placeholders to replace the required values from Securden repository at the time of launching the connections (**Admin >> Remote Sessions and Recordings >> Custom Application Launcher**).
22	Configure Just-in-time Access Workflow for Sensitive	You can establish an additional layer of security for sensitive accounts by enforcing your users to go through approval workflows. This also serves as a just-in-time access provisioning mechanism. Whenever the passwords of such accounts are to be accessed, users will have to raise a request and select administrators or account managers, who are designated as 'Approvers' will grant time-limited access. At the end of the usage period, the password will be automatically reset. This feature comes with adequate provisions to handle various scenarios

		such as obtaining permission in advance, granting automated approvals.
23	Configure Automated Remote Password Resets	You can periodically reset the passwords of accounts in a fully automated manner. You can create scheduled tasks for periodic password reset for all accounts belonging to a folder. Securden then takes care of assigning strong, unique passwords to each account at periodic intervals. The remote password reset could be configured only at the folder level. Navigate to **Folders >> Select a Folder >> Remote Password Reset** to configure this.
24	Credentials for Remote Operations	Securden establishes connectivity with the target machines to perform the Remote Password Reset with a predefined administrative account. You need to supply the credentials that are to be used by Securden for performing various remote actions such as fetching accounts, dependencies, and carrying out password resets. You have the option to specify the domain administrator credentials that will take effect globally for all accounts. You can also overwrite the global configuration for specific computers through the 'Specific Computer' option. Navigate to **Admin >> Account Management >> Device Level Configurations**. Select the required device type, then the specific device, and then click the 'Remote Credentials' tab in the GUI to perform
25	Explore APIs for managing non-human identities/ application n identities	Securden provides APIs for application-to-application and application-to-database communication. APIs can be used to connect to Securden and fetch the required data automatically. Navigate to **Admin >> General >> Authentication Token for API Access** to start using the APIs.

26	Explore Remote Gateway	By default, all remote sessions from user machines are tunneled through the Securden server, which acts as the gateway. If you want, you can configure a separate machine to serve as the remote gateway in the place of Securden server. Navigate to **Admin >> Remote Sessions and Recordings >> Remote Gateway** to configure this. If you intend to use Session Recording, you need to configure the remote gateway.
27	Configure Session Recording	After configuring the remote gateway as explained above, you need to configure session recording. The configuration is a two-step process: 1. First, you need to enable session recording and specify which sessions are to be recorded - RDP, SSH, and SQL. You also need to specify the location where the recorded files are to be stored. 2. In the second step, you need to switch on session recording at the accounts level or at the folder level. The sessions launched only by the accounts for which session recording is switched on will be recorded. Until the two steps are completed, sessions will not be recorded. In addition, you need to decide about the location where you want to save the recorded sessions. **Admin >> Remote Sessions and Recordings**
28	Application Servers for Distributed Networks	As part of product deployment, Securden offers the flexibility to deploy multiple application servers to take care of certain specific needs such as IT infrastructure spread across multiple networks.

28	Application Servers for Distributed Networks	If your IT assets/privileged accounts are distributed across multiple networks and if you want to manage all those devices using Securden, you can deploy Securden application servers in each of those networks and also associate each application server with a remote gateway. Application servers deployment is a three-step process - first, you need to add the required application servers, then associate each application server with a remote gateway, and finally associate the IT assets in each network with the gateway. Navigate to **Admin >> Remote Distributors >> Application Server** to configure this.
29	Configure Notifications	Securden can send email notifications upon the occurrence of certain events such as password retrieval, deletion, change in share permissions, and others. You can choose the events for which you want to receive notifications. The notifications can be triggered real-time or as one consolidated email once a day. Navigate to **Admin >> Notifications >> Event Notifications** section to configure notifications. You may configure notifications at the folder level too.
30	Granularly Customize Product Features	You can customize the features of Securden in a granular manner. You can switch on and switch off certain features anytime as desired. Navigate to **Admin >> Customization >> Configurations** section to exercise the customization options.

Miscellaneous		
31	Integrations	Securden integrates with SIEM solutions and ticketing systems. Navigate to **Admin >> Integrations** to explore integrations.
32	Configure Emergency Access	You can enable a designated list of users to access all passwords (work accounts) stored in Securden, breaking the usual access controls. This is to meet password access needs during certain emergencies. In this interface, you can designate the users who should get the emergency access privilege. You can define the maximum time duration until which the user should have emergency access. As an additional control, you can define a mandatory waiting period (in minutes) until the person should wait before gaining emergency access. All administrators will be notified when someone wants to gain emergency access. Navigate to **Admin >> Emergency Access** to configure this.
33	Rebrand Product Logo	You can replace Securden logo with your company logo from **Admin > Customization >> Logo, Theme, Text**.
34	Security Settings	You can restrict access to the Securden interface to users only from specific IP addresses. Explore various security settings from **Admin >> Security**.

35	Configure High Availability	To ensure uninterrupted access to accounts and passwords, Securden comes with high availability architecture. This is achieved by deploying another application server, which would serve as the secondary server. In the event ofthe primary server going down, users can connect to the secondary server. Navigate to **Admin >> High Availability** in the GUI to configure High Availability. Note: You can configure any number of additional application servers and deploy them in different locations. If you are using MS SQL server as the backend database, you can make use of SQL clusters.
36	Replace Self-signed Certificate	By default, Securden comes bundled with a self-signed certificate. You can add your own CA-signed certificate by following the steps below. Basically, Securden requires the certificate and the private key. Instructions to do this are available in the Quick Start
37	Configure Database Backup	To ensure access to your data and passwords even in the unlikely scenario of something going wrong with the current installation, Securden offers disaster recovery provisions. You can take backup of the entire database periodically. In the event of a disaster, you can recover data from the backup. Securden allows you to specify the “Backup Destination”. You may give the network path of a remote machine, where the backup copy will be stored. The periodicity could be as low as one hour and you may decide to maintain x number of past backup copies. Navigate to **Admin >> High Availability >> Database Backup** in the GUI to perform this.

38	Passwords Backup as Encrypted HTML file	Super Administrators can create a scheduled task for taking a backup of all work accounts in the form of an encrypted HTML file. When configuring the schedule, a passphrase has to be provided, which will be used as the encryption key. Whenever the backup copy is to be viewed, passphrase has to be supplied. Without the passphrase, the backup copy cannot be opened. The encrypted HTML file can be stored in a secure, remote location. Navigate to **Admin >> High Availability >> Passwords Backup** to perform this.
39	Monitor Product Upgrades	Securden releases minor and major upgrades periodically. You can monitor new releases from **Admin >> Product Upgrades** section and carry out upgrades from there.