Tech Note--Securlet Editions and Privileges

Symantec CloudSOC Tech Note

Copyright statement

Securlet editions and privileges

The following table shows the editions and license levels supported by CloudSOC Securlets. It also shows the account privileges that you must hold in order to activate the Securlet.

Securlet	**Supported edition/license**	**Required account privileges to activate**
AWS	All	IAM User with specific CloudTrail role
Azure	All	Global Administrator and Azure Subscription Reader role
Box	Box Enterprise	Administrator strongly recommended. Can support Co-Administrator with certain limitations
Google	All "G Suite" (G Suite Basic, G Suite Business, G Suite Enterprise)	Super Administrator
Office 365	Office 365 Enterprise	Global Administrator
ServiceNow	Eureka and later	Admin and RestAPI role
Salesforce	Group, Professional (EU cloud only), Enterprise, Unlimited, Performance Editions	System Administrator
Slack	Enterprise Grid	Org Owner
	Enterprise Select	Owner

FAQs

Q. Why must I be a global or super admin to activate the Securlet?

A. The Securlet must have adequate privileges to capture the activities of all users, inspect their data, and perform remediations such as quarantine of files or deletion of emails. When you activate the Securlet, you must have global or super admin privileges in order to authorize the necessary permissions.

For more detail, consider this example of why the Securlet must have Global Admin privileges for Office 365. Securlets for other cloud services are similar:

Symantec CloudSOC uses Global Administrator permissions to authorize the Securlet App to Office 365. This is done using Oauth 2.0 authorization grant flow. The Securlet must have Office 365 Global admin permissions because it uses app-based permissions vs. delegate based permissions. Simply put, app-based permission (or app identity) lets the Securlet authenticate as an application. Doing so avoids issues where you must re-activate the Securlet when an admin gets deleted or when the admin password is changed. For more information about the two types of permissions, see this article, specifically the section on configuring a client application to access Web APIs:

https://azure.microsoft.com/en-us/documentation/articles/active-directory-integrating-applications/

Also, the Securlet doesn't see or store the admin credentials, in this case because authentication is all done by AzureAD. At the time of activation, the Securlet re-directs you to the Microsoft Azure AD sign-in page to provide credentials, which are then used to authenticate using Oauth 2.0 authorization grant flow. At that point, you provide consent and authorize the Securlet to access users data in the Office 365 tenant. For more information on application identity and flow, see the diagram here:

https://azure.microsoft.com/en-us/documentation/articles/active-directory-authentication-scenarios/#web-application-to-web-api

One exception to Oauth 2.0 is when the Securlet collects top-level Sites for Sharepoint during Securlet activation phase -- this is done directly using the credentials, but they are discarded after activation and not stored in CloudSOC. Any newly added top level Sites or sub-sites can be queried using Oauth credentials.

At no point does the Securlet make settings changes to the O365 infrastructure. Write permissions are used for automated (policy based) or manual (admin initiated) actions such as change access permission on the documents that are shared or to put documents in quarantine/legal-hold. See the CloudSOC Tech Note *Office 365 Securlet* for more information.

Revision history

Date	Version	Description
23 August 2017	1.0	Initial release
13 November 2017	1.1	Address that Professional edition is only supported for the EU cloud
18 October 2018	1.2	Add Slack
	1.3	Add Cisco Webex Teams, Facebook Workplace, Workday
12 January 2021	1.4	Remove unsupported Securelets