General Alarms

General Alarms

General alarms include alerts within Intersight that are generic and not related to Server, Chassis and FEX, or Fabric Interconnect alarms categories.

Following table shows the description of the supported general alarms for Intersight.

Name	MO	Severity	Explanation	Recommended Action
ApiKeyExpiringWarning	iam.ApiKey	Warning	This alarm is raised when there is an API key that is about to expire in the next 30 days.	If permissible, extend the expiration date of the API key. If extension of expiry date is not possible, delete the API key and replace it with a new API key. If the API key is no longer required, disable and delete the API key.
ApiKeyExpiringCritical	iam.ApiKey	Critical	This alarm is raised when there is an API key that is about to expire in the next 7 days.	If permissible, extend the expiration date of the API key. If extension of expiry date is not possible, delete the API key and replace it with a new API key. If the API key is no longer required, disable and delete the API key.
ApiKeyExpired	iam.ApiKey	Critical	This alarm is raised when there is an expired API key.	Take action to rotate the API key. Delete the API key and replace it with a new API key. If the API key is no longer required, delete the API key.
ApiKeyIsNeverExpiring	iam.ApiKey	Info	This alarm is raised when there is an existing API key or a new API key is generated without a specified expiration date.	Keys that never expire pose a security risk. If required, delete the never-expiring key and replace it with a key with an expiration date or set an expiration date using the calendar.
OAuthApplicationExpiringWarning	iam.AppRegistration	Warning	This alarm is raised when there is an OAuth 2.0 Application that is about to expire in the next 30 days.	If permissible, extend the expiration date of the OAuth 2.0 Application. If extension of expiry date is not possible, delete the OAuth 2.0 Application and replace with a new OAuth 2.0 Application. If the OAuth 2.0 Application is no longer required, disable and delete the OAuth 2.0 Application.

Name	MO	Severity	Explanation	Recommended Action
OAuthApplicationExpiringCritical	iam.AppRegistration	Critical	This alarm is raised when there is an OAuth 2.0 Application that is about to expire in the next 7 days.	If permissible, extend the expiration date of the OAuth 2.0 Application. If extension of expiry date is not possible, delete the OAuth 2.0 Application and replace with a new OAuth 2.0 Application. If the OAuth 2.0 Application is no longer required, disable and delete the OAuth 2.0 Application.
OAuthApplicationExpired	iam.AppRegistration	Critical	This alarm is raised when there is an OAuth 2.0 Application that has expired.	Take action to rotate the OAuth 2.0 Application. Delete the OAuth 2.0 Application and replace with a new OAuth 2.0 Application. If the OAuth 2.0 Application is no longer required, disable and delete the OAuth 2.0 Application.
OAuthApplicationIsNeverExpiring	iam.AppRegistration	Info	This alarm is raised when there is an OAuth 2.0 Application that is set to never-expire.	OAuth 2.0 Applications that never expire pose a security risk. If required, delete the never-expiring OAuth 2.0 Application and replace with a new OAuth 2.0 Application with expiration date.
SingleAccountAdminLockoutStatus	iam.Account	Warning	The account is prone to lockout if the configured Account Administrator loses access.	Account is at risk of being locked out if the configured Account Administrator loses access. To mitigate this risk, either configure more than 1 user with the Account Administrator role or configure a User Group with the Account Administrator role assigned to it.