Mvision Release Notes

End-User Remediation

When a DLP Policy is violated, a SOC administrator is required to investigate each incident. Often, the admin doesn't have the context to resolve the incident immediately, and he or she must contact the end-user for more information. End-User Remediation allows admins to involve users in the remediation process via email so they can provide information directly, which reduces the number of incidents that admins must investigate, and also educates the user on corporate DLP policies. For complete details, see [End User Remediation](https://success.myshn.net/Policy/Data_Loss_Prevention_(DLP)_Policies/End_User_Remediation).

Integration with McAfee DLP

Customers who use both McAfee DLP and MVISION Cloud can now apply policies created in McAfee DLP to cloud content with MVISION Cloud. This provides new ways to enforce consistent classification behavior in on-premises and cloud policies. The incidents reported in MVISION Cloud can be used for analysis and reporting in the DLP Incident Manager, giving a merged view of DLP incidents occurring in both on-premises and cloud enforcement points. Once integrated, McAfee DLP administrators can edit or create classification definitions, add them to a policy, and then apply the McAfee DLP policy to MVISION Cloud.

Event ID for the Policy Incidents Page

When an event triggers multiple policies, and incidents are generated, the Event ID links all these incidents. An Event ID column has been added to the Policy Incidents Page grid. For details, see [Policy Incidents Page](https://success.myshn.net/Incidents/Policy_Incidents/02_Policy_Incidents_Page).

Connected Apps Policies

You can create policies to manage access to Connected Apps by the service or service instance, include or exclude users and user groups, and select rules, exceptions, and responses. A policy building wizard helps you define your policy. Then manage your policies on the Connected Apps Policies page. For details, see [About Connected Apps Policies](https://success.myshn.net/Policy/Connected_Apps_Policies/About_Connected_Apps_Policies).

Connected Apps Risk Score

The Analytics > Connected Apps page now provides the CloudTrust risk score for the Connected App. For details see [Connected Apps Page](https://success.myshn.net/Analytics/Connected_Apps/Connected_Apps_Page).

Notifications for Cloud Governance

Admins can add new Notifications to the Settings > Global Notifications page using Saved Views. These Notifications will become available for all users of a tenant. Notifications for Cloud Governance trigger an email notification for any changes that occur in Service Risk Saved Views. For details, see [Add a Notification for Cloud Governance](https://success.myshn.net/Start_Here_with_MVISION_Cloud/Notifications/Add_a_Notification_for_Cloud_Governance).

Notification for Failed On-Demand Scans

If an On-Demand Scan fails, the user who created the scan now receives an email, notifying the user that the scan failed. This allows the user to take steps to edit the scan, if possible, and then run the scan again.

IaaS

Quarantine Remediation Response for IaaS Scans

Policies used for IaaS-based On-Demand Scans and Malware Scans can now include the option to Quarantine files.

Additional AWS Policy Templates

The following AWS policy templates are now available:

* Amazon EBS Public Snapshots
* ELB Listener Security
* AWS Route 53 SPF DNS Records
* AWS IAM User Present