Introduction to AIOps Insights

About AIOps Insights

Firewalls are a critical component of any organization's network security architecture. However, as organizations expand and the threat landscape evolves, managing these firewalls becomes complex. Staying updated with the continuous changes and rules to adapt to new threats, network changes, and compliance requirements presents significant challenges. Improper management can lead to security gaps and vulnerabilities, posing risks to an organization's network security.

To effectively address these challenges, a new approach to firewall management is required. This is where AIOps becomes essential.

AIOps for firewalls leverages artificial intelligence (AI) and machine learning (ML) to streamline and enhance the management and security of network firewalls. By using dynamic baselines and advanced forecasting models, AIOps can detect policy anomalies and predict potential issues before they escalate, ensuring proactive maintenance and stability.

Note Currently, the AIOps features are available only for Firewall Threat Defense devices that are managed by Cloud-Delivered Firewall Management Center.

AIOps' key functionalities include:

- **Real-Time Traffic and Capacity Monitoring**: Monitors network traffic and system capacity in real-time, and detects anomalies such as elephant flows, ensuring that resources are optimized for peak performance.

- **Policy Anomaly Detection**: Analyzes firewall policies, and detects misconfigurations or anomalies before they impact performance or security.
- **Feature Adoption Insights and Best Practice Recommendations**: Provides insights into the level of feature adoption and suggests best practices to optimize security configurations.
- **Predictive Forecasting for Network Issues**: Predicts potential future network issues, allowing you to address them proactively and minimize downtime.
- **Critical Alerts**: Filters and prioritizes the most urgent security events helping you focus on critical issues.

AIOps' key features include:

- Summary Insights: Provides detailed information on all insights and insights trend. You can view a list of all the anomalies that are categorized by **Severity** and **Type**.
- Policy Analyzer and Optimizer: Analyzes security policies, detects anomalies, and provides recommendations on remediations that can be performed to optimize the policies, thereby improving the firewall performance.
- Best Practices and Recommendations: Generates detailed assessment reports that highlight failed checks against Cisco Secure Firewall best practices and provides actionable recommendations to resolve issues, ensuring optimal firewall performance.
- Feature Adoption: Provides insights into the features that are adopted and the percentage of adoption to modify the usage pattern and achieve optimal security. By analyzing the adoption rate of different features, you can take decisions on how to improve the usage pattern and enhance security measures.
- Configuration Settings: Provides the ability to configure thresholds for AIOps features and enable or disable insight preferences. You can customize these settings to suit your specific needs.

AIOps Licensing Requirements

If you have licenses for the Secure Firewall Management Center, you can access AIOps by enabling AIOps Insights in your tenant. The initial version of AIOps is included as part of your firewall license and is granted on a per-device basis.

Prerequisites to Use AIOps

- Ensure that you have access to a Security Cloud Control tenant where **AIOps Insights** is enabled and Cloud-Delivered Firewall Management Center is provisioned.
- Ensure that you have configured the thresholds and preferences for the AIOps features.
- You must have **Super Admin** or **Admin** user roles to enable **AIOps Insights** in your tenant.

View Summary Insights

The AIOps **Summary** page provides detailed information about all **Active insights**, including a categorized list of detected anomalies.

Procedure

Step 1 In the left pane, click **Monitor** > **Insights & Reports** > **AIOps Insights** > **Summary**.

Step 2 View the total number of **Active Insights**.

Insights are classified by:

- **Status**: Insights are classified by their statuses such as **Active** or **Resolved**.
- **Severity**: Insights are classified by their severity levels such as **Critical**, **Warning**, or **Informational**.
- **Category**: Insights are classified by their categories such as **Configuration**, **Traffic & Capacity**, **Health & Operations**.

Categories	Subcategories
Configuration	**Access control policy anomaly detection**
Traffic & Capacity	• **Elephant flow detection** • **RA VPN capacity assessment**
Health & Operations	• **High data plane CPU usage** • **Snort high CPU usage** • **High data plane memory usage** • **Snort high memory usage**

Step 3 You can filter insights by insight **Severity** and **Status**.

Step 4 Click **AIOps Insights** to open the dashboard.

Step 5 Click **Settings** to toggle insight preferences and adjust threshold configurations.

Step 6 Click the refresh icon to update the data.

Implement Best Practices and Recommendations

Enhance your organization's security posture by identifying deviations from Cisco Secure Firewall best practices. AIOps allows you to run assessments on your devices, generate reports, and receive actionable insights to help you achieve optimal performance.

- Assessment: Evaluates your firewall configuration across multiple categories. Each check determines alignment with Cisco Secure Firewall best practices. The report summarizes the total number of checks performed and categorizes the results into **Passed** and **Failed**. Failed checks indicate deviations that could impact firewall efficiency and security. Note that each failed check represents an opportunity for improvement and contributes directly to optimizing firewall performance when addressed.

- Recommendation: Provides specific recommendations to address identified issues, ensuring optimal firewall performance. These include detailed information such as the nature of the problem, symptoms, impact, and required actions.

The best practices and recommendations checks are developed with inputs from Cisco's Technical Assistance Center (TAC) and Customer Experience (CX) teams. These insights help address trending issues, incorporate industry best practices, and enhance the recommendations' reliability. By following the provided recommendations, you can resolve issues and align with the best practices, thereby strengthening your organization's security framework and optimizing firewall performance.

Procedure

Step 1 In the left pane, click **Monitor > Insights & Reports > AIOps Insights > Best Practices and Recommendations**.

- The **Assessment Summary** tile displays:
  - The total number of device assessment reports generated.
  - The total number of checks performed.
  - The number of Passed and Failed checks.
- The **Best practices assessment trend** graph helps you track assessment outcomes over time. The Y-axis represents the number of checks, and the X-axis shows assessment dates. Hover over data points to view summary statistics.

Step 2 In the **Device reports** section, you can view the list of all device reports.

- **Device name**: The device for which the assessment was conducted.
- **Device status**: Severity of the insight, categorized as **Critical**, **Warning**, **Informational**, or **Passed**.
- **Failed check**: Number of failed checks and the percentage of improvement potential.
- **Failed assessment category**: Category of the failed check.
- **Assessment Status**:
  - **In Progress**: The assessment is ongoing.
  - **In Queue**: A new assessment is scheduled due to outdated results.
  - **Updated**: The assessment is complete, and results are available.
  - **Error**: There was an issue generating the assessment. Hover over for troubleshooting tips.

Step 3 You can search for device reports by **Device name** or apply filters based on:

- **Device status**
- **Failed check categories**
- **Assessment status**

Step 4 From the three-dot menu icon next to each device:

a. Click **Run assessment** to initiate a new assessment.

b. Click **Download report** to export the Best Practices Assessment Report in PDF format.

Step 5 Click on a **Device name** to view the assessment report.

- In the **Best practices assessment** section, view the failed and passed checks.
- Expand each check to view the recommendations and corrective actions.

Assess and Improve Feature Adoption

Feature Adoption provides insights into the features that are adopted and the percentage of adoption. This information helps you modify your usage patterns to achieve optimal security. By analyzing the adoption rate of different features, you can take the right decisions to enhance your organization's security measures.

Procedure

Step 1 In the left pane, click **Monitor** > **Insights & Reports** > **AIOps Insights** > **Feature Adoption**.

- In the **Summary** tile, you can view the total number of features available, including how many are **Not Adopted**, **Partially Adopted**, and **Adopted**.
- In the **Feature Adoption** section, you can view the percentage of adoption of a particular feature . The feature adoption rate can vary between 0% and 100% depending on the usage.
- In the **Feature Recommendation** tile, you can watch short videos about recommended features that will help enhance your organization’s security.

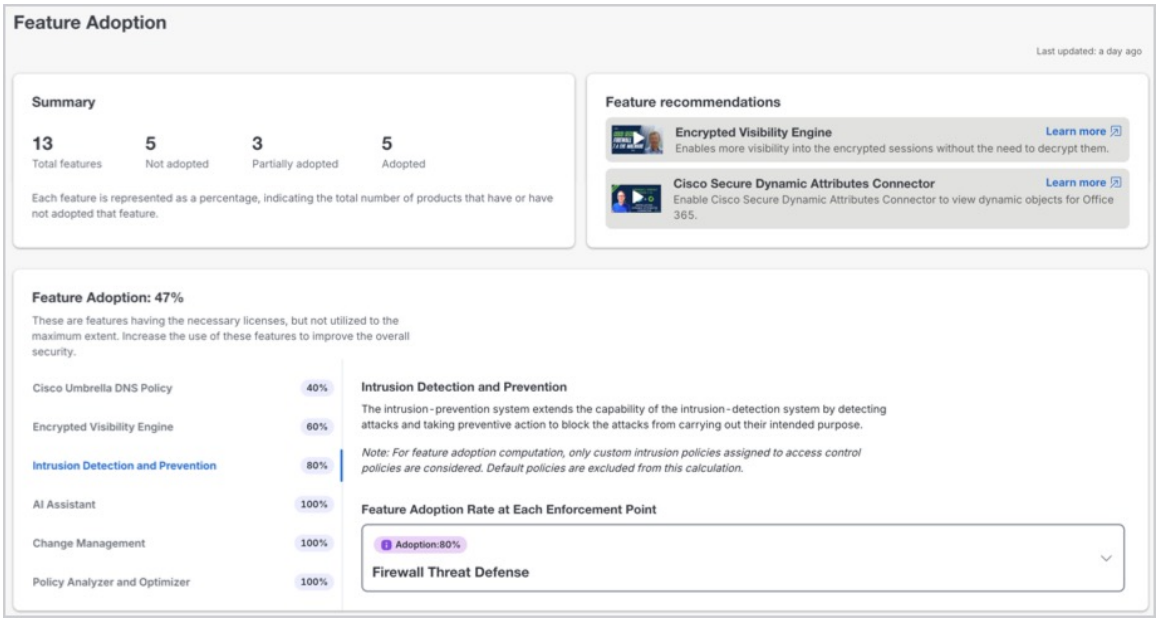
Note

- The feature adoption data is refreshed every 24 hours.
- We recommend that you increase the usage of these features to improve overall security.

Step 2 Click a feature name to view more details, such as:

- A short description of the feature
- Feature adoption rate
- Steps to improve your feature adoption rate efficiency

Figure 1: Feature Adoption



Enable or Disable Insight Preferences and Configure Threshold Settings

You can enable or disable insight preferences for your tenant and configure thresholds for the following AIOps features:

Enable AIOps Insights

To take advantage of AIOps' benefits, you must enable AIOps Insights. You must have **Super Admin** or **Admin** user roles to enable **AIOps Insights** in your tenant.

Procedure

Step 1 In the home page, click **Start Onboarding**.

Step 2 In the **AIOps Insights for Cisco Firewall** window, click **Setup**.

Step 3 In the **Setup AIOps** page, check the **Confirm AIOps activation** check box.

Step 4 Click **Get Started**.

The onboarding process begins, and it takes a few minutes to fetch the data that is required to provide the insights. When completed, the **AIOps** > **Summary** page is displayed.

Traffic and Capacity Insights

You can modify the preferences for traffic and capacity-related insights.

Note

- The settings for **Elephant Flow Detection** and **RAVPN Capacity Assessment** are enabled by default.
- The **RA VPN Capacity Assessment** runs every 24 hours, with changes applied in the subsequent assessment cycle.

Procedure

Step 1 In the left pane, click **Monitor** > **Insights & Reports** > **AIOps Insights** > **Settings**.

Step 2 Click **Traffic & Capacity**.

Step 3 Enable the **High Traffic Caused by Elephant Flow** toggle to detect the elephant flows that transfer large amounts of data and lead to system performance issues.

a) Choose the **Insight Severity** from the drop-down.
b) Click **Submit**.

For more information, see Elephant Flow Detection.

Step 4 Enable the **RAVPN Capacity Assessment** toggle to forecast the trajectory of RA VPN user sessions using the current data, and determine the anticipated time until maximum system capacity is reached.

a) Choose a value from the **Accuracy** drop-down list. . This determines the accuracy of the forecast based on the Root Mean Squared Error (RMSE) value.
b) Enter the **Max Session Threshold** value:
   - The default value is 90%.
   - The minimum value is 1%, and the maximum value is 100%.
c) Enter the **Forecast Duration in Days**:
   - The default duration is 90 days.
   - The minimum duration is 1 day, and the maximum duration is 90 days.
d) Click **Submit**.

For more information, see Remote Access VPN.

After you enable the features for the tenant, you can view the detected anomalies in the **Summary** page, and the respective widgets are displayed on the dashboard.

Best Practices and Recommendations Insights

You can modify the preferences for **Best Practices & Recommendations**-related insights.

Note The setting for **Best Practices & Recommendations** is enabled by default.

Procedure

Step 1 In the left pane, click **Monitor** > **Insights & Reports** > **AIOps Insights** > **Settings**.

Step 2 Click **Best Practices**.

Step 3 Enable the **Best Practices & Recommendations Analysis** toggle button to view the assessment categories, checks performed under each category, and the number of failed checks for each device.

Step 4 Click **Submit**.

After you enable the feature for your tenant, you can view the detected anomalies in the **Summary** page, and the respective widget is displayed on the dashboard.

Feature Adoption Insights

You can modify the preferences for **Feature Adoption**-related insights.

Note The setting for **Feature Adoption** is enabled by default.

Procedure

Step 1 In the left pane, click **Monitor** > **Insights & Reports** > **AIOps Insights** > **Settings**.

Step 2 Click **Feature Adoption**.

Step 3 Enable the **Feature Adoption** toggle to gain insights into feature adoption and the percentage of adoption.

Step 4 Click **Submit**.

After you enable the feature for your tenant, you can view the detected anomalies in the **Summary** page, and the respective widget is displayed on the dashboard.

Health and Operations Insights

You can modify your preferences for **Health and Operations**-related insights.

Note The settings for **Health & Operations** are enabled by default.

Procedure

Step 1 In the left pane, click **Monitor** > **Insights & Reports** > **AIOps Insights** > **Settings**.

Step 2 Click **Health**.

You can enable the following health-related insights:

Step 3 Enable the **Data Plane High CPU Usage** toggle button to monitor data plane CPU usage and detect when thresholds are exceeded.

a. Enter the **CPU Threshold** value:

- The default value is 80%.
- The minimum value is 0% and the maximum value is 100%.

b. Choose a value from the **Insight Severity** drop-down list.

Step 4 Enable the **Snort High CPU Usage** toggle button to monitor Snort CPU usage and detect when thresholds are exceeded.

a. Enter the **CPU Threshold** value:

- The default value is 80%.
- The minimum value is 0% and the maximum value is 100%.

b. Choose a value from the **Insight Severity** drop-down list.

Step 5 Enable the **Data Plane High Memory Usage** toggle button to monitor data plane memory usage and detect when thresholds are exceeded.

a. Enter the **Memory Threshold** value:

- The default value is 80%.
- The minimum value is 0% and the maximum value is 100%.

b. Choose the **Insight Severity** from the drop-down.

Step 6 Enable the **Snort High Memory Usage** toggle button to monitor Snort memory usage and detect when thresholds are exceeded.

a. Enter the **Memory Threshold** value:

- The default value is 80%.
- The minimum value is 0% and the maximum value is 100%.

b. Choose a valur from the **Insight Severity** drop-down list.

Step 7 Click **Submit**.

After you enable the feature for the tenant, you can view the detected anomalies in the **Summary** page, and the respective widget is displayed on the dashboard.

Frequently Asked Questions About AIOps

What is AIOps?

AIOps for firewalls leverages artificial intelligence (AI) and machine learning (ML) to streamline and enhance the management and security of network firewalls. By using dynamic baselines and advanced forecasting models, AIOps can detect policy anomalies and predict potential issues before they escalate, ensuring proactive maintenance and stability.

Are AIOps features available for all types of FMC-managed Firewall Threat Defense devices?

AIOps features are available only for Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense devices. Currently, there is no on-premises management center support.

Can enabling AIOps fail?

If an onboarding failure occurs, open a support ticket with Cisco Technical Assistance Center (TAC).

Can AIOps Insights be disabled?

Yes. Open a support ticket with Cisco Technical Assistance Center (TAC) to disable AIOps Insights.

Additional Resources

- Managing Firewall complexity and Augmenting Effectiveness with AIOps for Cisco Firewall
- Security Cloud Control: Pioneering the Future of Security Management

Troubleshooting for the Secure Firewall Threat Defense using Cloud-Delivered Firewall Management Center

The Security Cloud Control portal provides the following options for in-depth troubleshooting analysis on a Secure Firewall Threat Defense. Upon clicking any of these options, the user is directed to the relevant troubleshooting page in the Cloud-Delivered Firewall Management Center portal.

1. In the left pane, click **Security Devices** > **FTD**.
2. Select an FTD device and on the **Troubleshooting** pane on the right, click the option you want.

   - Packet-tracer allows a firewall administrator to inject a virtual packet into the security appliance and track the flow from ingress to egress. Along the way, the packet is evaluated against flow and route lookups, ACLs, protocol inspection, NAT, and intrusion detection. The power of the utility comes from the ability to simulate real-world traffic by specifying source and destination addresses with protocol and port information.

- Packet capture is available with the trace option, which provides you with a verdict as to whether the packet is dropped or successful.
- Threat Defense CLI allows executing selected threat defense diagnostic command line interface (diagnostic CLI) commands from the management center. These commands run in the diagnostic CLI rather than the regular CLI. These commands are ping (except ping system), traceroute, and select show commands.
- Troubleshoot File Download allows generating troubleshooting files with information targeted to specific functional areas, as well as advanced troubleshooting files that you can obtain in collaboration with Cisco Support. If you have a problem with your appliance, Cisco Support may request you to supply troubleshooting files to help them diagnose the problem.