

Introduction to AgenticOps insights

AgenticOps brings AI-driven intelligence to firewall management, helping you proactively identify issues, optimize configurations, plan software upgrades, analyze policy health, track feature adoption, and assess capacity requirements. Use AgenticOps capabilities to gain operational visibility, prioritize remediation efforts, and improve the performance, security, and reliability of your firewall deployment.

- AgenticOps insights, on page 1
- Capacity and traffic insights, on page 9
- About policy change impact insights, on page 12
- Best practices and recommendations, on page 18
- Feature adoption insights, on page 21
- Software upgrade insights, on page 23
- Application insights, on page 25
- Compliance insights, on page 27
- Insight preferences, on page 29
- Frequently asked questions about AgenticOps, on page 36
- Additional resources, on page 37

AgenticOps insights

AgenticOps insights is a firewall management solution that

- leverages artificial intelligence (AI) and machine learning (ML) to streamline and enhance firewall management and network security
- addresses the complexity of managing firewalls as organizations expand and the threat landscape evolves, and
- provides actionable operational guidance based on data collected from your environment to improve security posture, optimize performance, plan upgrades, and make informed operational decisions.

Supported devices and management platforms

Note Currently, AgenticOps supports:

- Firewall Threat Defense devices that are managed by Cloud-Delivered Firewall Management Center.
- Firewall Threat Defense devices managed by On-Premises Firewall Management Center integrated with Cisco Security Cloud.

  For information on supported versions, see AgenticOps Support for On-Premises Firewall Management Centers.

Key functionalities include:

- **Traffic and capacity monitoring**: Monitors network traffic and system capacity in real-time, and detects anomalies such as elephant flows. This ensures 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.
- **Operational insights**: Evaluates device readiness for software upgrades, suggests compatible versions, and helps plan upgrades to maintain consistency, stability, and compliance across deployments.
- **Critical alerts**: Filters and prioritizes the most urgent security events, helping you focus on critical issues.

Key features include:

- **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.
- **Policy Change Impact Analyzer**: Provides visibility into pending access control policy rule changes across devices, analyzes affected rules and traffic segments, and assesses potential traffic impacts to help you make informed deployment decisions.
- **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. Analyze the adoption rate of different features to improve usage patterns and enhance security measures.
- **Software Upgrade Planner**: Provides upgrade suggestions for your devices through a centralized dashboard. The dashboard displays the current and suggested versions and details about security vulnerabilities and bug fixes.

- **Application Outage Insights**: Detects application outages that may impact users, sites, and business-critical services. The feature correlates outage telemetry, operational insights, and affected resources to help you reduce troubleshooting time.
- **Capacity and Trend Analyzer**: Analyzes firewall capacity utilization and traffic trends to identify abnormal spikes, sustained resource consumption, and emerging performance risks. The feature provides operational visibility into throughput, connection behavior, and traffic patterns to optimize firewall performance.
- **Compliance Posture**: Assess firewall compliance posture against supported security standards. The feature evaluates firewall configurations, identifies compliance gaps, and provides actionable remediation insights to improve security posture
- **Configuration Settings**: Provides the ability to configure thresholds for AgenticOps features and enable or disable insight preferences. You can customize these settings to suit your specific needs.

AgenticOps licensing requirements

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

Requirements: Prerequisites to use AgenticOps

Ensure that these prerequisites are met before using AgenticOps:

- Ensure that AgenticOps Insights is enabled for your Security Cloud Control organization and that Cloud-Delivered Firewall Management Center is provisioned.
- You must have **Super Admin** or **Admin** user roles to opt in and opt out of AgenticOps Insights for your organization.
- If you are using an On-Premises Firewall Management Center, ensure it is integrated with Cisco Security Cloud before onboarding AgenticOps. For information on supported on-prem Firewall Management Center software versions, see AgenticOps Support for On-Premises Firewall Management Center.
- Configure the required thresholds and preferences for supported AgenticOps features.

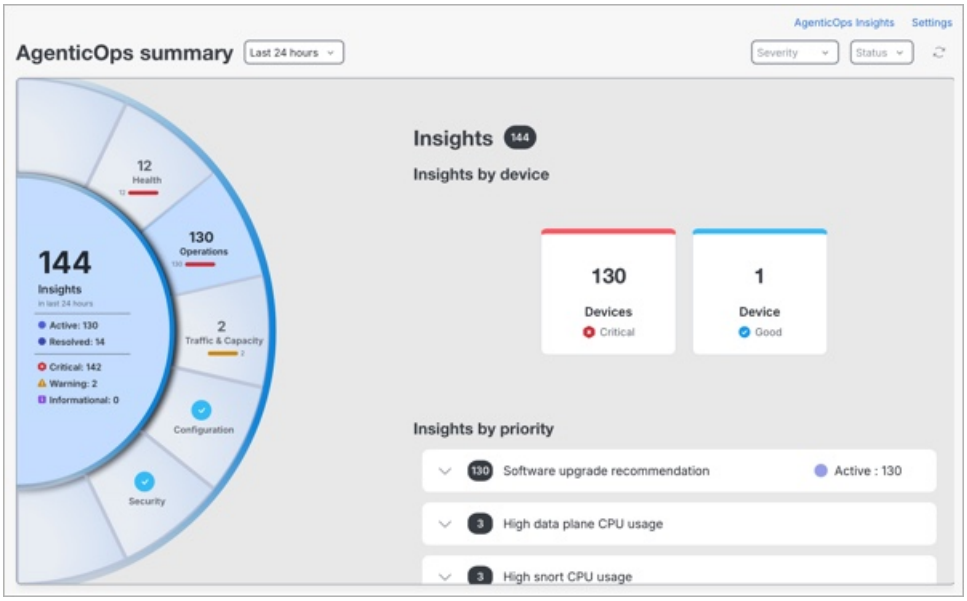
Meeting these prerequisites ensures that AgenticOps can collect the data needed to generate insights and recommendations.

View summary dashboard

The **Summary** dashboard provides a consolidated view of all insights across your environment. It enables identification of areas that require attention and gives you the ability to drill down for operational, configuration, and security analysis. You can filter insights by time range, severity, and status.

AgenticOps summary dashboard

Figure 1: AgenticOps summary



- **Insights visualization panel**: Visual representation of your insights, helping you quickly understand overall system posture and where to prioritize action.
  - The inner ring summarizes insights by status and severity.
  - The outer ring represents insight categories. Selecting a category displays related details.

    The insight categories include:

    - **Operations**: Focuses on insights that help maintain the operational health and software lifecycle readiness of your devices. This includes upgrade recommendations for your Firewall Threat Defense devices and End-of-Life notifications.
    - **Configuration**: Focuses on insights that evaluate your network policies, configurations, and adherence to Cisco Firewall best practices. This includes identifying misconfigurations, policy anomalies, and deviations that may impact performance, security, or compliance.
    - **Security**: Focuses on insights that detect suspicious, risky, or anomalous activities within your environment. These insights highlight behaviors that may indicate compromised accounts and malicious intent.

  Select any insight category to view the insights associated with it.
- **Insights by device**: Click on a device to view insights.
- **Insights by priority**: Expand the section to view all devices with related insights.
- Use the icons at the top right of the page for additional actions:
  - **AgenticOps Insights**: Navigate to the view of all AgenticOps insights.
  - **Settings**: Navigate to configure preferences and thresholds for insights.

Confidence levels in AgenticOps

A confidence level represents the reliability of a forecast-based insight generated by AgenticOps. It indicates how accurately AgenticOps can predict future behavior for a given condition, helping you decide when immediate action is required versus when monitoring is sufficient.

Applicable forecast-based insight types

Confidence levels are displayed for these forecast-based AgenticOps insights:

- Remote Access VPN – Maximum Sessions Nearing Limit
- CPU (LINA) Utilization Forecast Breach
- CPU (Snort) Utilization Forecast Breach
- Memory (LINA) Utilization Forecast Breach
- Memory (Snort) Utilization Forecast Breach

How AgenticOps determines confidence levels ?

For forecast-based insights, such as **High Snort Memory Usage**, **High Snort CPU Usage**, and **RA VPN Forecast**, AgenticOpsevaluates how accurately its machine learning models can predict future behavior using historical patterns and current trends.

Based on this forecast accuracy, each insight is automatically assigned a confidence level. Insights that do not meet a minimum reliability threshold are not generated.

- **High**
  - The forecast is highly reliable and strongly supported by historical data.
  - Recommended action: Prioritize the investigation and take proactive corrective measures.
- **Medium**
  - The forecast is reliable but may show moderate variability.
  - Indicates a strong trend that is likely to continue.
  - Recommended action: Review the insight and plan mitigation.
- **Low**
  - The forecast indicates a possible emerging condition.
  - Limited data or higher variability reduces certainty.
  - Recommended action: Monitor closely and validate with additional operational context.
- **Very low**
  - The forecast signal is weak or in an early stage.
  - Higher uncertainty due to insufficient or inconsistent data.
  - Recommended action: Observe trends. No immediate action is required.

Insight statuses and transitions

This table outlines the possible insight statuses, their descriptions, transitions, and examples.

Status	Description	Transition	Triggered by	Example
Active	• An issue is detected and ongoing. • This is the initial state when an issue is identified.	–	System	Upgrade options suggested for Firewall Threat Defense devices.
Resolved	• AgenticOps automatically marks an active insight as resolved when the issue no longer exists. • Historical details are available for reference.	**Active** to **Resolved**: After you fix the issue and the system confirms it in the next check.	• Automatically by the system for performance issues. • By the user (with system confirmation) for configuration issues.	Overlapping firewall rules corrected by the user.

Status	Description	Transition	Triggered by	Example
Not Applicable (N/A)	• The issue existed earlier but it is no longer present. • No historical data is available for reference.	**Active** to **Not Applicable**	System	• When an Access Control policy is deleted, the corresponding insight is marked as NA. • When a device is deleted from FMC inventory, all insights for that device are marked as NA. • When earlier Policy Analyzer and Optimizer results showed issues but a recheck finds zero issues and no details to display, the insight is marked as NA.

View AgenticOps insights

View AI-driven alerts that help you detect, prioritize, and resolve issues across your environment by accessing comprehensive insights from a centralized dashboard.

The **AgenticOps Insights** page provides AI-driven alerts that help you detect, prioritize, and resolve issues across your environment.

Procedure

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

Step 2 On the **Summary** page, click **AgenticOps Insights** at the top right.

Insights are displayed in chronological order and can be filtered by the following:

- **Time**: Select a time range to view insights generated within that window
- **Severity**: Select a severity level, such as **Critical**, **Warning**, or **Informational**.
- **Insight**: Select a type of insight to view.

- **Category**: Select a category such as **Configuration**, **Health**, **Operations**, and so on.
- **Impacted Resources**: Select a device or service affected by the insight.
- **Status**: Select a status, such as **Active**, **Not applicable**, or **Resolved** stauses.

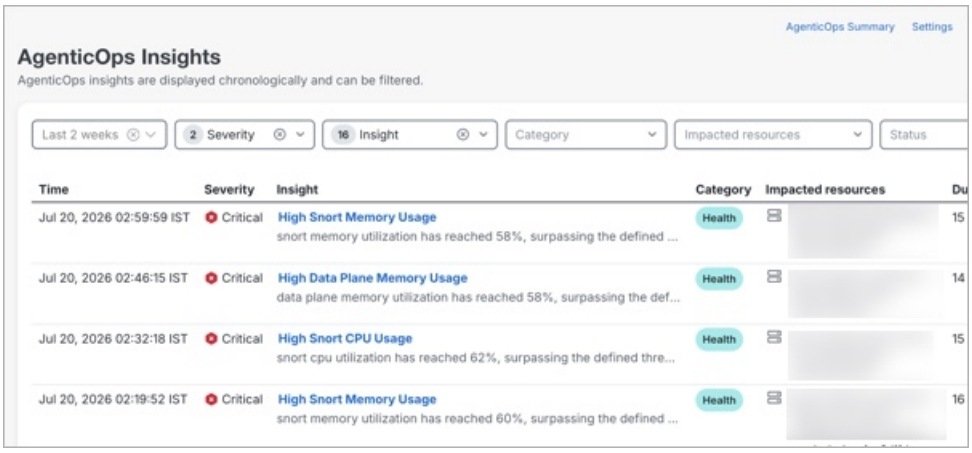
Clicking **Reset all** clears all applied filters and returns to the default view.

Step 3 In the insights table, click an **Insight** or **Impacted Resource** to view additional details.

The details include a summary of the issue, the probable cause, related metrics, and recommended remediation or upgrade actions to ensure optimal performance.

Step 4 Use the icons at the top right of the page for additional actions:

Figure 2: AgenticOps insights



- **AgenticOps Summary**: Navigate to the view the high-level summary of all insights.
- **Settings**: Navigate to configure preferences for AgenticOps features.

You can now view and filter AI-driven insights to identify issues, assess their impact, and prioritize remediation efforts across your environment.

AgenticOps for On-Premises Firewall Management Center

AgenticOps supports Firewall Threat Defense devices managed by an On-Premises Firewall Management Center that is integrated with Cisco Security Cloud and onboarded to AgenticOps. Support for individual AgenticOps features depends on the On-Premises Firewall Management Center software version.

Note Currently, On-Premises Firewall Management Center registered through Secure Device Connector (SDC) are not supported.

AgenticOps feature	Supported On-Premises Firewall Management Center versions
Capacity and Trend Analyzer	10.0.0+
Policy Analyzer and Optimizer	7.4.0+
Software Upgrade Planner	7.4.0+
Best Practices and Recommendations	10.0.0+
Feature Adoption	10.0.0+
Application Insights (ThousandEyes)	7.6.0+
User Risks Insights	10.0.0+
Policy Analyzer and Optimizer - Network Address Translation	7.6 +
Policy Analyzer and Optimizer - Access Control Policy	7.2.0 +

After onboarding, supported On-Premises Firewall Management Center- managed devices are available throughout AgenticOps, including the Summary page, AgenticOps Insights, and supported feature dashboards.

Capacity and traffic insights

Capacity and traffic insights are analytical capabilities that

- provide visibility into resource utilization across devices and highlight emerging risks
- predict when risks may lead to performance issues by combining historical trends with predictive insights
- enable proactive capacity planning by identifying future risks before they impact system performance, and
- anticipate problems and support action before they affect users.

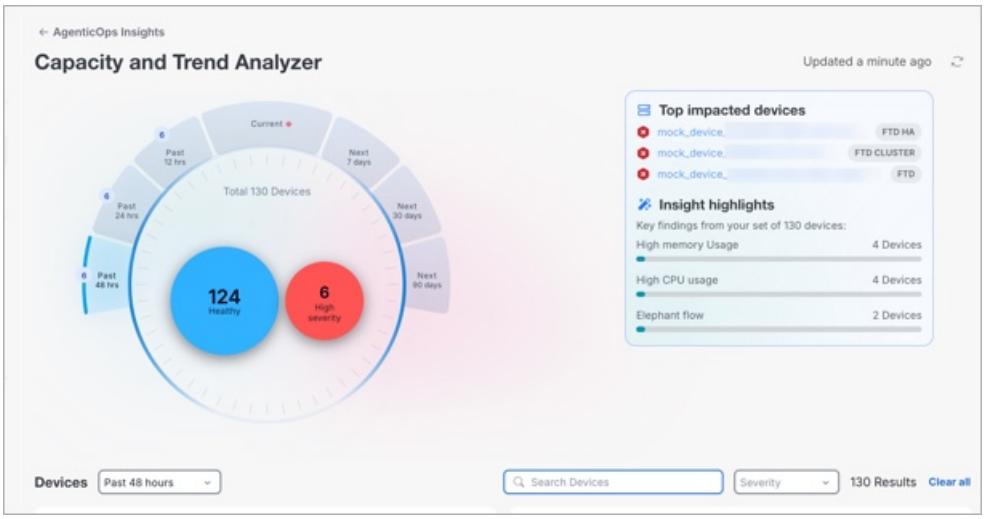
How AgenticOps generates capacity insights

Forecasted insights predict future resource utilization based on historical trends and patterns. AgenticOps continuously analyzes historical data and runs periodic forecasts to identify when resources are likely to reach configured thresholds.

AgenticOps uses multiple analytical approaches to identify and predict issues. AgenticOps runs forecasts on a recurring weekly basis to identify potential capacity risks in advance, including:

- Detect threshold breaches: Identifies when CPU or memory usage exceeds configured limits in real time.
- Detect anomalies: Identifies unusual deviations from expected behavior based on historical patterns.
- Detect elephant flows: Detects large traffic flows that can impact system performance and resource utilization.

- Detect Remote Access VPN session limits: Detects or predicts when VPN session capacity limits are reached.
- Forecast capacity risks: Predicts future threshold breaches using historical trends, enabling proactive planning.



Note

- The accuracy of insights depends on the availability and quality of historical data. Limited or inconsistent data may delay or reduce insight accuracy.
- In environments with limited activity or newly onboarded devices, insights and forecasts may take time to appear.

This table shows key features of Capacity and Trend Analyzer:

Table 1: Key features of capacity and trend analyzer

Feature	Description
Capacity insights dashboard	Provides a fleet-level view of device capacity status, displaying past, current, and predicted capacity insights across all monitored devices.
Capacity insights	Generates insights based on CPU, memory, connection, throughput, and VPN session activity to highlight potential resource constraints.
Device capacity analysis	Displays detailed capacity insights for an individual device, including resource metrics, AI-generated summaries, and forecast information.
Predictive capacity forecasting	Uses historical resource utilization data to predict future usage trends and identify potential capacity risks before thresholds are reached.

Feature	Description
Timeline-based analysis	Allows you to analyze capacity insights across different time windows, including past events, current conditions, and predicted future risks.
Device health indicators	Displays device health status based on active and predicted capacity insights, helping you quickly identify devices that require attention.

The Capacity and Trend Analyzer supports:

- Secure Firewall Threat Defense devices
- Secure Firewall Threat Defense High Availability (HA) deployments
- Secure Firewall Threat Defense cluster deployments



Note For High Availability (HA) and cluster deployments:

- Capacity analysis runs at the system level.
- Individual member devices are not displayed separately.

Analyze capacity trends and forecast resource usage

This task enables you to analyze historical data, identify growth patterns, and understand how resource consumption changes over time to support capacity planning and operational decision-making.

Use Capacity and Trend Analyzer to evaluate resource utilization trends across your environment. The analyzer helps you move from reactive troubleshooting to proactive capacity management by enabling you to identify risks early and take informed action.

Before you begin

Ensure that **Capacity and Trend Analyzer** is enabled under **Settings**. For more information, see enable Capacity and Trend Analyzer.

Follow these steps to analyze capacity trends and forecast resource usage:

Procedure

Step 1 In the left pane, click **Insights & Reports** > **Capacity and Trend Analyzer**.

This opens the dashboard where you can view capacity insights across your environment.

Step 2 Use the circular timeline to select a timeframe, such as **Current**, **Past (12 hours**, **24 hours**, or **48 hours)**, **Next (7 days**, **30 days**, or **90 days)**.

- **Current** shows active capacity insights.

- **Past 12, 24, or 48 hours** show insights from the selected past period.
- **Next 7, 30, or 90 days** show predicted capacity risks.

The timeline also displays the total number of devices and their health status, such as **Healthy**, **Needs attention**, and **High severity**.

Step 3 Review the summary panel.

- Use the **Top impacted devices** section to identify devices with the most critical capacity issues.
- Use the **Insight highlights** section to understand the most common capacity risks across your organization.

Step 4 Review device insights in the **Devices** section.

- Search for a device or use filters such as timeframe and severity to locate devices that require attention.
- Each device displays a summary of detected or predicted issues, along with associated insight tags.

Step 5 Select a device to view detailed insights.

This view provides summaries and detailed insights for the selected device.

Step 6 On the device details page, review the **AI summary**, **Resolved insights**, **Active insights**, and **Future insights**.

Step 7 In the **Device metrics** section, select a metric to view historical trends and forecast data.

Step 8 Use the insights and forecasts to determine appropriate actions, such as redistributing traffic, scaling resources, or planning capacity upgrades. After taking action, use the **Current** view to monitor whether the issue has been resolved.

The **Capacity and Trend Analyzer** helps you move from reactive troubleshooting to proactive capacity management by enabling you to identify risks early and take informed action.

You can now analyze capacity trends and forecast resource usage across your environment. The Capacity and Trend Analyzer provides insights into historical data, growth patterns, and resource consumption changes to support proactive capacity planning and operational decision-making.

About policy change impact insights

Changes to an access control policy can affect network traffic in unexpected ways. A modification that appears minor, such as updating a network object, expanding a rule, or changing rule conditions, can alter how traffic is evaluated by other rules in the policy. These effects are often difficult to identify before deployment.

Policy Change Impact Analyzer helps you review the potential impact of pending access control policy rule changes across devices before deployment. The analysis helps you identify affected rules, impacted connections, and traffic segments so that you can better understand the consequences of a change before deploying it. The **Policy Change Impact Analyzer** evaluates proposed policy changes and provides visibility into:

- The overall analysis result for each device
- Affected devices and rules
- Impacted traffic segments

- Historical connections affected by a changed rule, when traffic data is available
- Rule-level inferred impact
- AI-generated summaries that explain the potential effect of a rule change

Limitations and considerations

- Currently, **Policy Change Impact Analyzer** supports Cloud-Delivered Firewall Management Center -managed Firewall Threat Defense devices only.
- **Policy Change Impact Analyzer** is available only for deployments in the US, AUS and EU regions.
- High Availability and cluster deployments are represented by their parent target during analysis.
- Impacted connection counts are available only when **Security Analytics and Logging** is enabled and connection events are sent for FTD Management Services.
- Running an analysis does not deploy, edit, approve, or reject policy changes.
- AI-generated explanations support decision-making. Validate important findings against your security requirements and operational policies before deployment.
- Review analysis results before approving production changes, especially high-risk policy modifications.

Understand analysis results

Review the assessment result to understand the likely effect of pending policy changes and the recommended next steps.

Note An analysis result does not indicate whether a change is approved. Review the transition direction, affected rule, and traffic conditions before deployment.

Analysis result	What it means	Recommended action
Critical	One or more changes may expose the network to threats or disrupt services.	• Review affected rules and traffic segments before deployment. • Revise and rerun when the change is not intended.
Potential impact	One or more changes expand access or may affect traffic.	Validate the affected traffic and the expected business outcome before deploying.
Improved security posture	One or more changes reduce exposure or block risky traffic.	Confirm that the affected traffic is intentionally restricted, then continue through normal change review.

Analysis result	What it means	Recommended action
No traffic impact	No behavior-changing traffic transition was identified from the policy comparison.	• Confirm that the proposed rule is needed and is positioned as intended. • This result is different from a change that has zero observed connections.
Indeterminate	The available evidence was insufficient to determine a reliable impact.	• Review the changed rule and traffic criteria manually. • Consider gathering additional operational context and rerunning the analysis.

Understand job statuses

Job Status shows the current state of the policy impact analysis and whether the latest result is available and up to date.

Job status	Description
Verifying analysis is up to date	The system is checking whether the latest analysis still matches the pending policy changes.
Queued	The analysis request was accepted and is waiting to run. Wait for the status to change to **In progress** .
Completed	The latest analysis completed successfully. A warning icon may appear if a policy analysis returned an error.
Partial success	Useful assessment results are available, but one or more stages did not complete. Review the available details and **Workflows** before deciding whether to rerun.
In progress	The system is preparing policy data, calculating impact, or collecting connection evidence. Wait for the result or open **Workflows** to monitor progress.
Out of date	The policy changed after the analysis started, or the analysis is more than 24 hours old and its traffic evidence may no longer be current. Rerun the analysis to get the latest results.
Failed	The latest overall analysis failed. Review the error and **Workflows** details, then rerun the analysis if appropriate.

Job status	Description
Cancelled	The analysis was cancelled by an authorized user before completion.
Not analyzed	No analysis is available for the device, or the device has pending changes that have not yet been analyzed. Select a device and run the analysis.
Not applicable	No pending policy changes are available for analysis. Create or save the intended policy changes, then run the analysis.
Unknown	The system could not determine a reliable current status. Refresh the device list and try again later. If the issue persists, review the workflow details.

Understand inferred impact

Inferred Impact describes the likely effect of an individual changed rule or affected rule.

Inferred impact	Description
Potential threat exposure risk	The change may allow risky applications, risky URL categories, broad application or URL scope, sensitive destination ports, or broad Internet exposure.
Potential service disruption	The change may block sensitive services or high-volume business traffic.
Access expansion	The change may allow traffic that was previously blocked without a clear risky-application or sensitive-port signal.
Indeterminate	The available evidence was insufficient, or the impact assessment did not complete.
Improved security	The change blocks risky or untrusted traffic, or reduces broad external exposure.
No traffic impact	No behavior-changing traffic transition was detected.

Impacted traffic segments and connections

An **Impacted Traffic Segment** is a distinct combination of traffic conditions whose policy outcome, such as allow or block, changes when the proposed policy changes are deployed.

- Traffic conditions may include source and destination zones, networks, applications, URLs, users, services, ports, security-group tags, and geolocation identities.
- The number of impacted traffic segments is not the number of rules, packets, IP addresses, or historical connections.

Impacted Connections shows the number of historical connections associated with traffic affected by a changed rule.

- The count is based on available Security Analytics and Logging connection-event data. It represents observed historical activity, not a forecast of future traffic.
- If connection events are unavailable, the analyzer can still identify impacted traffic segments, but historical connection counts are not available.
- Review the policy comparison and traffic segments instead of treating unavailable data as zero traffic.

Understand policy analysis limitations

Some policy constructs are not fully evaluated during analysis. Review affected rules manually before deployment when these constructs are involved.

- Object overrides are not considered during analysis. For example, if a port object has the value `8080` but is overridden to `80` for a particular device, the device-specific value `80` is not considered.
- Country, continent, and custom geolocation objects are expanded to country-level identities. They are not expanded to IP-level identities, and individual IP addresses are not compared.
- URL category reputation is not considered. For example, if a new rule uses the same URL category with a different reputation, the analyzer may report **No Traffic Impact** even though the reputation changed.
- URL list and URL feed objects are not expanded into individual URLs. The analyzer reports an impact only when the object is used in an affected traffic fragment or segment. Individual entries in the list or feed are not evaluated separately.
- Time-range support is limited. Only active time ranges are considered. Rules with future or expired time ranges are treated as disabled. Changes to the time-range configuration itself are not considered during analysis.
- Dynamic-attribute support is limited to Security Group Tags (SGTs), including supported FMC and ISE SGT references. CSDAC-backed dynamic attributes and other unsupported dynamic-object criteria are not analyzed.
- Application filters entered directly in the application field, such as **Very High** or **High** risk or business relevance criteria, are not supported when they are inline filters rather than user-defined application filter objects. User-defined application filters, including filters that combine multiple criteria, are supported.

A policy change impact analyzer is a service that reviews potential impact of policy changes, identifies affected rules and connections, and provides AI-generated summaries.

- reviews potential impact of policy changes
- identifies affected rules and connections, and
- provides AI-generated summaries.

Analyze policy change impact

Analyze pending access control policy rule changes to understand their potential impact on network traffic before deploying the changes to production devices.

The Policy Change Impact Analyzer helps administrators assess the consequences of policy modifications by analyzing rule changes, identifying affected traffic segments, and providing historical connection data. This proactive analysis enables informed decision-making during the policy deployment process.

Before you begin

- Enable the **Policy Change Impact Analyzer** toggle under **Insights & Reports** > **Settings**.
- To view historical impacted connection counts, enable **Security Analytics and Logging**.
- **Policy Change Impact Analyzer** currently supports Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense devices.

Procedure

Step 1 In the left pane, click **Insights & Reports > Policy Change Impact Analyzer**.

The **Policy Change Impact Analyzer** page displays an **Impact Analysis** summary, including the number of identified impacts.

The device list displays:

- **Device Name**
- **Job Status**
- **Analysis Result**

Step 2 Select one or more devices, and then click **Run Impact Analyzer**.

You can select up to 10 devices for analysis. The analyzer evaluates the pending policy changes for the selected devices.

Step 3 Monitor the analysis in the device list.

Use the search field to search by device name, analysis result, or job status.

Step 4 Click a device row to open the details pane.

The pane displays the device status and may include these actions:

- **View change impact details** to open the detailed analysis.
- **Re-analyze** to generate an updated result.
- **Deploy** to open the standard deployment workflow.
- **Workflows** to review analysis execution details and errors.

Step 5 Click the device name to open the analysis report.

The analysis details page displays the overall impact assessment for the selected device.

Step 6 Review the **Analysis Result**, **Rule Change Summary**, **Impacted Traffic Segments**, **Impacted Connections**, and **Inferred Impact**.

Step 7 If the analysis is incomplete, failed, out of date, or indeterminate, review the policy manually before deployment and rerun the analysis as needed.

Note **Policy Change Impact Analyzer** does not deploy, edit, approve, or reject policy changes. Use the standard deployment and change-control process after reviewing the analysis results.

You can also run a **Pre-deployment Assessment**. It performs the basic assessment and uses Policy Change Impact Analyzer to evaluate saved, pending access control policy changes. The report summarizes affected rules and traffic decision changes, with historical connection evidence when available, to help you review potential impacts before deployment. See Pre-deployment assessments for more information.

The **Policy Change Impact Analyzer** displays the potential impact of pending access control policy changes, including changed rules, impacted traffic segments, historical connections, inferred impact, and rule change summaries.

Best practices and recommendations

Best practices and recommendations are a security assessment mechanism that

- enhances your organization's security posture with AgenticOps by identifying deviations from Cisco Secure Firewall best practices
- runs assessments on your devices, generates reports, and receives insights that guide you toward optimal performance, and
- addresses trending issues, incorporates industry best practices, and enhances the reliability of recommendations through input from Cisco's Technical Assistance Center (TAC) and Customer Experience (CX) teams.

Assessment and recommendation features

Best practices and recommendations include these key components:

- **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. It categorizes the results as **Passed** or **Requires review**.

  Checks that require review indicate deviations that could impact firewall efficiency and security. Each failed check presents an opportunity for improvement. Addressing these checks contributes directly to optimizing firewall performance.

- **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.

Implement these recommendations to resolve issues, align with best practices, and optimize firewall performance.

Table 2: Key features

Feature	Description
Automated assessments	Runs periodic evaluations of firewall devices against Cisco best practices.
Checks summary	Displays how many checks passed and highlights those requiring review.
Trend visualization	Shows the number of checks over time, helping you compare passed and failed checks across assessment cycles.
Device reports	Provides device-specific results and percentage of improvement potential.
Review category and check control	Enable or disable review categories or individual checks for future assessments.

Implement best practices and recommendations

This task enables you to implement best practices and recommendations by reviewing assessment results, managing device reports, and configuring automated assessments to maintain optimal network performance.

The Best Practices and Recommendations feature provides automated assessments of device configurations to identify potential improvements and ensure adherence to Cisco recommended practices. Use this workflow to review assessment results and implement necessary changes.

Before you begin

Ensure that **Best Practices** is enabled under **Settings**. For more information, see Enable Best Practices.

Follow these steps to implement best practices and recommendations:

Procedure

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

The **Assessment Summary** provides a high-level overview of assessment results. It includes two tiles:

- **Checks summary**: Displays the total number of checks and highlights those requiring review.
- **Best practices assessment trend**: Helps you track assessment outcomes over time. The Y-axis represents the number of checks, and the X-axis shows assessment dates. You can hover over data points to view summary statistics.
- **Feedback**: A mechanism for you to provide feedback on the assessments. You can enter optional comments and grant consent for follow-up contact regarding your feedback.

Step 2 In the **Device reports** section, you can view the list of all available device reports. Filter devices by **Device status, Review categories,** or **Assessment status** to narrow down results.

Assessment Statuses: Each device report has an **Assessment Status**, which indicates the current state of the assessment.

- In progress: An assessment is actively running. After completion, a report will be generated.
- In queue: The previous assessment is outdated, and a new one has been scheduled.
- Updated: The assessment is complete, and the latest report is available for review.
- Error: The assessment could not be completed due to an error. The report will be automatically generated after 24 hours. If the issue persists, contact **Cisco TAC** for assistance.

Step 3 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 summary report in PDF format.

Schedule Device Assessment

Periodic assessments run automatically, but you can also run assessments manually at any time. In environments with more than **50 devices**, only **50 devices can be analyzed per day**. Use the **Select devices** option on the **Best Practices and Recommendations** page to choose which devices are included in automated assessments.

- **Select devices for automated assessments**:
  a. Click **Select devices** in the notification banner to open the **Schedule devices for assessment** dialog. This dialog allows you to choose which devices run automated assessments.
  b. Devices in the **Scheduled devices** panel are included in automated assessments. Click **Save**.
- **Mange scheduled devices**: You can update the list of scheduled devices at any time. Devices removed from the **Scheduled devices** panel are no longer included in automated assessments. Devices added to this panel are included in future automated assessments.
- **Device scheduling limits**: You can schedule a maximum of **50 devices** for automated assessments. The **Scheduled devices** panel displays the number of currently scheduled devices, for example **48 / 50 devices**. When 50 devices are selected, further selection is disabled and a tooltip indicates that the maximum number of scheduled devices has been reached.

Step 4 Click on a **Device name** to view a detailed report for that specific device.

- Check the **Show passed checks** checkbox to view successful checks in the detailed view. This provides full visibility into all checks.
- In the **Best practices assessment** section, view the **Total checks**, how many **Passed** and **Require review**.
- Expand each check to view the remediations and corrective actions.

Step 5 Enable or disable an entire category from future assessments. You can also disable individual checks within a category.

- Disable the toggle to exclude a review category or check from future assessments.
- Enable the toggle to include it in future assessments.

Note Disabling a category or check does not affect the actual feature or its operation. The feature continues to function normally, but it is excluded from **Best Practices** assessments.

You have successfully implemented best practices and recommendations by reviewing assessment results, configuring device assessments, and managing category settings. The system will continue to run automated assessments based on your configuration and provide ongoing recommendations for maintaining optimal network performance.

Feature adoption insights

A feature adoption insight is a dashboard capability that

- provides a comprehensive view of how effectively different features are being utilized across your environment
- calculates adoption rates based on the total number of eligible devices and the number of those devices configured with the feature, and
- helps you identify underutilized capabilities and take steps to improve overall adoption.

Feature adoption insight capabilities

The dashboard groups features into license categories to help you understand adoption patterns:

- **Essentials**
- **IPS**
- **Remote Access VPN**
- **Features not requiring license**
- **Subscription-Based Features**

Note If a license is not available for a given category, the adoption rate for that category will always be **0%**.

By tracking the adoption rate at both the feature and license category levels, you can prioritize improvements and maximize the usage of available features. **Feature Adoption** helps you use available capabilities to achieve your intended outcomes

Assess and improve feature adoption

This task helps you evaluate the current adoption status of security features in your organization and provides actionable insights to improve overall security posture through better feature utilization.

Feature adoption assessment provides visibility into which security features are being used, partially used, or not used at all. This analysis helps security administrators identify opportunities to enhance their organization's security by enabling and configuring underutilized features. The assessment includes adoption rates, recommendations, and specific steps to improve feature usage.

Before you begin

Ensure that you have selected the list of features under **Insights & Reports** > **Settings** > **Feature Adoption**.

Follow these steps to assess and improve feature adoption:

Procedure

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

- The **Summary** tile provides a quick overview of overall adoption status:
  - **Adoption rate**: Percentage of features currently adopted across their applicable scope.
  - **Total features**: Total number of features available for adoption.
  - **Not adopted**: Number of features that have not been enabled or configured.
  - **Partially adopted**: Number of features that are enabled or in use but not fully across all applicable scope.
  - **Adopted**: Number of features that are fully enabled and in use.
- In the **Feature Recommendation** tile, you can watch short videos about recommended features that will help enhance your organization's security.



Note
- The data updates every 24 hours, but you can click **Refresh** to update it manually.
- We recommend that you increase the usage of these features to improve overall performance.

Step 2 Click on a feature name to view detailed information.

- A short description of the feature.
- The feature adoption rate can range from 0% to 100%, based on how much the feature is used. Enable the toggle to include the feature in adoption calculations or disable it to exclude it.



Note Enabling or disabling a feature affects only the adoption score and does not impact the functionality of the feature.

- Steps to improve your feature adoption rate.

You can view comprehensive feature adoption metrics, understand which features need attention, and access specific recommendations to improve your organization's security posture through better feature utilization.

Software upgrade insights

A Software Upgrade Planner is a firewall management tool that

- analyzes deployed Firewall Threat Defense devices and provides upgrade recommendations based on compatibility, stability, security vulnerabilities, and bug fixes
- provides a centralized view of the current software version running on each device along with the suggested version, and
- identifies potential risks and compatibility concerns before the upgrade process begins to reduce operational issues and minimize downtime.

Software upgrade planner capabilities

The feature provides these key capabilities to help you make informed upgrade decisions and maintain a consistent software version across the environment:

- Highlights important details such as bug fixes, vulnerability fixes, and upgrade readiness insights
- Simplifies firewall software upgrade planning and management
- Provides guided remediation insights for vulnerabilities and bugs affecting your devices
- Identifies devices that are exposed to active threat campaigns

Need a visual guide? Explore the Software Upgrade Planner feature walkthrough to see it in action.

When you view the details of a security vulnerability or bug, guided remediation provides AI-generated insights to help you understand the issue and determine an appropriate upgrade version. These insights can include:

- **Root cause analysis**: Summarizes the issue and its potential impact
- **Workaround**: When available, helps mitigate the issue before upgrading
- **Remediation guidance**: Identifies how many devices in your deployment are affected and recommends whether upgrading to a specific software version resolves the issue

When applicable, you can view the active threat campaigns affecting a device and access Cisco Talos intelligence resources to learn more about each campaign, including its scope, impact, and recommended mitigations.

Manage software upgrades

Use the Software Upgrade Planner to review suggested software versions for your Firewall Threat Defense devices and evaluate the security and operational benefits of upgrading. In addition to suggested upgrade versions, the planner provides insights into active threat campaigns and guided remediation for vulnerabilities and bugs affecting your devices.

The Software Upgrade Planner helps evaluate suggested software versions, review threat campaign exposure, analyze security vulnerabilities and bug fixes, and use AI-generated remediation insights to make informed upgrade decisions.

Before you begin

Ensure that the **Software Upgrade Planner** toggle is enabled under **Insights & Reports** > **Settings** > **Operations**.

Follow these steps to manage software upgrades:

Procedure

Step 1 In the left pane, click **Insights & Reports > Software Upgrade Planner**.

The **Software Upgrade Planner** page displays a summary of upgrade opportunities across your deployment. The **Summary** section provides an overview of:

- Devices with upgrades available
- Total available fixes
- Details on threat campaigns
- Security vulnerability fixes
- Bug fixes

You can click **View all** in the **CVE Fixes** or **Bug Fixes** tiles to review the corresponding issues across your deployment.

Step 2 Review the suggested upgrade versions for your devices.

- Multiple upgrade options are available based on vulnerabilities, bugs, and new features. The Cisco-suggested version is indicated by a gold star. Choose the version that suits your requirements.
- For each device, the planner displays the current software version and suggested upgrade versions. If a device is affected by one or more active threat campaigns, the current software version displays the number of threat campaigns affecting the device.
- Hover over the **Current version** to view additional details, including the current software version, vulnerabilities found, bugs found, and the active threat campaigns affecting the device.
- Select a threat campaign to open the corresponding Cisco Talos Intelligence blog and learn more about the campaign.

Step 3 To perform an upgrade, click **More actions** (⋮) for the device, and click **Go to product upgrade**

The **Product Upgrades** page opens in Cloud-Delivered Firewall Management Center, where you can perform the upgrade.

- View available upgrade packages.
- Perform an upgrade by clicking **Upgrade** in the **Actions** column. For more information, see Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-delivered Firewall Management Center.

Step 4 In the **Software Upgrade Planner** page, select a device to view more details.

The device details page displays **Suggested** and **Golden** versions. For each suggested version, you can review:

- Active threat campaigns resolved
- Security vulnerability fixes and bug fixes
- Estimated downtime
- New features included in the release
- Link to detailed release notes

Use this information to compare the available upgrade versions and determine the most appropriate upgrade version for your deployment.

Step 5 Review the **Security vulnerability fixes** or **Bug fixes** tabs.

- These tabs list the vulnerabilities and bugs affecting the selected device. You can search and filter the results or export the list as a CSV file.
- Select a CVE ID or bug ID to open the details pane. The details pane provides AI-generated insights to help you understand the issue, including:
  - **Root cause analysis** that summarizes the issue and its potential impact.
  - **Workaround** information, when available, to help mitigate the issue before upgrading.
  - **Remediation** guidance that identifies how many devices in your deployment are affected and explains whether upgrading resolves the issue.
- In the **Bug fixes** tab, bugs are categorized as **Impacting bugs** and **Other bugs**. Impacting bugs are affecting the selected device and its environment. You can search the list, filter bugs by status (**Fixed bugs**, **Open bugs**, or **All**), and export the results as a CSV file.

You can use the **Software Upgrade Planner** to evaluate suggested software versions, review threat campaign exposure, analyze security vulnerabilities and bug fixes, and use AI-generated remediation insights to make informed upgrade decisions.

You can now manage software upgrades using the Software Upgrade Planner, including reviewing suggested versions, evaluating security benefits, and performing upgrades with informed decision-making based on threat campaigns and vulnerability analysis.

Application insights

Application insights is a monitoring capability that

- provides visibility into application availability and outage events
- identifies service disruptions and assesses their impact
- enables more effective responses to application-related issues.

How application insights work

Application Insights identifies outages for monitored cloud applications by consuming outage intelligence provided by **ThousandEyes Internet Insights.**

ThousandEyes Internet Insights collects telemetry from globally distributed vantage points that continuously measure application and network availability. When an outage affecting a SaaS or cloud service is detected, an outage event is generated. Application Insights uses this intelligence to display outage details such as affected applications, outage duration, impacted regions, and affected domains for the applications you monitor.

For more information about **ThousandEyes Internet Insights**, see Internet Insights.

The application insights monitoring process works as follows:

1. Once **Application Insights** is enabled, AgenticOps periodically evaluates Cloud-Delivered Firewall Management Center policies to determine which applications are eligible for monitoring.
2. The Cloud-Delivered Firewall Management Center policy is scanned every 24 hours. Applications that are enabled in the policy are automatically monitored, and any detected outages are reported on the **Application Insights** page using outage intelligence from **ThousandEyes Internet Insights**.
3. On the **Settings** page, applications that are allowed in the Cloud-Delivered Firewall Management Center policy are preselected by default. You can optionally select additional applications from the list to include them in outage monitoring.

Need a visual guide? Explore the Application Insights feature walkthough to see it in action.

Detect application outages

This task enables you to monitor and investigate application outages for applications you are tracking.

Application Insights provides a comprehensive view of application outage events, allowing you to track both active and resolved outages across your monitored applications.

Before you begin

Ensure that the **Application outage insights** toggle is enabled under **Insights & Reports** > **Settings** > **Application Insights**.

Procedure

Step 1 In the left pane, click **Insights & Reports > Application Insights**.

The Application Insights page displays a summary of detected outages, including the total number of outages, active outages, resolved outages, and the number of applications being monitored for the selected time range.

Step 2 Review the list of affected applications. For each application outage, the following information is displayed:

- Application name
- Affected domains
- Outage duration
- Start and end timestamps

- Affected regions

Step 3 Click an application to view detailed outage information in the right pane.

You can now monitor application outages and access detailed information about affected services for both active and resolved outage events.

Compliance insights

Compliance insights are automated evaluation features that

- evaluate firewall configurations against supported compliance requirements and identify areas that may require attention
- highlight compliance gaps and potential risks, and
- provide actionable guidance to help maintain a compliant and secure deployment.

Compliance evaluation details

Organizations spend significant time and effort validating firewall configurations against industry security standards. This process is often manual, inconsistent, and dependent on specialized expertise. As compliance requirements evolve, teams must repeatedly revisit configurations, which slows down deployments and increases operational overhead.

Even small misconfigurations such as, overly permissive access rules or missing segmentation controls, can lead to compliance violations that are difficult to detect through manual review.

Compliance Posture in AgenticOps evaluates firewall configurations against industry-standard requirements. It translates compliance guidelines into programmatic checks that can be applied consistently across environments. The current implementation evaluates firewall configurations against the **Payment Card Industry Data Security Standard (PCI DSS) v4.0.1 framework**. Currently, **Compliance Posture** is available only for deployments in the US, EU, and AUS regions.

Disclaimer: The report is provided for informational purposes only and is created using AI. It does not constitute legal or professional compliance advice and is not a substitute for a formal audit or assessment performed by a qualified security assessor. You are responsible for independently verifying the contents of the report for accuracy and completeness. Cisco disclaims all liability related to the report.

Benefits of compliance insights:

- **Automate compliance validation** by evaluating firewall policies against predefined rules, eliminating manual review and reducing the risk of human error.
- **Generate compliance reports** that provide detailed findings and recommendations to help you assess and improve your security posture.
- **Review actionable recommendations** that guide remediation, such as restricting overly broad access, validating business intent, or removing redundant rules.
- **Review security zone mappings** to evaluate segmentation controls based on relationships between network zones.

Environment preparation requirements for compliance evaluation:

- Cloud-Delivered Firewall Management Center is provisioned in your organization.
- AgenticOps is activated in your organization.
- Firewall Threat Defense devices are onboarded and managed through Security Cloud Control Firewall Management.
- The device that you want to evaluate is online and reachable.

Generate compliance reports

Generate compliance reports to evaluate your firewall configuration against PCI DSS 4.0.1 compliance standards, review findings to identify security gaps, and export reports to support remediation efforts and compliance reviews.

Compliance reports help organizations assess their network security posture against industry standards. The PCI DSS 4.0.1 template evaluates firewall configurations for network security, access control, secure configuration, and logging requirements.

Procedure

Step 1 In the left pane, click **Insights & Reports** > **Compliance Posture**.

The **Compliance Posture** page displays previously generated reports and allows you to create new compliance evaluations.

Step 2 Click **Generate Report** to begin defining the report.

Step 3 Enter a name and choose the device to evaluate.

- Currently, **PCI DSS 4.0.1 Compliance Template** is the only supported template. This template evaluates firewall configurations against requirements for network security, access control, secure configuration, and logging.
- Only devices that are currently online are available for selection.

Step 4 Review the security zones.

PCI DSS requires the Cardholder Data Environment (CDE) to be accurately defined. The CDE includes systems that store, process, or transmit cardholder data or sensitive authentication data, as well as environments with unrestricted connectivity to systems handling such data. An automated assessment identifies security zones that are likely to be part of the CDE based on the existing configuration. Review the selected security zones and update the selections based on your knowledge of the network before generating the report.

Step 5 In the **Security Zones** table, select the checkbox in the **CDE** column for each security zone that is part of the CDE. Clear the checkbox for any zone that is not part of the CDE.



Note Incorrect security zone selections can result in inaccurate compliance findings, particularly for checks related to segmentation and traffic between network zones.

Step 6 Click **Generate Report** to begin the compliance evaluation process.

Note

- Compliance reports are generated manually and are not evaluated automatically.
- The system analyzes firewall policies and validates them against the selected compliance template. Report generation can fail due to device connectivity issues. Verify that the device is online and reachable.
- The page confirms that report generation has started. A comprehensive review and analysis of the policies on the selected device will be performed. This process may take some time.
- Click **Return to compliance reports** to return to the **Compliance Posture** page.

Step 7 Find the generated report.

Use the search field to search reports by name, user, or template. You can also click **Filters** to narrow the results. The **Compliance Status** column shows the number of checks that passed, need review, or failed.

Step 8 Click the report name to view the detailed compliance results.

- The report page displays the report name, evaluated device, last update time, compliance score, and compliance summary.
- The **Compliance Score** shows the number of compliant checks out of the total number of checks.
- The **Compliance Summary** displays total findings, checks that passed, need review, or failed.
- The report displays a list of **Compliance Checks**, each representing a specific requirement being evaluated (for example, restricting inbound traffic to the CDE or validating VPN security). Select a compliance check to view its details, which may include:
  - A description
  - References to relevant compliance standards
  - Identified findings associated with the check
  - Recommendations for remediation

The number next to each compliance check indicates how many findings were identified for that check.

Step 9 Click **Download Report** to export the report in JSON format for audit and offline review.

Step 10 Rerun a report.

After making changes to address compliance findings, rerun the report to evaluate the updated configuration.

You can view compliance findings from the **Summary** page. Navigate to **Insights & Reports > Summary** and click **Operations** to view compliance-related insights for the selected time range.

Insight preferences

Insight preferences are tenant-level configuration settings that

- enable or disable AgenticOps insights for your tenant
- allow configuration of feature-specific insight settings, and
- control insight preferences for multiple AgenticOps features.

Available features

You can enable or disable insight preferences for your tenant for these AgenticOps features:

Enable AgenticOps insights

Enable AgenticOps Insights to unlock AI-driven insights, recommendations, and planning tools for your firewall environment and improve performance, security, and operational efficiency.

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

Procedure

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

Step 2 Select **Confirm AgenticOps activation**, and click **Get Started**.

Step 3 Review the available AgenticOps features for each detected Firewall Management Center. The page displays the supported AgenticOps features, software version, and the number of managed devices for each Firewall Management Center. Click **Setup AgenticOps**.

Step 4 Click **Confirm Onboard**.

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

After onboarding, AgenticOps begins analyzing data and the summary page displays, providing AI-driven insights and recommendations for your firewall environment.

Disable AgenticOps insights

This task disables AgenticOps insights to stop data collection and insight generation. When opting out, you can choose to retain or permanently delete existing AgenticOps data.

You can choose to opt out of AgenticOps if you no longer want to use the capabilities. When you opt out, AgenticOps stops collecting data from your devices and deactivates all data processing and alerts. You must have **Super Admin** or **Admin** user roles to disable AgenticOps insights in your tenant.

Data cleanup options

When opting out, you can decide how existing data is handled:

- **Keep existing data**: Stops the AgenticOps service but retains your historical data. If you choose to opt in again later, this data can be reused for improved insights.

- **Remove all data**: Stops the AgenticOps service and permanently deletes all existing AgenticOps data. Deleted data cannot be recovered.

Procedure

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

Step 2 Click **Miscellaneous**.

Step 3 Under **Opt out of AgenticOps**, choose your preferred data cleanup option.

Step 4 Click **Opt out of AgenticOps**.

AgenticOps insights are disabled for your organization, and data collection stops according to your selected cleanup option.

Manage AgenticOps data sources

Manage data sources to control which Firewall Management Centers provide information to AgenticOps for generating insights and enabling AI-powered capabilities.

You can review newly detected data sources, onboard supported Firewall Management Centers, monitor onboarding status, and remove data sources that you no longer want AgenticOps to use.

Data sources include Cloud-Delivered Firewall Management Center and On-Premises Firewall Management Centers registered with Cisco Security Cloud. You can onboard data sources to enable AgenticOps capabilities or offboard data sources that you no longer want AgenticOps to use.



Note Cloud-Delivered Firewall Management Center is required for AgenticOps and can't be offboarded.

Before you begin

- Ensure that AgenticOps is enabled for your organization.
- If you're using an On-Premises Firewall Management Center, ensure that it is integrated with Cisco Security Cloud.

Procedure

Step 1 Navigate to **Insights & Reports > Settings**.

Step 2 Under **AgenticOps Settings**, click **Data Sources**.

Step 3 Choose one of these options:

- To onboard a data source: When AgenticOps detects a supported data source that isn't onboarded, a banner appears on the **Data Sources** page. Click **Review & Onboard**, review the supported AgenticOps features for the selected data source, then click **Confirm Onboard**.

- To offboard a data source: Locate the onboarded data source and turn off the toggle for the data source.

- When onboarding: The selected data source becomes available for supported AgenticOps features.
- When offboarding: AgenticOps no longer collects data or generates insights from the selected data source.

Capacity and traffic insights

Enable Capacity and Traffic insights to review insights that help identify resource constraints, track growth trends, and support capacity planning.

You can modify the preferences for Capacity and Traffic-related insights. These insights help monitor firewall performance, detect anomalies, and identify potential capacity risks.

Procedure

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

Step 2 Click **Capacity & Traffic Analysis**.

Step 3 Enable the toggle buttons for the insights you want to monitor:

a. Traffic-related insights

- High traffic caused by elephant flow
- RAVPN capacity assessment

b. System health-related insights

- High data plane CPU usage
- High snort CPU usage
- High data plane memory usage
- High snort memory usage

c. Anomaly detection-related insights

- Connections rate (CPS) anomaly
- Network throughput anomaly

Step 4 For each insight, expand the section and configure the available settings. Depending on the insight, you can select severity levels, configure thresholds, or specify forecast parameters.

Step 5 Click **Submit**.

After you enable the feature for the organization, you can view the detected anomalies in the **Summary** page, and the respective widgets are also displayed in the dashboard.

Best practices and recommendations insights

Enable Best Practices and Recommendations insights to evaluate your firewall deployment against Cisco Secure Firewall best practices and optimize firewall operations.

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 **Insights & Reports** > **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 Enable the **Automatic assessment** toggle to activate automated report generation.

Step 5 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.

Policy change impact analyzer insights

Enable Policy Change Impact Analyzer to assess the potential impact of pending access control policy changes before deployment. AgenticOps provides visibility into affected rules, traffic segments, and historical connections to help you make informed deployment decisions.

You can modify the preferences for Policy Change Impact Analyzer-related insights.

Note The **Policy Change Impact Analyzer** toggle is enabled by default.

Procedure

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

Step 2 Click **Policy Change Impact Analyzer**.

Step 3 Enable the **Policy Change Impact Analyzer** toggle.

This feature helps you review the potential impact of pending rule changes in Access Control policies before deployment. It currently supports Cloud-delivered Firewall Management Center-managed Firewall Threat Defense devices.

Step 4 Click **Submit**.

After the feature is enabled, you can access it by clicking **Insights & Reports** > **Policy Change Impact Analyzer**.

Policy change impact analyzer insights

Enable Policy Change Impact Analyzer to assess the potential impact of pending access control policy changes before deployment. AgenticOps provides visibility into affected rules, traffic segments, and historical connections to help you make informed deployment decisions.

You can modify the preferences for Policy Change Impact Analyzer-related insights.

Note The **Policy Change Impact Analyzer** toggle is enabled by default.

Procedure

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

Step 2 Click **Policy Change Impact Analyzer**.

Step 3 Enable the **Policy Change Impact Analyzer** toggle.

This feature helps you review the potential impact of pending rule changes in Access Control policies before deployment. It currently supports Cloud-delivered Firewall Management Center-managed Firewall Threat Defense devices.

Step 4 Click **Submit**.

After the feature is enabled, you can access it by clicking **Insights & Reports** > **Policy Change Impact Analyzer**.

Enable operational insights

Enable Software Upgrade Planner to evaluate the readiness of your Firewall Threat Defense devices for software upgrades. Use upgrade insights and recommendations to identify potential issues and support a smoother upgrade process.

You can modify the preferences for operations-related insights.

Note The setting for **Software Update Planner** is enabled by default.

Procedure

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

Step 2 Click **Operations**.

Step 3 Enable the **Software Update Planner** toggle. You can view the software versions running on your devices and our upgrade recommendations.

Step 4 Click **Submit**.

After you enable this feature for your tenant, detected insights are listed in the **Summary** page.

Software Upgrade Planner is enabled and will begin evaluating device readiness for software upgrades. Insights and recommendations will appear in the Summary page.

Application insights

Enable Application Insights to automatically detect application outages and receive proactive notifications when service disruptions occur across your monitored applications.

You can modify the preferences for application outages-related insights.



Note The setting for **Application Insights** is enabled by default.

Procedure

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

Step 2 Click **Application insights**.

Step 3 Enable the **Application outage insights** toggle button to receive insights and notifications when application outages occur.

Step 4 In the **Selected applications** list, search for an application and check the checkbox to include it for monitoring. Clear the checkbox to remove an application from monitoring.

Step 5 Click **Submit**.

After you enable the feature for your organization, you can view detected application outages on the **Application Insights** page, and corresponding insights are displayed on the **AgenticOps Summary** dashboard under the **Operations** category.

Frequently asked questions about AgenticOps

This section helps you understand how AgenticOps Insights, Best Practices and Recommendations, Feature Adoption, Software Upgrade Planner, Capacity and Trend Analyzer, and other AgenticOps services operate within your environment.

What is AgenticOps?

AgenticOps for firewalls leverages artificial intelligence (AI) and machine learning (ML) to streamline and enhance firewall management. By continuously analyzing the data, AgenticOps provides insights that help you:

- Optimize firewall policies and configurations.
- Detect misconfigurations before they impact performance.
- Improve feature adoption and adherence to best practices.
- Receive upgrade suggestions for Secure Firewall Threat Defense devices, including bugs fixes and security vulnerabilities fixes.

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

AgenticOps supports Firewall Threat Defense devices managed by Cloud-Delivered Firewall Management Center and On-Premises Firewall Management Centers registered with Cisco Security Cloud. Feature availability varies by management type. For details, see AgenticOps Support for On-Premises Firewall Management Centers.

Can onboarding AgenticOps fail?

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

Can AgenticOps Insights be disabled?

Opting out of AgenticOps stops data collection and disables insights. You can choose whether to retain or permanently delete historical data. For more information, see Disable AgenticOps insights, on page 30.

Can I disable specific AgenticOps modules?

Yes. From AgenticOps Settings, you can enable or disable modules such as Feature Adoption, Best Practices & Recommendations, and Operations. Disabled modules stop generating insights but do not affect device functionality.

Can i manually run best practices and recommendations assessments?

Periodic assessments run automatically, but you can also run assessments manually at any time. For large-scale deployments with more than 50 devices, you must run assessments manually due to processing limits.

Does AgenticOps automatically make changes to my firewall configuration?

No. AgenticOps provides recommendations and guidance based on analysis of your environment. Configuration changes are not automatically applied unless you explicitly review and implement them.

Additional resources

This reference provides links to additional resources for AIOps in Security Cloud Control, including blog posts about AI-driven firewall operations and autonomous security management evolution.

- From AIOps to AgenticOps: The Autonomous Evolution of Firewall Operations
- Managing Firewall complexity and Augmenting Effectiveness with AIOps for Cisco Firewall
- Security Cloud Control: Pioneering the Future of Security Management