

Introduction to Agent Workforce

This chapter introduces Agent Workforce, an AI-driven operational framework in Security Cloud Control that helps you troubleshoot network issues, analyze operational behavior, and manage firewall policies using natural language interactions.

Agent Workforce uses specialized agents to assist with operational workflows such as VPN troubleshooting, traffic remediation, and policy analysis. You can interact with agents conversationally to investigate issues, review recommendations, and perform guided operational tasks.

- About Agent Workforce , on page 1
- VPN agent, on page 3
- Elephant flow agent traffic congestion remediation, on page 6
- Firewall insight agent, on page 8

About Agent Workforce

Agent Workforce is an AI-driven operational framework that

- enables you to interact with specialized agents using natural language to troubleshoot issues, analyze network behavior, and manage firewall policies
- allows you to describe operational problems or intended actions conversationally instead of relying solely on manual investigation, command-line analysis, or complex configuration workflows, and
- provides insights, recommendations, diagnostics, or policy actions through agents that are optimized for specific operational areas and perform focused analysis based on their specialization.

How Agent Workforce works

Based on the user query, the appropriate agent analyzes telemetry, configurations, policies, and operational data to provide insights, recommendations, diagnostics, or policy actions. Each agent is optimized for a specific operational area and performs focused analysis based on its specialization.

Available agents in Agent Workforce

Agent Workforce includes specialized agents designed to assist with different operational and security workflows. Each agent focuses on a specific operational domain and uses relevant telemetry, protocol awareness,

policy analysis, and contextual operational data to provide diagnostics, recommendations, and actionable outcomes.

When you enter a query, Agent Workforce interprets the intent and automatically routes the conversation to the most appropriate agent. You can describe operational issues or tasks in natural language without determining which agent should handle the request.



Note Currently, Agent Workforce capabilities are available only for deployments in the US, EU, and AUS regions.

Depending on the workflow, Agent Workforce may also present contextual quick actions to help you initiate common investigative or remediation tasks more efficiently. Currently, Agent Workforce includes these agents:

- **VPN agent** helps troubleshoot site-to-site VPN connectivity, routing, tunnel negotiation, and secure traffic flow issues.
- **Elephant flow agent** helps analyze and remediate high-bandwidth traffic flows that may impact firewall performance and operational stability.
- **Firewall insight agent** helps analyze firewall inventory, configurations, policies, routing, and device status.

Manage Conversations in Agent Workforce

This task enables you to create new conversations, monitor active investigations, and interact with specialized agents for troubleshooting, investigation, and remediation workflows.

Use the **Conversations** page to create new conversations, monitor active investigations, and interact with specialized agents for troubleshooting, investigation, and remediation workflows.

Procedure

Step 1 From the Security Cloud Control Home page, click **Firewall**.

Step 2 Choose **Insights & Reports** > **Agent Workforce** > **Conversations**.

Step 3 Review the list of available conversation threads.

Each conversation displays information such as the thread title, assigned agent, workflow status, creator, and creation date.

Step 4 To locate a specific conversation, use the **Search** field to search by keywords.

Step 5 To narrow the conversation list, click **Filters** and filter conversations using one or more criteria.

Step 6 To create a new conversation, click **New Conversation**.

Step 7 Enter your query in natural language.

Agent Workforce automatically selects the most appropriate agent based on the operational intent of the request.

Step 8 Continue interacting with the assigned agent if additional investigation, troubleshooting, or remediation actions are required.

You have successfully created and managed conversation threads with specialized agents for your troubleshooting, investigation, and remediation needs.

Considerations for agent workforce limitations and deployment

Consider these limitations and requirements when deploying and using Agent Workforce:

- Currently, Agent Workforce capabilities are available only for deployments in the US, EU, and AUS regions.
- AI-generated insights, recommendations, and remediation actions must always be reviewed and validated before deployment.
- The accuracy of generated responses depends on the availability, completeness, and correctness of telemetry, policies, device configurations, logs, objects, and operational context within the environment.
- Missing, incomplete, or unresolved configuration entities may prevent certain workflows, recommendations, remediation actions, or deployment operations from completing successfully.
- Agent responses and operational analysis may vary depending on the enabled platform capabilities, configured integrations, available data sources, and device reachability.
- Some workflows may require manual validation, administrative approval, or additional configuration updates before operational changes can be applied to managed devices or policies.
- AI-generated operational guidance is intended to assist administrators and must not replace standard security review, compliance validation, or change-management procedures.

VPN agent

A VPN agent is an intelligent troubleshooting agent that

- diagnoses and resolves site-to-site VPN connectivity and access issues
- analyzes operational telemetry, VPN configurations, routing behavior, packet flow, and access control policies to identify issues affecting secure connectivity between sites, and
- provides protocol-aware diagnostics across technologies such as BGP, EIGRP, OSPF, IPsec, and IKE to accelerate root-cause analysis and reduce manual troubleshooting effort.

Benefits of using the VPN agent

The VPN agent provides operational and troubleshooting benefits for network analysis and packet-level investigation of VPN communication issues.

- Investigate VPN tunnel failures and connectivity disruptions.
- Analyze traffic flow between remote networks.

- Detect routing inconsistencies affecting VPN communication.
- Identify access control or policy-related packet drops.
- Perform packet-level troubleshooting and operational analysis.

Use the VPN agent to investigate connectivity issues

The VPN agent helps you investigate VPN connectivity issues by analyzing operational data and correlating VPN-related telemetry. The agent evaluates routing behavior, tunnel states, traffic flow activity, and policy enforcement to generate actionable insights for troubleshooting site-to-site VPN configurations.

When a query is submitted, the VPN agent correlates operational data across routing protocols, tunnel negotiation states, traffic flow behavior, and policy enforcement to identify the most likely root cause and provide actionable insights. Depending on the issue being investigated, the VPN agent can:

- Identify affected site-to-site VPN tunnels.
- Analyze IKE Phase 1 and Phase 2 negotiation states.
- Review tunnel establishment and peer connectivity status.
- Investigate routing behavior across the VPN tunnel.
- Evaluate traffic flow behavior between local and remote networks.
- Correlate logs, telemetry, and operational events to identify likely root causes.
- Generate operational findings, root-cause analysis, and remediation recommendations.



Note The VPN agent works only for Firewall Threat Defense site-to-site VPN configurations managed by Cloud-delivered Firewall Management Center or On-Premises Firewall Management Center.

Procedure

Step 1 Choose **Insights & Reports** > **Agent Workforce** > **Conversations**.

Step 2 Click **New Conversation**.

Step 3 Enter a query describing the VPN connectivity issue or traffic-flow problem.

Agent Workforce automatically assigns the request to the VPN agent based on the operational intent.

Step 4 Review the generated diagnostics, tunnel analysis, routing behavior, traffic flow analysis, and remediation recommendations.

Step 5 Continue refining the investigation by providing additional operational details such as affected sites, peer devices, tunnel names, or observed behavior.

Step 6 Review the recommended remediation actions and validate the operational impact before applying configuration changes.

After the analysis is completed, the VPN agent summarizes operational findings, identified root cause, impact assessment, additional observations, recommended remediation steps and next actions.

Best practices for using the VPN agent

To improve troubleshooting accuracy and reduce analysis time:

- Include source and destination networks whenever possible.
- Specify the affected VPN tunnel, site, or peer device if known.
- Clearly describe observed behavior such as packet drops, intermittent connectivity, or failed tunnel establishment.
- Refine prompts with additional operational context if further analysis is needed.
- Validate recommended remediation steps before deployment.

Example prompts and expected outcomes for the VPN agent

This reference provides example prompts and describes the expected operational outcomes generated by the VPN agent. Use these examples to understand supported workflows and improve conversational interactions during investigations.

User intent	Example prompt	Expected outcome
Troubleshoot connectivity between remote sites	Troubleshoot why the connectivity is down between [remote site 1] and [remote site 2].	VPN agent identifies the relevant Site-to-Site VPN tunnel associated with the affected networks and performs guided troubleshooting analysis.
Troubleshoot a VPN tunnel outage	My VPN tunnel is down. Help me troubleshoot the issue.	VPN agent identifies available VPN tunnels, allows tunnel selection if needed, and analyzes tunnel state, negotiation behavior, routing, and connectivity conditions.
Investigate VPN traffic flow issues	Investigate why VPN traffic is not flowing across the [tunnel name].	VPN agent analyzes traffic forwarding behavior, routing conditions, and policy enforcement affecting traffic flow across the VPN tunnel.
Review configured VPN tunnels	How many VPN tunnels are configured and what state are they in?	VPN agent displays configured site-to-site VPN tunnels along with operational state, tunnel health, and connectivity status details.

User intent	Example prompt	Expected outcome
Visualize VPN routing paths	Visualize the routing between various devices connected by my VPN tunnels.	VPN agent analyzes VPN topology, connected networks, and routing relationships, and provides communication paths across VPN tunnels.

Elephant flow agent traffic congestion remediation

The Elephant flow agent is an intelligent remediation agent that

- Helps you remediate high-bandwidth traffic flows that impact network performance and critical applications
- Relies on a valid AgenticOps-generated insight and uses the device and application information provided in the insight to construct a trust rule and guide the remediation workflow
- Provides a guided remediation experience directly within the conversation workflow.

Elephant flow impact and remediation approach

Large traffic flows, commonly referred to as elephant flows, can consume excessive bandwidth, increase firewall processing overhead, and degrade application performance across the network. Unlike traditional troubleshooting workflows that require manual investigation across multiple dashboards and telemetry sources, the Elephant flow agent provides a guided remediation experience directly within the conversation workflow.



Note The Elephant flow agent remediates only high-bandwidth traffic flows identified in a valid AgenticOps-generated insight; it does not detect elephant flows.

Benefits of using the elephant flow agent

The Elephant flow agent helps identify traffic patterns, investigate congestion issues, and recommend remediation actions for affected devices and applications.

- Analyze previously detected elephant flows affecting network performance.
- Investigate abnormal traffic spikes and sustained utilization.
- Identify applications or traffic flows contributing to congestion.
- Recommend remediation actions to reduce processing overhead and congestion.
- Stage policy updates associated with remediation workflows.

Configure elephant flow remediation workflow

This task enables you to configure and execute the Elephant flow remediation workflow to address high traffic issues caused by elephant flows through guided analysis and automated policy recommendations.

The Elephant flow agent provides an automated workflow to analyze traffic insights and recommend remediation actions. This process helps network administrators efficiently manage high-impact traffic flows that can affect network performance.

Before you begin

- Ensure that **Cloud-Delivered Firewall Management Center** is provisioned in your organization.
- Ensure that AgenticOps is onboarded in your organization.
- Ensure that **High traffic caused by elephant flow** is enabled under **Insights & Reports** > **AgenticOps Insights** > **Settings** > **Capacity & Traffic Analysis**. For more information, see Capacity and traffic insights.
- Ensure that valid AgenticOps-generated elephant flow insights exist. Remediation cannot begin without a valid insight.

Follow these steps to configure the Elephant flow remediation workflow:

Procedure

Step 1 Choose **Insights & Reports** > **AgenticOps Insights** > **Summary**.

Step 2 On the AgenticOps **Summary** page, select the **Traffic & Capacity** insights category.

Step 3 In the **High traffic caused by elephant flow** section, select the affected device.

Step 4 Review the detected elephant flow insight details, affected resources, applications, and traffic impact information.

Step 5 Click **Review proposed remediation** to open the remediation workflow in **Insights & Reports** > **Agent Workforce** > **Conversations**.

a. Alternatively, navigate to **Insights & Reports > Agent Workforce > Conversations**.

b. Click **New Conversation** and select **View elephant flow insights** to start the remediation workflow.



Note Manual prompt entry is not required to start the workflow.

Step 6 Review the proposed remediation actions, operational warnings, shared policy impact, and success criteria.

Step 7 Approve or cancel the remediation workflow as required.

Step 8 Deploy the generated policy updates to the affected devices.

Note Elephant flow events displayed in the Unified Event Viewer might not be available to the remediation agent if AgenticOps did not generate a corresponding insight.

The Elephant flow remediation workflow is configured and executed. Policy updates are deployed to the affected devices to address high traffic issues caused by elephant flows.

Best practices for using the elephant flow agent

To improve remediation accuracy and operational visibility:

- Review affected applications before approving remediation actions.
- Verify the operational impact of policy updates before deployment.
- Review shared policy impact warnings before approving remediation actions.
- Monitor application and network behavior after remediation is completed.

Firewall insight agent

A Firewall insight agent is an analysis tool that

- investigates the configuration and operational state of managed firewalls
- provides information about device inventory, interfaces, routing, policies, licensing, compliance, software, and security configuration, and
- identifies conflicts, inconsistencies, and other issues that may require attention.

Benefits of using the firewall insight agent

The Firewall insight agent provides comprehensive operational and troubleshooting capabilities for firewall management and monitoring.

- View firewall inventory by device type, connectivity state, licensing status, compliance status, and onboarding state.
- Identify unlicensed or out-of-compliance devices.
- Identify access control or policy-related packet drops.
- Review routing configuration, BGP configurations, and route exchange between devices.
- Review interface status and device connectivity information.
- Review syslog and email alert configuration.
- Ask follow-up questions to investigate findings in greater detail.

How firewall insight agent works

The Firewall insight agent analyzes operational data and correlates firewall-related telemetry to investigate issues. It provides information about device inventory, interfaces, routing, policies, licensing, compliance, software, and security configuration, and identifies conflicts, inconsistencies, and other issues that may require attention.

When you submit a query, Firewall insight agent identifies the relevant devices, configurations, policies, or operational data and returns the associated information. The agent can:

- Identify the devices, policies, routes, interfaces, or configurations related to the query.
- Correlate information across devices, policies, routing, security configuration, and operational state.
- Compare related configurations and identify conflicts, overlaps, redundancies, or inconsistencies.
- Explain when a device or configuration cannot be found and identify the information required to continue the investigation.
- Generate operational findings, root-cause analysis, and recommended next steps.

Procedure

Step 1 Choose **Insights & Reports** > **Agent Workforce** > **Conversations**.

Step 2 Click **New Conversation**.

Step 3 Enter a query about firewall inventory, device state, routing, policies, security configuration, or operational data.

Agent Workforce automatically assigns the request to an agent based on the operational intent.

Step 4 Review the returned firewall information, analysis, and key observations.

The Firewall insight agent analyzes firewall data and reports findings, comparisons, and recommended next steps. It does not modify configurations, create or deploy policies, or approve changes.

Step 5 Continue the investigation by providing additional context, such as device names, policy names, object names, interfaces, or other relevant identifiers.

Step 6 Review the recommended next steps and validate the operational impact before applying configuration changes.

After the analysis is completed, Firewall insight agent summarizes the operational findings, identified root cause, impact, additional observations, and recommended next steps.

Best practices for using the firewall insight agent

To improve troubleshooting accuracy and reduce analysis time:

- Include device names, policy names, object names, or other identifiers when available.
- Clearly describe observed behavior such as packet drops, intermittent connectivity, unexpected policy behavior, or configuration inconsistencies.
- Provide additional operational context if further analysis is needed.

- Review recommended next steps and validate their operational impact before deployment.

Example prompts and expected outcomes for the firewall insight agent

Use these examples to understand supported workflows and improve conversational interactions during investigations.

User intent	Example prompt	Expected outcome
Review firewall inventory	What devices do I have in my firewall inventory?	The agent summarizes devices by type and connectivity state. It can also provide software versions, addresses, manager associations, licensing status, and compliance status.
Review interfaces	List all interfaces and their status for `[device name]`.	The agent lists the device interfaces and their status. If the device cannot be found, it explains the lookup failure.
Review BGP configuration	Show the current BGP configuration on `[device name]`.	The agent returns BGP neighbors, local and remote AS numbers, peering type, tunnel interfaces, redistribution, and related configuration details.
Review licensing and compliance	Which Firewall Threat Defense devices are unlicensed or out of compliance?	The agent lists affected devices and provides their license and compliance status, software version, and other relevant device details.
Review software updates	Which Firewall Threat Defense devices have a recommended software update?	The agent identifies devices with available updates and provides current versions, target versions, fixes, and affected defects or threats.