Cisco Services Q & A for ThreatGRID Customers

Contents

Introduction

This document provides answers to some of the most common questions regarding service offer integration, support and delivery, and service agreement migration for legacy ThreatGRID products.

Service Offer Integration and Orderability

Q. What is Orderability?

A. Orderability enables customers to quote and order using Cisco® processes and tools. In addition, orderability allows partners and their customers to utilize Cisco service and support tools and processes for products, RMAs and licensing. Orderability begins on January 7, 2015.

Q. How will the legacy ThreatGRID product and service offerings be integrated into the Cisco Security portfolio?

A. Tables 1 and 2 show how the ThreatGRID products, services, and trainings are being mapped to Cisco products, services, and trainings.

Table 1. Mapping of ThreatGRID products to Cisco Products

ThreatGRID Product Names	New Cisco Names
ThreatGRID	Cisco AMP Threat Grid

Table 2. Mapping of ThreatGRID services to Cisco Services

ThreatGRID Service Offer	Cisco Services
1 orderable, bundled solution consists of: • Hardware Appliance, Platform Software, Cloud Subscription and Hardware + Software Support **- or -** • Cloud Service Subscription	Hardware solution consists of 3 orderable components: • Hardware Appliance + Operating Software • Hardware Appliance Service (SMARTnet Service) • Software Subscription + Software Support **- or -** Cloud-based solution consists of 1 orderable component: • Software Subscription + Software Support
Architecture Review	Cisco Security Design Assessment Service
• Configuration Review • Policy Review	Cisco Network Device Security Assessment Service

Cisco Technical Services

Cisco SMARTnet Service

Q. What is Cisco SMARTnet service?

A. As part of the Cisco Technical Support Services portfolio, the Cisco SMARTnet® program provides your staff direct, anytime access to Cisco Technical Assistance Center (TAC), and an extensive range of online resources. You receive fast, expert technical support, flexible hardware coverage, and smart, personalized capabilities to help you resolve critical network issues.

Q. What is included with Cisco SMARTnet service?

A. SMARTnet includes:

- Global 24 hour access to Cisco Technical Assistance Center (TAC)
- Access to online knowledge base, communities and tools
- Current hardware replacement option: next business day delivery, where available, for Security products
- Operating system software updates
- Smart, proactive diagnostics and real-time alerts on devices enabled with Smart Call Home

Q. Why should a customer buy Cisco SMARTnet support services?

A. By covering Cisco products with a Cisco SMARTnet contract, a customer can:

- Maximize product and network availability, reliability, stability and security
- Reduce the cost of network ownership by using Cisco expertise, knowledge, and availability
- Increase return on investment (ROI) by having access to Cisco operating system software enhancements
- Better manage scarce internal expert resources at all locations
- Improve productivity and revenue per employee with access to tools and technical support documentation that can increase self-sufficiency and technical knowledge
- Opportunity to obtain global TAC support across all Cisco network devices

Q. Are Cisco AMP Threat Grid Appliance operating system software updates included with the Cisco SMARTnet contract?

A. Yes. For security hardware appliances, all platform software updates will be included as part of the SMARTnet contract to ensure operating system support for the hardware deployment.

Q. Are security software feature updates included with the Cisco SMARTnet contract?

A. No. These are included in the software subscription support that is included with the purchase of your software subscriptions. Although this coverage is not included directly in your SMARTnet coverage, the SMARTnet and software subscription support are linked so that your support experience is seamless.

Q. Why does the appliance purchase come with a recommended attach of Cisco SMARTnet Service?

A. Technical service is required to attach at the point of the ThreatGRID product sale so that customers get the necessary support and entitlement and the best possible return on investment.

Q. How can you purchase SMARTnet services?

A. You may purchase SMARTnet services directly from Cisco through your Cisco account manager, or through our global network of highly qualified Cisco partners. You may find a partner near you through the Cisco Partner Locator tool.

Software Subscription Support

Q. What is the software subscription support that is included with the Cisco AMP Threat Grid subscription software licenses?

A. The software subscription support includes:

- Access to the Cisco TAC 24 hours a day, 7 days a week
- Online repository of application tools and technical documents
- Collaborative learning through several online activities and environments

- Registered access to Cisco.com, for easy access to online technical information and service request management

Q. How do customers check their entitlement for their software subscription support?

A. The software subscription support is embedded with every purchased subscription of Cisco AMP Threat Grid.

Cisco Advanced Services

Cisco Security Design Assessment Service

Q. What is the Cisco Security Design Assessment Service?

A. The Cisco Security Design Assessment Service helps customers understand and strengthen their organization's security infrastructure. By undertaking a Cisco Security Design Assessment, an organization will:

- Create a robust and scalable security architecture using a business-focused, risk-avoidance approach
- More effectively protect the infrastructure by identifying architectural network-device vulnerabilities and deviations from security best practices
- Safeguard employee productivity, primary intellectual property, and sensitive customer data by mitigating security risks

Q. What is included with the Cisco Security Design Assessment Service?

A. In conducting the assessment, Cisco security experts will:

- Review the organization's business goals, objectives, and requirements
- Review the existing network and security architecture and design documentation, including physical and logical designs, network topology diagrams, device configurations, and blueprints as needed
- Evaluate whether each of the recommended controls in the Cisco Security Control Framework is present in the security infrastructure
- Evaluate the security architecture for scalability, performance, and manageability
- Identify vulnerabilities in the security infrastructure
- Provide a prioritized and actionable report that highlights the critical assets and risks and identifies security gaps
- Provide an executive presentation of findings and prioritized recommendations

The Cisco Security Design Assessment includes one business-critical asset and a sampling of one device from each of the following network areas: data center, internal network, perimeter network.

For more details download the Cisco Security Design Assessment Service Description.

Q. How are the services delivered?

A. The U.S.-based Advanced Services practice will manage and deliver service remotely, and/or the local theater practice will deliver onsite services.

Q. How can you purchase the Cisco Security Design Assessment Service?

A. Services are available and orderable through the Advanced Services Transaction (AS-T) service type using a Statement of Work (SOW). Partners and customers will need to work with their Cisco Services Account Manager to order these services.

Cisco Network Device Security Assessment Service

Q. What is the Cisco Network Device Assessment Service?

A. The Cisco Network Device Security Assessment Service helps protect customer's network against old and new threats by working together to identify gaps in the safeguards around their Cisco network infrastructure. The assessments are performed by consultants who have extensive security experience in a variety of vertical industries and government agencies.

Q. What is included with the Cisco Network Device Assessment Service?

A. Cisco Network Device Assessment Service includes a detailed review of your Cisco wired and wireless network and firewall devices. The assessment includes device configurations and access policies. After identifying gaps in device configurations and policies, our experts recommend prioritized mitigations that you can act on. The service covers a broad variety of Cisco platforms, including routers and switches, firewall and VPN devices, intrusion detection devices, and others.

For more details, download the Cisco Network Device Assessment Service At-t-Glance.

Q. How are the services delivered?

A. The U.S.-based Advanced Services practice will manage and deliver service remotely, and / or the local theater practice will deliver onsite services.

Q. How can you purchase the Cisco Network Device Assessment Service?

A. Services are available and orderable through the Advanced Services Transaction (AS-T) service type using a Statement of Work (SOW). Partners and customers will need to work with their Cisco Services Account Manager to order these services.

Cisco Technical Assistance Center

Q. What is the Cisco Technical Assistance Center?

A. The Cisco Technical Assistance Center (TAC) provides technical support for all Cisco products, including Cisco security products.

Q. What service does the Cisco TAC offer?

A. The Cisco TAC provides service contract holders with:

- **Expert assistance:** The Cisco TAC employs a highly skilled staff who offer you years of security and networking experience, as well as research and development engineers.
- **Fast problem resolution:** The Cisco TAC provides a constant measurement of customer satisfaction and time-to-resolution tracking.
- **High level of knowledge:** The Cisco TAC offers depth and breadth of expertise with Cisco devices and operating system software.
- **Support 24 hours a day, 365 days a year in multiple languages:** By email or telephone, the Cisco TAC is there when you need it.

Q. How does a customer open a case with Cisco TAC?

A. Customers and partners with an active service contract can open a case through Cisco.com. Customers or partners must have their Cisco service contract number, a Cisco.com user ID, and software product family when opening a case using the web.

Customers with severity (priority) 1 or 2 cases must call the TAC at 800 553-2447 or 408 526-7209 in the United States. For more information on opening a technical support case, and for regional TAC telephone numbers, refer to Cisco Worldwide Contacts.

Customers can also open technical support cases by sending an email to tac@cisco.com.

Q. What do customers and partners need to open a TAC request?

A. To open a TAC request, you must do the following:

- Register for a Cisco.com user ID.
- Associate your contract number to your Cisco.com user ID

Q. How do I get a Cisco.com user ID?

A. Register for a Cisco.com user ID and create a Cisco.com profile. Your Cisco user ID will give you access to the tools that will help you view, renew, and manage contracts, and open a support case.

Q. How do I associate my new Cisco Service Agreement Contract Number to my Cisco.com user ID?

A. ThreatGRID customers will need to add their Cisco Service Agreement Contract Number to their user ID in the Cisco Account Profile. From there, select the "Access" tab and click the "Add Access" button, then select the "Full Support" radio button on the pop-up screen, and then click "Go" to enter your Service contract number(s). If you have multiple service contract numbers, please separate them by commas.

Q. How does the Cisco TAC prioritize support service requests?

A. Cisco processes allow for customers to designate the severity of every service request reported. Priorities are based on the assigned severity levels.

Q. What support is provided through Cisco.com?

A. Cisco.com includes interactive consulting tools, a database, and knowledge transfer resources. It also includes product documentation.

Online troubleshooting tools and support resources include:

- TAC Case Collection: Identifies and troubleshoots common problems
- My Tech Support: Offers a personalized web page with customized links
- Peer-to-peer online forums: Enable sharing with others in your industry
- Technical Support Newsletter: Keeps you up to date and informed

These and other help tools and resources are available on the Technical Support and Document website at www.cisco.com/techsupport.

Q. What are the problem severity levels and associated responses?

A. To help ensure that all service requests are reported in a standard format, Cisco has established the service request severity definitions indicated below. These severity levels might not be applicable across all market segments and technologies. Severity levels and escalation guidelines might also vary based on the existing applicable agreement.

- **Severity 1 (S1):** Network is "down," or there is a critical impact to business operations. Customer and Cisco will commit all necessary resources around the clock to resolve the situation.
- **Severity 2 (S2):** Operation of an existing network is severely degraded, or significant aspects of business operation are negatively affected by inadequate performance of Cisco products. Customer and Cisco will commit full-time resources during normal business hours to resolve the situation.

- **Severity 3 (S3):** Operational performance of the network is impaired, although most business operations remain functional. Customer and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- **Severity 4 (S4):** Customer requires information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on business operations.
- **For S1 or S2 service requests:** If the customer's production network is down or severely degraded, the customer must contact the Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep the customer's business operations running smoothly.

Q. What is the escalation process?

A. If a customer does not feel that there is adequate forward progress or feels that the quality of Cisco service is not satisfactory, Cisco encourages the customer to escalate the problem ownership to the appropriate level of Cisco management by asking for the TAC duty manager.

Note: Severity 1 and 2 escalation times are measured in calendar hours, 24 hours per day, 7 days per week. Severity 3 and 4 escalation times correspond with standard business hours.

For more information, download the Severity and Escalation Guide.

Return Materials Authorization (RMA)

Q. How will customers get a return materials authorization (RMA) for defective products after Cisco orderability?

A. After a customer or partner has a service request open with TAC, an RMA will be initiated according to the case resolution procedures.

Q. When will Cisco start providing support for RMA?

A. Support for RMA for products covered by an active service agreement sold by ThreatGRID or Cisco starts on January 7, 2015, after the active service agreements have been migrated into the Cisco installed base. ThreatGRID customers should continue to use their existing RMA process for installed ThreatGrid products until their legacy appliances have been migrated.

Q. Who is responsible for updating the site addresses?

A. Partners and customers have the responsibility of updating the site addresses.

Q. What happens if the site addresses are incorrect?

A. If the site addresses are incorrect, the Service Supply Chain depot might not have the replacement units, and thus there will be a delay in delivery.

Q. Does Cisco provide a prepaid airway bill for RMA returns?

A. The RMA status page will include a link to the Product Online Web Return (POWR) tool. For further instructions and to see if the RMA type qualifies for free pickup, go to the POWR tool webpage.

Q. How many days does a partner or customer have to return defective products to Cisco?

A. A partner or customer under an advanced replacement service contract is responsible for returning defective products back to Cisco within ten (10) days.
For non-returned defective products that are open for more than thirty (30) days, Cisco reserves the right to charge partners or customers at current list prices.

Q. I received a replacement unit from Cisco Service Supply Chain for an RMA. However, the unit is dead on arrival (DoA). How do I get another replacement unit?

A. Contact TAC using your previous case number and RMA number to report that the unit is DoA. After the TAC has determined the product to be DoA and eligible for replacement, a request for a replacement and new RMA will be submitted.

Q. I opened a support case, and an RMA was created before the contract migration date. How is this RMA handled?

A. RMAs for legacy ThreatGRID contracts opened through the ThreatGRID process prior to January 7, 21015 will be handled by the ThreatGRID process, and the defective units should be returned to ThreatGRID using the instructions provided.

Licensing

Q. Will newly purchased Cisco AMP Threat Grid appliance products continue to ship with preinstalled software?

A. Yes; newly purchased security products will continue to ship with preinstalled software.

Q. How will I get assistance with software licensing issues for installed ThreatGRID products?

A. The Global Licensing Operations (GLO) team provides support for ThreatGRID software licensing issues. Service requests can be opened online.

Warranty

Q. What is the Cisco warranty?

A. Warranties are short-term commitments for Cisco to replace defects in Cisco products. They are limited in duration and the support they offer. Also, warranties do not include Cisco TAC support, software updates, or any of the additional benefits obtained under a support service contract. It is the responsibility of Cisco to replace the Cisco product during the warranty duration.

Elements covered under a Cisco warranty are:

- **Hardware:** This guarantees that the piece of hardware will be free of defects in material and workmanship under normal use, or it will be replaced by Cisco.
- **Software:** This guarantees that the physical media are free from defects, or they will be replaced by Cisco. Also, the warranty guarantees that the software generally conforms to the published specifications for the product. The warranty is explicitly “as is,” and no new releases are included.

To find the warranty information that applies to a specific product or product family, visit the Cisco Warranty Finder.

Q. What are the warranty terms for Cisco Security products?

A. ThreatGRID products assumed the Cisco Security 90-day limited hardware and software warranty. Effective January 7, 2015, the ThreatGRID 90-day warranty will be replaced with the standard Cisco 90-day warranty (with an additional 90-day grace period).This change brings the ThreatGRID warranty in line with Cisco‘s standard warranty offering.

For details on Cisco’s warranty, visit www.cisco.com/en/US/products/prod_warranties_listing.html.

Q. How will warranty end dates be calculated for migrated records?

A. Original ThreatGRID warranty end dates will be migrated from ThreatGRID and will be honored at Cisco.

New Product Dead on Arrival (DOA)

Q. I purchased a product from Cisco (not ThreatGRID) with Cisco product IDs that was delivered recently. This newly shipped product was dead on arrival (DOA). What process should I follow for a replacement?

A. The DOA criteria are as follows:

- DOA is defined as a new product that fails at initial power-up.
- The DOA process is separate from any warranty programs.
- DOAs must be claimed within three months of the ship date to the partner.
- Products must have been purchased directly from Cisco. Purchases from a distributor (i.e. not directly from Cisco) must be returned to entity where it was purchased.
- The customer must provide the serial number and purchase order/sales order for the purchase.

The DOA request process:

- Contact the Cisco Technical Assistance Center (TAC) to report the defective product.
- Once the TAC has determined the product to be DOA and eligible for new product, a request for a replacement will be submitted. The replacement will be invoiced against your original purchase order.
- Standard lead-time to ship a replacement product is two to five business days, as new products are made to order and are not “in-stock” items.
- The replacement product can take 2 to 10 days to arrive after shipment as transit time varies by location.
- Credit will be issued after the product is physically returned to Cisco's designated location.

For more details on DOA, review www.cisco.com/web/ordering/cs_info/or3/o32/Return_a_Product/WWRL_HOME.html#2

Q. I purchased a product using the legacy ThreatGRID (not Cisco) process with ThreatGRID product IDs that was delivered recently. This newly shipped product was dead on arrival (DOA). What process should I follow for a replacement?

A. For this DOA product, work through the legacy ThreatGRID process and contact the Cisco TAC and they will create a ticket which will be addressed by the correct support team.

End of Life

Q. How is product “end of life” handled?

A. As a general rule, Cisco will provide six months’ notice of the affected product’s end-of-sale date and/or the last day on which the affected product can be ordered. This notice will appear on the Cisco.com site (www.cisco.com/en/US/products/prod_end_of_life.html). Customers are encouraged to visit this site regularly because it contains useful information regarding Cisco’s end-of-life program. Sign up to receive notifications here: www.cisco.com/cgibin/Support/FieldNoticeTool/field-notice.

For an end of product life cycle overview and policy on product discontinuance, refer to www.cisco.com/en/US/products/products_end-of-life_policy.html.

Service Agreement Migration

Q. When will ThreatGRID service agreements be migrated to Cisco tools?

A. Cisco plans to migrate ThreatGRID active service agreements to Cisco tools by January 7, 2015.

Q. What service agreements will be migrated?

A. All active and overdue service agreements for both software and hardware products will be migrated.

Q. What will not be migrated?

A. End of Life equipment that is no longer eligible for support coverage will not be migrated.

Q. Is end customer information required for service orders and renewals?

A. Yes. End customer address information will be required for service orders and renewals. To make sure of timely service delivery to end customers, accurate installed-at information is required.

Q. How will warranty end dates be calculated?

A. Original ThreatGRID warranty end dates will be migrated from ThreatGRID and will be honored at Cisco. New purchases will have warranty end dates calculated based on the Cisco Warranty period of 90 days.

Q. What happens to multiyear agreements?

A. Multiyear agreements and their respective end dates will be included in the migration.

Service Agreement Content

Q. What is the key difference between my Cisco service agreements and my ThreatGRID service agreements?

A. Instead of one service agreement for each software subscription, there will be one service agreement contract number for all software subscriptions. Hardware technical support services (i.e. SMARTnet) will be on a different service contract than the software subscription contract.

Q. Are my serial numbers going to be the same?

A. Yes; migrated service agreements will include the same serial numbers, so you can search your contracts by serial number if you desire.

Q. Are my service agreement contract numbers going to be the same?

A. No. You will be assigned new contract numbers for hardware and software subscription support.

Service Contract Migration Mapping

Q. How will legacy ThreatGRID service contracts map to Cisco service contracts?

A. All ThreatGRID hardware contracts will be migrated to a SMARTnet Cisco service contract. All ThreatGRID Term Licenses Software will be migrated to a Cisco-ThreatGRID software subscription contract.

Additional Information

Q. Describe the available user manuals and product documentation.

A. User manuals and other product documentation are available on Cisco.com at www.cisco.com/public/support/tac/documentation.html.

Q. Where can I go for more information?

A. For more information visit the following webpages:

Service and Support for ThreatGRID Acquisition website: www.cisco.com/web/services/acquisitions/threatgrid.html

Cisco Security Services: www.cisco.com/go/services/security

Support Case Manager Tool: tools.cisco.com/ServiceRequestTool/scm/mgmt/case

Licensing requests: www.cisco.com/go/license

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA 1/15