Intel Security Business Support User Guide

Information about Your Support Entitlement

2015 Q3 Edition

Table of Contents

1 Quick Reference Guide

Intel Security Technical Support has multiple global and regional support centers. It is your 24x7x365 source for post-sales account customer service and technical security support on McAfee products.

1.1 Online Self-Help Resources (Section 3)

ServicePortal (https://support.mcafee.com)

- KnowledgeBase — thousands of articles, release notes, product guides, troubleshooting documents
- Support Tools — repair, diagnostic, anti-malware, and other tools and utilities
- Patches and Downloads — search for patches and downloads by logging in to the ServicePortal
- Malware Submission — safely send malware samples to McAfee Labs for review
- Service Request Management — create, track, and manage Service Requests (SRs)

Intel Security Community (https://community.mcafee.com) — join our Community of security users.

1.2 Customer Service Account Questions (Section 2)

For assistance with **non-technical questions**, including product activations, licensing questions, grant numbers, entitlements, SaaS login/password set up, and ServicePortal passwords, contact Customer Service online at https://secure.mcafee.com/apps/support/customer-service/request-form.aspx, or in the U.S., call 1 888 847 8766. Additional Customer Service phone numbers by country can be found on the McAfee website *Contact Us* page at: http://www.mcafee.com/us/about/contact-us.aspx#ht=tab-techsupport.

1.3 Opening a Technical Service Request (Section 4)

Non-Urgent — ServicePortal Options

- Chat Support with Remote Assistance — rapid access to an expert with remote device access
- Post an Online Service Request (SR) — create, track, and manage SRs and malware submissions

Urgent — Technical Phone Support

Support phone numbers for all regions can be found on the Contact Us page at: http://www.mcafee.com/us/about/contact-us.aspx#ht=tab-techsupport.

2 Setting Up Your Online Support Account

2.1 Your Grant Number

Your grant number allows you to access the ServicePortal, get product downloads, and call Support. You will receive it by email after product purchase. If you lose your grant number, contact Customer Service.

2.2 Your ServicePortal Account

Your ServicePortal account enables you to create and update support cases, submit malware samples, access tools, and chat with a technician online in English. To set up your account, go to https://support.mcafee.com and click "Register" in the Customer Login section. Input all information and create a valid password.

Your email domain must match that of other users registered to that grant number. If you need to register under another domain, contact Customer Service at: http://www.mcafee.com/us/about/contact-us.aspx.

2.3 Checking Your Entitlements

Once you have logged into the McAfee ServicePortal, you can check your support entitlements by selecting the My Account tab. If you have multiple grant numbers, each one must be registered to your account to enable visibility to those entitled products. If you do not see all of your entitlements, contact Customer Service.

2.4 Getting Product Notices and Alerts

The Support Notification Service (SNS) is the official product communications vehicle for Intel Security. SNS provides email notifications of all changes and critical incidents regarding your products. You must subscribe to SNS via the SNS Subscription Center at https://sns.snssecure.mcafee.com/content/signup_login. Go to Section 7 to see the **Product Information Communications Policy**.

2.5 Contacting Customer Service

Intel Security Customer Service is available around the clock for assistance with non-technical questions, including product activations, licensing questions, grant numbers, entitlements, SaaS and ServicePortal login/passwords. See the most common customer issues at http://www.mcafee.com/us/support/customer-service-faq.aspx. Former Secure Computing customers can view FAQs at http://www.mcafee.com/us/support/secure-computing-customer-service-faq.aspx.

Contact Customer Service via the online form at https://secure.mcafee.com/apps/support/customer-service/request-form.aspx. Customer Service phone numbers by country can be found on the *Contact Us* page under the "Support" tab at http://www.mcafee.com/us/about/contact-us.aspx#ht=tab-techsupport.

3 Online Self-Help Technical Tools and Resources

Intel Security has designed a sophisticated yet easy-to-use ServicePortal at https://support.mcafee.com with access to the following tools and resources:

Knowledge Center

- Product Documentation and Walk-through Guides
- Troubleshooting and How-To Articles: Articles and step-by-step instructions to resolve issues
- Release Notes: Technical documentation of new product version features
- Security Bulletins: confirmation of resolved issues with McAfee products
- Threat Advisories: Critical global malware threat news issued by McAfee Labs

Intel Security Community

(https://community.mcafee.com) — Join our Community of security users to connect with other customers and share solutions about McAfee products, post discussions, and more.

Intel Security Download Portal

(http://www.mcafee.com/us/downloads/downloads.aspx) — Authenticate with your grant number to display all products available for download under your support entitlement.

MVT Diagnosis and Remediation Tool

McAfee Virtual Technician (MVT) can find and resolve most common product issues. After scanning the device, MVT will ask for permission to resolve any detected issue. The scan results will be passed to Support should a Service Request be opened.

- MVT Walk-through Guide https://mvt.mcafee.com/mvt/Documents/WalkThruGuide/en-us/MVTWalkThroughGuide.pdf
- Run MVT at http://support.mcafee.com/mvt or when creating a Service Request
- Run MVT remotely on a client device using ePolicy Orchestrator (ePO-MVT) https://kc.mcafee.com/corporate/index?page=content&id=PD22556
- Download the MVT-ePO package at http://mer.mcafee.com/enduser/downloadepomvt.aspx

Intel Security Free Tools

(http://www.mcafee.com/us/downloads/free-tools/index.aspx) — A repository of assessment utilities and anti-malware, forensic, Foundstone SASS, intrusion detection, scanning, stress testing and other useful tools.

Endpoint Encryption Code of the Day

Accessing certain functions within the device encryption disaster recovery toolkit (SafeTech/WinTech toolkit) requires a unique code that changes on a daily basis. Click on ServicePortal “Tools” tab and select “Endpoint Encryption Code of the Day.”

Threat Center

(http://www.mcafee.com/us/threat-center.aspx) — Access the Threat Library, trend reports, malware tools, DAT release notes, McAfee Labs blogs, and other information.

4 Reporting and Resolving Product Problems

4.1 Issue Severity and Response Charter

If you have a product question or issue that you cannot resolve yourself, the first step is to identify the severity of the issue. Intel Security defines the severity of an issue based on how it impacts your ability to conduct business. A severity code is associated with all service requests, failures, and enhancement requests to indicate the impact and the urgency of the request.

Severity Definitions

Severity 1—Business has stopped

- Your organization cannot conduct business based on failure of a Intel Security product.
- There is loss of protection to most of your infrastructure.
- All Internet connectivity or email flow has stopped.
- There is no viable workaround for this issue.

Intel Security's Client Engagement Requirements: Customer to participate on a technical fault isolation call (24x7) until a solution and or work around is found.

Severity 2—Business is severely impeded

- Your organization's business is severely impeded but can continue to operate.
- There are widespread symptoms across your organization's infrastructure.
- Failure of a major product deployment resulting in a significant loss of protection
- Loss of management to a significant portion of your infrastructure

Intel Security's Client Engagement Requirements: Customer to be available (24x7) to provide access/data to assist with fault isolation until a solution and or work around is found.

Severity 3—Business is impacted, but your organization can function normally

- Your organization's ability to conduct business is not affected.
- Symptoms affect isolated parts of your environment.
- Specific functionality is not working.

Severity 4—Business is not affected, but there are noticeable problems

- Your organization's ability to conduct business is not affected.
- Symptoms affect only a few systems.
- Functionality loss has an easy workaround.

Severity 5—Requests for information or feature modifications

- You request product documentation or other information that does not require troubleshooting and issue resolution.
- You request modifications to the functionality or design of Intel Security products.

NOTE: If a customer cannot commit to the 'Intel Security Client Engagement Requirement' as detailed below the Severity 1 and Severity 2 definitions, we reserve the right to lower the severity of the issue reported to support until such time as this can be met.

Response Charter

Each Intel Security Enterprise Technical Support interaction begins with your Support Engineer and the creation of a unique Service Request (SR) number to track resolution of the issue. We attempt to resolve every issue on the first call. Unresolved customer issues are evaluated based on severity and priority of resolution. Based on this evaluation, they are assigned a numerical impact level value.

If the Support Engineer is unable to resolve the issue or it is assigned a high-impact level, it is escalated to successive tiers as needed for resolution. Each tier in the Intel Security support organization will use all available resources to resolve the issue. These processes apply to all Service Requests that are escalated within the Intel Security Technical Support organization.

	Severity 1	Severity 2	Severity 3	Severity 4	Severity 5
Response Time	Telephone < 5 Minutes Chat <15 minutes				
			ServicePortal < 24 hours		
Escalation to Tier 2	30 Mins	1 hour	3 Days	7 Days	14 Days
Escalation to SEO (Tier 3)	1 hour	4 hours	5 days	14 days	14 days
Escalation to Engineering	4 hours	6 hours	7 days	14 days	14 days

NOTE: Response Charter times reflect Calendar hours and days.

For complete escalation and response definitions, see https://support.mcafee.com/SPR/WebContent/ProgramsAndPolicies/faq-corporate-technical-support.pdf.

4.2 Information Required for Assisted Support

For the fastest resolution, ensure you have the following information available:

- Support Grant Number
- Previously assigned Service Request (SR) case number (if applicable)
- Geographic location of the software installation
- Detailed description of the problems or errors
- Description of the hardware on which the software is installed, including serial number or service tag where applicable (hardware must meet published specifications)
- Names/versions of OS, network, and software running with McAfee software, including patches and fixes
- Minimum Escalation Requirements (MER) tool output

WebMER (Minimum Escalation Requirements) Tool

WebMER is a utility to collect product and system information to assist Support in diagnosing issues. Information gathered includes an MSD report (or other OS equivalent), event logs, product registry keys, log files, and current product .EXE files, which are automatically compressed in a .TGZ file for sending to Support.

NOTE: This is frequently the required first step in getting assisted Technical Support. To access WebMER, go to http://support.mcafee.com/webmer.

4.3 Chat Support with Remote Assistance

For non-urgent issues

Use Chat Support to check the status of existing cases or get live, interactive problem solving.

To start chat session, log in to the ServicePortal, click the "Service Request" tab, then the "Create a Service Request" tab. After selecting the severity, product and version, and entering a brief description, the option to select chat will appear (if available for that product) in the "How would you like to contact us?" dropdown. After completing Step 3, a chat window will open and give a status on where you are in the queue. The chat window allows you to discuss your issue with a Support technician and send files.

With your permission, the Support technician can open a remote control/share connection to view your desktop and work directly with you to diagnose and resolve issues.

4.4 Posting a Service Request Online

For non-urgent issues

To create an Online Service Request for a severity 3, 4, or 5 issue, log in to the ServicePortal, click the "Service Request" tab, then the "Create a Service Request" tab. After selecting the severity, product and version, and entering a brief description, select "Post Service Request Online" in the "How would you like to contact us?" dropdown.

Step 2 will provide diagnostic recommendation and Knowledge Center resource list as an SR alternative. To move forward, scroll to the bottom of the page and click "Continue to Step 3." Complete all required fields, and attach any additional log files or information that could assist your Support technician. An expert should respond within 24 hours. Depending on the complexity of the issue, the technician may contact you by phone.

Support will make several attempts to contact you. If we receive an out-of-office notification, we will postpone follow up attempts for that period. After several unsuccessful attempts, we will assume that your issue is resolved and send a notification that the request has been closed. You can call Support at any time within the next 30 days to reopen the request.

4.5 Calling Support

For any urgency level

Technical Support provides telephone access to our technical support technicians 24/7/365. Commercially reasonable effort is made to provide local language support for your product in most countries during business hours and in English at all other times. Because Intel Security strives to provide the best possible support, all customer calls are recorded for quality purposes.

Support phone numbers for all regions can be found on the *Contact Us* page under the "Support" tab at: http://www.mcafee.com/us/about/contact-us.aspx#ht=tab-techsupport. Click your language/location of choice in the upper right corner of the web page.

4.6 Submitting Malware Samples

You can now submit potentially infected samples via the ServicePortal as an online Service Request. Follow the process in KB68030 (https://kc.mcafee.com/corporate/index?page=content&id=KB68030)

To help speed the sample review process, please provide the following information with your sample:

- A list of all files in the sample submission, including a brief description of where or how you found them
- What symptoms cause you to suspect that the sample is malicious
- Whether any security products find a virus (tell us the security vendor, its product name, the version number, and the virus name assigned to the sample)
- Your McAfee product information (product name, engine, and .DAT version)
- Any system details that may be relevant, including operating system and service packs in use

Finding Samples to Submit

Article KB53094 (https://kc.mcafee.com/corporate/index?page=content&id=KB53094) can assist you in finding malicious samples on your systems.

What Not to Submit

Please do not send screenshots, anti-virus or HijackThis logs, or prefetch files through the ServicePortal or email. Send only the suspected malicious files. If you need help with these items, contact Technical Support.

How to Submit Malware Samples

When submitting a sample to McAfee Labs for review, you may use one of these delivery methods:

- **ServicePortal.** This is the preferred method for customers to submit malware or virus samples. Log into the ServicePortal, click the Service Requests tab, then click “Submit a Sample”
- **GetSusp.** Intel Security recommends that you first use GetSusp when analyzing a potentially infected PC. See KB69385 https://kc.mcafee.com/corporate/index?page=content&id=KB69385) for full instructions. To download GetSusp, go to http://getsusp.mcafee.com. Even if you do not have a valid Grant Number, GetSusp allows you to submit samples to McAfee.
- **Email.** Submit samples directly to McAfee Labs by attaching the file(s) in an email to virus_research@mcafee.com. The samples must be archived in a password-protected ZIP file with the password “infected” (all lowercase). For instructions on how to create a ZIP file and password protect it, see the Microsoft articles Using WinZip and Using Windows File Compression.

5 Accessing and Upgrading Products

Intel Security recommends you review the resources available on the ServicePortal at https://support.mcafee.com to make your deployment and configuration as easy as possible.

5.1 Downloading Your Products

Intel Security constantly enhances its products to combat new attacks and prevent data loss. Regularly upgrading products ensures that systems have the maximum level of protection, while minimizing the possibility of encountering an issue that has already been addressed in a later version.

McAfee software can be downloaded at http://www.mcafee.com/us/downloads/. Authenticate with your grant number to display all products available for download under your support entitlement.

5.2 Configuring ePO for Updates/Upgrades

Intel Security recommends that you use ePolicy Orchestrator (ePO) to automate the deployment of your McAfee software, updates, and virus definitions. For instructions on how to deploy updates via ePO, see the Product Guide for your version of ePO, or watch the Quick Tips Video Walkthrough.

5.3 Product Activations

Some McAfee products, including McAfee Firewall appliances, McAfee SmartFilter, and McAfee Web Reporter, require activation. Go to https://www.securecomputing.com/index.cfm?skey=231 for more information.

5.4 Patches and Hotfixes

From the ServicePortal, click the "Downloads" tab to find available product patches and hotfixes. To access downloads for former Secure Computing products, see: https://www.securecomputing.com/index.cfm.

5.5 Global Threat Intelligence (GTI)

Global Threat Intelligence (GTI) provides an always-on, real-time protection that reduce potential exposure to threats, leveraging McAfee Labs threat intelligence to prevent damage and data theft even before a signature update is available.

GTI supplements detection in DAT signatures with real-time behavior analysis. It works with selected McAfee products to query the GTI cloud about a potential threat, get a reputation score, and alert the McAfee product to take appropriate policy-based action.

How GTI Works

- A user receives a file that the scan agent deems suspicious (for example, an encrypted or packed file) and for which there is no signature in the current local DAT files.
- Using Global Threat Intelligence, the agent sends a fingerprint of the file for instant lookup in the comprehensive real-time database at McAfee Labs.
- If the fingerprint is identified as malicious, an appropriate response is sent to the user to block or quarantine the new threat.

To learn what products support GTI and how to enable it, go to Knowledge Base article KB70130 at: https://kc.mcafee.com/corporate/index?page=content&id=KB70130.

5.6 End of Life Policy

Intel Security has an established product End of Life (EOL) policy outlining the level of support a product will receive as it moves through its life cycle. During the end-of-life period, Intel Security will meet existing support agreements, notify you of impending product support termination, and encourage you to move to a supported version. See the Product and Technology Support Lifecycle page at: http://www.mcafee.com/us/support/support-eol.aspx to ensure you are using the most current product version.

6 Hardware Support

Intel security Hardware Support provides a maintenance program for service and repair of McAfee appliances with several programs available to assist customers with appliance diagnosis in the event of a failure or other issue. See https://support.mcafee.com/SPR/WebContent/ProgramsAndPolicies/wp-hardware-support-user-guide.pdf for more information.

6.1 Hardware Support Process

Intel Security Hardware Support options supplement the Business Support contract with solutions specific to the hardware and appliances purchased. If you have issues with an appliance, contact Support as noted in Section 4.5 of this Guide. Your request will be escalated to the Hardware Support team.

- Tier 1 Support will undertake initial diagnosis and escalate to Tier 2 if a hardware fault is suspected
- Tier 2 will undertake a full analysis of the issue, and initiate a Return Materials Authorization (RMA) or onsite visit once a hardware fault has been identified

6.2 Hardware Support Availability

Availability of specific Intel Security Hardware Support options is dependent on the physical location of the appliance and type of appliance. Should the location of your hardware be in a location which Intel Security cannot provide specific onsite service, Intel Security reserves the right to change the deliverables of either Same Day 7x24 or Next Business Day On Site. For a list of supported countries for McAfee appliances, see: http://www.mcafee.com/us/resources/misc/rm-hw-supported-locations.pdf.

6.3 Advanced Replacement (RMA)

Products with Advanced Replacement RMA support will be shipped replacement hardware (a customer replaceable part or replacement appliance) of like or better quality, to the location of the defective hardware, without waiting for the return of original appliance. Intel Security offers Same Day/Next Business Day shipment of replacement parts depending on the time that the issue is diagnosed. Delivery times are subject to carrier transit times and customs processing.

6.4 On-site Repair

Upon diagnosing a hardware failure, Intel Security will dispatch an authorized service technician to the location of the defective hardware with parts of like or better quality and labor necessary to repair or replace the hardware at no additional charge. The service technician will arrive at the location during normal business hours (8am–6 pm) local time, except holidays observed by McAfee, to begin hardware repair or replacement. If the hardware requiring replacement is considered a customer replaceable unit (CRU), the replacement hardware will be shipped to arrive the next business day. For CRUs, an onsite technician will not be dispatched.

6.5 Hardware Limited Warranty

Intel security strongly recommends keeping hardware support agreements current. In the event you do not purchase hardware support, you will not be covered under warranty outside the initial 90 days from ship date from the facility of your hardware purchase. In the event your hardware support agreement has expired, please contact Intel Security or your authorized reseller to determine options and the associated costs. See hardware warranty details at http://www.mcafee.com/us/resources/misc/mfe-hw-warranty.pdf.

7 Product Information Communications Policy

The Support Notification Service (SNS) is the official product communications vehicle for Intel Security standard and critical incident advisories.

Standard Product Notices: Email sent within four (4) hours of receipt. Standard notices include product updates, releases, EOL notices; content releases; other non-critical advisories. Standard notices are also sent in the Weekly Roundup email, and posted to the Intel Security Community at https://community.mcafee.com/community/business/support/sns.

Alert Advisories: Critical incidents with an urgency factor; email and SMS-text message (to subscribers with validated cell phones) sent within two (2) hours of receipt; follow-up frequency will be noted in each email. Critical incidents are flagged as widespread or with severe impact and require immediate action by the customer.

You must subscribe to SNS to receive these notifications. For instructions on how to subscribe, see **Section 2.4** of this document.

8 Notifications

8.1 Support Notification Service (SNS)

SNS delivers the latest McAfee product information by email — End of Life, patch and upgrade notifications; threat reports; DAT notices; and critical alerts that require immediate attention. Select from 18 product and three special information options. Distribution types include:

- **Notices** — standard product news and updates sent the same day
- **Alerts** — critical and urgent information requiring immediate action
- **Weekly Roundup** — all product news for the last seven days in one weekly email (Thursdays CT)
- **ProTips** — best practices, troubleshooting, how-to, and breaking tips with links to in-depth KnowledgeBase resources
- **SNS Journal** — newsletters featuring technical product, new technology, malware trends, and security awareness content
- **Executive Journal** — thought-leading articles about the business of security from Intel Security leaders (bi-monthly)

To get these notices, you must subscribe to SNS. Go to the SNS Subscription Center and create a new account: https://sns.snssecure.mcafee.com. For further information, see the SNS FAQ at https://kc.mcafee.com/corporate/index?page=content&id=KB67828.

8.2 McAfee Labs Security Advisories

McAfee Labs Security Advisories are notifications created by the global research team to map high-profile threats to the technologies that remediate against that threat. Sign up for McAfee Labs Security Advisories at: http://www.mcafee.com/apps/mcafee-labs/signup.aspx.

8.3 McAfee DAT Delay Notifications

Virus definition or DAT files contain virus signatures and other information that McAfee anti-virus products use to protect systems against existing and new potential threats. For a complete list of products using DAT files, go to https://kc.mcafee.com/corporate/index?page=content&id=KB55986.

The daily DAT files are generally available by 19:00 (UTC/GMT). However, if a new threat warrants this, daily DAT files may be released earlier. Under some circumstances daily DAT releases may be delayed. To receive alerts regarding delays or important notifications, subscribe to the Support Notification Service (SNS) at https://sns.snssecure.mcafee.com.

To ensure that your anti-virus software can protect your system or network against the latest threats, confirm you are using the latest DAT files, which are available from the Security Updates page in XDAT and SDAT format at: http://www.mcafee.com/apps/downloads/security-updates/security-updates.aspx. This site also provides access to Beta DAT files.

Appendix

Appendix A
Premium Support Offerings

Business Support (formerly Gold Support) provides the highest level of self-help and responsive service. Some customers have complex or mission-critical environments which need a more proactive and personalized support solution that Intel Security Premium Support options can provide.

Enterprise Support (formerly Platinum)

Enterprises worried about business continuity and compliance need a higher level of accountability and predictive support. An assigned Support Account Manager (SAM) provides personalized support, risk assessments, proactive advice, and escalation for complex technical issues. Customers also gain the benefit of direct access to Product Specialists for detailed technical assistance on their products.

Global Enterprise Support

For multi-national organizations with a headquarters location, Global Enterprise Support is valuable. This offering includes an assigned Global Support Account Manager who provides centralized account management in addition to Product Specialists in each region. By leveraging Support Product Specialists worldwide, Intel Security can help you resolve issues faster, anytime, anywhere, by providing global product, technical, and problem-solving coverage.

Large Enterprise Support

Tailored to large and complex organizations focused on minimizing disruptions and reducing their total cost of ownership. The Large Support Account Manager acts as an extension to your IT security team, working closely on solutions planning assistance, pre-emptive advice, and direct intercession for the fastest possible resolution to complex technical issues. Assigned Product Specialists are on call to provide detailed technical assistance when required.

Resident Enterprise Support

Organizations requiring the highest level of direct assistance to manage their complex environments gain significant benefit from a dedicated Resident Support Account Manager or Resident Product Specialist working on site with your IT security team. An onsite expert can engage directly for pre-deployment planning and best practices implementation to maximize protection and minimize risk.

Appendix B
Additional Services

Solution Services

Many customers do not have the time or resources to fully deploy their security products. What's more, an improperly configured security product could result in reduced protection, increased vulnerability to attack, and degradation of system performance. Intel Security Professional Services can help organizations quickly realize the value of their McAfee solutions and accelerate the return on investment. Additionally, Professional Services consultants can provide onsite assistance for installation planning, product deployment, and other expert services. See http://www.mcafee.com/us/services/solution-services/index.aspx

Quickstart Services

Smaller organizations can benefit from security experts for installation, deployment, configuration, or fine-tuning assistance with Intel Security Quickstart Services. These experts can remotely connect to your system and take the time and frustration out of implementing, optimizing, and configuring your McAfee security solutions. See http://www.mcafeequickstart.com/

Product Education

Learn the real-world skills you need to increase product functionality and effectively prevent security threats. McAfee Product Education combines hands-on experience with expert instruction so you can get the most from your McAfee security products. See http://www.mcafee.com/us/services/solution-services/solution-services-packages.aspx#vt=vtab-QuickstartServices

Training and Professional Services

If you would like assistance with your deployment or checking the health of your installation, Intel Security offers a number of professional services. For on-site assistance, contact Solution Services at solution_services@mcafee.com. Intel Security also provides online and classroom training courses. For more information visit: http://www.mcafee.com/us/services.aspx

Strategic Security Education

Give your in-house security team the tools and methodologies they need to defend your business. Foundstone combines interactive classroom demonstrations with hands-on labs. Your team leaves armed with a real-world understanding of critical security issues, and how to address them. See http://www.mcafee.com/us/services/strategic-security-education/index.aspx

Feedback on This Document

If you would like to see additional information included in this guide or if you discover any discrepancies, please contact us at customer_feedback@mcafee.com. We welcome your comments.

About Intel Security

Intel Security combines the expertise of McAfee with the innovation, performance, and trust of Intel to empower businesses, the public sector, and home users to safely experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence network, Intel Security is focused on keeping its customers safe. http://www.mcafee.com