



**IBM Security**

Intelligence. Integration. Expertise.

# ***Virtual Security Operations Center (SOC) Portal User Guide***

April 2017



# Table of Contents

<b>PREFACE .....</b>	<b>4</b>
<b>OVERVIEW .....</b>	<b>5</b>
<b>CUSTOMER ENABLEMENT ASSETS .....</b>	<b>6</b>
MSS BEST PRACTICES .....	6
MSS eLEARNING COURSES .....	7
MSS EDUCATION PAGE .....	8
MSS KNOWLEDGEBASE.....	8
PORTAL MEDIA LIBRARY .....	10
SECURITY SERVICES RESOURCES .....	11
<b>LOGIN PAGE.....</b>	<b>12</b>
<b>HOME PAGE .....</b>	<b>13</b>
<b>CUSTOMIZING YOUR PORTAL.....</b>	<b>15</b>
CHECK NOTIFICATIONS .....	18
CURRENT THREAT ASSESSMENT .....	19
ACTIVE TICKETS & XPS ALERTS .....	21
EVENT TRENDS – QUICK GLIMPSE.....	23
<b>SUSPICIOUS HOSTS DASHBOARD .....</b>	<b>26</b>
IP INTELLIGENCE REPORTING FEATURE .....	28
<b>DEVICE MANAGER .....</b>	<b>29</b>
INTERFACE ENHANCEMENTS.....	30
DEVICE DETAILS .....	31
DEVICE GROUPS .....	32
ULA SOFTWARE .....	34
<b>ASSET CENTER .....</b>	<b>35</b>
Essential Features .....	35
Getting Started.....	35
Adding or Editing an Asset .....	36
Exporting Assets.....	36
<b>VULNERABILITY MANAGER.....</b>	<b>37</b>
<b>TICKETS AND INCIDENTS.....</b>	<b>39</b>
TICKET MANAGER – SECURITY & SERVICE RELATED TICKETS.....	39
TICKET MANAGER – TICKET DETAILS .....	42
TICKET MANAGER REPORTS – POLICY CHANGE REQUEST.....	43
SUBMIT A POLICY CHANGE REQUEST.....	44
SUBMIT A GENERAL SERVICE REQUEST .....	47
CREATE AN INTERNAL TICKET.....	48
CREATE AN INTERNAL SECURITY INCIDENT.....	49
<b>REPORTS .....</b>	<b>50</b>
IDS/IPS SENSORS REPORTS .....	52
ATTACK METRICS .....	53
EXPLANATION OF ATTACK TYPES.....	54

<b>SECURITY LOGS AND EVENTS .....</b>	<b>57</b>
LOGS DROP DOWN MENU .....	57
LOG QUERY.....	57
LOG QUERY – ADVANCED OPTIONS.....	58
LOG QUERY – RESULTS.....	59
LOG SEARCH.....	60
ACTIVE ANALYZER .....	61
ACTIVE ANALYZER – CONTEXT BASED MENUS .....	61
ACTIVE ANALYZER – QUERY CRITERIA.....	62
<b>CREATING VIRTUAL SOC PORTAL USERS.....</b>	<b>64</b>
<b>SOC COMMUNICATIONS.....</b>	<b>66</b>
SERVICE ESCALATION.....	66
SOC ESCALATION .....	67
CHAT FEATURE: .....	67
MEDIA LIBRARY .....	68
<b>LOG OUT.....</b>	<b>69</b>
<b>REFERENCE .....</b>	<b>70</b>
SOC CONTACTS.....	70

# Preface

This document is designed to show you how to make the most out of the IBM Security Services Managed Security Services (“MSS”) customer Portal or sometimes referred to as the Virtual Security Operations Center. The Portal home page is both your snap shot of the most critical security information potentially impacting your network and a jumping point to all of the resources and rich feature sets available to you.

In recognizing the time constraints you face and the security challenges you must overcome, this guide has been organized to provide a strategy of how to efficiently access information when you’re only able to use the portal for brief amounts of time each day.

The screenshot displays the IBM Security Services Managed Security Services (MSS) customer Portal home page. The interface includes a navigation bar at the top with links for Home, Tickets, Alerts (196), Logs, VMS, Intelligence, Email and Web Security, Devices, Analytics, Reports, and Support. The user is logged in as Mister Anderson. The main dashboard is divided into several sections:

- Notifications:** A list of notifications including IBM Content Update XPU 32.041 (Apr 22 2012), VMS Content Release 2012-04-21 (Apr 20 2012), and IBM Content Update XPU 32.040 (Apr 09 2012).
- Recent XPS Alerts:** A table showing alert IDs, creation times, event names, and statuses. It includes a "View All" link and a "Displaying last 12 hours" indicator.
- Current Security Assessment:** A section titled "Microsoft Security Bulletin Advance Notification for May 2012" providing information about upcoming security bulletins.
- Active Security Incidents (81):** A table listing incidents with columns for Ticket ID, Type, Priority, Status, Created, and Last Updated (EST). It includes a "View All" link.
- Active Service Requests (7):** A table listing service requests with columns for Ticket ID, Type, Priority, Status, Created, and Last Updated (EST). It includes a "View All" link.
- XPS Alerts Trend:** A line graph showing the count of alerts over time, with a peak around May 8th. It includes a "View All" link and a "Displaying last 48 hours" indicator.
- XPS Alert Breakdown:** A bar chart showing the count of alerts by rule name, with a single bar for "FWNewEntryInTopAllowed...". It includes a "View All" link and a "Displaying last 24 hours" indicator.

The footer of the page contains copyright information: Copyright © 2012 IBM Corporation, Privacy, Terms of use, and the date/time: 05/07/12 00:12 EST - 05/07/12 05:12 GMT. It also shows the last login time: Last Login: 05/06/12 14:19 EST and a user ID: #02.66591.

---

# Overview

This guide has been organized to provide a strategy for how to best use the portal and its many features for brief amounts of time each day. The below checklist items facilitate this strategy and will quickly highlight the key feature sets in an easy to follow step-by-step process.

Feature sets vary based on the MSS services you have subscribed to:

Ordered checklist of things to do when making a quick review:

- ☐ [Log In](#)
- ☐ [Check Notifications](#)
- ☐ [Check Alertcon](#)
- ☐ [Check Tickets](#)
- ☐ [Check XPS Alerts](#)\*
- ☐ [Event Trend – Quick Glimpse](#)
- ☐ [Check Suspicious Host Dashboard](#) \*
- ☐ [Log Out](#)

Selected actions when needed:

- ☐ [Check Security Event Manager](#)\*
- ☐ [Check Vulnerability Status](#)\*
- ☐ [Device Manager](#)
- ☐ [Check Ticket Manager](#)
- ☐ [Submit Policy Change Request](#)
- ☐ [Submit Service Request](#)
- ☐ [Create an Internal General Ticket](#)
- ☐ [Create an Internal Security Incident](#)
- ☐ [Monitor Live IDPS Events via Active Analyzer](#) \*
- ☐ [View and Query Logs](#)
- ☐ [Run a Report](#)
- ☐ [Cursory Log Review](#)
- ☐ [Create VSOC Users](#)
- ☐ [Check Downloads](#)
- ☐ [Service Escalation](#)
- ☐ [SOC Contacts](#)

\*Appropriate Service/Service level subscription required

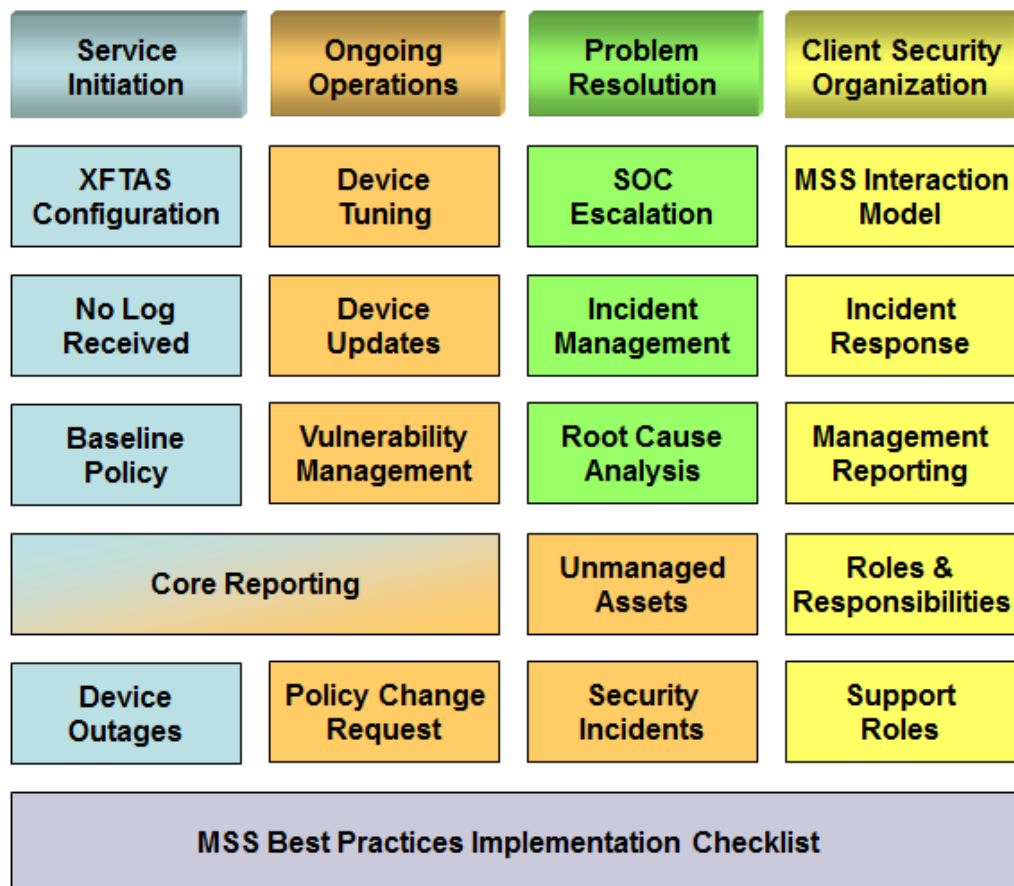
---

# Customer Enablement Assets

IBM Security Services provides numerous education and enablement resources to assist you and support your team's day-to-day security practices. Most MSS resources are available from the Portal's Support menu, including Best Practices, eLearning courses, Demonstration and Best Practices videos, core documentation, KnowledgeBase articles, Media Library repository, and Security Services Resources.

## MSS Best Practices

IBM Managed Security Services (MSS) Best Practices use an operational framework to articulate recommended activities around MSS processes and procedures that can maximize the value of your subscribed services.



## MSS eLearning Courses

IBM Managed Security Services eLearning allows you to learn at your own pace, using our engaging and interactive online content. The following eLearning job-focused courses, which include hands-on simulations, are available in the virtual SOC Portal:

- MSS Managed SIEM Analysis and Reporting
- MSS Security Intelligence and Analysis
- MSS Security Incident Response
- MSS Security Metrics and Reporting



## MSS Education Page

The three tabs on the MSS Education page provide access to eLearning courses, demonstration and best practices videos, and core documentation. You can access the MSS Education page from the Portal Support menu.



IBM Security Services

### Security Services Education Resources

Smarter training to grow your security skills

**IBM Security**  
Intelligence. Integration. Expertise.

[eLearning](#) [Videos](#) [Documentation](#)

[Send us your feedback](#)

#### Online Training

IBM Managed Security Services (MSS) eLearning allows you to learn at your own pace, using our engaging and interactive online content. Use the links on this page to access full courses, or to review individual [course simulations](#) at any time.

To learn about the full range of enablement resources available, view the video, [MSS New User Learning Path: Taking Advantage of MSS Education Resources](#), and review the [MSS New User Learning Path diagram](#).

#### eLearning Course Offerings

The following eLearning courses are available at no charge:

- MSS Managed SIEM Analysis and Reporting** – Focuses on helping you get the full value from your SIEM technology and the IBM Managed SIEM service. The course describes key IBM roles and responsibilities associated with the service, and how to use essential client tools, including how to:
  - Use the Virtual SOC Portal to create a ticket to request a Managed SIEM policy change.
  - Access QRadar console from the Virtual SOC Portal.
  - Use the QRadar Dashboard tab to create and configure dashboards.
  - Use the QRadar Log Activity tab to view and search log data.
  - Use the QRadar Reports tab to view and generate a report, create and edit a report template, and manage reports and report groups.

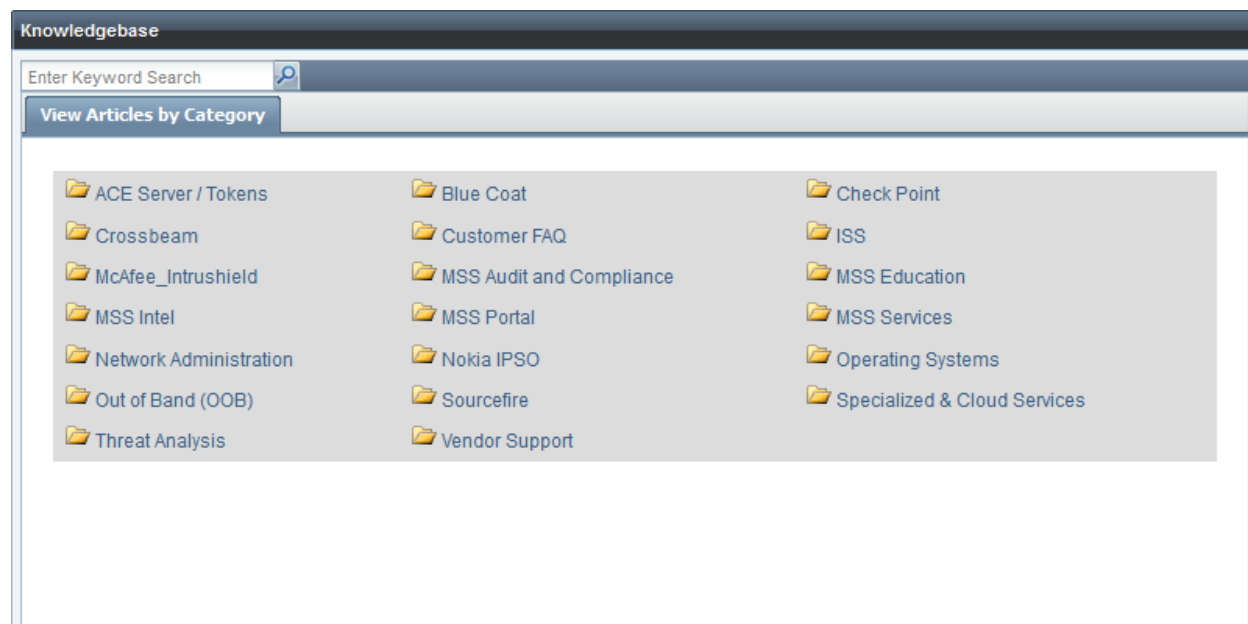


## MSS KnowledgeBase

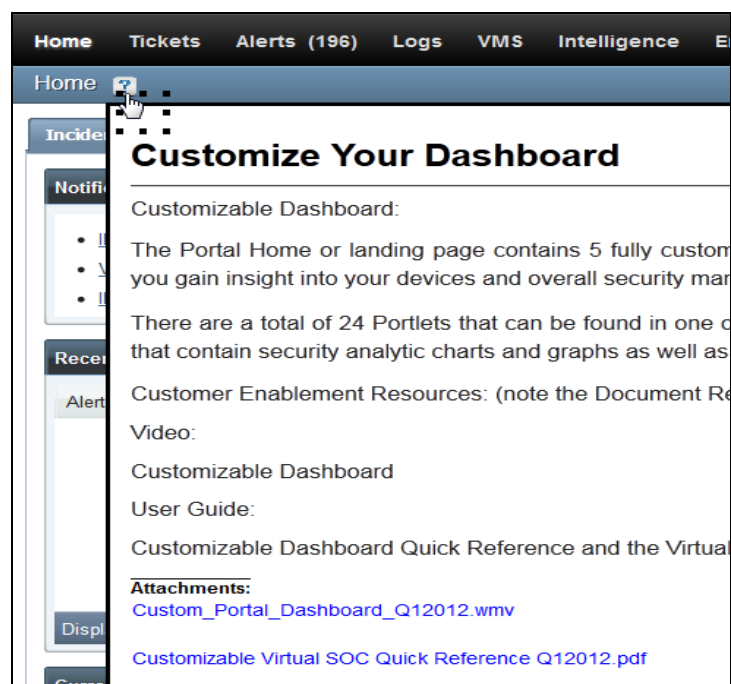
The KnowledgeBase (KB) is populated with technical articles authored by senior Security Operation Center resources that will help answer some of the most frequently asked questions. You can search by keyword or select an article by category, as shown below. You can access the KB by clicking “Help” in the top right side of the portal, or by selecting the Knowledgebase option from the Support menu.



*The KnowledgeBase opens in a separate window.*



Located throughout the Virtual SOC Portal's user interface, you also can access Knowledgebase articles with links to many self-service educational videos and documents designed to provide information on many of the Portal's features and services.



See examples below:

- **Introduction to the Virtual Security Operations Center** A quick overview of the various Portal features and resources available to assist customers in securing their networks on a daily basis
- **Introduction to the Suspicious Host and IP Intelligence Features** (10 minutes) A video that demonstrates how to navigate the dashboard and reporting feature as well as some best practices associated (There is also an associated Webcast)
- **Introduction to VMS** (15 minutes) A video that provides a detailed overview of the service and demonstrates how to use the features
- **Introduction Security Event and Log Management** (20 minutes) A video that provides a detailed overview of the service and demonstrates how to use the features

## Portal Media Library

The Portal Media Library provides download access to various documents, including user guides and threat research papers, as well as training videos and simulations, and webcast replays.

Home Tickets Alerts (724) Logs VMS Intelligence Devices Analytics Reports Support More MSS Education 2 Help IBM

Support > Media Library

Filters

Categories: All Media types: All

Date uploaded: Any time from to Apply Reset

Download... Delete Add...

Title	Category	Author	Size	Date Uploaded
<b>Documents (92)</b>				
<b>Recorded Webcasts (27)</b>				
<b>Videos (22)</b>				
<a href="#">Video: Managing Portal Reports (18 minutes)</a>	General Portal	MSS Education	38.47 MB	Sep 18 2013
<a href="#">Video: Managing Support Roles (Security Contacts) (6 minutes)</a>	General Portal	MSS Education	11.06 MB	Aug 23 2013
<a href="#">Video: Configuring Acceptable Traffic and Network Objects (6 minutes)</a>	General Portal	MSS Education	11.47 MB	Aug 15 2013
<a href="#">Simulation: Create and Monitor Policy Change Requests (3 minutes)</a>	General Portal	MSS Education	1.61 MB	May 31 2013
<a href="#">Simulation: Configure, Run, Schedule Alert Activity Report (3 minutes)</a>	General Portal	MSS Education	1.34 MB	May 28 2013
<a href="#">Video: Exporting Portal Data and Using Excel to Manipulate Data and Create Pivot Tables (1...</a>	General Portal	MSS Education	12.25 MB	Mar 15 2013
<a href="#">Video: Using the Asset Center for Critical Assets (9 min)</a>	Device & Asset Management	MSS Education	14.24 MB	Jan 28 2013
<a href="#">Virtual SOC Portal Active Analyzer Video (3 mins)</a>	General Portal	MSS Education	6.14 MB	Feb 14 2012
<a href="#">Virtual SOC Portal Tickets Menu video (6 mins)</a>	General Portal	MSS Education	18.65 MB	Feb 14 2012
<a href="#">Virtual SOC Customizable Dashboard Video (4 mins)</a>	General Portal	MSS Education	13.33 MB	Feb 07 2012
<a href="#">Introduction to the Virtual SOC Portal Video</a>	General Portal	MSS Education	18.81 MB	Feb 06 2012
<a href="#">Virtual SOC Portal Support Menu Video (3 mins)</a>	General Portal	MSS Education	5.48 MB	Feb 05 2012
<a href="#">Virtual SOC Settings Video (3 min)</a>	General Portal	MSS Education	4.73 MB	Feb 05 2012
<a href="#">Virtual SOC Portal Intel Menu Video (5.5 mins)</a>	General Portal	MSS Education	8.2 MB	Feb 05 2012

Copyright © 2013 IBM Corporation Privacy Terms of use 10/01/13 09:31 EST - 10/01/13 14:31 GMT Last Login:09/30/13 12:56 EST at101b.61930\_a3b3cb5

# Security Services Resources

The Portal Resources site provides access to security research, videos, webcasts, and other information related to IBM Security Services.

The screenshot shows a web browser window displaying the IBM Security Services Resources portal. The browser's address bar shows the URL [https://portal.sec.ibm.com/mss/html/en\\_US/sup](https://portal.sec.ibm.com/mss/html/en_US/sup). The page features the IBM logo and the text "IBM Security Services" at the top. Below this, the main heading "Security Services Resources" is displayed, followed by the tagline "Smarter security to protect your organization". To the right of the heading is the IBM Security logo and the tagline "Intelligence. Integration. Expertise.".

The main content area is divided into several sections:

- X-Force Command Center:** A large banner image showing a control room with multiple monitors. Text overlay reads "X-Force Command Center" and "Take command of your security posture". Below the banner are four small circular icons and the text "Click dots to view a specific item."
- Research and Intelligence:** A section with three cards:
  - Ponemon 2016 Cyber Resilient Organization:** Includes a download report link.
  - IBM X-Force Exchange:** Includes a share and collaborate link.
  - 2016 Cyber Security Intelligence Index:** Includes a gain insights link.
- SecurityIntelligence.com:** A section with a link to IBM Security research, analysis, and insight for information security professionals.
- Events & Webinars:** A section with a link to view the calendar of upcoming security events and webinars on IBM's Security Intelligence website.
- MSS Education Resources:** A section with a link to take advantage of eLearning courses, videos, and documentation to learn how to use IBM services more effectively.
- X-Force Interactive Security Incidents:** A section with a link to stay up to date on the latest breaches and security incidents as they are confirmed by public sources.
- U.S. National Institute for Standards and Technology Computer Security Resource Center:** A section with a link to find resources regarding information.

# Login Page

Open up your web browser and go to the following URL:

<https://portal.sec.ibm.com>

This is the first page you see when you visit the site is the Client Sign In page. It allows you to log in directly to the Portal, or sign in using your IBM id. Signing in with your IBM id enables the Portal's single sign-on functionality, which allows you to seamlessly access X-Force Exchange and other IBM Security Services tools.

**Virtual Security Operations Center** IBM

■ RSA Token Users and IBM Employees should continue to login with their Portal id

**Client Sign In**  
Username:   
Password:   
[Forgot Password](#)  
**Sign in**

**IBM id**  
One key, many possibilities.  
Your IBM id provides access to services, communities, support, online purchasing, and much more. You can create an IBM id to access new tools in the vSOC Portal such as X-Force Exchange.  
**Sign in with IBM id** **Create IBM id**

**Important SOC Announcement** ALERTCON 1

At the present time, all services are actively being delivered from our Global Security Operations Centers in North America, South America, Europe, Australia and Asia. All systems within the Security Operations Centers are operating under normal conditions.

Currently, there are no Internet Emergencies active or pending. In the event of an Internet Emergency, a status update will be provided at this URL, and Managed Security Services customers will be notified accordingly.

Copyright © 2015 IBM Corporation [Privacy](#) [Terms of use](#) [in](#) [f](#) [v](#) [t](#) [m](#) [IBM Employee sign in](#)

**Note:** For more information about using your IBM to access the Portal, refer to the user guide, “VSOC Portal Single Sign-On Using IBM id,” which is available for download in the Portal Media Library.

# Home Page

The home page acts as a launch pad to the various subscribed features and resources. You have the ability to customize your landing page with security analytic or informational based Portlets (or windows) associated with your security role or personal preference.

## Use Case:

Most security teams are made up of more than one professional with a division of duties. For example one may specialize in Threat Analysis or Security Incident response and mitigation and another may focus more on device policy or device maintenance; another may focus strictly on the overall security posture and / policy. With this new enhancement in place each member of your security team has the ability to customize a series of informative Portlets associated with their business role which enables a more efficient customer experience.

## Highlights:

- Predefined (and customizable) dashboards based on the business roles of Security Analyst, Operations Manager, and Executive
- Ability to create and personalize multiple dashboard views
- Enhanced security analytic Portlets with drill in and hover over capabilities for quick and efficient access important information (Example below)

The screenshot displays a portlet titled "Active Security Incidents (64)" with a "View All" link and several icons. Below the title is a table with columns: Ticket ID, Type, Priority, Status, Created, and Last Updated (EST)... . The table lists several incidents, with the second row (Ticket ID 0700726296) highlighted. A tooltip is shown over this row, providing detailed information about the incident.

Ticket ID	Type	Priority	Status	Created	Last Updated (EST)...
0700726295				11/05/11	11/09/11 13:23
0700726296				11/05/11	11/09/11 13:23
0700726297					9/11 13:23
0700726300					9/11 13:23
070030821					9/11 07:05

Ticket	SOCJ00700726296
Issue	SI Probes and Scans
Description	QA Test Prod Release
Attack	Nmap_OS_Fingerprint
Device	DEMO , atl-stg-provsrv-01 .....
Src IP	207.231.140.222
Src Port	
Dest IP	10.200.1.12 , 10.200.1.13 ...
Dest Port	
Reason	Test

- 25 Portlets categorized by Alerts, Firewall, IDPS, Information and Tickets

## Home Landing Page:

[Home](#)
[Tickets](#)
[Alerts \(196\)](#)
[Logs](#)
[VMS](#)
[Intelligence](#)
[Email and Web Security](#)
[Devices](#)
[Analytics](#)
[Reports](#)
[Support](#)

Mister Anderson
Help

Home ?

Portlet Dashboards

Search Portal...

Incidents and Alerts\*

Sensor Activity

Operations

Management

News

My Dashboards

Resilience

Legacy

Notifications

Notification Archive

- IBM Content Update XPU 32.041 ( Apr 22 2012 )
- VMS Content Release: 2012-04-21 ( Apr 20 2012 )
- IBM Content Update XPU 32.040 ( Apr 09 2012 )

Recent XPS Alerts

View All

Alert ID	Created (EST)	Event Names	Status

Displaying last 12 hours

Current Security Assessment

View All

**Microsoft Security Bulletin Advance Notification for May 2012**

For the month of May, Microsoft is planning to release seven bulletins on Tuesday, May 8th. Three of these bulletins are rated Critical, while the remaining four are rated Important. Five of the seven are noted as allowing for remote code execution. The seven bulletins address issues identified in Microsoft Windows, Microsoft .NET Framework, Microsoft Silverlight and Microsoft Office amongst other products. Administrators should plan ahead to

Active Security Incidents (81)

View All

Ticket ID	Type	Prio...	Status	Created	Last Updated (EST)...
0701013968				May 05 12	May 06 12 23:52
0701013975				May 05 12	May 06 12 23:52
0701010506				May 02 12	May 06 12 23:52
0700625612				Aug 06 11	May 05 12 11:26
0701013931				May 05 12	May 05 12 11:05

Active Service Requests (7)

View All

Ticket ID	Type	Prio...	Status	Created	Last Updated (EST)...
0701013916				May 05 12	May 05 12 12:56
0701013901				May 05 12	May 05 12 10:29
0701010261				May 02 12	May 03 12 20:05
0701001013				Apr 25 12	Apr 25 12 14:27
0700947464				Apr 11 12	Apr 11 12 04:34

XPS Alerts Trend

View All

Displaying last 18 hours

XPS Alert Breakdown

View All

Displaying last 24 hours

Copyright © 2012 IBM Corporation

Privacy

Terms of use

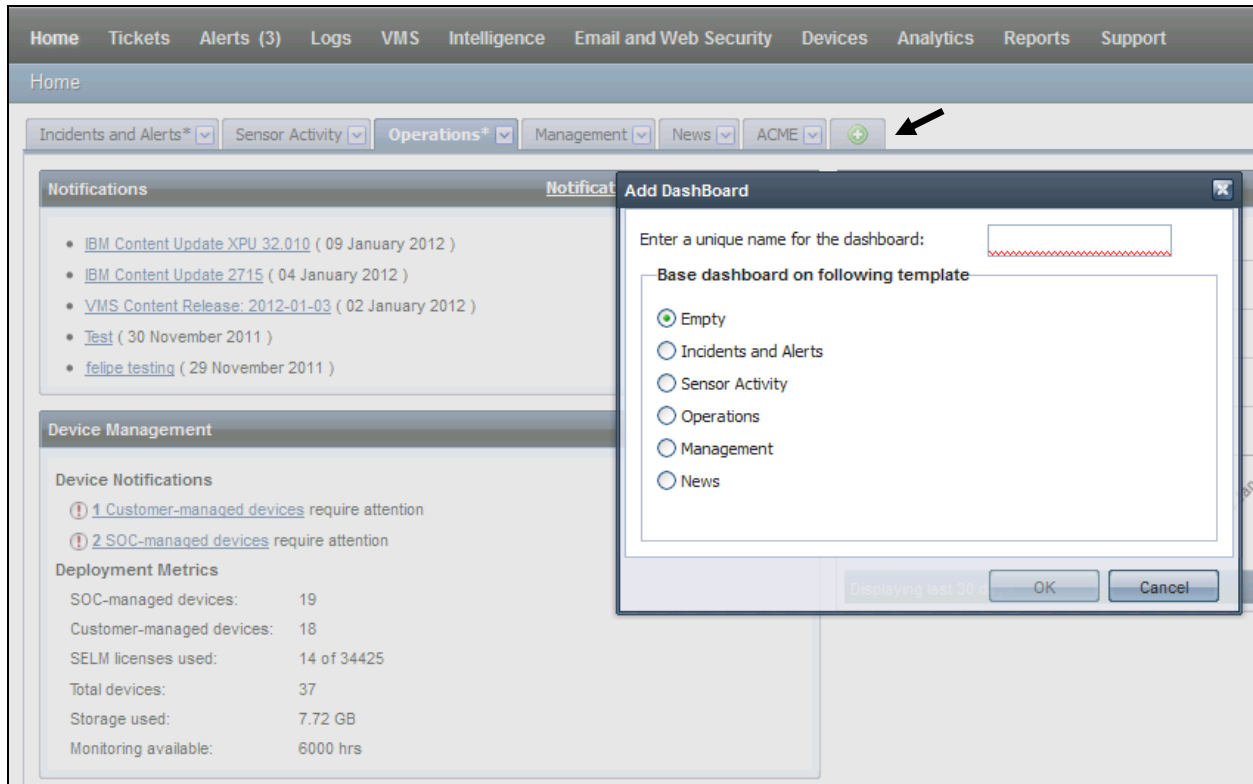
05/07/12 00:12 EST - 05/07/12 05:12 GMT

Last Login:05/06/12 14:19 EST

#02.66591

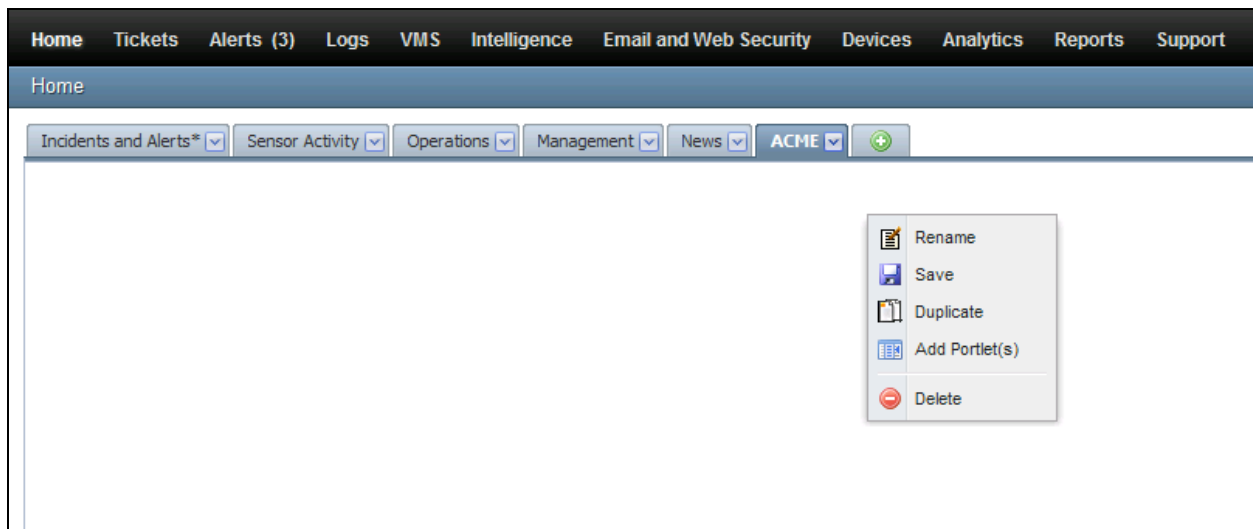
# Customizing your Portal

To add a new dashboard click on the green plus icon to add a new tab.



You can customize an existing type of dashboard or select, “Empty” to start from scratch. Right click in the open space to edit your dashboard.

## Selecting your desired Portlets:



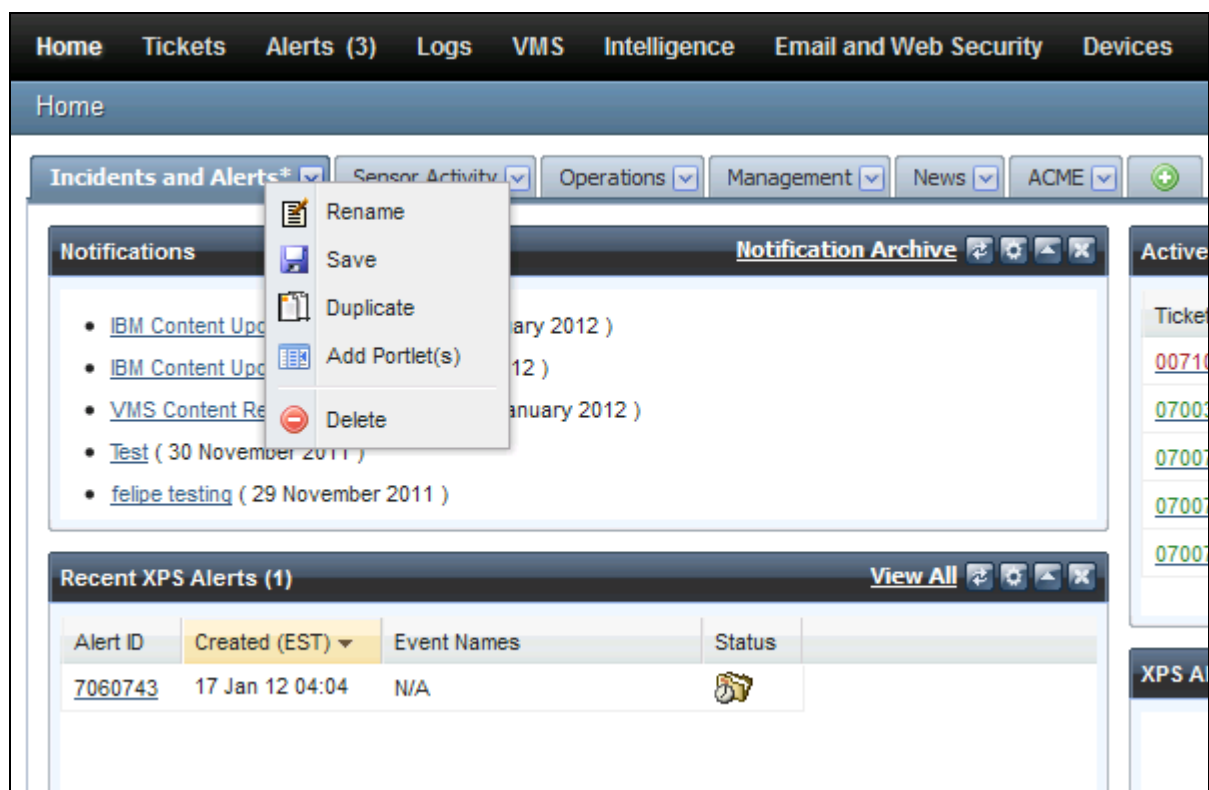


Select Portlets to Add

<input type="checkbox"/>	Portlet Name ▲
<b>Alerts (3 Portlets)</b>	
<input type="checkbox"/>	<b>Recent XPS Alerts</b> Summary of the most recent XPS Alerts. Provides links to alert detail.
<input type="checkbox"/>	<b>XPS Alert Breakdown</b> Bar graphs showing breakdown of alerts for the configured period
<input type="checkbox"/>	<b>XPS Alerts Trend</b> Line graph showing trend in alerts over a configured time frame with links to alert breakdowns
<b>Firewall (2 Portlets)</b>	
<input type="checkbox"/>	<b>Firewall Dropped/Rejected Traffic</b> Grid display of the top sources of dropped or rejected firewall events for configured time frame
<input type="checkbox"/>	<b>Firewall Event Trend</b> Column graph showing FW traffic for a configured time frame.
<b>IDS/IPS (6 Portlets)</b>	
<input type="checkbox"/>	<b>Changes In Sensor Activity</b> List of sensors that have shown the greatest increase or decrease in recent activity
<input type="checkbox"/>	<b>IPS/IDS Top Destinations</b> Bar chart showing top destinations for IPS/IDS events for configured time frame
<input type="checkbox"/>	<b>IPS/IDS Top Sources</b> Bar chart showing top sources for IPS/IDS events for configured time frame
<input type="checkbox"/>	<b>Most Active Unblocked High Risk Events (Graph)</b> Bar chart of most active events during a configured time frame with a comparison to the previous time



Editing existing dashboards: Right click on the dashboard's name tab to open the edit menu.



Be sure to save any desired changes.

Portlet controls; you have the option to Refresh, Configure, Hide and Remove any Portlet.



You can return to the home page at any time from any screen by clicking the “Home” menu option.

## Check Notifications

Located under the Operations Portlet Dashboard, you can reference the Notifications and Device Manager Portlets for MSS News and recent changes in a device status that may require your attention.

The screenshot displays the VSOC Portal interface. At the top is a navigation bar with links: Home, Tickets, Alerts (3), Logs, VMS, Intelligence, Email and Web Security, and Devices. Below this is a 'Home' section with a row of tabs: Incidents and Alerts\*, Sensor Activity, Operations\* (selected), Management, News, and ACME. The main content area features two portlets. The 'Notifications' portlet lists several items: IBM Content Update XPU 32.010 (09 January 2012), IBM Content Update 2715 (04 January 2012), VMS Content Release: 2012-01-03 (02 January 2012), Test (30 November 2011), and felipe testing (29 November 2011). The 'Device Management' portlet contains 'Device Notifications' with two items: '1 Customer-managed devices require attention' and '2 SOC-managed devices require attention'. Below this is a 'Deployment Metrics' section with a table of statistics. A callout box points to the '2 SOC-managed devices require attention' link with the text: 'Click on the Hypertext to launch a Device Details view'. At the bottom is a 'Changes In Sensor Activity' portlet with a table header: Sensor name, % Ch..., Co..., and Newest Log (EST).

**Notifications**

- [IBM Content Update XPU 32.010](#) ( 09 January 2012 )
- [IBM Content Update 2715](#) ( 04 January 2012 )
- [VMS Content Release: 2012-01-03](#) ( 02 January 2012 )
- [Test](#) ( 30 November 2011 )
- [felipe testing](#) ( 29 November 2011 )

**Device Management**

**Device Notifications**

- ❗ [1 Customer-managed devices](#) require attention
- ❗ [2 SOC-managed devices](#) require attention

**Deployment Metrics**

SOC-managed devices:	19
Customer-managed devices:	18
SELM licenses used:	14 of 34425
Total devices:	37
Storage used:	7.72 GB
Monitoring available:	6000 hrs

**Changes In Sensor Activity**

Sensor name	% Ch...	Co...	Newest Log (EST)
-------------	---------	-------	------------------

## Current Threat Assessment

After reviewing any potential device status issues you should then review the current AlertCon level and the Current Internet Security Assessment. You can get to the current threat assessment page which may have additional data, by selecting “more” or clicking on “View All” to view Historical Assessments” within the Security Assessment Portlet.

Home Tickets Alerts (3) Logs VMS Intelligence Email and Web Security

Intelligence > Security Assessment

Click on AlertCon icon to access more information

Date	AlertCon Level
01/02/12	ALERTCON 1
01/03/12	ALERTCON 1
01/04/12	ALERTCON 1
01/05/12	ALERTCON 1
01/06/12	ALERTCON 1
01/07/12	ALERTCON 1
01/08/12	ALERTCON 1
01/09/12	ALERTCON 1
01/10/12	ALERTCON 2
01/11/12	ALERTCON 1

Intelligence > Security Assessment

- X-Force Threat Analysis
- Security Assessment
- Alerts / Advisories
- Vulnerabilities
- News
- Worms & Viruses
- Port Metrics
- References
- XFTAS Preferences

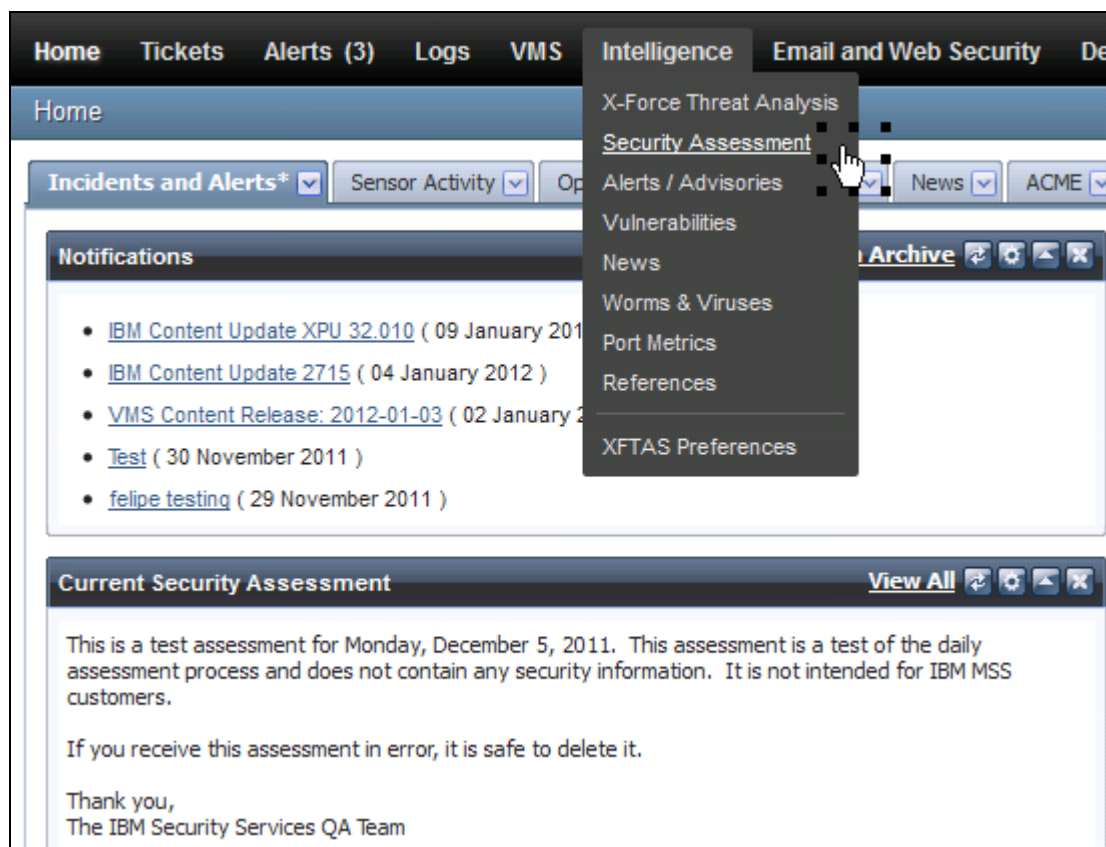
Virtual Security Operations Center

Dashboards Tickets Alerts (1) Logs VMS Intelligence Email and Web Security Reports Support

Security Assessment Alerts / Advisories Vulnerabilities News Worms & Viruses Port Metrics References

### AlertCon Definitions

AlertCon Level	Definition
1	Regular vigilance. Ordinary activity compromises an unprotected network minutes to hours after first being connected to the Internet.
2	Increased vigilance. Vulnerabilities or threats to computer networks require vulnerability assessment and corrective action.
3	Focused attacks. Specific vulnerabilities and weaknesses are the target of Internet attacks and require immediate defensive action.
4	Catastrophic threat. Critical security situations within a network dictate an immediate and focused defensive action. This condition may be imminent or ongoing.



**\* Features available in the Portal are dependent on the MSS Service subscription and device type.**

## Active Tickets & XPS Alerts

Next you will want to focus on Active tickets, X-Force Protection System or XPS Alerts and Vulnerability Management Service or VMS Remediation Tickets (VMS customers only). **Note:** A full list of all active tickets can be accessed via the Ticket Manager dashboard. Clicking, “View All” in any ticket related Portlet will also launch the Ticket Manager Dashboard. There you can modify query criteria to search for tickets.

To view the details click on the desired Ticket ID hypertext. For a summary hover you're the Ticket ID:

The screenshot shows the 'Active Security Incidents (61)' portlet. It contains a table with columns: Ticket ID, Type, Priority, Status, Created, and Last Updated (EST)... A tooltip is displayed over the ticket ID 0700726296, showing the following details:

- Ticket: SOCI00700726296
- Issue: SI Probes and Scans
- Description: QA Test Prod Release
- Attack: Nmap\_OS\_Fingerprint
- Device: DEMO , atl-stg-provsrvr-01 .....
- Src IP: 207.231.140.222
- Src Port:
- Dest IP: 10.200.1.12 , 10.200.1.13 ...
- Dest Port:
- Reason: Test

The Recent XPS Alert Portlet will list new alerts. Clicking on, “View All” will launch the Alert Monitor.

The screenshot shows the 'Recent XPS Alerts (1)' portlet. It contains a table with columns: Alert ID, Created (EST) ▾, Event Names, and Status. The table lists one alert with ID 14249067, created on 11/09/11 at 02:04, with event names N/A and a status icon.

Alert ID	Created (EST) ▾	Event Names	Status
<a href="#">14249067</a>	11/09/11 02:04	N/A	

Displaying last 48 hours

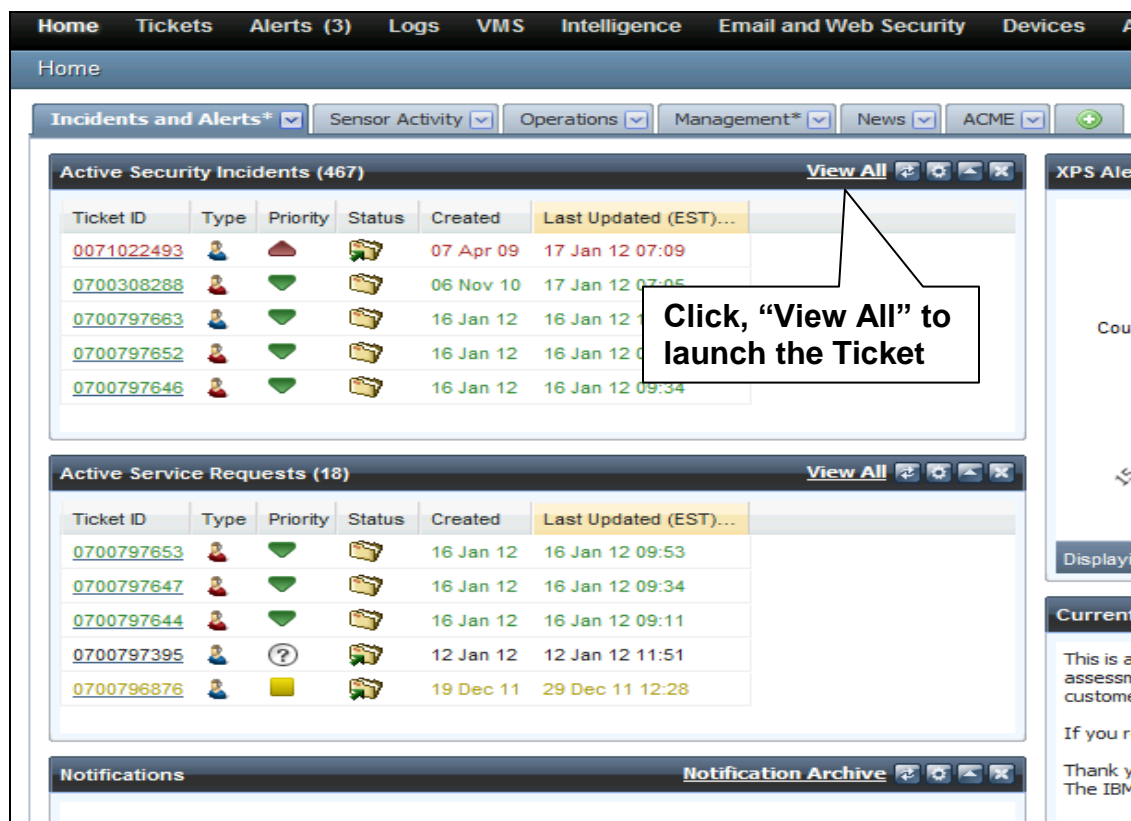
Notice that under ticket “Type”, some tickets have blue user icons while others have red user icons. The ticket color represents whether the ticket is an IBM Security Services SOC ticket or your internal ticket. Blue user icon tickets indicate that some sort of SOC intervention has or will occur. Tickets with red user icons are those worked by your own internal work force and have No SOC intervention whatsoever. **Note:** MSS SOC analysts do not have a view into your grey internal tickets.



Ticket ID	Type	Priority	Status	Created	Last Updated (EST)...
<a href="#">0700726295</a>				11/05/11	11/09/11 13:23
<a href="#">0700726296</a>				11/05/11	11/09/11 13:23
<a href="#">0700726304</a>				11/05/11	11/09/11 13:23
<a href="#">0700726307</a>				11/05/11	11/09/11 13:23
<a href="#">0700308288</a>				11/06/10	11/09/11 07:05

Click this hyperlink for additional information regarding [SOC Communications](#) including tickets. The screenshot below shows the Incidents and Alerts Portlet Dashboard.

**\* Features available in the Portal are dependent on the MSS Service subscription and device type.**



Home Tickets Alerts (3) Logs VMS Intelligence Email and Web Security Devices A

Home

Incidents and Alerts\* Sensor Activity Operations Management\* News ACME

**Active Security Incidents (467)** [View All](#)

Ticket ID	Type	Priority	Status	Created	Last Updated (EST)...
<a href="#">0071022493</a>				07 Apr 09	17 Jan 12 07:09
<a href="#">0700308288</a>				06 Nov 10	17 Jan 12 07:05
<a href="#">0700797663</a>				16 Jan 12	16 Jan 12 09:34
<a href="#">0700797652</a>				16 Jan 12	16 Jan 12 09:34
<a href="#">0700797646</a>				16 Jan 12	16 Jan 12 09:34

Click, “View All” to launch the Ticket

**Active Service Requests (18)** [View All](#)

Ticket ID	Type	Priority	Status	Created	Last Updated (EST)...
<a href="#">0700797653</a>				16 Jan 12	16 Jan 12 09:53
<a href="#">0700797647</a>				16 Jan 12	16 Jan 12 09:34
<a href="#">0700797644</a>				16 Jan 12	16 Jan 12 09:11
<a href="#">0700797395</a>				12 Jan 12	12 Jan 12 11:51
<a href="#">0700796876</a>				19 Dec 11	29 Dec 11 12:28

Notifications [Notification Archive](#)

IBM Content Update XPL 23.010 (09 January 2012)

XPS Alerts

Cour

Displayin

Current

This is a assessm customer

If you re

Thank yo The IBM

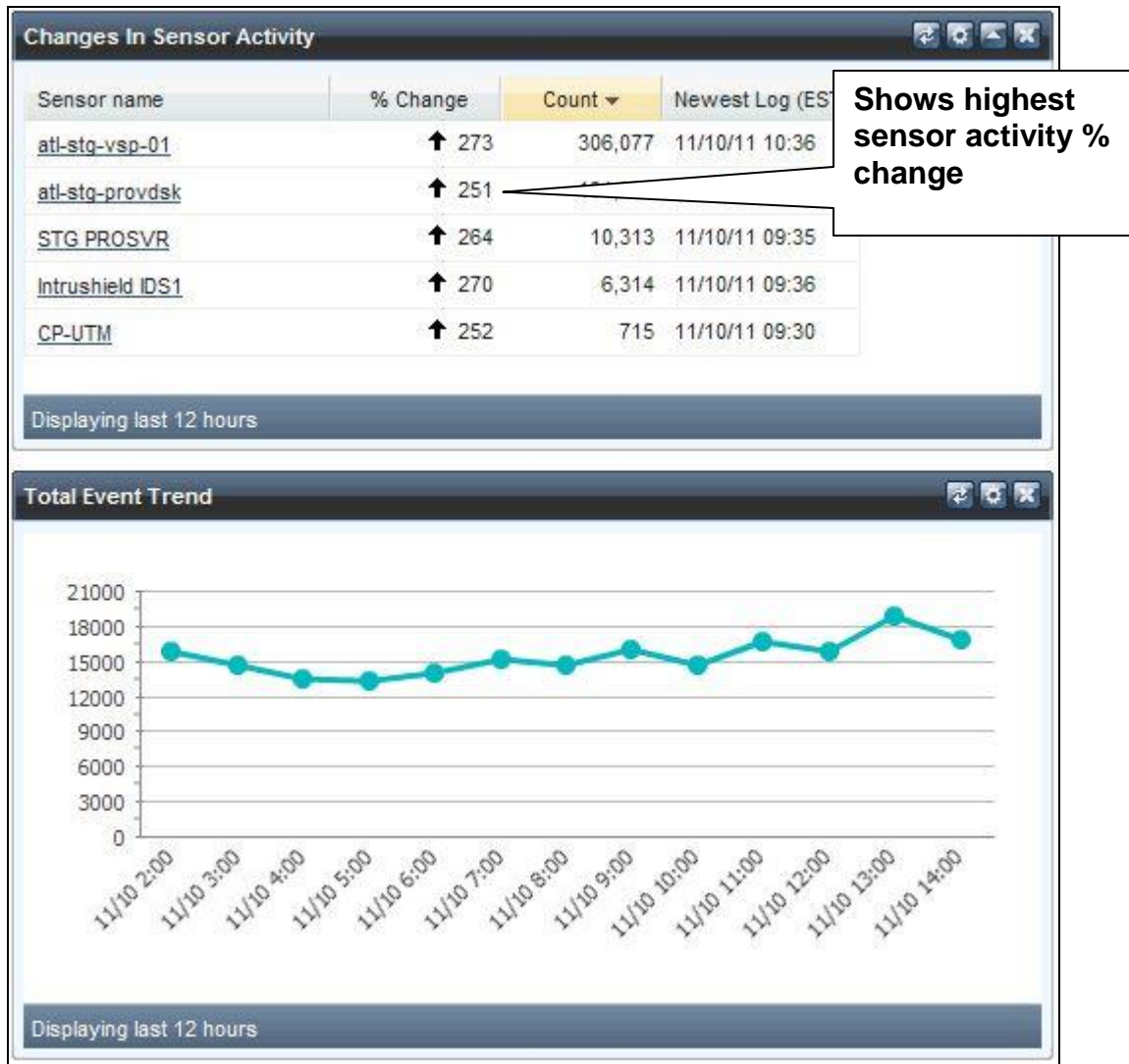


## Event Trends – Quick Glimpse

Next, in the default configuration, the Sensor Activity Portlet Dashboard contains several bar graphs and tables that provide a quick glimpse of your IDPS and Security Event trends. Hover your mouse pointer over to view count information.

Full reports on firewall and IDPS data are available in the Reports section of the portal.

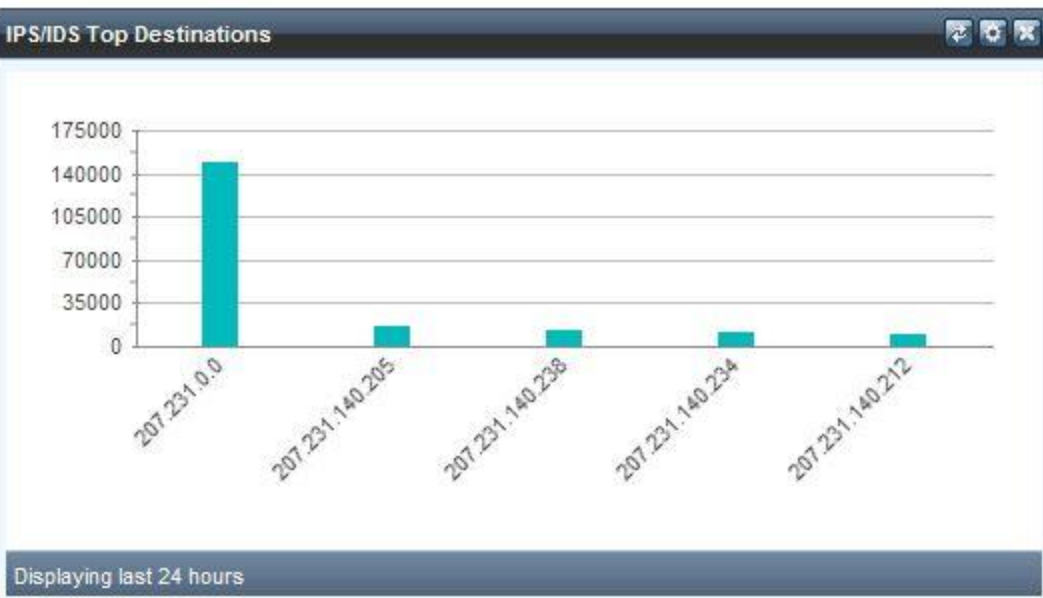
Note: These Portlet reports are designed for quick reference to flag anomalies or suspicious traffic.



Event name	% Total	Count
SSH_Brute_Force	57	449
TCP Control Segment Anomaly	13	105
nbss_decoder: NBSS.Invalid.Fragment	12	98
Inbound TCP SYN or FIN Volume Too ...	5	39
1456: MS-SQL Slammer-Sapphire W...	5	37

Shows most active events and total % amount

Displaying last 7 days







**\* Features available in the portal are dependent on the MSS Service subscription and device type.**

# Suspicious Hosts Dashboard

The Suspicious Hosts Dashboard provides real-time analysis of in and outbound firewall events and IDPS signatures that triggered within this same time period, identifying and tracking activities such as infection attempts.

A Suspicious Host is a public IP address that has been identified to be participating in malicious activities or communicating from vantage points that obfuscate behavior, such as open proxies. The intelligence used to identify this traffic comes from IBM X-Force Research & Development, IP reputation data, and other trusted 3rd parties.

**Please note; if you rearrange your columns you may need to “Reset” your data and then “Apply” your filter / query again.**

**\* Features available in the portal are dependent on the MSS Service subscription and device type. (FW associated service /data is needed to generate the dashboard)**

**Analytics > Suspicious Hosts**

Filters:

Devices: All devices | Direction: All | Firewall action: Accept, Log, Mo | Dest Port: | Source or Dest IP: |

Time Interval: Last 30 days | from Apr 07 2012 | to May 07 2012 | Apply | Reset

% Change	Count	Source IP	Dest IP	Dest Port	Protocol	Device	Site	Action	Last Event (EST)	IPS Severity (H/M/L)	30d FW Trend	Category
1233 ↑	40	207.231.140.183	207.231.140.183	80	TCP	atl-stg-cpfrw-01	Atlanta	Accept	Apr 26 12 14:36	0 / 0 / 0		Botnet
720 ↑	41	106.187.38.250	106.187.38.250	80	TCP	atl-stg-cpfrw-01	Atlanta	Accept	Apr 26 12 14:36	9 / 18 / 8		Botnet
550 ↑	39	207.231.140.11	207.231.140.11	80	TCP	atl-stg-cpfrw-01	Atlanta	Accept	Apr 26 12 14:36	0 / 0 / 0		Botnet
475 ↑	46	207.231.140.78	207.231.140.78	80	TCP	atl-stg-cpfrw-01	Atlanta	Accept	Apr 26 12 14:37	0 / 0 / 0		Botnet
463 ↑	45	182.72.4.108	182.72.4.108	80	TCP	atl-stg-cpfrw-01	Atlanta	Accept	Apr 26 12 14:38	7 / 12 / 8		Botnet
438 ↑	43	112.175.243.22	112.175.243.22	80	TCP	atl-stg-cpfrw-01	Atlanta	Accept	Apr 26 12 14:36	9 / 20 / 14		Botnet
390 ↑	49	207.231.140.171	173.165.98.90	13001	TCP	atl-stg-cpfrw-01	Atlanta	Accept	Apr 26 12 14:37	0 / 0 / 0		Botnet
380 ↑	48	140.174.196.174	207.231.140.78	80	TCP	atl-stg-cpfrw-01	Atlanta	Accept	Apr 26 12 14:37	6 / 9 / 7		Botnet
325 ↑	51	173.165.98.90	207.231.140.171	80	TCP	atl-stg-cpfrw-01	Atlanta	Accept	Apr 26 12 14:37	13 / 30 / 22		Botnet
250 ↑	47	207.231.140.171	207.231.140.171	80	TCP	atl-stg-cpfrw-01	Atlanta	Accept	Apr 26 12 14:36	0 / 0 / 0		Botnet
200 ↑	36	207.231.140.171	207.231.140.171	80	TCP	atl-stg-cpfrw-01	Atlanta	Accept	Apr 26 12 14:36	10 / 19 / 10		Botnet
180 ↑	56	207.231.140.171	207.231.140.171	80	TCP	atl-stg-cpfrw-01	Atlanta	Accept	Apr 26 12 14:39	0 / 0 / 0		Botnet
174 ↑	52	207.231.140.171	207.231.140.171	80	TCP	atl-stg-cpfrw-01	Atlanta	Accept	Apr 26 12 14:37	10 / 29 / 16		Botnet
173 ↑	41	98.222.26.73	207.231.140.24	80	TCP	atl-stg-cpfrw-01	Atlanta	Accept	Apr 26 12 14:39	0 / 0 / 0		Botnet

Displaying 1 - 30 of 44 (Apr 07 2012 through May 07 2012 for All devices)

Page 1 of 2

Additional Suspicious Hosts Dashboard features shown below:

### Filtering options:

The screenshot shows the 'Analytics > Suspicious Hosts' dashboard. The top navigation bar includes links for Home, Tickets, Alerts (196), Logs, VMS, Intelligence, Email and Web Security, Devices, and Analytics. The main section is titled 'Filters' and contains several dropdown menus and input fields. Callouts highlight specific filtering options:

- Filter by Inbound and Outbound traffic:** Points to the 'Direction:' dropdown menu.
- Filter by Specific IP:** Points to the 'Source or Dest IP:' dropdown menu.
- Filter by Specific Date or Time Interval:** Points to the 'Time Interval:' dropdown menu and the date range input fields.

The 'Filters' section includes the following controls:

- Devices:** A dropdown menu currently set to 'All devices'.
- Direction:** A dropdown menu currently set to 'All'.
- Firewall action:** A dropdown menu currently set to 'Accept, Log, Mo'.
- Dest Port:** A dropdown menu.
- Source or Dest IP:** A dropdown menu.
- Time Interval:** A dropdown menu currently set to 'Last 30 days'.
- Date Range:** Input fields for 'from' (Apr 07 2012) and 'to' (May 07 2012).

### Features Highlights:

% Change	Count	Source IP	Dest IP	Dest Port	Last Event (EST)	30d FW Trend	IPS Severity (H/M/L)
New	1	38.229.84.1	atl-stg-srx-01	80	Apr 18 12 08:00		0 / 0 / 0
New	1	atl-stg-srx-01	38.229.84.0	51987	Apr 18 12 08:00		0 / 0 / 0
1233 ↑	40	207.231.140.183	106.187.38.250	1866	Apr 26 12 14:36		0 / 0 / 0
720 ↑	41	106.187.38.2	207.231.140.183	80	Apr 26 12 14:36		9 / 18 / 8
550 ↑	39	207.231.140.183	106.187.38.2	4466	Apr 26 12 14:36		0 / 0 / 0
438 ↑	43	207.231.140.183	106.187.38.2	80	Apr 26 12 14:36		0 / 0 / 0
83 ↑	33	207.231.140.183	106.187.38.2	8680	Apr 26 12 14:36		0 / 0 / 0
95 ↑	37	114.255.96.2	207.231.140.42	80	Apr 26 12 14:36		10 / 16 / 16
250 ↑	49	118.218.219.175	207.231.140.39	80	Apr 26 12 14:36		10 / 19 / 10
292 ↑	47	207.231.140.39	118.218.219.175	31337	Apr 26 12 14:36		0 / 0 / 0
167 ↑	47	207.231.140.39	118.218.219.175	31337	Apr 26 12 14:36		0 / 0 / 0
141 ↑	47	207.231.140.39	118.218.219.175	31337	Apr 26 12 14:36		11 / 26 / 17
-13 ↓	47	207.231.140.39	118.218.219.175	31337	Apr 26 12 14:36		0 / 0 / 0
0	31	123.212.193.88	207.231.140.194	80	Apr 26 12 14:36		11 / 32 / 18

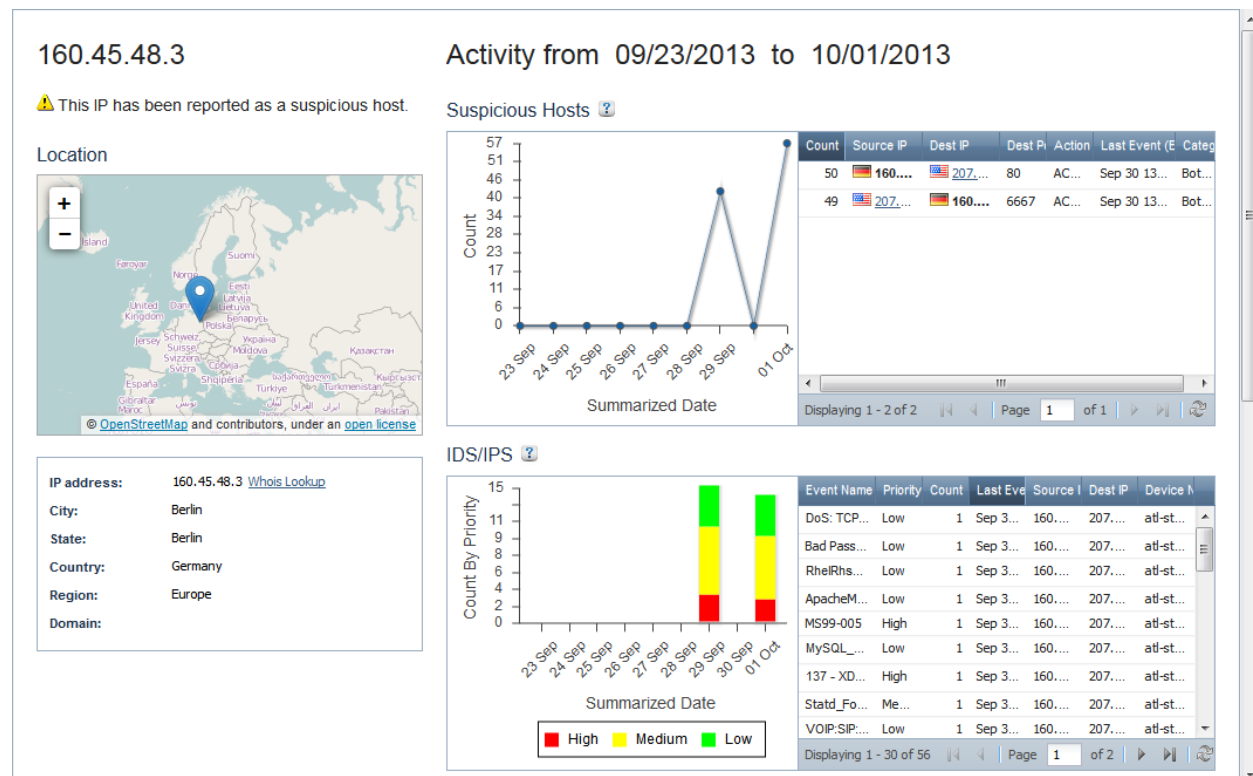
Callouts highlight specific features in the table:

- Source and Destination IPs:** Points to the 'Source IP' and 'Dest IP' columns.
- Last Event:** Points to the 'Last Event (EST)' column.
- IDPS Event Summary:** Points to the 'IPS Severity (H/M/L)' column.
- Geographic Location:** Points to the flag icons next to the IP addresses.
- 30 Day FW Sparkline Trend:** Points to the '30d FW Trend' column.

# IP Intelligence Reporting Feature

The IP Intelligence Report expands on the Suspicious Hosts Dashboard, providing an even deeper analysis of individual IP addresses, including their Geo-IP location and whois information, and correlation of firewall events (Suspicious Hosts), IDPS events, asset intelligence, vulnerability scan results and associated tickets.

Access to the IP Intelligence Report has also been made easy via shortcuts embedded throughout the Portal. The most common access points to the IP Intelligence report are through the Suspicious Hosts Dashboard, Log Query and Security Event Monitor.



# Device Manager

Device Manager provides an interface to view and edit device details and can be found under the “Device” menu. A listing of associated active tickets, group membership, and device information can be found for each device by clicking on the “+” icon next to the desired device.

Home Tickets Alerts (57) Logs VMS Intelligence Email and Web Security Devices Analytics Reports Support									
Devices > Device Manager									
View By: <span>All Devices</span> <a href="#">Edit Device Groups</a>									
	Managed By	Application	Site	Machine Host Name	Customer Device Name	Platform	Status	Newest Log	Tickets
+	SOC	Anti-Virus / Firewall / ...	Atlanta	atl-lab-pafw 1	atl-lab-pafw 1	PA-4020	Agent is healthy	05 Feb 12 20:59:59 EST	12
+	SOC	IDS	Main Office	atl-stg-provsvr-01	STG PROSVR	Generic IBM Server	Agent is healthy	06 Feb 12 09:59:59 EST	23
+	SOC	IDS	Atlanta	atl-stg-g400-01a	Demo G400	ISS Proventia G400	Agent is healthy	06 Feb 12 10:59:59 EST	16
+	Customer	IDS	Atlanta	atla-sp-ec7a		System x3250	Agent is healthy		9
+	Customer	IDS	Atlanta	atl-stg-sf-01		Sourcefire Sensor IS...	⚠ No recent logs from device (58 d)	09 Dec 11 13:59:59 EST	11
+	SOC	IDS / System Activity	Atlanta	atl-stg-vsp-01	atl-stg-vsp-01	Generic IBM Server	Agent is healthy	07 Jan 12 21:59:59 EST	19
+	SOC	Firewall / IDS	Main Office	atl-stg-asa-01a		Cisco ASA 5510	Agent is healthy	09 Dec 11 13:59:59 EST	22
+	SOC	Anti-Spam / Anti-Viru...	Atlanta	atl-stg-mx-01	atl-stg-mx-01	ISS Proventia MX3006	Agent is healthy (175 d)	06 Feb 12 10:59:59 EST	16
+	SOC	Firewall / IDS	Atlanta	atl-stg-srx-01		Juniper SRX 210	Agent is healthy (63 d)	06 Feb 12 10:59:59 EST	12
+	Customer		UNKNOWN	host-207.231.140.62	SELM Server S	Other	Agent is healthy	04 Feb 12 06:59:59 EST	5
+	SOC	Firewall	Atlanta	atl-stg-ns204-01a	bla3	NetScreen 200	Agent is healthy	06 Feb 12 10:59:59 EST	11
+	Customer	Firewall	Atlanta	atl-stg-ssg-01		NetScreen SSG 5	Agent is healthy	06 Feb 12 10:59:59 EST	11
+	SOC	IDS	Main Office	atla-lab-lp-sensor		TP-50	⚠ Host unreachable (2 d) ⚠ No recent logs from device (35 d)	09 Dec 11 13:59:59 EST	7
+	SOC	IDS	Southfield	DEMO	atl-stg-provdsk	Generic Intel	Agent is healthy	06 Feb 12 09:59:59 EST	16
+	Customer	System Activity / ULA	Atlanta	atl-stg-linux-ula-2	atl-stg-linux-ula-02	Generic Intel	Agent is healthy (82 d)	06 Feb 12 10:59:59 EST	18
+	Customer	Management Platform	Atlanta	demo-atla-us-junosp...		Generic Intel	Agent is healthy		7
+	SOC	Anti-Spam / Anti-Viru...	Atlanta	atl-stg-ftg-01a		Fortigate-100A	Agent is healthy	06 Feb 12 10:59:59 EST	18
+	Customer	IDS	Atlanta	atl-stg-mids-01a		ISS Proventia A201	Agent is healthy (175 d)	20 Jan 12 01:59:59 EST	15
+	Customer		UNKNOWN	host-207.231.140.63		Other	Agent is healthy	16 Jan 12 04:59:59 EST	5
+	SOC	Anti-Spam / Anti-Viru...	Atlanta	atl-stg-cpfw-01	CP-UTM	CP UTM-1 270	Agent is healthy (2 h)	06 Feb 12 10:59:59 EST	10
+	Customer	System Activity / ULA	UNKNOWN	IBM-47C24445683		Other	⚠ No recent logs from device (20 d) Agent is healthy (27 d)	10 Jan 12 22:59:59 EST	9
+	Customer	System Activity / ULA	Atlanta	atl-stg-win-ula-01	demo ula	Generic Intel	⚠ Agent queue at capacity (1 h)	06 Feb 12 10:14:41 EST	8
+	Customer	Log Aggregator	Main Office	atl-stg-oademo-01		System x3250	Agent is healthy	06 Feb 12 10:14:35 EST	8
+	SOC	Firewall	Atlanta	atl-stg-isr-01a		Cisco ISR 1841	Agent is healthy	06 Feb 12 10:59:59 EST	20
Displaying 1 - 25 of 25									

## Interface Enhancements

New enhancements provide a faster and more scalable user interface. You have the ability to customize most of your views.

Home Tickets Alerts Logs VMS Intelligence Devices Analytics Reports Support

Devices > Device Manager

View By: All Devices [Edit Device Groups](#)

Managed By	Application	Site	Machine Host Name	Customer Device Name	Platform	Status
Customer		Snakes	Sort Ascending Sort Descending	Test the cache again	Generic Intel	Agent is healthy
<b>Details</b> Tickets						
<b>Service Type:</b> Customer Enablement						
<b>Service Level:</b> SELM Server Select						
<b>Site:</b> Snakes						
<b>Platform Information</b>						
<b>Platform:</b> Generic Intel						
<b>Operating System:</b> VMware ESXi						
<b>Timezone:</b>						
<b>Customer System Notes</b>						
test						
QA						
SOC	IDS	Snakes	cisco-ids-stageb	Cisco IDS StageB	Cisco 4215	Agent is healthy
Customer		Snakes	cache_test	another cache test	Generic Intel	Agent is healthy

- ☒ Machine Host Name
- ☒ Managed By
- ☒ Application
- ☒ Site
- ☒ Machine Host Name
- ☒ Customer Device Name
- ☒ Platform
- ☒ Status
- ☒ Newest Log
- ☒ Tickets

**\* Features available in the Portal are dependent on the MSS Service subscription and device type.**

## Device Details

Device Manager contains context based menus that allow you to view and in some cases, edit the device details, such as defining any protected critical servers and monitored networks. You can also view health charts, XPS Alert Policy Editor, IDPS policy, and Firewall policy. IDPS and Firewall Policy options reflect any tuning and/or policy changes performed by the Security Operations Center. The context based menus can be located by right-clicking on the name of the device. You also have access to a troubleshooting guide within the Media Library or within the Details menu under the “Device Status” field.

Devices > Device Manager

View By:  [Edit Device Groups](#)

Managed By	Application	Site	Machine Host Name	Customer Device Name	Platform	Status	Newest Log
SOC	Anti-Spam / Anti-Viru...	Atlanta	atl-stg-flg-01a		Fortigate-100A	Agent is healthy	06 Feb 12 10:59
Customer	IDS	Atlanta	atl-stg-mids-01a		ISS Proventia A201	Agent is healthy (175 d)	20 Jan 12 01:59
Customer		UNKNOWN	host-207.231.140.63		Other	Agent is healthy	16 Jan 12 04:59
SOC	Anti-Spam / Anti-Viru...	Atlanta	atl-stg-cpfw-01	CP-UTM	CP UTM-1 270	Agent is healthy (2 h)	06 Feb 12 10:59
Customer	System Activity / ULA	UNKNOWN	IBM-47C24445683		Other	No recent logs from device (20 d) Agent is healthy	10 Jan 12 22:59
Customer	System Activity / ULA	Atlanta	atl-stg-win-ula-01	demo ula	Generic Intel	Agent queue	
Customer	Log Aggregator	Main Office	atl-stg-oademo-01		System x3250	Agent is healthy	

**Details** Applications Tickets

**Service Type:** Managed **IP Address:** 207.231.140.225 **Machine Host:** atl-stg-oademo-01

**Service Level:** SELM - Onsite Aggregator Management **Physical IP Address:**  **Customer Device Name:**

**Site:** Main Office **Serial Number:**  **Partner Device Name:**

**Platform Information**

**Platform:** System x3250 **Operating System:** RHEL 5.3 Server\_32bit **Timezone:** (GMT) Greenwich Mean Time

**Logs**

**Log Storage Used:** 6.95 KB **Oldest Log:** 05 Feb 11 19:00:00 EST **Newest Log:** 06 Feb 12 10:14:35 EST **Log Retention Period:** One Year

**Device Status**

[SELM Troubleshooting Guide](#)

Agent is healthy

**Customer System Notes**

**Group Membership**

## Device Groups

Custom device groups can be created by clicking on the Edit Device Groups option located on the Device Manager page. Custom groups can be created in order to set up granular user permissions or for running custom reports and queries. Once you have defined your customer group click submit to save.

### Custom Device Groups Management

[\[PRINT\]](#) [\[CLOSE\]](#)

Select Custom Device Group

Group Name	# Dev.	
<a href="#">ATT-GM</a>	2	
<a href="#">bbw-test</a>	3	
<a href="#">billy</a>	1	
<a href="#">Branch View</a>	1	
<a href="#">Bridget Group</a>	6	
<a href="#">bridget-test</a>	5	
<a href="#">Checkpoint-Group</a>	1	
<a href="#">Chris Group</a>	3	
<a href="#">Cisco-Netscreen</a>	2	
<a href="#">CNTesGroup</a>	2	
<a href="#">Correlated Events</a>	8	
<a href="#">COTestGroup</a>	1	
<a href="#">Custom Group A</a>	2	
<a href="#">Custom Group B</a>	1	
<a href="#">Custom Group C</a>	2	
<a href="#">Demo</a>	3	

Add/Modify Device Group

---

Device Group Details

Group Name:   
Group Description:

Grouped Devices Assignment

Show the following device types:  
☒Firewall ☒IDS/IPS ☒Desktop Group ☒ULA ☒Log Aggregator ☒Vulnerability Scanner ☒Multi-Function

All Devices

Aggregator - SFLD#1 [LA]  
atl-stg-oademo-01 [LA]  
atl-stg-prosvr-01 [IDS/IPS]  
atl-stg-ssg-01 [FW]  
atla-lab-demo-0a [LA]  
Cisco ASA: 12.173.210.37 [Multi]  
Cisco IDS [IDS/IPS]

>>>

>

<

<<<

Devices in Group

Submit

Reset

Add Critical Assets and Monitored Networks by Right Clicking on the Host Name and selecting Device Details:

<a href="#">Home</a> <a href="#">Tickets</a> <a href="#">Alerts (196)</a> <a href="#">Logs</a> <a href="#">VMS</a> <a href="#">Intelligence</a> <a href="#">Email and Web Security</a> <a href="#">Devices</a> <a href="#">Analytics</a>					
Devices > Device Manager <a href="#">?</a>					
View By: <span>All Devices</span>		<a href="#">Edit Device Groups</a>			
	Managed By	Application	Site	Machine Host Name	Customer Device Name
	SOC	Anti-Virus / Firewall /...	Atlanta	atl-lab-pafw1	atl-lab-pafw1
	SOC	IDS	Main Office	atl-stg-prosvr-01	STG PROSVR
	SOC	IDS	Atlanta	atl-stg-g400-01a	Demo G400
	SOC	IDS	Atlanta	atla-sp-ec7a	
	SOC	IDS	Juneau	atl-stg-sf-01	
	Customer	IDS / System Activity	Atlanta	atl-stg-vsp-01	atl-stg-vsp-01
	SOC	Firewall / IDS	Main Office	atl-stg-asa-01a	
	SOC	Anti-Spam / Anti-Viru...	Atlanta	atl-lab-fg100a	atl-lab-fg100a
	SOC	Anti-Spam / Anti-Viru...	Atlanta	atl-stg-mx-01	atl-stg-mx-01
	SOC	Anti-Spam / Anti-Viru...	Atlanta	atl-stg-mx-01	
	Customer		UNKNOWN	host-	
	SOC	Firewall	Atlanta	atl-stg-	
	SOC	Firewall	Atlanta	atl-stg-	
	Customer	IDS	Southfield	DEMO	
	SOC	IDS	Main Office	atla-lab-	
	Customer	System Activity / ULA	Atlanta	atl-stg-mux-0a-z	atl-stg-mux-0a-z

View Device Details

View IDS Policy

View Firewall Policy

SOC Event Monitoring Scheduling

XPS Alert Policy Editor



Device Details

[\[PRINT\]](#)
[\[CLOSE\]](#)

Device Details

Machine Host Name: atl-stg-srx-01
Customer Device Name: atl-stg-srx-01

Virtual Security Operations Center - - Mozilla Firefox

iss.net
https://portal.mss.iss.net/mss/criticalServerDetails.mss?devicename=atl-stg-srx-01

Virtual Security Operations Center

[\[PRINT\]](#)
[\[CLOSE\]](#)

Server Name:
Platform:

IP Address:
OS:

IDS Detector Name: atl-stg-srx-01
Monitored Network:

Proxy Server: Yes

Applications:
Ports:

Save Critical Server

Click to add Critical Server (Opens in separate window)

Protected Critical Servers

No critical servers found for this IDS device([Add a critical server](#))

Monitored Networks

No monitored networks found for this IDS device ([Add a Monitored Network](#))

**\* Features available in the Portal are dependent on the MSS Service subscription and device type.**

## ULA Software

This page can be used to obtain the binary distributions of the ULA software (SELM customers only). There are installers for AIX, Windows, HP-UX (ia64 & PA-RISC), Linux and Solaris.

\* ULA installation instructions can be accessed from the Media Library.

Home Tickets Alerts (3) Logs VMS Intelligence Email and Web Security Devices Analytics Reports Support

Devices > ULA Software

Device Manager  
ULA Software

Package	Package
<a href="#">mss-ula-install.aix.bin</a>	aix
<a href="#">mss-ula-installer.exe</a>	windows
<a href="#">mss-ula-install.hpux-ia64.bin</a>	hpux
<a href="#">mss-ula-install.hpux-parisc.bin</a>	hpux
<a href="#">mss-ula-install.linux.bin</a>	linux
<a href="#">mss-ula-install.solaris.bin</a>	solaris

Copyright © 2012 IBM Corporation Privacy Terms of use 01/17/12 14:00 EST - 01/17/12 19:00 GMT

# Asset Center

The Asset Center is a repository that facilitates management of information about critical assets that are not managed by IBM Security Services. This tool gives customers a way to upload or manually enter critical server and device information, and upload third-party vulnerability scan data, which can be used in the correlation and reporting capabilities of the X-Force Protection System (XPS).

## Essential Features

- Manual upload of asset details and vulnerability scan results (CSV file)  
**Note:** This feature supports IBM Hosted Vulnerability Management Service (VMS), as well as third-party scan data.
- Critical server administration; integration with correlation and reporting capabilities
- Advanced filtering and single-click access to IP reputation and profiling reports

**Note:** For more details about Asset Center features, refer to the Asset Center Quick Reference Guide, which is available in the Portal [Media Library](#).

## Getting Started

Open your web browser and browse to the following URL: <https://portal.mss.iss.net>

After logging into the portal, you can access the Asset Center from the “Devices” menu.

The screenshot displays the IBM Security Services Portal interface. The top navigation bar includes links for Home, Tickets, Alerts (765), Logs, VMS, Intelligence, Devices, Analytics, Reports, and Support. The 'Devices' menu is expanded, showing options like Device Manager, ULA Software, and Asset Center, with a red arrow pointing to 'Asset Center'. Below the navigation bar, the 'Assets' tab is selected, showing a table of assets with columns for Validated, Host Name, MAC Address, and IP Address. The table lists four assets: www-nyc.iss.net, www-atl.iss.net, app-atl.iss.net, and www-chi.iss.net. Above the table, there are filters for IP Address, Host Name, Sites, Business units, Last updated, and Groups.

Validated	Host Name	MAC Address	IP Address
✓	www-nyc.iss.net	11:22:88:77:33:44	<a href="#">134.19.41.211</a>
✓	www-atl.iss.net	23:60:7b:be:96:d9	<a href="#">216.185.126.125</a>
	app-atl.iss.net	11:55:44:44:66:22	<a href="#">100.45.88.10</a>
✓	www-chi.iss.net	1d:77:66:23:9e:58	<a href="#">5.5.5.5</a>

**Note:** Customers who subscribe to Hosted Vulnerability Management Services will find their asset details have automatically populated the Asset Center.

## Adding or Editing an Asset

To add an individual asset, click the “Add” icon. To edit an asset, select the asset and click the “Edit” icon. You also can right click the asset and select the “Edit” option.

Devices > Asset Center ?

Assets Networks Acceptable Traffic

Filters

IP Address: IP/CIDR Host Name: Sites: All Business units: All

Last updated: Last 30 days from Aug 24 2013 to Sep 23 2013 Groups: All

Validate Edit... Delete Add... Import... Export...

Validated	Host Name	MAC Address	IP Address
✓	www-nyc.iss.net	11:22:88:77:33:44	<a href="#">134.19.41.211</a>
✓	www-atl.iss.net	23:60:7b:be:96:d9	<a href="#">216.185.126.125</a>
	app-atl.iss.net	11:55:44:44:66:22	<a href="#">100.45.88.10</a>
✓	www-chi.iss.net	1d:77:66:23:9e:58	<a href="#">5.5.5.5</a>

Validate Edit... Delete

## Exporting Assets

The Asset Center allows you to export asset information to a CSV file. Click the “Export” icon to download a CSV file that includes the current data set.

Devices > Asset Center ?

Assets Networks Acceptable Traffic

Filters

IP Address: IP/CIDR Host Name: Sites: All

Last updated: Any time from to

Validate Edit... Delete Add... Import... Export...

Validated Host Name MAC Address

**Note:** The exported data set is based on your asset filter settings. Be sure to configure filters appropriately before exporting asset data.

---

# Vulnerability Manager

Vulnerability Manager is located under the VMS menu, and is available to those customers subscribing to the Vulnerability Management Service ("VMS"). The Hosted Vulnerability Management Service (VMS) is a vulnerability scanning service that provides the tools required to support a range of needs, including internal audit and risk assessment, regulatory compliance, and industry compliance requirements. VMS includes a comprehensive suite of functionality, including certified Payment Card Industry (PCI) approved scanning vendor reports. The PCI Approved Scanning Vendor (ASV) service is included for IBM Enterprise VMS customers via a separate tool.

**Note:** For the ASV service tool, scan source IP addresses will be different than those used for the Enterprise VMS tool, and scan results might differ slightly from Enterprise VMS scans. Consequently, the ASV service tool must be enabled and configured separately by IBM MSS. Please work with the SOC to enable the ASV service.

IBM provides VMS as a solution to be operated by you and will provide the scanning application and technical support for the application from the services. VMS is provided in two distinct types of scanning, external and internal, which can be employed together or separately.

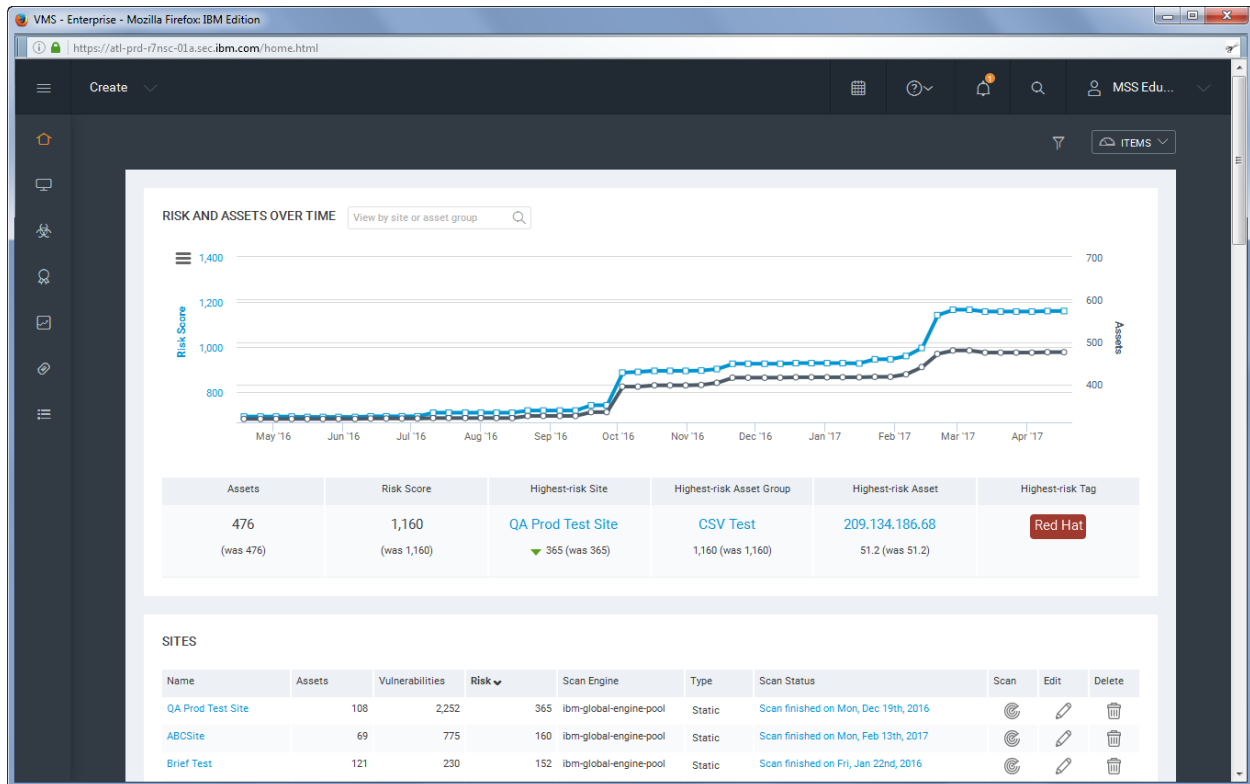
External - IBM hosts and manages vulnerability scanners on the Internet. These groups of scanners are known as the IBM Global Scan Pool. External scan engines detect security risk exposures open to the Internet, and thus focus on scanning your public-facing IP addresses and web applications.

Internal - IBM also supports scanning within your enterprise network, using an IBM-managed, on-premises scanning device (called a "scan engine"). These are dedicated engines and cannot be used for any other purpose while under IBM management. They are accessible only via the MSS virtual SOC Portal interface.

This unified vulnerability solution scans your networks to identify assets, and probe for vulnerabilities. The vulnerability checks in VMS identify several sources of security weakness, including operating systems, databases, network protocols, and applications. VMS can even detect some malicious programs and worms, identify areas in your infrastructure that may be at risk for an attack, and with additional access, verify patch updates and security compliance measures.

VMS generates scan data for analysis directly in the Portal interface, where you also have access to customizable reports to facilitate risk assessment and asset remediation. VMS reports are available in multiple formats, and they allow you to filter scan data by vulnerability category and severity, as well as by site, asset group, or specific range and type of assets.

## The VMS Console:



**\* For more VMS information, please access the Help option available from the question mark drop-down menu in the VMS Console.**

# Tickets and Incidents

## Ticket Manager – Security & Service Related Tickets

The Ticket Manager provides an interface to view all of your tickets, which includes Security Incidents, Internal Security Incidents, Service Requests, Policy Change Requests, VMS Remediation tickets (VMS customers only) and Commented Security Investigations. Columns are sortable.

All tickets are available in the Portal for up to one year.

Enhanced filtering and querying options allow you to search by device, issue type, status, event name, and source and / or destination IP. You can also query by last updated dates.

**\*Note:** IBM SOC analysts have no visibility of your internal tickets.

The screenshot shows the Ticket Manager interface. At the top is a navigation bar with links: Home, Tickets, Alerts (402), Logs, VMS, Intelligence, Devices, and Analytics. Below this is a breadcrumb trail: Tickets > Ticket Manager. A 'Filters' section contains dropdowns for 'Devices' (set to 'All'), 'Issue Types' (showing '1 type(s), 7 issue(s)...'), and 'Statuses' (showing 'New, Assigned'). There is also a 'Last Updated' section with a date range from 'Aug 05 2012' to 'Aug 12 2012'. Below the filters is a table of tickets with columns: Ticket ID, Managed By, Created (GMT), Issue Type, and Issue. The first row is expanded, showing details for ticket 0701144701. The details are organized into three columns: Device(s), Source IP(s), and Destination IP(s). Under Device(s), there are links for 'atl-stq-q400-01a' and 'atl-stq-ishield-01a'. Under Source IP(s), there is a link for '207.231.140.62'. Under Destination IP(s), there is a link for '207.231.140.81'. Below these are sections for Event Name(s), Source Port(s), and Destination Port(s). Under Event Name(s), there are links for 'NMAP: XMAS Probe', 'Nmap\_OS\_Fingerprint', and 'TCP: Fingerprinting NM...'. A context menu is open over the 'NMAP: XMAS Probe' link, showing options: 'View security information', 'View IDS/IPS logs for this event', 'What are the sources of this event?', 'What are the destinations of this event?', and 'Which sensors detected this event?'. At the bottom of the table, two more tickets are visible: 0701144710 and 0701144791, both managed by SOC.

Ticket ID	Managed By	Created (GMT)	Issue Type	Issue
0701144701	SOC	Aug 11 12 13:24	Security Incident	Probes
0701144710	SOC			Probes
0701144791	SOC			Maliciou

Enhanced filtering options including; issue types, statuses, priorities, dates and IP addresses

Quick access to ticket details by expanding the “+” icon on the left side

Quick view access to Event details (of ticket details)

Priorities:

X

All

Ticket ID:

Enter part or all..

Names:

Source IP:

Destination IP:

Apply

Reset

**Hover over feature pop ups will provide a summary of the most recent worklog entry**

Latest Worklog						Rating	Last Updated (GMT) ▾	Contact Name	Status	Priority	Report
Event Name	Source	Destination	Earliest	Latest	Nmap_OS_Fingerprint...	★★★★☆✎	Aug 12 12 23:18		Assigned	Low	

tion:

Latest Worklog:

**Ticket rating system to provide feedback and track satisfaction with ticket handling (To add a comment click on the “pencil icon” feedback will be monitored by the SOC to ensure customer satisfaction)**

**Quick access to  
worklog  
information (Click  
“Add” to update)**

Event Name	Source	Destination	Earliest	Latest	HTTP_Unix_Password...	★★★★★	Aug 12 12 23:18	Assigned	Low	
Event Name	Source	Destination	Earliest	Latest	SQL_Injection 78.31....	★★★★★	Aug 12 12 23:18	Assigned	Low	



## Ticket templates:

The screenshot displays the VSOC Portal interface. The top navigation bar includes links for Home, Tickets, Alerts (724), Logs, VMS, Intelligence, Devices, Analytics, and Reports. The 'Tickets' dropdown menu is open, showing a list of templates: Ticket Manager, VMS Enterprise Tickets, VMS PCI Tickets, Compromised Host/Network Incident, Firewall Policy Request, IDS Signature Change, IPS Host/Network Block/White List, General Policy Request, Porta/VMS/SELM Incident, VPN/Connectivity Incident, Other Service Request, Internal Security Incident, Internal Ticket, and Acceptable Traffic. A callout box points to this list with the text: "Multiple templates for more efficient and effective ticket handling".

Below the dropdown, the main content area shows a table of tickets. The table has columns for Ticket ID, Status, Issue Type, and Date/Time. The first few rows show tickets with status 'Outage' and issue types like 'Outage' and 'Security Incident'.

Ticket ID	Status	Issue Type	Date/Time
0701783113	Outage	Security Incident	Oct 01 13 09:21
0701697855	Outage	Outage	Aug 10 13 11:55
0701719415	Outage	Outage	Aug 21 13 10:48

*\* Features available in the Portal are dependent on the MSS Service subscription and device type.*

# Ticket Manager – Ticket Details

If you were to click on a ticket ID from either a Home Dashboard or the Ticket Manager, a window such as the following will pop up which includes all the details provided in the ticket:

Virtual Security Operations Center

IBM

Ticket Details

[PRINT] [CLOSE]

NewAssignedWork in ProgressPendingResolved, Pending ClosureClosed

Ticket DetailsCustomer Ticket Details

Service TicketSave

Ticket Number:0700016757

Rating:☆☆☆☆☆

Created On:08/08/13 15:10

Last Modified On:10/01/13 09:52

File Attachments:0files

Attach a file

Status:Work In Progress

Resolution:N/A

Priority:Medium

Requested Implementation Time:at

Notification Status:No

Modify Notifications

Issue DetailsResearch

Reason for Escalation:

A SQL Injection attack involving a defined critical asset has occurred. SQL Injection attacks are potentially dangerous when they are used to gather confidential information from a back end database or are used to modify contents within a database.

A common reason for this type of activity is:

- modification of data to allow additional attacks or compromises
- extraction of confidential information
- a penetration test / security audit
- a false positive involving a web server which is coded in ways that mimic SQL injection activity.

Issue Code:

SI Probes and Scans

Device Name:

cert-q200 (Proventia - G 3rd floor)

Attack Name:

HTTP\_GET\_SQL\_UnionSelect

Src. IP:

12.173.210.9

Dest. IP:

12.173.210.3

Src. Port:

Dest. Port:

Critical Server Src. IP:

IP Included In Critical Server List

Critical Server Dest. IP:

IP Not Included In Critical Server List

Source IP Block Owner:

OrgName: INTERNET SECURITY SYSTEMS

OrgID: ISS-100

Address: 25400 DENSO DR

City: SOUTHFIELD

Destination IP Block Owner:

OrgName: INTERNET SECURITY SYSTEMS

OrgID: ISS-100

Address: 25400 DENSO DR

City: SOUTHFIELD

SOC Actions Taken:

asdf

Recommended Customer Actions:

If the source is internal:

- Is the source an authorized scanner? If so, we recommend creating a filter for this type of activity for the specific host.

Raw Event Data:

SourceUtlp=209.134.191.85

AlertFormatVersion=85

AlertNameType=5

AlertName=HTTP\_GET\_SQL\_UnionSelect

Worklog:

1 worklog entries (show all)

Add a worklog entry

submitted by ati-prd-webapp-02b

Ticket updated via SOC Console by user: twallace

Event Name Source Destination Earliest Latest

HTTP\_GET\_SQL\_UnionSelect 12.173.210.9 12.173.210.3 Mon Apr 12 13:16:54 GMT 2010 Mon Apr 12 13:47:15 GMT 2010

Chat Transcripts

Contact NameStart TimeEnd Time

No items match your request.

Copyright © 2010 IBM CorporationPrivacyTerms of use

© Copyright IBM Corporation 2006, 2008, 2010, 2013, 2014, 2015

VSOC Portal User Guide  
Page 42 of 71

## Ticket Manager Reports – Policy Change Request

Below is an example of a firewall policy change request report. You will see similar data after clicking on the report icon for a policy change request ticket. Reports are also available for Security Incidents.

**Ticket Details** [\[PRINT\]](#) [\[CLOSE\]](#)

NewAssignedWork in ProgressPendingResolved, Pending ClosureClosed

Ticket DetailsCustomer Ticket Details

Service Ticket

Chat OnlineSave

Ticket Number:	0700720447	Status:	Resolved, Pending Closure
Created On:	11/01/11 11:27	Resolution:	PCR - Completed
Last Modified On:	11/10/11 08:24	Priority:	Medium
File Attachments:	0 files <a href="#">Attach a file</a>	Notification Status:	No <a href="#">Modify Notifications</a>

Issue Details

Issue Code:	PCR - Change Policy
Device Name:	<a href="#">atl-stg-provsrv-01</a> (STG PROSVR)
Description :	test test
Src. IP:	
Dest. IP:	
Worklog:	4 worklog entries ( <a href="#">show all</a> ) <a href="#">Add a worklog entry</a> 11/10/2011, 13:24:14 GMT: submitted by torresa PCR Email sent to leandroj@br.ibm.com;  A report of Policy Change Request SOCJ00700720447 is presented below. If you have any question or concerns, please contact your Security Operations Center (SOC) and reference the ticket number provided.  Policy Change Request =====

Policy Change Request Number: SOCJ00700720447  
Customer Name: Demo Customer  
Contact: Leandro Jordino  
Status: Resolved, Pending Closure

## Submit a Policy Change Request

The options to submit a Policy Change Request (PCR) are located under the Tickets menu. Select the appropriate PCR template for your device type. (Firewall or IDPS)

First, select a device, or device group for the change to be applied to by clicking on, "Select Devices." Next, provide the change details in the fields provided.

This screenshot shows the 'Firewall Policy Request' form with four callout boxes indicating the first four steps of the process:

- Step 1: Select PCR implementation time** points to the 'Requested implementation time' dropdown menu.
- Step 2: Add the affected devices** points to the 'Add Devices...' button in the 'Device(s)' section.
- Step 3: Select applicable action and interface** points to the 'Action' dropdown (set to 'Allow') and the 'Apply to interface' radio buttons (set to 'Inbound').
- Step 4: Complete source and destination information** points to the 'Sources' and 'Destinations' input fields.

The form includes a top navigation bar with links like Home, Tickets, Alerts (721), Logs, VMS, Intelligence, Devices, Analytics, Reports, Support, and More. A search bar is located in the top right corner.

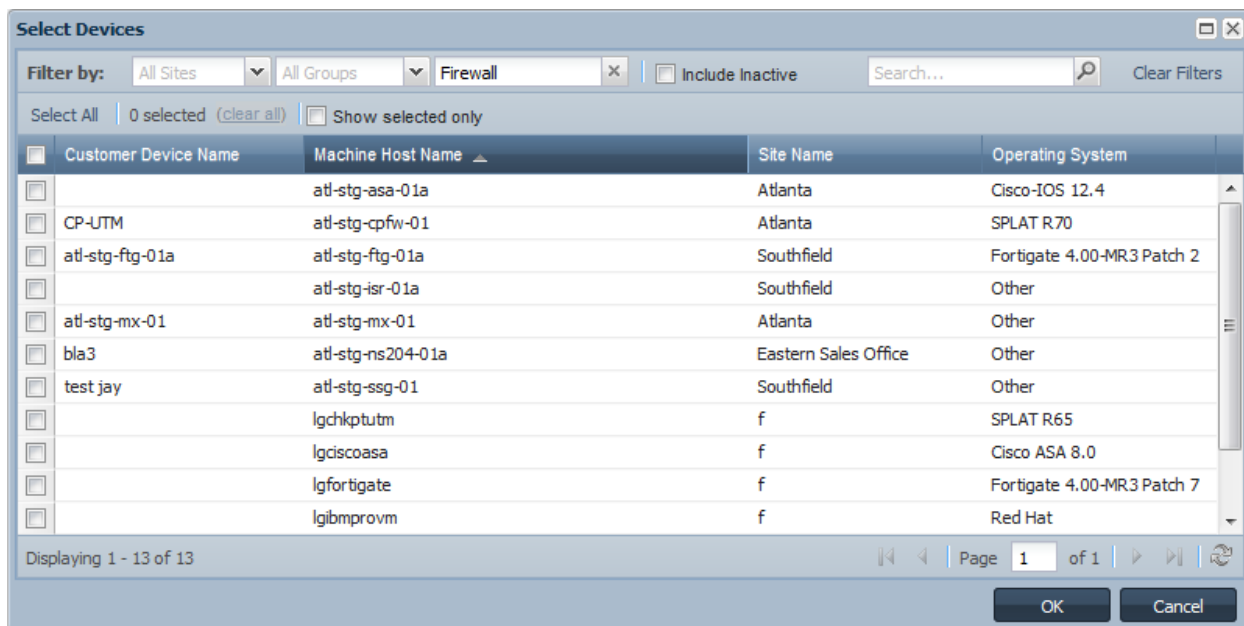
This screenshot shows the lower portion of the 'Firewall Policy Request' form with three callout boxes indicating the final steps:

- Step 5: Select applicable service** points to the 'Protocol/Service' dropdown menu (set to 'TCP/IP').
- Step 6: Add any special instructions in the notes field** points to the 'Notes' text area.
- Step 7: Attach file if applicable and submit change** points to the 'File attachment' section, which includes a 'Browse...' button and a note: 'Please note, the maximum size for file upload is 5MB.'

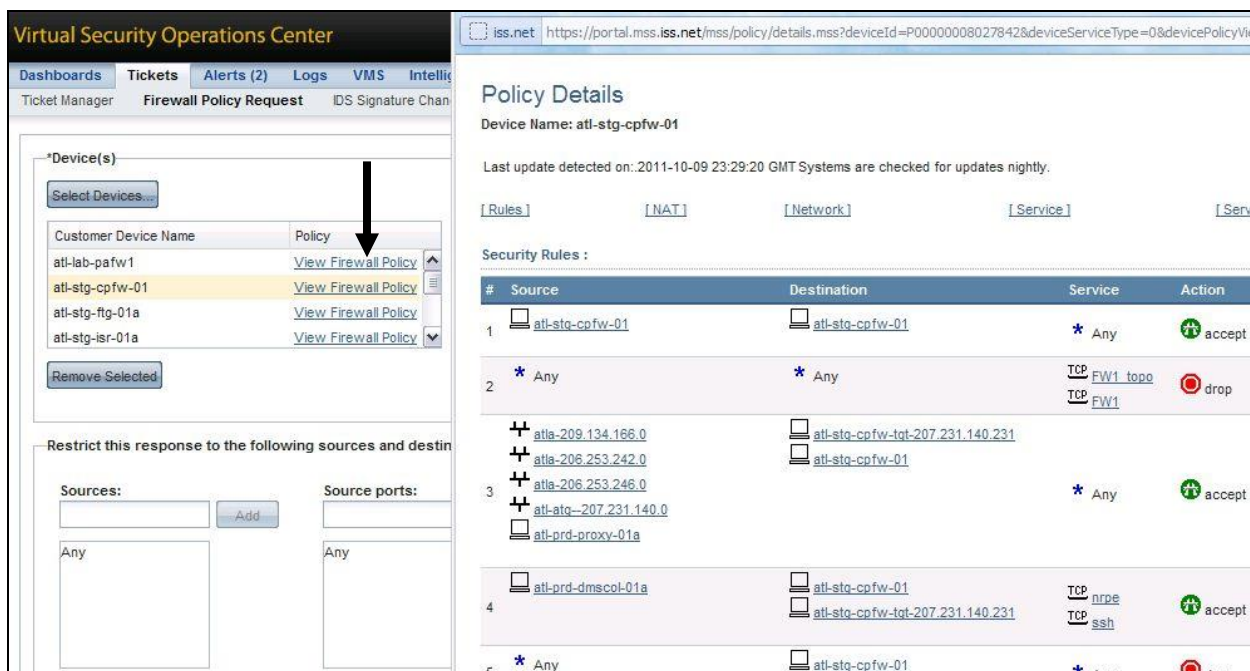
Below the file attachment section, there is a checkbox for 'Send email notifications on updates', a 'Reference ticket ID' field, a 'PIN' field, and a 'Submit' button.

The bottom of the page features a footer with copyright information: 'Copyright © 2013 IBM Corporation' and '10/01/13 10:15 EST - 10/01/13 15:15 GMT'.

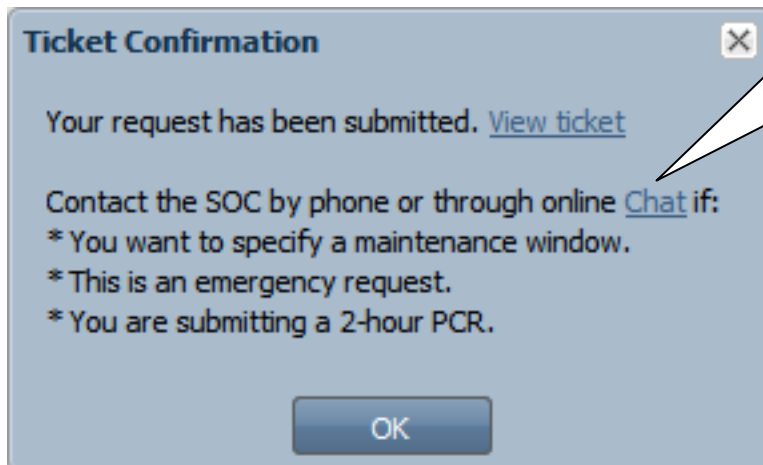
Selecting Devices: The device selecting interface contains filters and a search field to efficiently locate and choose your desired device or group of devices.



After you have selected your device you can review the policy prior to submitting your change request. Click on, "View Firewall Policy" to launch a separate policy window.



After you have submitted your change request a confirmation window will appear with an option to review the ticket details or link to the Chat client for further interaction with the SOC.



After creating your ticket, you can chat with the SOC to schedule a maintenance window or raise the priority of the request.

## Submit a General Service Request

General (or “Other”) Service Requests are located under the Tickets menu. You can use this request for general inquiries, as well as requesting delivery of logs (additional charges apply for delivery of logs).

Home	Tickets	Alerts (728)	Logs	VMS	Intelligence	Devices	Analytics	Reports	Support
------	---------	--------------	------	-----	--------------	---------	-----------	---------	---------

Tickets > Other Service Request

Select the appropriate devices

Select a device group

No devices, select a device group.

Classify the ticket

Request Type:

Request Physical Logs Delivery

Your reference ticket ID:

Describe the request

Request:

File Attachment:

Browse...

No file selected.

Email Notification on Update?

No

Please note, the maximum size for file upload is 5MB.

Submit

Copyright © 2013 IBM Corporation

Privacy

Terms of use

10/01/13 12:04 EST - 10/01/13 17:04 GMT

# Create an Internal Ticket

You can create an Internal Ticket via the Tickets menu. This ticket will be assigned to your internal staff.

**\* Please note no SOC intervention will occur.**

[Home](#) [Tickets](#) [Alerts \(728\)](#) [Logs](#) [VMS](#) [Intelligence](#) [Devices](#) [Analytics](#) [Reports](#) [Support](#)

Tickets > Internal Ticket

NOTICE: SOC personnel do not have access to Customer Internal tickets. Any information you submit or update in this ticket will not be accessible by SOC personnel. If you need the SOC to work or see this ticket, please submit it as one of the types that is visible to the SOC.

Select the appropriate devices

Select a device group

No devices, select a device group.

Classify the ticket

Assigned To:

Please select a contact.

Issue Type:

General Ticket

Priority:

Low

Your reference ticket ID:

Describe the request

Request:

File Attachment:

Browse...

No file selected.

Email Notification on Update?

No

Please note, the maximum size for file upload is 5MB.

Submit

Copyright © 2013 IBM Corporation   Privacy   Terms of use   10/01/13 12:09 EST - 10/01/13 17:09 GMT



## Create an Internal Security Incident

Like the Internal general Ticket you can also create your own Internal Security Incidents, and assign it to your internal staff under the Tickets menu (Create Internal Security Incident). Once you have filled out the incident, and assigned it to your internal staff click “submit” to save.

**Note: No SOC intervention will occur.**

[Home](#) [Tickets](#) [Alerts](#) [Logs](#) [VMS](#) [Intelligence](#) [Devices](#) [Analytics](#) [Reports](#) [Support](#)

Tickets > Internal Security Incident

*NOTICE: SOC personnel do not have access to Customer Internal tickets. Any information you submit or update in this ticket will not be accessible by SOC personnel. If you need the SOC to work or see this ticket, please submit it as one of the types that is visible to the SOC.*

Select the appropriate devices

Select a device group

No devices, select a device group.

Classify the ticket

Assigned To:  
Please select a contact.

Issue Type:  
SI Denial of Service

Event Name:  
N/A

Priority:  
Low

Source Address:

Source Port:

Your reference ticket ID:

Destination Address:

Destination Port:

Describe the request

Request:

File Attachment:

Email Notification on Update?

# Reports

The “Reports” menu contains links to many useful service report templates that will assist you and your security team in day-to-day research and audit control/compliance.

For more information and best practices, please reference the Reports user guide located in the Media Library.

## The Reports Dashboard:

The screenshot displays the 'Reports > Report Dashboard' interface. It is organized into several sections:

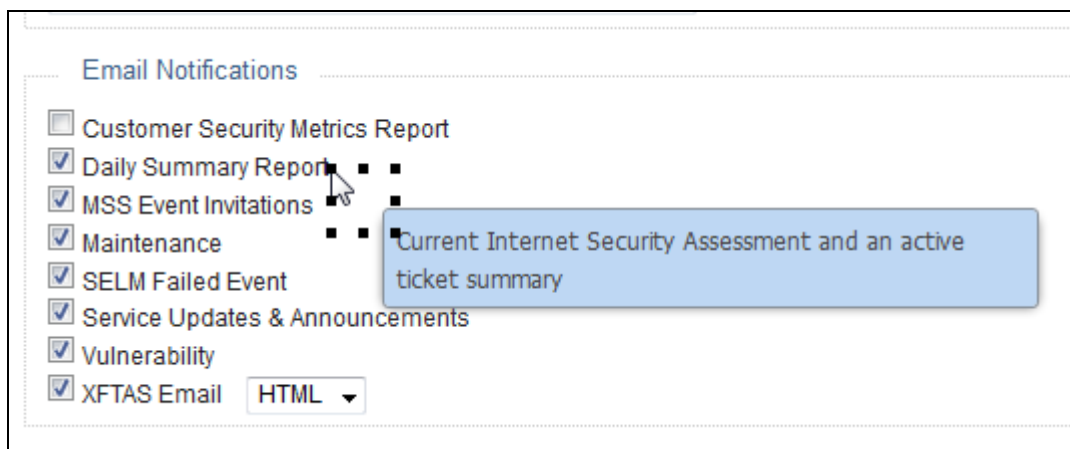
- General Service Related:** Includes links for [Service Level Agreement](#), [Service Overview](#), and [Security Manager Overview](#).
- IDS/IPS Sensors:** Includes links for [Global Attack Metrics](#), [Your Attack Metrics](#), [Attacks on Vulnerable Assets](#), [Prevented Attacks Report](#), [Vulnerability Impact](#), and **Event Counts By** (with sub-links for Source IPs, Destination IPs, Event Names, Sensors, and Sensors, Event Names, IPs). It also features [Event Trend](#), [Event Name Trend](#), and [Multiple Events Breakout Trend](#).
- Vulnerability Management:** Includes **Enterprise** (with [Reports \(Create New\)](#), [Vulnerabilities](#), and [Sites](#)) and **PCI** (with [Reports \(Create New\)](#)).
- Firewall:** Includes links for [Firewall Summary Report](#), [Traffic Analysis - Denied](#), [Traffic Analysis - Email](#), [Traffic Analysis - Web Activity by IP](#), [Traffic Analysis - Web Activity by Website](#), [Protocol Usage - Allowed](#), [Protocol Usage - Denied](#), [Connections Summary - Allowed](#), [Connections Summary - Denied](#), [Targeted IP Addresses](#), [Rule Utilization Analysis](#), and [Suspicious Host Correlation Report](#).
- Log Management:** Includes [SELM Server Device Listing By Site](#), **Event Counts By** (with [Device](#) and [Log Aggregator](#)), [System Activity Events](#), [System Activity Events Details](#), [System Activity Events By User](#), and **System Activity Events by PCI Requirement** (listing PCI 1 through PCI 6).

A callout box with the text "Quick access to report templates by pre-set time intervals" points to a grid of report template icons in the IDS/IPS Sensors section.

Below are some examples of additional reports:

### Daily Summary Report:

We recommend that you subscribe to the Daily Summary Report located under Settings/ My Profile (Email Notifications). You will receive an email with important information including the Current Internet Security Assessment and an active ticket summary.



**Email Notifications**

- ☐ Customer Security Metrics Report
- ☒ Daily Summary Report
- ☒ MSS Event Invitations
- ☒ Maintenance
- ☒ SELM Failed Event
- ☒ Service Updates & Announcements
- ☒ Vulnerability
- ☒ XFTAS Email

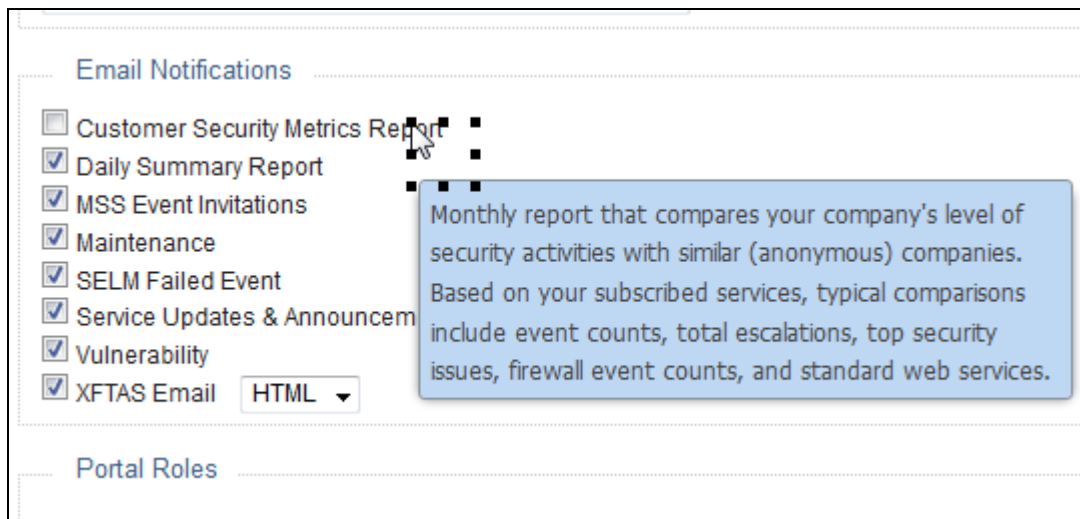
HTML ▾

Current Internet Security Assessment and an active ticket summary

### Customer Security Metric Report:

The CSM report is specifically targeted at executive level customer contacts that don't regularly log into the Portal. The report provides a "sense" for the overall status of the services you have subscribed to and highlights any high level security observations that may be related to security posture and risk.

If you are interested in this report and do not currently have this option please contact the SOC.



**Email Notifications**

- ☐ Customer Security Metrics Report
- ☒ Daily Summary Report
- ☒ MSS Event Invitations
- ☒ Maintenance
- ☒ SELM Failed Event
- ☒ Service Updates & Announcements
- ☒ Vulnerability
- ☒ XFTAS Email

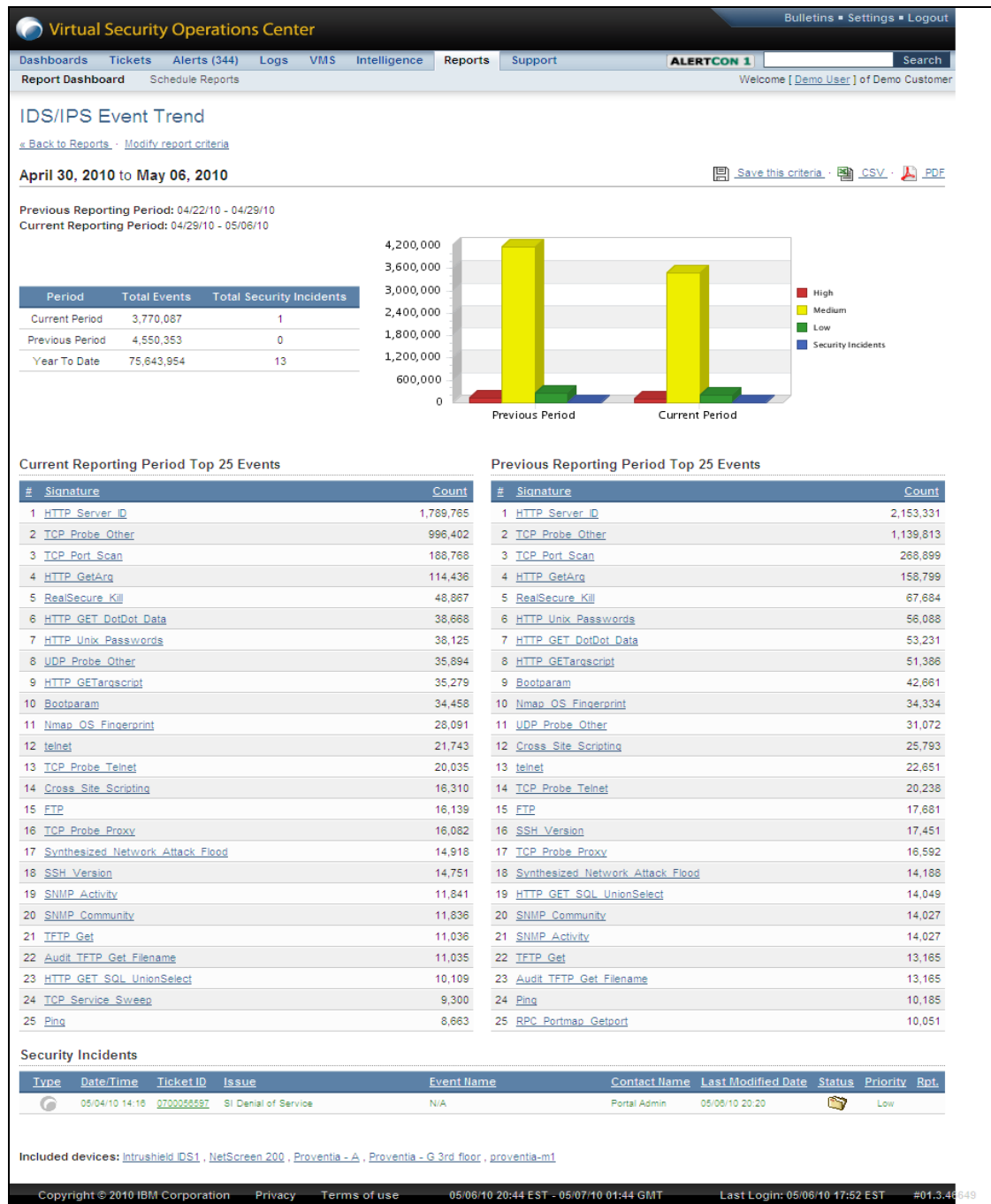
HTML ▾

Monthly report that compares your company's level of security activities with similar (anonymous) companies. Based on your subscribed services, typical comparisons include event counts, total escalations, top security issues, firewall event counts, and standard web services.

**Portal Roles**

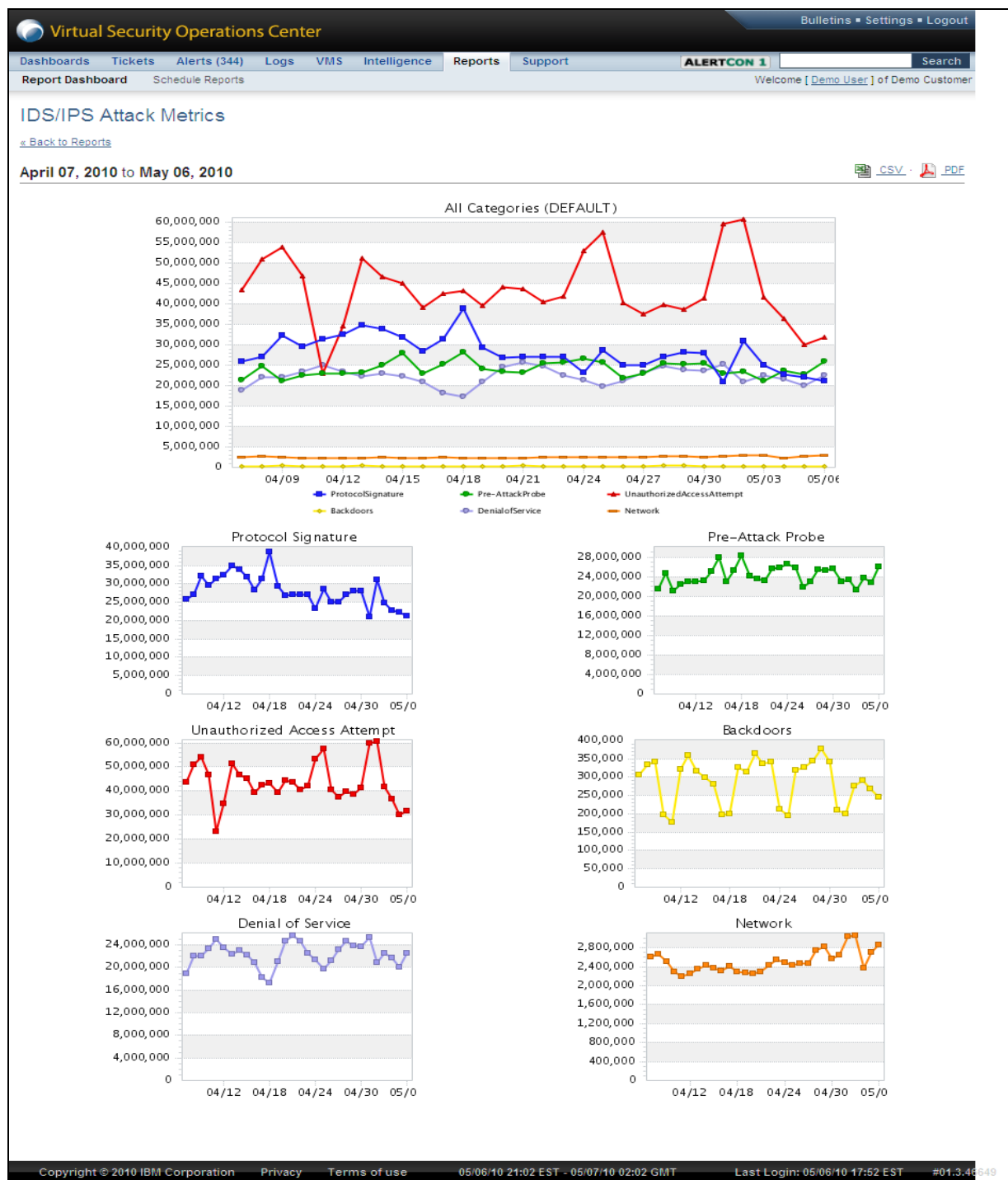
# IDS/IPS Sensors Reports

The “Event Trend” report gives a comparison of the current period events and trends with the previous period events and trends and also lists any security incidents.



# Attack Metrics

This report displays several graphs of information, detailing the numbers and types of attacks detected during the past 30 days. Click on the graph for additional drill-in reporting information.



## Explanation of Attack Types

The attack types included in the Attack Metrics report, along with brief descriptions and examples, are listed below.

- **ProtocolSignature**

A large number of these events in a short time period could indicate an attack.

**Example:** TLS\_Weak\_Cipher\_Suite

Servers and clients use X.509 certificates when establishing communication using Secure Sockets Layer (SSL). An SSL server that allows weak ciphers (with key-lengths less than 128-bits) could allow a remote attacker to obtain sensitive information.

**How to remove this vulnerability:** Consult server documentation to disable weak ciphers.

- **Netbios\_Session\_Request**

A request to initiate a NetBIOS session between two computers. A large number of these events in a short time period could indicate a brute force attack.

**How to remove this vulnerability:** Analyze the nature of the traffic to determine if this is normal usage. You might want to fine-tune the threshold so that normal use does not trigger this event, while brute force attempts would still be detected.

- **Pre-AttackProbe**

An attempt to gain access to a computer and its files through a known or probable weak point in the computer system.

**Example:** Ping\_Sweep

As a prelude to an attack, subnets are often swept with ICMP or other packets that elicit known responses from active hosts. This sort of probe is used to enumerate active hosts on the subnet, and identify potential attack targets. Normal hosts on a network should never engage in sweeps unless they are performing network monitoring or management tasks.

**How to remove this vulnerability:** Always filter inbound ICMP (other than replies to outbound requests) through your firewall or filtering router, if possible. If a stateful inspection filter is not available inbound, then block all ICMP outbound to prevent replies from reaching the attacker.

- **UnauthorizedAccessAttempt**

This usually denotes suspicious activity on a system, or failed attempts to access a system, by a user or who does not have access.

**Example:** SSH\_Brute\_Force

This event detects an excessive number of very short SSH sessions initiated by a single client to one or more servers within a specified timeframe. It may indicate a username/password guessing attack, or a DoS attack. To qualify as this type of attack, a session must have completed encryption negotiations so that a login may be attempted, and the time elapsed from the first encrypted client

data until the TCP session ends with a TCP FIN or server RST must be less than the pam.login.ssh.short.session.time (default 4 seconds). The signature is tunable via the pam.login.ssh.count p (default 12) and the pam.login.ssh.interval setting (default 60 seconds).

This signature also detects an excessive number of SSH Server Identifications from an SSH server within a specified timeframe. This may indicate a username/password guessing attack. The signature is tunable via the pam.login.ssh.count, pam.login.ssh.interval and pam.ssh.server.bruteforce.chars settings.

- **Backdoors**

Hidden programs that attackers use to access your computer without your knowledge or consent.

**Example:** RDP\_Brute\_Force

This signature detects worms, such as Win32/Morto, that allow unauthorized access to an affected computer. These worms spread by trying to compromise administrator passwords for Remote Desktop connections on a network.

**Example:** NetController\_TCP\_Request

This signature detects a request on port 6969/TCP that may indicate a NetController backdoor running on your network.

**How to remove this vulnerability:** Use an up-to-date antivirus program to scan the target computer to determine if it is infected with a backdoor program. If the program detects a backdoor, follow its instructions to disinfect and repair the computer.

- **DenialofService**

An attack that attempts to prevent legitimate users from accessing information or services. By targeting a user's computer and its network connection, or the computers and network of the site a user is trying to access, an attacker may be able to prevent a user from accessing email, websites, or online accounts for banking or other services that rely on the affected computer or network.

**Example:** Smurf\_Attack

In a Smurf denial of service (DoS) attack, ICMP echo request (ping) packets addressed to an IP broadcast address cause a large number of responses. When each host on the subnet replies to the same ping request, the large number of responses can consume all available network bandwidth, especially if data is appended to the ping request. This can prevent legitimate traffic from being transmitted during the attack. This attack is frequently used against third parties, where an attacker forges the target's source address in a Smurf attack against a different target. At the extreme, this attack can simultaneously disable both targets.

Windows systems do not respond to broadcast pings. However, this does not mean that all Microsoft networks are invulnerable to Smurf attacks.

**How to remove this vulnerability:** Reconfigure your perimeter router or firewall to block ICMP echo requests on your internal network and block ICMP echo replies from entering your network. This prevents an internal attacker from using your network to mount a SMURF attack against another target. It also prevents an external attacker from targeting your hosts. However, neither of these actions will stop internal SMURF attacks.

- **Network**

An attack that uses various types of network traffic and protocols for malicious activities.

**Example:** HTTP\_eDirectory\_Multiple\_Connection

Novell eDirectory is vulnerable to a denial of service, caused by an error in the dhost.exe service when processing Connection headers. By sending multiple HTTP requests containing specially-crafted "Connection" headers, a remote attacker could exploit this vulnerability to consume all available CPU resources, resulting in a denial of service.

**How to remove this vulnerability:** Refer to Novell Security Alert Document ID: 3829452 for patch, upgrade or suggested workaround information.

**Example:** ICMP\_Redirect

ICMP redirects detected on a network or targeted at hosts with weak TCP/IP stack implementations have been shown to cause system failures and other adverse effects. Some versions of NetWare, Windows, and embedded systems like Microware OS-9 have been shown to be susceptible to attacks using ICMP redirects. An attacker could forge ICMP Redirect packets, and possibly alter the host routing tables and subvert security, by causing traffic to flow on a path the network manager did not intend.

**Caution:** Various networked, embedded controllers may hang or shut down, if they receive an ICMP redirect with an invalid Code. If your network contains controllers attached to automation equipment, manufacturing equipment, HVAC (Heating, Ventilation, and Air Conditioning) equipment, and medical equipment, do not perform ICMP redirects.



# Security Logs and Events

## Logs Drop Down Menu

There are 4 menu options when viewing the 'Logs' drop down menu:

- Log Query
- Log Search (No export option but is more advanced)
- Log Downloads
- Log Parser

The Log Analysis features of the portal include powerful query engines, with granular query criteria, and filters, than enable you to query multiple log types, and events from multiple devices, and correlate the results through the display in a common interface. You also have the option to schedule log downloads. Log downloads can be retrieved from the Log Downloads menu.

## Log Query

The log query enables you to query multiple log types, and correlate the results through a common display. The query criteria are displayed below. There are five steps:

1. Select the time/date or select a time interval. Note that you can also select your time zone so that the correct time is displayed in your results.
2. Select the devices to be included in the query. You can select by device, custom group or site. Refer to page (14) for more information on creating custom groups.
3. Select the log types you would like returned in your search.
4. Select your query criteria is to select options such as logs per page, DNS resolution, sort, and scheduling a download.
5. Enter search terms if applicable. Click on the “?” next to the text box for examples.

There is also the option for Advanced Query Criteria (circled below in red) for more granular control of your queries.

Home Tickets Alerts Logs VMS Intelligence Devices Analytics Reports Support AnacondaPre Admin 14 Help

Logs > Log Query Search Portal

Query Criteria

Select saved criteria

1. Date/Time

Start Date Start Time  
01/17/2012 07:46:26

End Date End Time  
01/17/2012 11:46:26

Time interval  
Range of time

Timezone  
(GMT-07:00) Chihuahua, La Paz

2. Devices Included in Query

Select a device group

No devices, select a device group.

☐ Include inactive Devices (\*)

3. Applications

☐ Firewall  
☐ IDS/IPS  
☐ SMS  
☐ Anti-Virus  
☐ Anti-Spam  
☐ URL Filtering  
☐ Universal Log  
☐ System Activity

4. Options

Logs per page 100

Resolve DNS No

Sort Type Oldest on top

☐ Schedule CSV download

☐ Save this criteria

5. Full Text Search

Search Terms

Advanced query criteria Submit

## Log Query – Advanced Options

The advanced query criteria can be seen at the bottom of the screen image below. The “=” denotes include, and “!=” denotes exclude. Examples of how to use the filters, can be displayed by clicking on the “?”, or the magnifying glass next to the “Type” field.

[Hide advanced query criteria](#)

**6. Filters**

NOTE: Separate multiple filters with commas (e.g. "192.168.0.1, 192.168.0.2")

Action	=	<input type="text"/>		Protocol	=	<input type="text"/>	
Source IP	=	<input type="text"/>		S. Port	=	<input type="text"/>	
Destination IP	=	<input type="text"/>		D. Port	=	<input type="text"/>	
Predefined							
Event Name	=	<input type="text"/>					
Firewall							
Rule	=	<input type="text"/>					
IDS/IPS							
Priority	=	<input type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High					
Anti-Virus							
Attacker	=	<input type="text"/>		Virus Name	=	<input type="text"/>	
				File Name	=	<input type="text"/>	

# Log Query – Results

There are context based menu's available, for your use in the results of your log queries. Clicking on the "+" next to the log type, will display the raw log. Clicking on the device will give you the option, of viewing the device details, as well as any recently opened tickets relating to the device. Clicking on the event name, will provide filter options, as well as the option to view the security event details. Clicking on the Source/Destination IP, Source/Destination Port, or Action will provide filtering options. There is also an option, to add or remove table columns, to assist you in customizing your results, in a manner that caters to your needs.

Home Tickets Alerts (57) Logs VMS Intelligence Email and Web Security Devices Analytics Reports Support									
Logs > Log Query									
Start Over • Modify query criteria									
Add / remove table columns									
02/06/12 07:27:58 EST - 02/06/12 07:30:05 EST									
Type	Timestamp	Device	Event Name	Source IP	S. Port	Destination IP	D. Port	Action	Count
FW	02/06/12 07:27:58 EST	atl-stc-scr-01a						LOG	1
Feb 6 2012 12:27:58: %ENVMON-3-FAN_FAILED: Fan 1 is malfunctioning									
FW	02/06/12 07:27:58 EST	atl-stc-scr-01a						LOG	1
FW	02/06/12 07:27:59 EST	atl-stc-ssg-01						NOTIFICATION	1
FW	02/06/12 07:27:59 EST	atl-stc-ssg-01						NOTIFICATION	1
FW	02/06/12 07:27:59 EST	atl-stc-ssg-01						NOTIFICATION	1
FW	02/06/12 07:27:59 EST	atl-stc-ssg-01						NOTIFICATION	1
FW	02/06/12 07:28:05 EST	atl-stc-scr-01a		10.200.1.35	0	10.200.1.255	0	ACCEPT	1
FW	02/06/12 07:28:05 EST	atl-stc-scr-01a		10.200.1.35	0	10.200.1.255	0	ACCEPT	1
FW	02/06/12 07:28:28 EST	atl-stc-scr-01a						LOG	1
FW	02/06/12 07:28:28 EST	atl-stc-scr-01a						LOG	1
FW	02/06/12 07:28:55 EST	atl-stc-flt-01a		10.200.1.6	65140	209.134.187.5	389	ACCEPT	1
FW	02/06/12 07:28:55 EST	atl-stc-flt-01a		10.200.1.6	65140	209.134.187.5	389	ACCEPT	1
FW	02/06/12 07:28:58 EST	atl-stc-scr-01a						LOG	1
FW	02/06/12 07:28:58 EST	atl-stc-scr-01a						LOG	1
FW	02/06/12 07:29:01 EST	atl-stc-flt-01a		207.231.142.90	35446	207.231.140.239	7971	START	1
FW	02/06/12 07:29:02 EST	atl-stc-flt-01a		10.200.1.6	7971	10.200.1.206	63730	DROP	1
FW	02/06/12 07:29:04 EST	atl-stc-flt-01a		10.200.1.6	65142	209.134.187.5	445	ACCEPT	1
FW	02/06/12 07:29:04 EST	atl-stc-flt-01a		10.200.1.6	65143	209.134.187.53	445	ACCEPT	1
FW	02/06/12 07:29:09 EST	atl-stc-flt-01a		10.200.1.6	65138	209.134.187.5	389	ACCEPT	1
FW	02/06/12 07:29:10 EST	atl-stc-flt-01a		10.200.1.6	65146	209.134.187.5	389	ACCEPT	1
FW	02/06/12 07:29:10 EST	atl-stc-flt-01a		10.200.1.6	65145	209.134.187.5	389	ACCEPT	1
FW	02/06/12 07:29:13 EST	atl-stc-flt-01a		207.231.142.90	0	207.231.140.206	2048	START	1
FW	02/06/12 07:29:13 EST	atl-stc-flt-01a		207.231.142.90	35446	207.231.140.239	7971	ACCEPT	1
OS/IPS	02/06/12 07:29:18 EST	Demo G400	Ping Sweep	207.231.142.90		207.231.0.0		LOG	1
FW	02/06/12 07:29:20 EST	atl-stc-flt-01a		10.200.1.6	65144	209.134.189.86	445	ACCEPT	1
FW	02/06/12 07:29:28 EST	atl-stc-scr-01a						LOG	1
FW	02/06/12 07:29:28 EST	atl-stc-scr-01a						LOG	1
FW	02/06/12 07:29:52 EST	atl-stc-flt-01a		10.200.1.6	58409	209.134.187.5	53	ACCEPT	1
FW	02/06/12 07:29:52 EST	atl-stc-flt-01a		10.200.1.6	60931	209.134.187.5	53	ACCEPT	1

# Log Search

Log search is the next generation log query tool. First select a device or group of devices then your desired log type (s). You can then select the appropriate date / time range. The fields and details options will allow you to control the information output.

There is an Overview document that will assist you in general use including how to build your log search syntax.



The screenshot shows the Log Search interface. At the top is a navigation bar with links: Home, Tickets, Alerts (3), Logs, VMS, Intelligence, Email and Web Security, Devices, Analytics, Reports, Support. On the right of the navigation bar is the user name 'Scott K Demo', a dropdown menu with '11', and a 'Help' link. Below the navigation bar is a breadcrumb trail 'Logs > Log Search' and a 'Search Portal...' button. The main search area contains a large text input field labeled 'Search...', a 'Search' button, and a 'Log Types (0)' dropdown menu. Below these are filters for 'Devices (0)' and a date/time range selector showing 'From 01/17/2012 09:57:02 to 13:57:02 01/17/2012'. There are also radio buttons for 'Fields', 'Details', and 'Both', with 'Both' selected. A horizontal slider is visible below the filters. A text block states: 'Log Search offers a variety of filtering, display and enhanced usability features designed to assist you in efficiently navigating your logs.' Below this is a link 'Become a power user, read the online help'. A callout box points to this link and contains the text 'Customer Enablement Resource'. Below the callout box is a list of links: 'Overview of search capabilities and advanced interactions', 'Detailed explanation of search syntax', 'Examples of searches', and 'List of searchable fields'.

Home Tickets Alerts (3) Logs VMS Intelligence Email and Web Security Devices Analytics Reports Support Scott K Demo 11 Help

Logs > Log Search Search Portal...

Search... Search

Devices (0) Log Types (0)

From 01/17/2012 09:57:02 to 13:57:02 01/17/2012

Fields Details Both

Log Search offers a variety of filtering, display and enhanced usability features designed to assist you in efficiently navigating your logs.

Become a power user, [read the online help](#)

• [Overview](#) of search capabilities and advanced interactions

• Detailed explanation of [search syntax](#)

• Examples of searches

• List of [searchable fields](#)

**Customer Enablement Resource**

# Active Analyzer

Active Analyzer provides close to real-time event monitoring of your IDPS events, with auto-refresh, as well as manual refresh options. With each refresh, the baselines increase in events, and deltas are reflected. You can also view the events from event view, sensor view, source view, or destination view via the “Selected view” drop down menu located at the top right above the auto-refresh options.

## Active Analyzer – Context Based Menus

Active Analyzer offers context based menus to assist you in your research and investigation. You can access the context based menus, by clicking on the event name, or the arrow located to the right of the event name.

Home Tickets Alerts (196) Logs VMS Intelligence Email and Web Security Devices Analytics Reports Support Mister Anderson 0 Help									
Analytics > Active Analyzer ? Search Portal...									
Go to Default View · Modify query criteria Selected view: Event Name View									
05/07/12 00:00:00 EST to 05/07/12 01:59:59 EST Save query criteria Auto-refresh Refresh									
Event Name	Priority	% Total	Count	Sources	Destinations	Sensor Count	First Event	Last Event	
System Error	▲	<1%	118	1	1	1	05/07/12 00:00:12 EST	05/07/12 01:59:15 EST	
HTTP IndexServer Source Disclosure	▲	<1%	40	1	1	1	05/07/12 00:14:21 EST	05/07/12 00:21:06 EST	
Packet Sanitv	▲	<1%	8	1	2	1	05/07/12 00:35:58 EST	05/07/12 01:38:14 EST	
Non-MDS Authenticated BGP Connections	▲	<1%	6	1	3	1	05/07/12 00:31:08 EST	05/07/12 01:33:00 EST	
SSH Brute Force	▲	<1%	4	1	2	1	05/07/12 00:08:51 EST	05/07/12 01:11:16 EST	
nla	▲	<1%	2	1	1	1	05/07/12 00:30:01 EST	05/07/12 01:30:02 EST	
nbss_decoder: NBSS.Invalid Fragment	▲	<1%	2	1	1	1	05/07/12 00:36:45 EST	05/07/12 01:36:59 EST	
Non Compliant SSL	▲	<1%	2	1	1	1	05/07/12 00:32:23 EST	05/07/12 01:32:05 EST	
HTTP MSIS Script	▲	<1%	1	1	1	1	05/07/12 00:17:20 EST	05/07/12 00:17:20 EST	
TCP Port Scan	■	22.54%	5,354	4	41	4	05/07/12 00:07:35 EST	05/07/12 01:31:36 EST	
HTTP IS Double Eval Evasion	■	1.35%	321	2	6	1	05/07/12 00:00:10 EST	05/07/12 01:59:38 EST	
Cross Site Scripting	■	<1%	190	1	1	1	05/07/12 00:00:50 EST	05/07/12 01:59:32 EST	
Synthesized Host Attack Flood	■	<1%	149	1	12	2	05/07/12 00:11:31 EST	05/07/12 01:18:24 EST	
Ping Sweep	■	<1%	121	2	12	2	05/07/12 00:00:08 EST	05/07/12 01:58:52 EST	
Synthesized Network Attack Flood	■	<1%	63	1	1	2	05/07/12 00:11:46 EST	05/07/12 01:18:55 EST	
TCP Fingerprinting NMAP	■	<1%	63	1	19	1	05/07/12 00:33:59 EST	05/07/12 01:37:16 EST	
NMAP_XMAS Probe	■	<1%	50	2	14	1	05/07/12 00:33:58 EST	05/07/12 01:38:19 EST	
HTTP IS Hit Highlighting Auth Bypass	■	<1%	40	1	1	1	05/07/12 00:15:06 EST	05/07/12 00:21:51 EST	
TCP SYN Port Scan	■	<1%	39	1	20	1	05/07/12 00:30:06 EST	05/07/12 01:36:47 EST	
SNMP Default Backdoor	■	<1%	16	1	1	1	05/07/12 00:45:32 EST	05/07/12 00:45:41 EST	
System Clock Zero Size DoS	■	<1%	10	1	5	1	05/07/12 00:27:06 EST	05/07/12 00:27:37 EST	

# Active Analyzer – Query Criteria

Active Analyzer's powerful query tool gives you the ability to query your IDPS events by time interval, sensor, priority, event, and source and destination. To execute a successful query, it's helpful to be familiar with all the options of this screen.

## Custom Query

**Time Interval** Defaults to "Last 2 Hours"

**Number of Results** Defaults to 500

**Refresh Interval** Defaults to 30 seconds

**Device Selection** Defaults to "All Devices"

**Submit Query button** Click this button or press enter when you want to generate the report

## Applied Filters

**Priority** Low, Medium, or High. Leave blank to query all priorities.

**Event Names** One or more tag names (aka: signatures). Use the "|" in between multiple entries. Spaces are ignored.

**Source IPs** One or more source IP address(es). Use "|" for multiples.

**Destination IPs** One or more destination IP address(es). Use "|" for multiples.

**Virtual Security Operations Center**

Bulletins • Settings • Logout

Dashboards Tickets Alerts (344) Logs VMS Intelligence Reports Support

Log Query Log Search (beta) Active Analyzer Log Downloads ULA Software

ALERTCON 1 Search

Welcome [ Demo User ] of Demo Customer

Go to Default View · Hide query criteria

Selected view: Event Name View

**Query Criteria**

Select saved criteria

**1. Date Range**

Time Interval: Last 2 Hours

**2. Options**

Number of Results: 500

Refresh Interval: 30 seconds

☐ Save this criteria

**3. IDSIPS Sensors**

All devices

Cisco ASA: 12.173.210.37

Cisco IDS

CP Main office.....

Desktops - Fnce

Desktops - Mkt test

Intrushield DS1

NetScreen 200

Proventia - A

Proventia - G 3rd floor

proventia server

☐ Include Inactive Devices (\*)

**4. Filters**

Priority: ☐ Low ☐ Medium ☐ High

Event Names: [ ]

Source IPs: [ ]

Destination IPs: [ ]

Submit Query Reset

05/06/10 21:00:00 EST to 05/06/10 22:59:59 EST

Save query criteria Auto-refresh Refresh now

Event Name	Priority	% Total	Count	Sources	Destinations	Sensor Count	First Event	Last Event
HTTP_GETscript	High	<1%	86	3	2	2	05/06/10 21:13:43 EST	05/06/10 22:14:17 EST
HTTP_Unix_Passwords	High	<1%	58	1	2	2	05/06/10 21:13:43 EST	05/06/10 22:13:46 EST
HTTP_CrystalReports_FileAccess_DoS	High	<1%	43	1	2	2	05/06/10 21:13:52 EST	05/06/10 22:19:39 EST
TFTP_Traversal	High	<1%	15	1	1	1	05/06/10 21:49:00 EST	05/06/10 21:50:34 EST
SQL_Injection	High	<1%	6	1	1	1	05/06/10 21:49:40 EST	05/06/10 21:49:43 EST
HTTP_IndexServer_Source_Disclosure	High	<1%	4	1	1	2	05/06/10 21:19:41 EST	05/06/10 22:19:35 EST
TFTP_File_Brute_Force	High	<1%	4	1	1	1	05/06/10 21:49:00 EST	05/06/10 21:50:36 EST
TFTP_Password_File	High	<1%	4	1	1	1	05/06/10 21:49:00 EST	05/06/10 21:49:00 EST
SSH_Brute_Force	High	<1%	2	1	2	1	05/06/10 21:49:36 EST	05/06/10 21:49:39 EST
TCP_NULL_Packet	High	<1%	2	1	2	1	05/06/10 21:06:39 EST	05/06/10 21:59:30 EST

## Log Parsers

If you have the subscribed service you can monitor and report upon activity from previously unknown systems and applications that have been missing from your Virtual SOC analysis and / or compliancy initiatives.

The log parser extracts data from raw OS or application log files and then formats them in a way that can be recognized and organized by the MSS Log Management System.

Delete	Enabled	Name	Log Type	Owner	
	<input type="checkbox"/>	<a href="#">Release02 Testing</a>	System Activity	Customer	<a href="#">Copy to new</a>
	<input type="checkbox"/>	<a href="#">CreatNewRelease02</a>	System Activity	Customer	<a href="#">Copy to new</a>
	<input type="checkbox"/>	<a href="#">01bCreateNew</a>	System Activity	Customer	<a href="#">Copy to new</a>
	<input type="checkbox"/>	<a href="#">01bCreateNew02</a>	System Activity	Customer	<a href="#">Copy to new</a>
	<input type="checkbox"/>	<a href="#">パーサテスト11-巻</a>	System Activity	Customer	<a href="#">Copy to new</a>
	<input type="checkbox"/>	<a href="#">parsertest inJapanese02(日本語テスト01)</a>	System Activity	Customer	<a href="#">Copy to new</a>
	<input checked="" type="checkbox"/>	<a href="#">Symantec Endpoint Protection Log Parser (pfio...</a>	System Activity	Customer	<a href="#">Copy to new</a>
	<input type="checkbox"/>	<a href="#">Apache Access Log [Do Not Delete or Modify]</a>	System Activity	Customer	<a href="#">Copy to new</a>

Embedded access to Customer Enablement resources on the right side shown below:

Scott K Demo 11 Help IBM

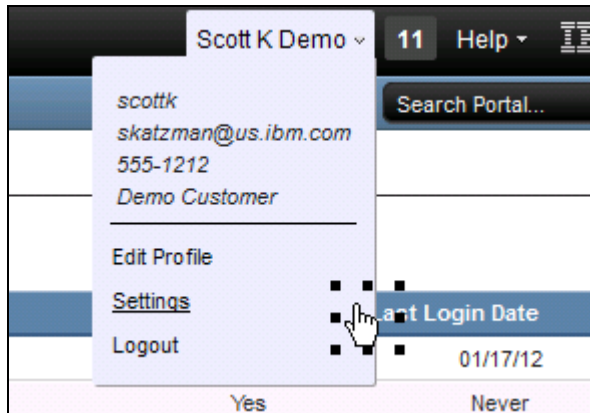
Search Portal...

[Help me write a parser](#)

[Click here for a video tutorial](#)

# Creating Virtual SOC Portal Users

Authorized Security Contacts can create users, by clicking on “Settings” which is located in the top right hand corner underneath your username of any screen. Next select “Users” from the left side of the screen. You can then select “Create a New User.”



Home Tickets Alerts (728) Logs VMS Intelligence Devices Analytics

Users ?

Account Management XFTAS Preferences

[My Profile](#)

[Users](#)

[Audit Reports](#)

[Sites](#)

[Support Roles](#)

[Create a New User](#)

Type	Site	Name	Email
Global User	Atlanta	Portal Demo User	nobody@ibm.com
Global User	Atlanta	Tom Watson	demo@pl.ibm.com
Site User	Atlanta	Tom Wallace	tomwallace@us.ibm.com



After you have created the new users login credentials, personal information, and email notifications you will need to create portal roles and device permissions for the user.

**Portal Roles**

LMS:	None
Web Defense:	None
IAM:	None
Malware:	None
VMS - PCI:	None
XFTAS:	Regular
Firewall:	Subordinate User
IDS/IPS:	Admin
MSIEM:	None
VMS - Enterprise:	None
Content Filtering:	None

A description of roles can be viewed by clicking on “Show description of roles.” Note that devices and device groups will not be visible until you select a role, as only groups pertinent to that role will be displayed.

# SOC Communications

## Service Escalation

This form provides feedback directly to the IBM Security Services Customer Problem Management team. It can be found under the “Support” menu, and then within the “Report a Service Problem” option.

\* Note this is not a path for technical escalations but for issues regarding service delivery.

The screenshot shows a web application interface for reporting a service problem. At the top is a navigation bar with links: Home, Tickets, Alerts (728), Logs, VMS, Intelligence, Devices, Analytics, Reports, Support, and More. The 'Support' menu is open, showing options: SOC Contacts, Escalation Contacts, Report a Service Problem (highlighted), Best Practices, eLearning Courses, KnowledgeBase, Media Library, Resources, and Search. Below the navigation bar, the breadcrumb 'Support > Report a Service Problem' is displayed. The main heading is 'Please complete the following form'. A text block explains the form's purpose: 'Please use this form to alert or provide feedback regarding ongoing service issues or concerns. If you wish to report a high priority issue, incident or outage concern, you must telephone the Security Operations Center for immediate assistance.' Below this is a 'Priority' dropdown menu set to 'High'. A large text input area is provided for the user's message. At the bottom of the form are 'Submit' and 'Clear' buttons. The footer contains copyright information: 'Copyright © 2013 IBM Corporation', links for 'Privacy' and 'Terms of use', a timestamp '10/01/13 12:28 EST - 10/01/13 17:28 GMT', and a partially visible 'Last L' link.

Home Tickets Alerts (728) Logs VMS Intelligence Devices Analytics Reports Support More ▾

Support > Report a Service Problem

**Please complete the following form**

Please use this form to alert or provide feedback regarding ongoing service issues or concerns. If you wish to report a high priority issue, incident or outage concern, you must telephone the Security Operations Center for immediate assistance.

Priority  
High ▾

Submit Clear

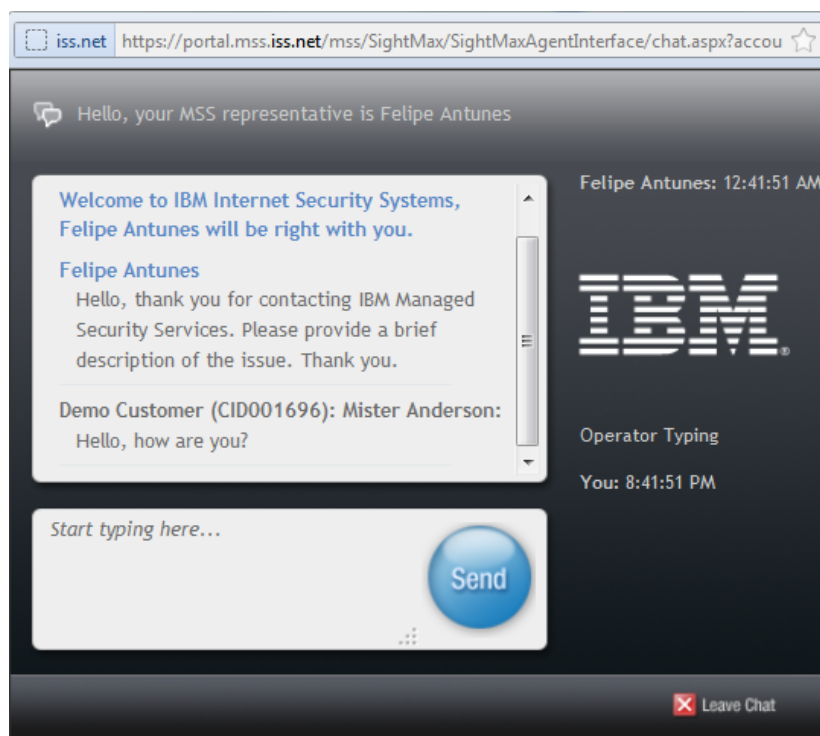
Copyright © 2013 IBM Corporation Privacy Terms of use 10/01/13 12:28 EST - 10/01/13 17:28 GMT Last L

## SOC Escalation

You have the ability to contact the SOC for technical support via email, phone or a private and secure chat session. For critical issues we recommend that you call the SOC directly. Please see, "References" for SOC contact information under the Support menu option.

(Toll-Free US: 877-563-8739)

### Chat feature:



# Media Library

This page found under the Support menu section of the portal, allows the client to download service-related documentation and education resources. SOC engineers also can post files, such as diagrams, here for clients to download in a secure manner. It will be noted within the MSS bulletins whether a document or file will be available.

Home Tickets Alerts (724) Logs VMS Intelligence Devices Analytics Reports Support More

MSS Education 2 Help IBM

Support > Media Library

Filters

Categories: All Media types: All

Date uploaded: Any time from to Apply Reset

SOC Contacts

Escalation Contacts

Report a Service Problem

Best Practices

eLearning Courses

KnowledgeBase

Media Library

Resources

Search

Download... Delete Add...

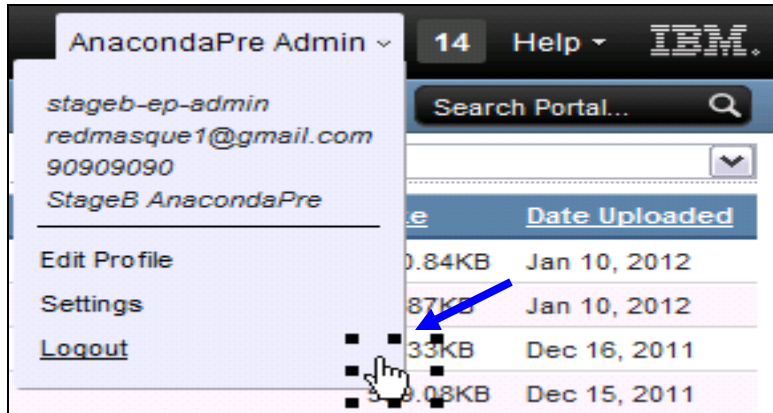
Title	Category	Author	Size	Date Uploaded
Documents (92)				
Recorded Webcasts (27)				
Videos (22)				
<a href="#">Video: Managing Portal Reports (18 minutes)</a>	General Portal	MSS Education	38.47 MB	Sep 18 2013
<a href="#">Video: Managing Support Roles (Security Contacts) (6 minutes)</a>	General Portal	MSS Education	11.06 MB	Aug 23 2013
<a href="#">Video: Configuring Acceptable Traffic and Network Objects (6 minutes)</a>	General Portal	MSS Education	11.47 MB	Aug 15 2013
<a href="#">Simulation: Create and Monitor Policy Change Requests (3 minutes)</a>	General Portal	MSS Education	1.61 MB	May 31 2013
<a href="#">Simulation: Configure, Run, Schedule Alert Activity Report (3 minutes)</a>	General Portal	MSS Education	1.34 MB	May 28 2013
<a href="#">Video: Exporting Portal Data and Using Excel to Manipulate Data and Create Pivot Tables (1...</a>	General Portal	MSS Education	12.25 MB	Mar 15 2013
<a href="#">Video: Using the Asset Center for Critical Assets (9 min)</a>	Device & Asset Management	MSS Education	14.24 MB	Jan 28 2013
<a href="#">Virtual SOC Portal Active Analyzer Video (3 mins)</a>	General Portal	MSS Education	6.14 MB	Feb 14 2012
<a href="#">Virtual SOC Portal Tickets Menu video (6 mins)</a>	General Portal	MSS Education	18.65 MB	Feb 14 2012
<a href="#">Virtual SOC Customizable Dashboard Video (4 mins)</a>	General Portal	MSS Education	13.33 MB	Feb 07 2012
<a href="#">Introduction to the Virtual SOC Portal Video</a>	General Portal	MSS Education	18.81 MB	Feb 06 2012
<a href="#">Virtual SOC Portal Support Menu Video (3 mins)</a>	General Portal	MSS Education	5.48 MB	Feb 05 2012
<a href="#">Virtual SOC Settings Video (3 min)</a>	General Portal	MSS Education	4.73 MB	Feb 05 2012
<a href="#">Virtual SOC Portal Intel Menu Video (5.5 mins)</a>	General Portal	MSS Education	8.2 MB	Feb 05 2012

Copyright © 2013 IBM Corporation Privacy Terms of use 10/01/13 09:31 EST - 10/01/13 14:31 GMT Last Login:09/30/13 12:56 EST at001b.61930\_a3b3cb5

---

# Log Out

To log out of the Portal, from the username menu located in the top right corner of the Portal, select "Logout". You will be returned to the login screen.



# Reference

## SOC Contacts

This page provides contact information for IBM Security Services support. It can be found under the support menu.

Home

Tickets

Alerts (728)

Logs

VMS

Intelligence

Devices

Analytics

Reports

Support

More ▾

Support > SOC Contacts

SOC Contacts

Escalation Contacts

Report a Service Problem

Best Practices

eLearning Courses

KnowledgeBase

Media Library

Resources

Search

Contact Matrix

Contact Method	Hours	Details	Authentication
Online Chat	24x7x365	<a href="https://portal.mss.iss.net/">https://portal.mss.iss.net/</a> Chat Online button under Portal's Help menu	Portal Authentication
Telephone	24x7x365	Toll-Free US: 877-563-8739 Toll US: +1-404-236-3290  ARGENTINA: 08006662974 AUSTRALIA: 1800038641 AUSTRIA: 0800 203513 BELGIUM: 0800 80882 BRAZIL: 08008914935 CHILE: 12300200392 COLOMBIA: 018009440747 DENMARK: 80600067 FINLAND: 08009 8875 FRANCE: 0805540052 GERMANY: 0800 3304874 GREECE: 00800 4414 7173 HONG KONG: 800962198 INDIA: 000 800 440 1785 IRELAND: 1 800 81 2599 ITALY: 800 923032 JAPAN: 0120-995720 KENYA: 0800-10 866-266-4882 LUXEMBOURG: 080080837 MEXICO: 18001231747 NETHERLANDS: 0800 0201125 NEW ZEALAND: 09 913 0091 PERU - 0800 77 082 PORTUGAL - 800 208 325 SINGAPORE: 1800-6221109	Contact ID + PIN or Verbal Pass Phrase (manual authentication)



© Copyright IBM Corporation 2006-2017

IBM Global Services  
Route 100  
Somers, NY 10589 U.S.A.

Produced in the United States of America  
April 2017

IBM, the IBM logo and ibm.com, X-Force, Express and Express Advantage are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml).

Other company, product or service names may be trademarks or service marks of others. References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.