Cisco OnPlus Advanced Security Application

Last Revised: October 30, 2012

This application note is intended for use by Cisco OnPlus Customers and Partners that want to install the OnPlus Advanced Security application to provide managed security services for their networks or for their customer's networks.

Contents

Overview

OnPlus Advanced Security is an incremental OnPlus module. It provides a comprehensive security management solution that complements Cisco's latest security platforms, such as the Cisco ISA500 series. It includes intelligent security reporting and customizable alerting from a centralized management interface. OnPlus Advanced Security service is offered as a simple, cloud-based subscription service. It eliminates the high costs and hassles of on-site maintenance while providing a complete set of features to optimize security performance and scale for growth. When coupled with the Cisco ISA500 Series, Cisco Advanced OnPlus Security is designed to enable Customers and Partners to easily and cost effectively use or offer Managed Security Services to their customers.

Advanced Security Management Features

When OnPlus Advanced Security is added to the OnPlus Service, it allows OnPlus Customers and Partners to:

- Generate comprehensive security reports from the Cisco ISA500 Series in key areas such as:
  - Network resource and bandwidth usage
  - Security threats and security attacks, including threats detected through IPS (Intrusion Prevention System)
  - Web, VPN, FTP, and email usage
  - Spam attacks
  - ISA500 device logins
- View security service reports and events in a separate, consolidated dashboard
- Schedule security reports to be automatically and directly sent to customers
- Personalize reports for individual customers
- Include custom recommendations based on observations of data and trends captured in reports
- Archive reports safely in the cloud without hassle of storage
- View executive summaries and detailed reports

Baseline OnPlus Features

When the ISA500 Series is present in the network, you can use the OnPlus Service to:

- Discover and view the ISA500 appliance in the OnPlus Portal customer network topology and inventory views
- Get information about other devices connected to the ISA500 appliance
- Access ISA500 appliance information such as MAC Address, IP address, serial number, firmware version, and device model name
- Perform basic device and network monitoring, including monitoring of ISA500 up/down status with simple alerting via mail or SMS text messages
- Upload and manage ISA500 appliance firmware
- Back up and restore ISA500 appliance configuration
- Connect to the Web-based ISA500 Series Configuration Utility remotely via the portal.
- View information about Warranty and Service Contracts when the ISA500 Security Appliance is available for purchase

Before You Begin

This section covers pre-requisites and configuration steps that must be performed before installing and the OnPlus Advanced Security Application:

- **Requirements and Availability**
- **Configuring Settings on the ISA500 Security Appliance**
- **Configuring Settings on the OnPlus Portal**

Requirements and Availability

Cisco OnPlus Advanced Security is currently available to Cisco OnPlus Customers and Partners that have a Cisco ISA500 Series Security Appliance installed on the network. If you have not installed and activated the Cisco ISA500, see www.cisco.com/go/isa500resources for information about installing and activating the Cisco ISA500.

For the ISA500 Series6, ISA500 Series Firmware Version 0.5.5 or later is recommended for OnPlus Advanced Security Application.

Configuring Settings on the ISA500 Security Appliance

Verify That Cisco OnPlus Support is Enabled

In order for the ISA500 to communicate with the OnPlus Portal, support for the Cisco OnPlus Service must be enabled on the ISA500. Cisco OnPlus support is enabled by default.

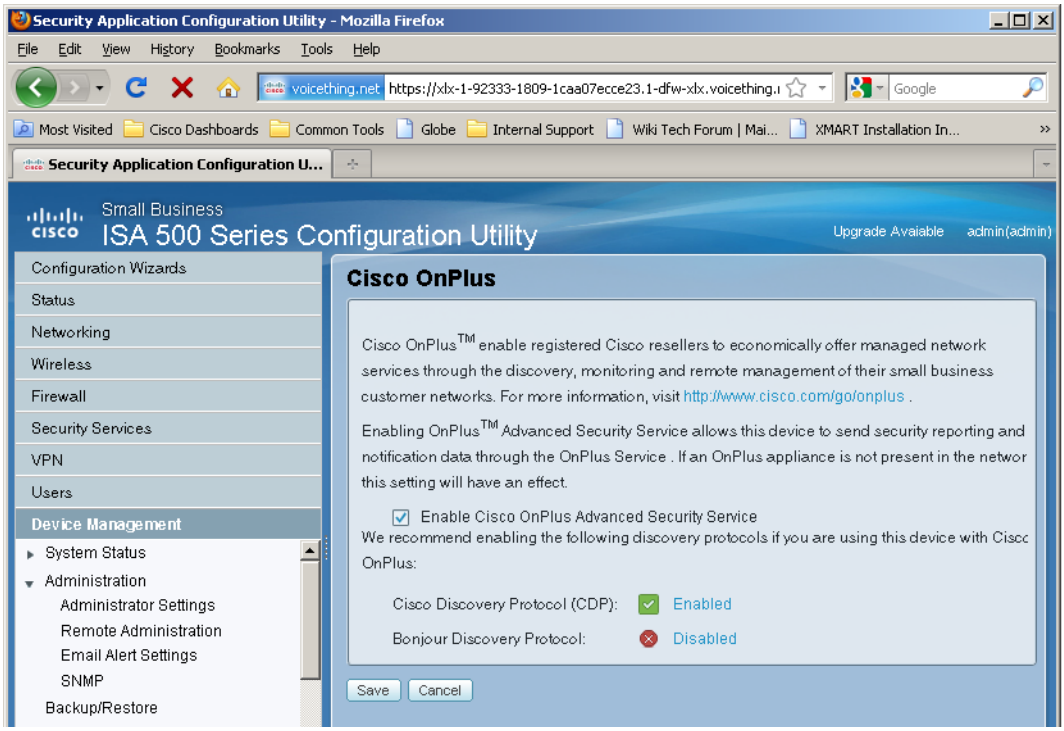
For optimal device discovery and topology support via the OnPlus portal, you must also enable CDP and/or Bonjour discovery protocols on the ISA500.

NOTE These settings can also be configured via the ISA500 Series Setup wizard.

To view or modify Cisco OnPlus support settings on the ISA500, follow these steps.

STEP 1 Log in to the ISA500 appliance as administrator.

STEP 2 Navigate to **Device Management** > **Cisco Services & Support** > **Cisco OnPlus**.



STEP 3 On the Cisco OnPlus page, make sure that **Enable Cisco OnPlus Advanced Security Service** is checked.

STEP 4 Enable **Cisco Discovery Protocol (CDP)** and **Bonjour Discovery Protocol**. For optimal device discovery with OnPlus, enable both discovery protocols.

STEP 5 Click **Save.**

Verify ISA500 Series Security Services License

Some reports, such as Web Threats, Virus Attacks, SPAM Filter, and IPS Threats, require a valid Security Services license to be installed on the ISA500 appliance.

To verify license status on the ISA500, open the **Dashboard** on the ISA500 and look under **Licenses**. It should display "Security Services License Installed." To view, add, or renew licenses on the ISA500, choose **Device Management** > **License Management**.

Configure Security Services

As a best practice, you should enable and configure Security Services on the ISA500 Security Appliance before installing the Advanced Security App.

For Advanced Security reports such as Web threats, virus attacks, spam filter, IPS threats, firewall attacks, and Web usage, Security Services must be enabled and configured on the ISA500 Security Appliance so that the relevant data can be collected.

To configure these settings on the ISA500, log in as administrator and choose **Security Services** from the navigation menu on the left.

For information about these settings, see the Cisco ISA500 Security Appliance Administration Guide or online help.

For information on ISA500 Security Services settings that are required to collect data for specific OnPlus Advanced Security reports, see **Security Report Descriptions, page 13**.

Configuring Settings on the OnPlus Portal

Enter ISA500 Login Access Credentials on the Portal

You must enter administrator-level access credentials for the ISA500 Series Security Appliance on the OnPlus Portal before you can enable the Advanced Security Application for a customer. The portal uses these credentials for device discovery, security reporting, and portal features such as configuration backup/restore, and firmware upgrades for the ISA500 appliance.

TIP As a best practice, we recommend that you create a separate administrator account for OnPlus Portal login access.

To enter login access credentials on the OnPlus Portal, follow these steps.

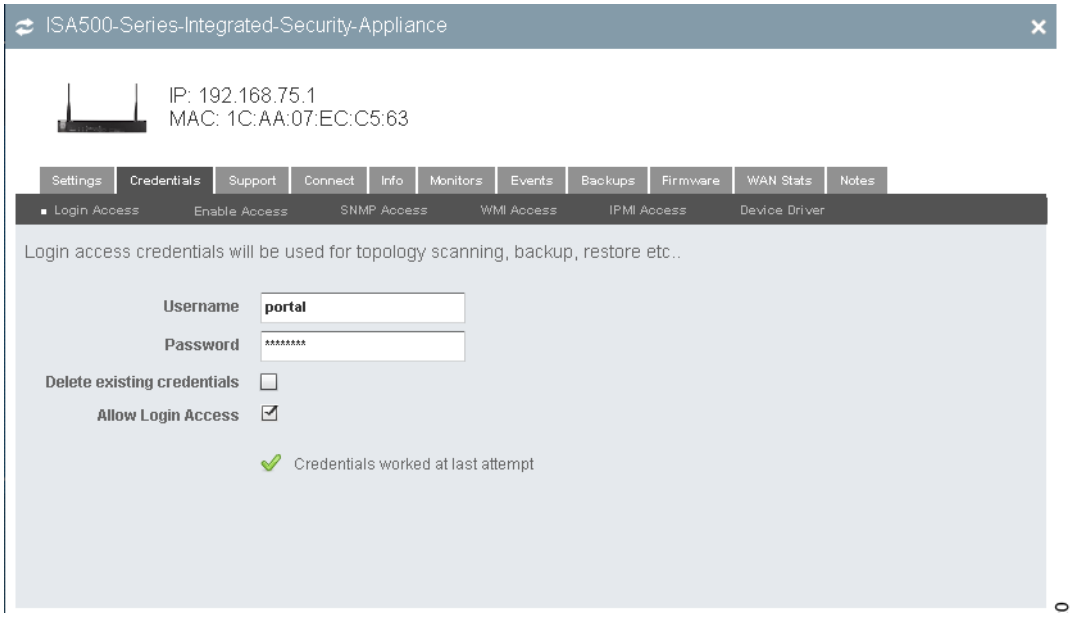
STEP 1 Log in to the portal and open the Topology view.

STEP 2 Locate the ISA500 Series Security Appliance icon in the Topology.

STEP 3 Click the Device Information icon to open the Device Information window.

STEP 4 In the Device Information window, select the **Credentials** tab.

STEP 5 On the Credentials tab, click **Login Access** and enter the admin account username and password for the ISA500.



STEP 6 Click **OK**.

When the credentials are successfully applied, a green check mark and the message “Credentials worked at last attempt” appears on the Credentials tab.

Verify Web Connection Settings for Remote Access

To verify that the Web connection settings for remote access to the ISA500 Series management interface are correct on the portal, follow these steps.

STEP 1 Log in to the portal and open the Topology view.

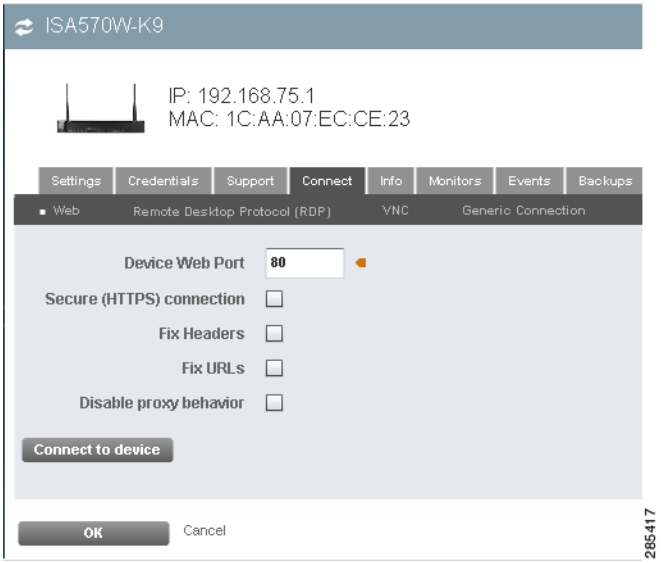
STEP 2 Locate the ISA500 Series Security Appliance icon in the Topology.

STEP 3 Click the Device Information icon to open the Device Information window.

STEP 4 In the Device Information window, select the **Connect** tab.

As soon below, recommended Web connection settings for remote access to the ISA500 Series device manager via the portal are as follows:

- Device Web port: **80**
- Secure (HTTPS) connection, Fix Headers, Fix URLs, and Disable proxy behavior. Unchecked (disabled).



STEP 5 After modifying settings, click **OK**.

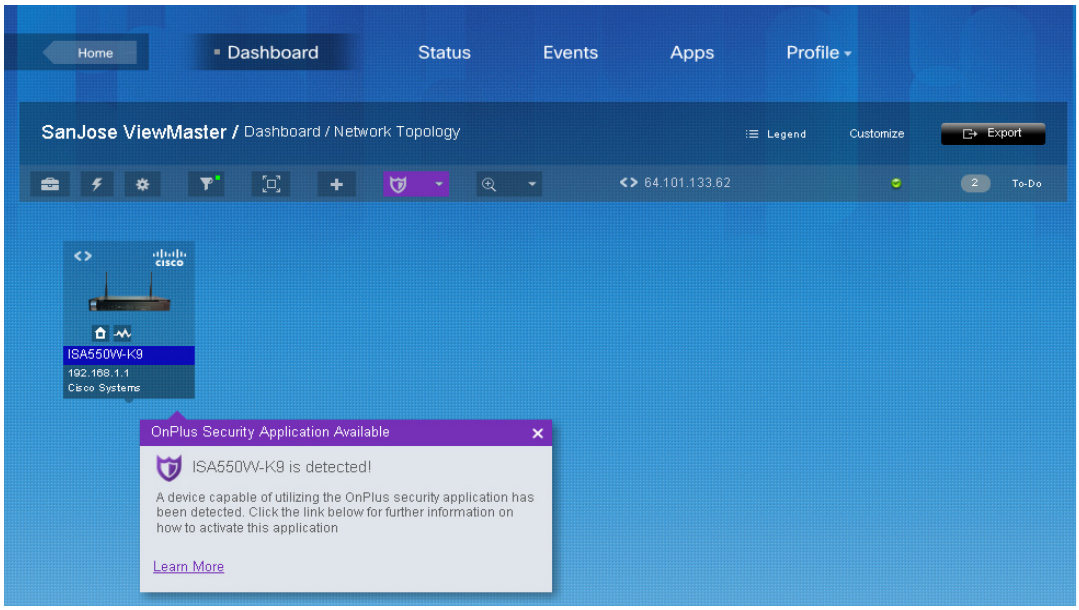
For more information, see the *Cisco OnPlus Portal User Guide*. To access the HTML version of the guide from the portal, click the **Documentation** link at the top of the page. The guide is also available on Cisco.com at the following URL:

www.cisco.com/en/US/products/ps11792/products_user_guide_list.html

Installing the OnPlus Portal Advanced Security App

IMPORTANT The purple OnPlus Security Application Available recommendation dialog in the Topology view does not appear immediately after you enter login access credentials for the ISA500 device. After you enter credentials, the OnPlus Portal discovery process must run and successfully log in to and verify the appliance before the recommendation dialog will appear. This can take 2 to 3 minutes or longer.

If the login access credentials you entered on the portal are valid and the portal can successfully discover and log in to the ISA500 device, the OnPlus Security Application tooltip appears in the Topology view and a purple Security icon appears on the dashboard toolbar.



To install the Advanced Security Application for a customer, follow these steps.

STEP 1 Click the Learn More link in the tooltip to go to the Apps page, where you can install the Advanced Security Application.

If you are a Cisco Customer and you have closed the tooltip, from the Dashboard, choose **Apps** from the menu at the top of the page.

If you are a Partner and you have closed the tooltip, go to the Partner Account Overview page, select the customer, and choose **Apps** from the menu at the top of the page.

STEP 2 On the Apps page, choose **Security** from the menu on the left. The Security menu displays the following message when an ISA500 is not installed in the network:

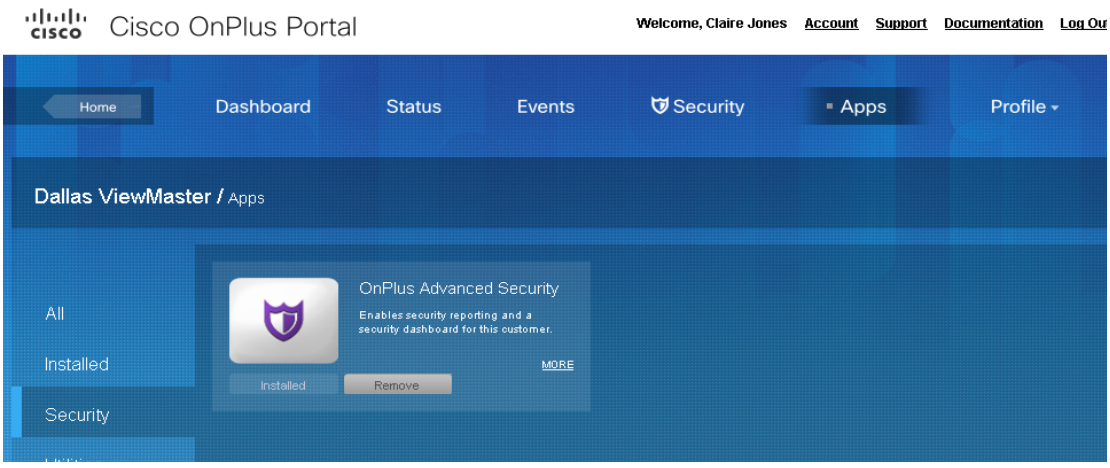
ISA570 or ISA500 Not Detected

STEP 3 Locate the Advanced Security Application and click **FREE**.

STEP 4 In the Add App window, click **Add** to sign up for the application and install the Advanced Security application.

STEP 5 Click **OK** to confirm the installation.

After the application is installed, the Security menu is added to the customer dashboard, and the Apps page on the portal shows that the app has been successfully installed.



For descriptions of available reports, see **Security Report Descriptions, page 13**.

To learn how to generate a report, see the section **Generating Security Reports, page 11**.

Removing the Advanced Security App

IMPORTANT When you remove the Advanced Security App, all ISA500 device data collected and stored on the OnPlus Network Agent by the security application is deleted and cannot be recovered.

To remove the Advanced Security application for your network or for a specific customer, follow these steps.

STEP 1 From the Customer Account Dashboard, choose **Apps** or from the Partner Account Overview page, select the customer and choose **Apps**.

STEP 2 In the list of Installed apps, locate the Advanced Security icon and click **Remove**.

STEP 3 Click **OK** to confirm.

When you remove the Advanced Security application, all ISA500 data collected and stored on the OnPlus Network Agent by the application is deleted.

Data Collection on the OnPlus Network Agent

When the Advanced Security application is installed, the user registers with the ISA500 (this requires device access credentials for the admin user to be entered on the portal). See **Installing the OnPlus Portal Advanced Security App, page 8**.

Data from the ISA500 Security Appliance is collected on the OnPlus Network Agent.

Data samples from the ISA500 Security Appliance are sent to the OnPlus Network Agent at 1-minute intervals.

- Numerical data samples are consolidated into hourly, daily, and monthly data samples.
- As the data is collected, it is stored in RAM on the OnPlus Network Agent.
- Once every twenty four (24) hours, at the OnPlus Portal maintenance window, the data in RAM on the OnPlus Network Agent is written to flash memory on the OnPlus Network Agent.

Generating Security Reports

To create an Advanced Security report, follow these steps.

STEP 1 To access the Create Report window, use one of the following methods:

- From the Customer Account Dashboard, choose **Security** to open the Security dashboard. Select Reports and click **+ Create Report**.
- From the Partner Account Overview, select a customer, then choose **Security** to open the Security dashboard. Select the **Reports** tab and click **+ Create Report**.
- From the Partner Account Overview page, choose **Reports** > **Report Listing**, then click **+ Create Report**.

STEP 2 In the Create Report window, choose a report type, select a customer (only if this is a Partner Account), and specify a format (PDF, CSV, or HTML).

For Partner Accounts, when you select a security report, only customers that have the Advanced Security Application installed appear in the Customer list.

Advanced Security reports are prefixed with the word “Security” in the report Type drop-down menu.

STEP 3 Choose sections to include in the report.

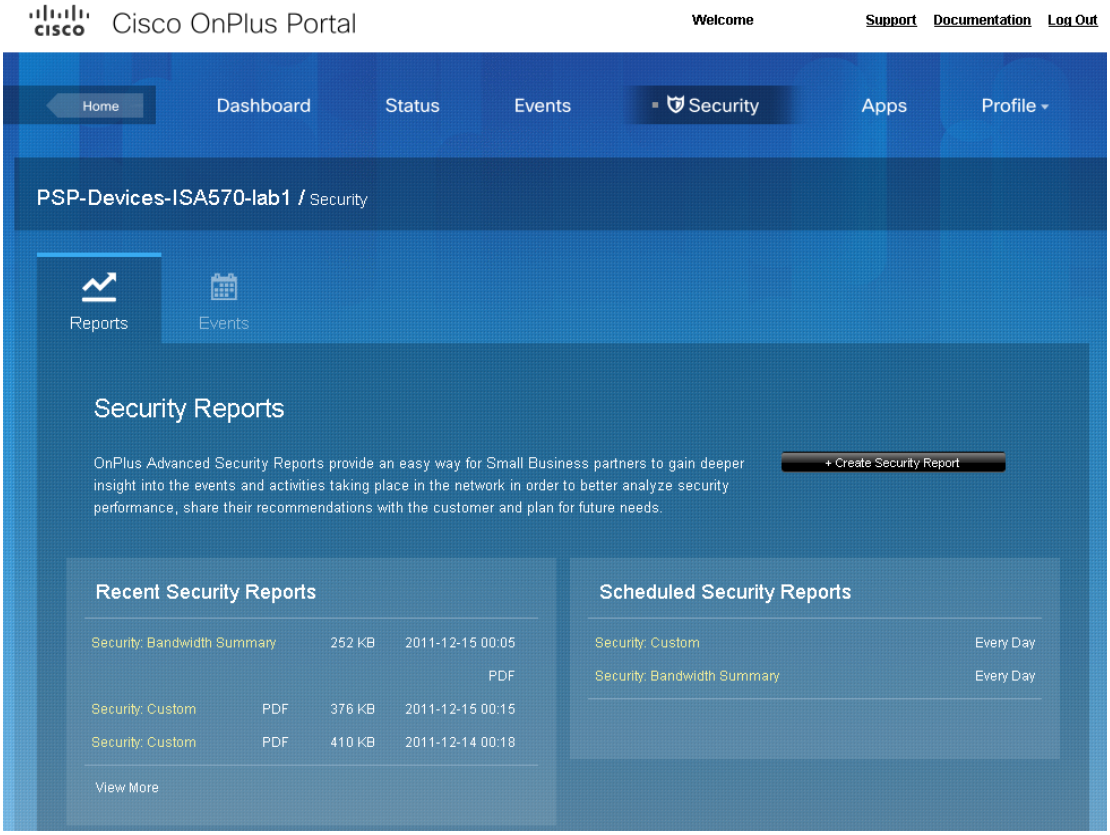
STEP 4 Choose scheduling options. You can create on-demand reports and specify begin and end dates for the reporting period or you can schedule recurring reports.

STEP 5 Click **Save**.

For Customer Accounts, Advanced Security reports can be viewed by selecting the **Reports** tab on the Security option of the Deathbed.

For Partner Accounts, Advanced Security reports for each customer can be viewed by selecting the **Reports** tab on the Security option of the customer's dashboard.

If the report does not appear in the list, try refreshing your Web browser.



These reports are also available from the **Reports** > **Reports** Listing page.

For more information, see the "Reports" section of the *Cisco OnPlus Portal User Guide*. To view the HTML version of the guide from the portal, click the **Documentation** link at the top of the page (to the left of the Logout link).

Security Report Descriptions

Refer to the following sections to learn more about the data that is collected and displayed in each type of report.

- Device Utilization
- Network Usage
- Bandwidth Summary
- Device Logins
- WiFi Report
- VPN Report
- Firewall Attacks
- Web Usage
- Web Threats (Security Services License Required)
- Virus Attacks (Security Services License Required)
- Spam Filter
- IPS Threats
- Custom

Device Utilization

Percent utilization of the CPU, compact flash, and RAM on the ISA500 Security Appliance, presented in graph and table formats.

Section	Description
CPU	Percent CPU utilization for the ISA500 Security Appliance.
Flash	Percent of compact flash memory in use on the ISA500 Security Appliance.
RAM	Percent of RAM storage in use on the ISA 500 security appliance.

Network Usage

Network usage in bytes and packets by protocol: HTTP, HTTPS, Email, SSH, and FTP, presented in graph and table formats.

Section	Description
HTTP Usage	HTTP traffic in bytes and packets on its well-known port, port 80.
HTTPS Usage	HTTPS traffic in bytes and packets on its well-known port, port 443.
Email Usage	Email traffic in bytes and packets. The email usage report aggregates traffic for Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), and Internet Mail Access Protocol (IMAP), by their respective well-known ports: ▪ Port 25, SMTP ▪ Port 465, secure SMTP ▪ Port 587, SMTP (message submission) ▪ Port 110, POP3 ▪ Port 995, secure POP3 (POP3 protocol over TLS/SSL) ▪ Port 143, IMAP4 ▪ Port 993, secure IMAP (IMAP4 protocol over TLS/SSL)
Top Mail Users	Reports the top email users by the amount of bandwidth consumed.
SSH	Secure Shell (SSH) traffic in bytes and packets on its well-known port, port 22.
FTP Usage	File Transfer Protocol (FTP) traffic in byes and packets on its well-known port, port 21.
Top FTP Users	Reports the top FTP users by the amount of bandwidth consumed.

Bandwidth Summary

Graphical and tabular format report of inbound and outbound traffic in bytes, by type.

When CSV is selected as the report format, the following additional data is provided: number of dropped packets (in), dropped packets (out), error packets (in), and error packets (out).

Section	Description
WAN Bandwidth	Inbound and outbound traffic in bytes for each WAN port (WAN port 0/1).
LAN Bandwidth	Inbound and outbound traffic in bytes for all LAN ports. LAN port dated is aggregated into a single number.
VLAN Bandwidth	Inbound and outbound traffic in bytes for each VLAN, VLANs are identified in the report by VLAN name and ID.
WiFi Bandwidth	Inbound and outbound traffic in bytes for each SSID. SSIDs in the report are identified by SSID name. The default SSID names are cisco1 through cisco4.
VPN Bandwidth	Inbound and outbound traffic in bytes, by protocol: IPSEC, site-to-site VPN, and SSLVPN. The data for site-to-site VPN includes site-to-site traffic.

Device Logins

ISA500 Security Appliance administrator logins, user account logins, and failed logins.

Section	Description
Admin Login	Timestamp, user ID (admin), and IP address of the computer being used to access the ISA500.
ISA User Logins	Timestamp, user ID, and IP address of the computer being used to access the ISA500.

Section	Description
ISA Failed Logins	Timestamp, user ID, and IP address of computer being used to attempt access to the ISA500.

WiFi Report

Reports WiFi usage.

The duration column for an entry is empty if the VPN user is connected when the report is generated.

Section	Description
WiFi Activity	Timestamp, user ID, IP address, and duration for each of the following events: ▪ Successful IPSec VPN login ▪ Failed IPSec VPN login ▪ Successful SSL VPN login ▪ Failed SSL VPN login

VPN Report

IPSec and SSL VPN login tracking.

The duration column for an entry is empty if the VPN user is connected when the report is generated.

Section	Description
VPN Login	Timestamp, user ID, IP address, and duration for each of the following events: ▪ Successful IPSec VPN login ▪ Failed IPSec VPN login ▪ Successful SSL VPN login ▪ Failed SSL VPN login

Firewall Attacks

Displays summary and detail information for firewall attack events detected by the Firewall Attack Protection Security Service on the ISA500 security appliance.

IMPORTANT The data available for this report depends on how the firewall attack settings are configured on the ISA500 device. If firewall attack settings are not configured in the ISA500, no data will be available. For information about configuring firewall attack settings on the ISA500, refer to the ISA500 Series Security Appliance administration guide or online help.

Section/Category	Description
Attacks by Date	Graph of firewall attacks by date and summary table for each time period showing the attack type, number of attacks, and percentage of total attacks.
Attacks by Category	Pie chart showing percentage of total attacks for the report period by category and table showing attack details by category for the reporting period. For each category, the summary line in the table displays the attack type, number of attacks, and percentage of total attacks. Detailed information for each attack includes the source and destination IP address for the attack, total number of attacks from each source IP, and percentage of attacks from each source IP.

Section/Category	Description
Attack Categories	
Block ICMP	Attack that attempts to discover network through ICMP Echo (ping) requests on the WAN interface. **Related ISA500 Settings**: Firewall > Attack Protection, WAN Security Checks: Block Ping WAN Interface.
Port Scan	Attack that sends inbound connection requests to WAN ports on the ISA500. **Related ISA500 Setting**: Firewall > Attack Protection, WAN Security Checks: Enable Stealth Mode.
TCP Flooding	A SYN flood attack, in which an attacker sends a succession of SYN (synchronize) requests to a target system (more than 200 simultaneous TCP packets per second) from the WAN ports. **Related ISA500 Setting**: Firewall > Attack Protection, WAN Security Checks: Block TCP Flood.
UDP Flooding	LAN security attack in which the attacker attempts to creates more than 200 simultaneous, active UDP connections per second from a single computer on the LAN. **Related ISA500 Setting**: Firewall > Attack Protection, LAN Security Checks: Block UDP Flood.
ICMP Notification	Notification of ICMP request to sender was silently blocked by the ISA500. **Related ISA500 Setting**: Firewall > Attack Protection > Block ICMP Notification.
Fragmented Packet	Fragmented packet from any zone to any zone were detected and blocked by the ISA500. **Related ISA500 Setting**: Firewall > Attack Protection, Firewall Settings: Block Fragmented Packets.

Section/Category	Description
Block Multicast	Multicast packets were detected and blocked by the ISA500. **Related ISA500 Setting**: Firewall > Attack Protection, Firewall Settings: Block Multicast Packets.
SYN Flooding	SYN flood attack in which the attacker sends a succession of SYN (synchronize) requests to a target system in excess of the SYN flood detect rate specified on the ISA500 Firewall Protection Settings page. **Related ISA500 Setting**: **Firewall** > **Attack Protection, DoS Attacks**: **SYN Flood Detect Rate (max/sec).**
Echo Storm	An ICMP flood attack in which the attacker sends ping requests to the WAN interface in excess of number of Echo Storm (ping pkts./sec) specified on the ISA500 Firewall Protection Settings page. **Related ISA500 Setting**: **Firewall** > **Attack Protection**, **DoS Attacks: Echo Storm (ping pkts./sec)**.
Ping Flooding	An ICMP flood attack in which the attacker sends ICMP packets (including ping packets) to the WAN interface in excess of the number of ICMP (ICMP pkts./sec) specified on the ISA500 Firewall Protection Settings page. **Related ISA500 Attack Protection Settings**: **Firewall** > **Attack Protection** > I**CMP Flood (ICMP (pkts./sec)**.
Other	Firewall attack detected and logged by the ISA500 that is not currently categorized by the OnPlus Advanced Security Application.

Web Usage

Displays summary and detail information for Web usage by category, top visited sites, top users, and blocked sites.

Section	Description
Web Usage by Category	Top Web site categories are ranked by the amount of HTTP/HTTPS traffic in bytes. For each category, a summary of the data appears on the first line, followed by details by site (site URL, number of hits, traffic in bytes, and percent of traffic for that category). **Related ISA500 Setting**: To categorize sites in the Web Usage report, you must enable Web URL filtering on the ISA500 (Security Services > Dashboard, Settings, Web URL Filtering. If Web URL filtering is not enabled, all sites are listed under "Other."
Top Visited Web Sites	Top-visited sites are ranked by the amount of HTTP/HTTPS traffic in bytes. For each of the top sites, the hit count, bytes transferred, and percent of total HTTP/HTTPS bytes transferred are listed. **NOTE** The Cisco ON100 Network Agent (ON100) device can appear in the Top Visited Web Sites, because data collected for OnPlus security reporting is transferred via HTTPS once per minute.
Top Users	Top users are ranked by the amount of HTTP/HTTPS traffic in bytes. For each of the top users, the hit count, bytes transferred, and percent of total HTTP/HTTPS bytes transferred are listed.

Section	Description
Blocked Web Sites	If you have blocked any Web sites via Policy Settings on the ISA500, attempts to visit to these blocked sites are listed in this section. For each event, the name of the blocked site, the name of the local host on the network accessing the site, and the site category are shown. **Related ISA500 Settings**: No data appears in this report unless you have enabled Web URL filtering and blocked sites using via a Policy Profile. To access these settings on the ISA500, choose **Security Services** > **Web URL Filtering** > **Policy Profile**.

Web Threats (Security Services License Required)

Displays summary and detail information for Web threats detected by the Web Reputation Filtering service or Security Policy Profile configured on the ISA500 appliance.

This report can only be generated if a valid Security Services license is installed on the ISA500. See **Verify ISA500 Series Security Services License, page 5**.

Section	Description
Web Threats Summary	Graphic and tabular display of Web threat events for the specified reporting period. Based on Security Services Web Reputation Filtering and Security Policy Profile settings in the ISA500 appliance, sites can be blocked by reputation, category, or site URL. The Filter column in the Web Threats table indicates which security filter on the ISA500 generated the event in response to an attempt access the blocked sites. For each time period, the number of threats and percent of total threats are shown. **Related ISA500 Settings**. This report is based on settings for **Security Services** > **Web Reputation Filtering**, **Security Services** > **Web URL Filtering** > **Policy Profile** (select URL categories to block or specify specific URLs to block), and **Security Services** > **Dashboard**, **Settings**, **Web URL Filtering** (Web URL filtering must be enabled in order to categorize Web threats.
Web Threats by Category	Number of Web threat events that occurred during the reporting period and percent of total Web threat for each event. **Related ISA500 Settings**. If you have enabled Web URL filtering on the ISA500 (**Security Services** > **Dashboard**, **Settings**, **Web URL Filtering**), Web Threats will be listed in the categories that appear under Web URL filtering. If Web URL filtering is not enabled, all threats will be categorized under “Other.”

Virus Attacks (Security Services License Required)

Displays summary and detail information for virus attack events detected by the ISA500 Anti-Virus Security Service.

This report can only be generated if a valid Security Services license is installed on the ISA500. See **Verify ISA500 Series Security Services License, page 5**.

Section	Description
Virus Attack Summary	Graphical and tabular display of virus attack events detected by the ISA500 anti-virus service. Summary data includes graphic and tabular display of the number of attacks and percent of total attacks for the reporting period. **Related ISA500 Settings**: This report will only have data if the anti-virus service is enabled on the ISA500. This setting is located under **Security Services** > **Anti-Virus** > **General Settings**.
Virus Attacks by Category	Graphical and tabular display of virus attacks by category. For each category, the total number of hits (attacks) are displayed. For each attack, the report shows the site that generated the attack, the local host accessing the site, and the type of security filtering that detected and generated the virus alert or blocked access. **Related ISA500 Settings**. This report will only have data if the anti-virus service is enabled on the ISA500. This setting is located under **Security Services** > **Anti-Virus** > **General Settings**. Also, If you have enabled Web URL filtering on the ISA500 (**Security Services** > **Dashboard**, **Settings**, **Web URL Filtering**), Web Threats will be listed in the categories that appear under Web URL filtering. If Web URL filtering is not enabled, all threats will be categorized under “Other.”

Spam Filter

Displays summary and details for emails blocked by the Spam Filter service on the ISA500. An email is classified as spam if the sender's reputation is below the SPAM threshold configured on the ISA500. This report can only be generated if a valid Security Services license is installed on the ISA500. See **Verify ISA500 Series Security Services License, page 5**.

Section	Description
Spam Filter Summary	Displays summary information collected by the spam filter on the ISA500. This data includes graphic and tabular display of the number of blocked emails and the percent of the total number of blocked emails for each segment of the reporting period. **Related ISA500 Settings**: This report will only have data if the spam filter is enabled and configured on the ISA500. These settings are located under **Security Services** > **Spam Filter**.
Top Spam Filters	Lists the SMTP servers that generated the greatest number of blocked emails. For each SMTP server, the report shows the server IP address or hostname, the number of blocked emails, and the reputation score. **Related ISA500 Settings**. This report will only have data if the spam filter is enabled and configured on the ISA500. These settings are located under **Security Services** > **Spam Filter**.

IPS Threats

Displays summary and detail information about security threats blocked by the Intrusion Prevention System (IPS) on the ISA500.

When CSV is selected as the report format, additional data is provided (for example, the source IP address of the blocked threat).

This report can only be generated if a valid Security Services license is installed on the ISA500. See **Verify ISA500 Series Security Services License, page 5**.

Section	Description
IPS Threats	Summary information about threats that were blocked by the Intrusion Prevention (IPS) service on the ISA500. Summary data includes graphic and tabular display of the number of blocked threats and the percent of the total number of blocked threats for each segment of the reporting period. **Related ISA500 Settings**. This report will only have data if Intrusion Prevention (IPS) is enabled and configured on the ISA500. These settings are located under **Security Services** > **Intrusion Prevention (IPS)**.
IPS Threats by Category	Displays detailed information for blocked threats by category. For each category of threat (Virus/Work, Access, Other, and so on), the report shows the total number of threats that were blocked and details for each threat, including the signature name, local hostname or IP address of the target of the threat, and the protocol used. **Related ISA500 Settings**. This report will only have data if Intrusion Prevention (IPS) is enabled and configured on the ISA500. These settings are located under **Security Services** > **Intrusion Prevention (IPS)**.
Top IPS Threats	Lists the most frequently blocked threats detected by IPS. For each threat, the report shows the signature name, category (for example, virus, Web attack, Access, and so on), and the number of times the threat was blocked (hits). **Related ISA500 Settings**. This report will only have data if Intrusion Prevention (IPS) is enabled and configured on the ISA500. These settings are located under **Security Services** > **Intrusion Prevention (IPS)**.

Custom

A Custom Security report can be generated by choosing sections from any of the Security reports listed in this section when generating the report.

For custom security reports, a Recommendation field is provided where you can enter specific comments or recommendations for the customer.

Sample Reports

WiFi Bandwidth (from Bandwidth Summary Report), Daily

WIFI Bandwidth

WIFI SSID: 570-data

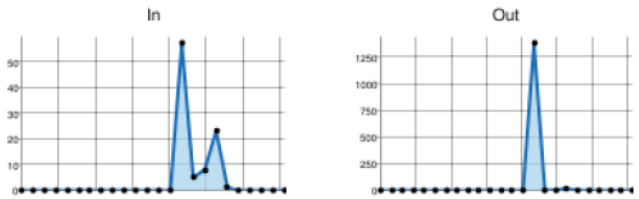


Table 5. WIFI SSID570-data: WIFI Bandwidth Bytes by Hour

	Hour	Bytes In	Bytes Out
1	00:00 - 01:00	0 B	0 B
2	01:00 - 02:00	0 B	0 B
3	02:00 - 03:00	0 B	0 B
4	03:00 - 04:00	0 B	0 B
5	04:00 - 05:00	0 B	0 B
6	05:00 - 06:00	0 B	0 B
7	06:00 - 07:00	0 B	0 B
8	07:00 - 08:00	0 B	0 B
9	08:00 - 09:00	0 B	0 B
10	09:00 - 10:00	0 B	0 B
11	10:00 - 11:00	0 B	0 B
12	11:00 - 12:00	0 B	0 B
13	12:00 - 13:00	0 B	0 B
14	13:00 - 14:00	0 B	0 B
15	14:00 - 15:00	57 B	1.342 KB

285416

Firewall Attack Summary, Attacks by Category, Daily

FW Attack Summary

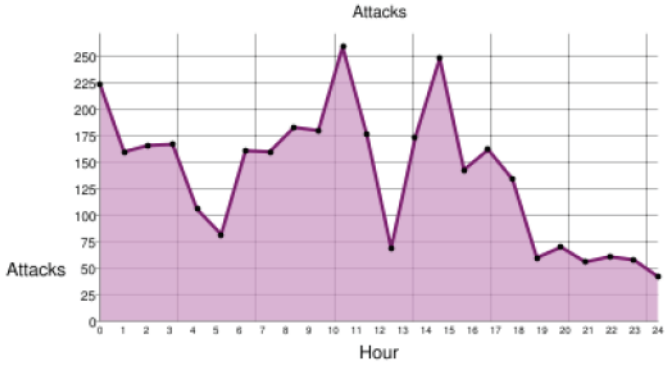


Table 15. FW Attack Summary

	Hour	Attacks	% of Attacks
0	05:00 - 06:00	224	7 %
1	06:00 - 07:00	160	5 %
2	07:00 - 08:00	166	5 %
3	08:00 - 09:00	167	5 %

285413

FW Attacks by Category

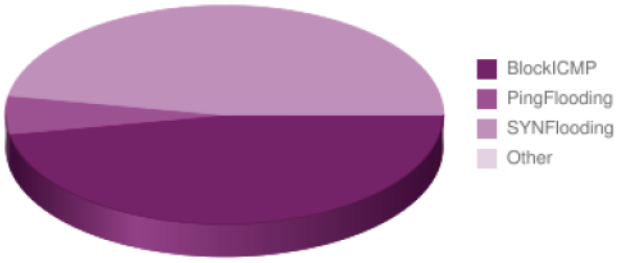


Table 16. Firewall Attacks by Category

	Type	Attacks	% of Attacks
1	Block ICMP	2816	86%

Source	Destination	Attacks	% of Attacks
192.168.10.40	171.68.226.120	2590	92%
192.168.10.40	72.163.47.11	125	5%
192.168.10.40	74.125.157.188	2	1%
192.168.10.1	192.168.75.100	75	3%
192.168.75.1	192.168.75.1	24	1%

	Type	Attacks	% of Attacks
2	Ping Flooding	12	1%

Source	Destination	Attacks	% of Attacks
192.168.75.100	64.102.121.149	12	100%

285427

Web Usage (Top Visited, Top Users)

NOTE The Cisco ON100 Network Agent (ON100) device can appear in the Top Visited Web Sites, because data collected for OnPlus security reporting is transferred via HTTPS once per minute.

Top Visited Web Sites

Top Users of Web

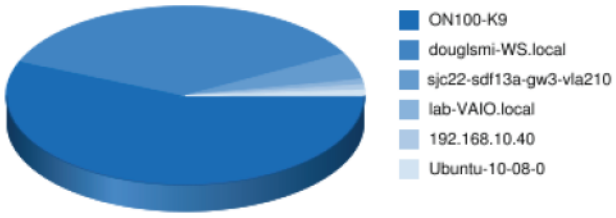


Table 3. Top Users of Web

	Local Host	Hits	Bytes	% of Bytes
1	ON100-K9	423	193.896 MB	58%
2	douglsmi-WS.local	2122	124.360 MB	37%
3	sjc22-sdf13a-gw3-vla210	352	15.620 MB	5%
4	lab-VAIO.local	4	3.365 MB	1%
5	192.168.10.40	223	1.395 MB	1%
6	Ubuntu-10-08-0	54	3.164 KB	1%

285414

Notes, Limitations, and Caveats

The following notes, limitations, and caveats apply to the Cisco OnPlus Advanced Security Application:

- When you remove the Advanced Security application on the portal, all ISA500 data that is stored on the OnPlus Network Agent by the security application is deleted.
- When the OnPlus Network Agent loses power, all ISA500 data stored in the RAM since the last successful maintenance window will be lost. There is no recovery. For more information, see **Data Collection on the OnPlus Network Agent, page 10**.
- If Cisco OnPlus support is disabled on the ISA500 Security Appliance, the Cisco OnPlus Service will be unable to communicate with the ISA500 device, and device management, monitoring and reporting will not function. Only basic device discovery and remote connectivity will be available through the OnPlus Service.
- If the reports indicate “No data is available,” the possible causes are as follows:
  - There was no relevant data to capture.
  - The Security Services license is not installed on the ISA500.
  - Security Services settings required to generate data for the report are not configured on the ISA500.
  - Device access credentials are invalid. This can occur if the password for the admin account used for login access by the portal is changed in the ISA500 Series Configuration Utility and is not updated on the portal.

Known Issues

The following known issues apply to the OnPlus Advanced Security App in Release 6.6 of the OnPlus Portal.

Ref #	Description
CSCtw72803	Firewall attack summary has inconsistent data in % of attacks. **Symptom:** Security report for firewall attack displays the attacks with percent in the summary chapter, and does not display the percent in the Attacks by Category section. **Recommended Action:** None.
CSCtw72872	Report types for unavailable services can be requested. **Symptom:** Security reports for unconfigured services can be requested. As an example, a virus attack report can be requested even if the ISA500 doesn't have a security services license or an anti-virus has not been enabled. The report will always return with no information available. **Recommended Action:** None.
CSCtw72819	XHTML firewall attack report header and data are offset. **Symptom:** Security report for firewall attack information is offset from the report header. **Recommended Action:** None.
CSCuc84317	Empty report is sent after modifying the default VLAN IP address of the Cisco ISA500. **Symptom:** An empty report is sent after the user modifies the default VLAN IP address of the Cisco ISA500. **Recommended Action:** If re-subnetting your whole network (via DHCP Server) you should manually release/renew your IPs to allow the client network devices to more quickly converge on the new subnet. If you cannot perform this step on the client device, then reboot the device to force the client to obtain a new IP from the DHCP server.

Where To Go From Here

Cisco provides a wide range of resources to help you and your customer obtain the full benefits of the Cisco OnPlus Portal.

Community	
Cisco Small Business Support Community for the OnPlus Service	https://supportforums.cisco.com/community/netpro/small-business/onplus
Cisco Small Business Support Community for the ISA500 Market Trial	https://supportforums.cisco.com/community/netpro/small-business/partnerzone/eft/isa500
OnPlus Training Library videos and podcasts	https://supportforums.cisco.com/docs/DOC-17701
OnPlus Device Compatibility Matrix	https://supportforums.cisco.com/docs/DOC-17501
Cisco Software Downloads	
Cisco Software Download Center	Downloads for all Cisco Small Business products are available in the Download area on Cisco.com at www.cisco.com/go/software (registration/login required).
OnPlus Portal and Documentation	
All Cisco OnPlus Technical Documentation	www.cisco.com/go/onplus
Small Business Support Community OnPlus Documentation	https://supportforums.cisco.com/docs/DOC-17447
For Partners	
Cisco OnPlus Portal Partner Account Signup and Login	www.cisco-onplus.com
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb

Document Number: 78-21035-01