TREND MICRO™
InterScan™ Web Security Appliance 2500 Quick Start Guide

InterScan™ Web Security Appliance (IWSA) helps protect LAN users against Internet threats including worms, network viruses, phish sites, spyware, and viruses. Optional IWSA modules can also provide Web content filtering and security against malicious Java applets and ActiveX controls.

Use this Quick Start Guide to get IWSA up and running on your network, and then use the Administrator's Guide to configure, update, and test IWSA.

1 Open and inspect the IWSA carton

Please verify that your IWSA carton contains each of the following items:

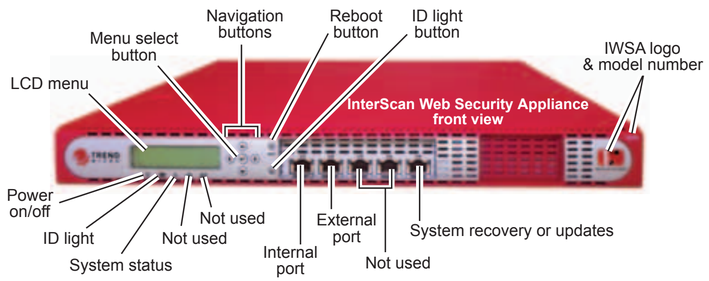
 InterScan Web Security Appliance	 Power Cord	 Cross-over Cable
 Console Cable (RS-232)	 Mounting Rail	 CD, Jacket & Safety Card, License & warranty

Contact Information

- Local offices: http://www.trendmicro.com/en/about/contact/us.htm
- Phone: + 1 (800) 228-5651 or + 1 (408) 257-1500
- Address: Trend Micro, 10101 N. De Anza Blvd., Cupertino, CA - 95014, USA

2 Understand the IWSA server

Unless you modify the proxy settings, IWSA is pre-configured to transparently scan all inbound and outbound Web traffic — your end-users do not need to modify their browser settings. You can also configure IWSA to work with an ICAP client.

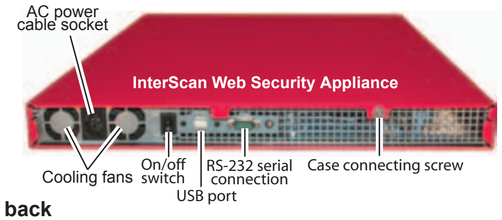


Explanation of indicator lights and ports

The front of the IWSA server contains three indicator lights to reflect its operational status, and three ports. The lights and ports are explained in the table that follows.

Light	State	Description
Power	Orange–steady	IWSA server is on and operating normally.
	Off (no color)	Device is off.
ID	Blue–steady	The unit identification light is on; use it to identify the IWSA server in a crowded server room.
	Orange–flashing	The IWSA server is booting.
System	Red–one flash	Power-On Self-Test (POST).
	Yellow–steady	IWSA firmware is ready.
	Off	Not used.

Port	Cable	Description
Port 1 (INT)	Ethernet	Use an Ethernet cable to route internal network traffic to IWSA.
Port 2 (EXT)	Ethernet	Route scanned traffic from IWSA to an external device (for example, a firewall); this port is used only in bridge mode.
Port 3	Disabled	This port is not used.
Port 4	Disabled	This port is not used.
Port 5	Cross-over	Update or recover system files and firmware (DOM).



IWSA server back

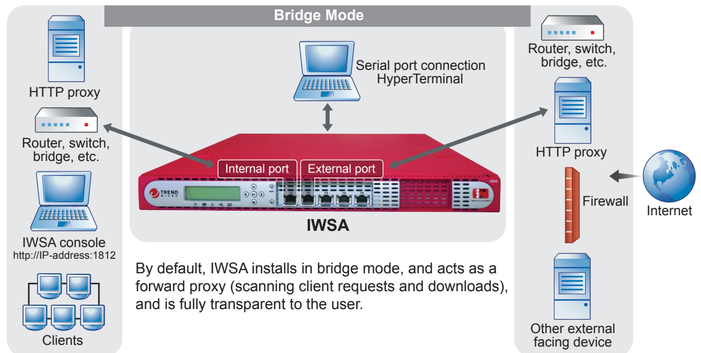
Port	Cable	Description
RS-232	Console cable	Connect a laptop to the RS-232 port to configure IWSA hardware settings, update the firmware, or reinstall IWSA program files. Requires Microsoft HyperTerminal (or a similar program) on the laptop. See the Administrator's Guide for details.
USB port	USB cable	Not used.

3 Decide the network configuration

Before proceeding with the IWSA setup, decide where on the LAN you want the IWSA server to sit. IWSA supports three topologies:

Network Bridge

- Clients — network device — IWSA — network device — Internet



Pass traffic from one network device such as a switch, router, or firewall to another device for delivery to the requesting client. IWSA acts as a bridge between the devices and transparently scans passing HTTP and FTP traffic.

Configurations

- If your physical network is comprised of multiple IP segments, and IWSA will scan traffic for clients from a different segment, join IWSA to the clients' segment by giving it a bridge ID from that segment. You can set bridge ID settings from the IWSA console (**Administration** > **Bridge ID Settings**).
- If an L3 switch or router that receives client traffic from one segment will connect to an IWSA server residing in a different segment, modify the IWSA routing table or static route settings so it points to the device.

  Note: If your physical network has VLAN settings, bind the management IP or bridge IDs to the specific VLANs. See the IWSA Solutions CD or online help for details.
- If the clients and IWSA are in the same segment, no configuration is required.

HTTP proxy

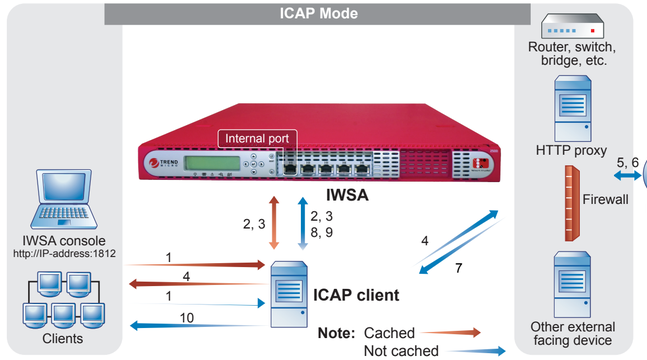
- Clients — IWSA — Internet

  In HTTP proxy mode, configure client browsers to use IWSA as a proxy. Connect your network (device) to IWSA port 1. The default proxy port number is 8080.

ICAP mode

- Clients — ICAP capable cache server — Internet
  |
  IWSA (acting as ICAP server)

  Choose this topology if you have an ICAP server on the network and you want it to pass traffic to IWSA for scanning. IWSA will act as an ICAP server (and the original ICAP server then behaves as an ICAP client). Connect your network device to IWSA port 1.



Notes on port usage

Use both the internal and external ports if you will be installing IWSA in bridge mode. Use only the internal port for the other modes. Use port 5 to connect a laptop to the IWSA server and run the system utilities from the IWSA Solutions CD.

Hardware setup

Use the chart below to prepare the network values for which IWSA will prompt you.

Value	Your Answer
IP address for IWSA server:	
Host name (domain.com):	(supports a-z, 0-9, -, and .)
Netmask (subnet):	
Gateway:	
Primary DNS:	
Secondary DNS:	
TMCM server IP address:	(requires Control Manager)
TMCM account: (the user name IWSA will use to log in to the TMCM server)	(supports A-Z, a-z, 0-9, -, and _)

4 Mount the IWSA server

Mount the IWSA server in a standard 19-inch 4-post rack, or on a free-standing device such as a sturdy desktop. Instructions can be found in the back of the Administrator's Guide, which is available on the IWSA Solutions CD and from the Trend Micro Update Center.

When mounting the server, be sure to allow at least two inches clearance in all directions for cooling.

5 Power IWSA on and off

To power on IWSA, press and release the **power on/off** switch of the IWSA device.

IWSA would normally be powered off during maintenance (such as upgrading the memory) or when moving it to a different physical location.

Notes:

- Power off IWSA only during maintenance to minimize the impact on HTTP and FTP traffic interruption
- If IWSA is powered off by unplugging the device, traffic will be interrupted
- If IWSA is on network bridge mode and "Fail-open on system error" is enabled in the Web console (**IWSA Web Console** > **HTTP** > **Configuration** > **Proxy Scan Settings**):
  - HTTP and FTP traffic will not be interrupted
  - If IWSA is powered off, HTTP and FTP requests and responses will be passed but the traffic will not be scanned, leaving your network unprotected

To power off IWSA, press and then hold the Power on/off switch for 5 to 10 seconds. In noisier environments, users will feel that the device stops vibrating.

TREND MICRO™ InterScan™ Web Security Appliance 2500 Quick Start Guide

6 Configure the network settings

You can configure network settings using HyperTerminal or the LCD panel and navigation keys on the front of the device.

To configure network settings using HyperTerminal:

1. Check that the computer you are using for preconfiguration has HyperTerminal.
2. Connect one end of the included console cable to the CONSOLE port on the back panel of the device and the other end to the serial port (COM1, COM2 or other COM port) on a computer.
3. Click **Start** > **Programs** > **Accessories** > **Communications** > **HyperTerminal**.
4. Specify a name for the connection. In the next screen, specify the communications port where the cable is connected.
5. To prepare HyperTerminal for optimal use, set the following properties:
   Bits per second: 115200
   Data Bits: 8
   Parity: None
   Stop bits: 1
   Flow control: None
   Emulation: VT100 (You can set this value by selecting **File > Properties | Settings** tab.)
6. Press **Enter**. The User name logon prompt displays.
7. Type the default administrator user name and password.
   User name: root
   Password: iwsa
8. Access the preconfiguration screen, and select **System Configuration**.
9. Select **Configure Device Settings**, and then select **Change Device Network Settings**.
10. Specify all the required network settings.
    Note: If IWSA will be deployed to an environment with a specific VLAN, the management IP should be bound to the specific VLAN. Specify the VLAN ID to which the Management IP address will bind. Consult the Administrator's Guide for a discussion of the different scenarios when deploying IWSA to a VLAN environment.
11. Select **Back to Top** to save the settings.

To configure network settings using the LCD panel and navigation keys:

1. With the IWSA server powered on, press any of the navigation buttons to enable the LCD.
2. Press ↵ to see Configure Device.
3. Press ▼ to move from "Go Back" to Configure Device, and then press ↵ again.
4. When prompted to **Modify Settings?**, press ↵ for **Yes**.

5. Use the navigation buttons on the front of the IWSA server to assign an IP address and provide the other required network settings.
   - Press ▲ or ▼ to navigate to the correct number
   - Press ▼ once to get the dot (.) used between numbers
   - Press ► to move to the next number
   - Press ◄ to erase a number
   - Press ↵ to accept the settings and move to the next
6. Next, follow the same procedure to configure the following:
   - Host name (supports a-z, 0-9, - , and .)
   - Netmask, gateway, primary and secondary DNS
7. When prompted to **Enable TMCM?**, choose **Yes** if you are running Trend Micro Control Manager version 3.0 with Service Pack 5 and want to manage the IWSA server with it. Choose **No** if you are not using TMCM or have a different version.
   To configure the TMCM connection, provide the IP address of the TMCM server and an account name IWSA can use to log on to the TMCM server.

Returning to the configuration menu...

After the initial configuration, you can re-enter the menu at any time:

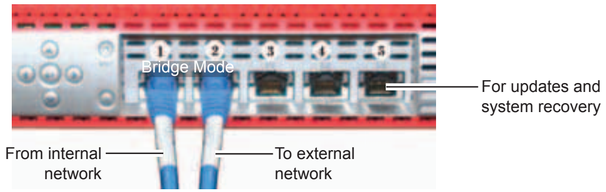
1. Press ↵ to open the menu, and then ▼.
2. Choose **Configure Device**, and then press ↵.
3. Choose **Yes** to **Modify Settings?**, and then press ↵ to review or navigate through the settings.
   a. To fix an incorrect value, use ◄ to return to the error and then ▲ or ▼ to correct it.
   b. Press ↵ to navigate past the settings you do not want to change until you reach the **Save changes?** prompt. Press ↵ to accept the changes.

7 Connect IWSA to your network

When powered on, IWSA begins proxying Web traffic as soon as the cables are connected. Scanning will not begin, however, until you activate the IWSA software as explained in task 11.

To connect the IWSA server to your network:

1. Connect an Ethernet cable to the internal IWSA port (port 1) and to the device from which IWSA will receive Web traffic (such as a firewall).
2. If you are setting up IWSA in bridge mode, use a second Ethernet cable to connect the device to which IWSA will deliver scanned Web traffic (such as a proxy server) to the external IWSA port (port 2).



3. Hardware configuration is now complete. To test the hardware setup and complete the IWSA configuration, relocate to a computer with access to the IWSA server and open a Web browser. Enter the URL for the IWSA console:
   `http://[IP Address]:1812`

Notes:

- If the management IP is bound to a specific VLAN, the IWSA console will only be connected with this specific VLAN tagged.
- If IWSA and the client/server are on different network segments, or if there is a router/gateway (not the default gateway) between IWSA and the client/server, configure static route settings in the IWSA console. See the IWSA Solutions CD or online help for details.

8 Register IWSA

To enable virus pattern file and other updates, you need to access the Trend Micro Web site, register IWSA, and activate it using the key you receive after registering.

To register IWSA and receive an Activation Code:

1. Using a desktop or other machine with access to the Internet, enter the following URL in a Web browser to access Online Registration:
   `https://olr.trendmicro.com/registration`
   Already registered
   - Enter your Logon ID and password if you already have a registration account, and follow the on-screen instructions.

   First visit
   - Choose your location and click **Continue** if you have previously registered with Trend Micro.
2. In the Web page that appears, enter your Registration Key and click **Continue**.
3. Select the product(s) that you will register and click **Continue**. IWSA includes basic scanning (viruses, spyware, and other Internet threats), an optional Web filtering module, and optional ActiveX and JavaScript protection.
4. In the License Agreement screen that appears, select **I accept...** and then click **Submit**.
5. Fill out the requested information and follow the on-screen instructions to complete the process and receive your Activation Code online.
6. Save the Activation Code or codes you receive.

9 Log on and change the IWSA password

Open the IWSA console from a desktop or laptop on the network that can access the IWSA server (and is running Internet Explorer version 6.0 or later).

To open the IWSA console:

- Enter the following URL in your Web browser's address field:
  `http://[IP Address]:1812`

To log on to the IWSA console:

- In the **Password** field that appears, enter the following:
  adminIWSS85

To change the default password:

- From the main IWSA menu, click **Administration > Password**.

10 Specify the proxy mode

If you have cabled IWSA in your network to work with an HTTP proxy or ICAP server, you need to configure the IWSA software to support that configuration before activating the product. Once activated, IWSA will automatically begin to scan Web traffic using a default set of robust settings.

To modify the IWSA proxy mode:

1. From the IWSA menu, click **HTTP > Configuration > Proxy Scan Settings**.
2. Choose how you want IWSA to process traffic:
   - **Network bridge** — IWSA acts as a network bridge, scanning all HTTP and FTP traffic routed through it.
   - **HTPP proxy** — IWSA works with an upstream or downstream proxy server.
   - **ICAP Server** — IWSA scans all Web traffic to and from the LAN as it is proxied by an ICAP server (which then acts as a client) already on the network.
3. The remaining options on the Proxy Scan Settings page are explained in the online help. From any IWSA console screen, click the help icon ? in the upper right corner for information on how (and why) to configure the rest of the settings on the page.

11 Activate IWSA and start scanning

IWSA contains three modules, two of which are optional. To begin scanning after installation, each module must be individually activated.

- InterScan Web Security Appliance (main program)
- URL Filtering (optional, Web content control)
- Malicious Mobile Code (optional, protection against malicious JavaScript and ActiveX)

You must register IWSA to receive your Activation Code(s), which will be sent to the email address specified during registration.

To activate the IWSA module(s):

1. From the main IWSA menu, click **Administration > Product License**. The Product License screen appears.
2. Click the **Enter New Code** link for InterScan Web Security Appliance and then, in the Enter A New Code screen that appears, type the Activation Code you received after registering.
3. Click the **Activate** button. Scanning and/or content filtering automatically begins for each module you activated.

12 Default scan settings

Upon activation, IWSA begins processing traffic using the following default settings:

- Scans all HTTP and FTP uploads and downloads for viruses (does not scan HTTPS traffic)
- Scans downloads/uploads of files not exceeding 2048MB (HTTP) and 1024MB (FTP)
- Cleans infected files, deletes uncleanable ones (such as Trojans and worms), and skips password-protected or encrypted files
- Encrypts quarantined files
- Does not scan traffic for spyware/grayware
- Blocks access to known phish sites
- Checks Web traffic for malicious JavaScript and ActiveX code
- Identifies users by IP address in logs and reports

13 Test and finish setting up IWSA

Trend Micro recommends that you update the IWSA pattern files, specify an email server and address for automatic notifications (the default is "root"), and test your installation to confirm that it works. Instructions for these and other important first-use tasks are described in the online help.

- Using HyperTerminal to access all the IWSA hardware settings, including the server password
- Securing the IWSA console using HTTPS
- Configuring notification messages

For additional Trend Micro recommendations, various best practices, tips on optimizing performance, troubleshooting tips, and error messages see the online help and Administrator's Guide.

Item Code: IHEQ02872/60928