



CHAPTER 31

Cisco Incident Control Server

The Cisco Incident Control Server (Cisco ICS) enables extended protection across Cisco IOS routers, switches, and IPS devices. In coordination with Trend Micro's incident control solutions, Cisco ICS prevents the spread of day-zero outbreaks in three ways:

- First, Cisco ICS issues temporary ACLs to those Cisco mitigation devices that can block such traffic, typically using a protocol and port pair block. This temporary block is referred to as an Outbreak Prevention ACL (OPACL).
- Second, as soon as a signature is available, Cisco ICS updates all Cisco IPS and IDS devices running on your network with the signature required to detect and prevent the specific threat. This signature is referred to as an Outbreak Prevention Signature (OPSig).
- Third, Cisco ICS can manage supporting products (sold separately), such as Trend Micro's Damage Cleanup Services (DCS), which cleans infected hosts by removing trojans and other malware.

To complete the Cisco ICS communication settings, you must perform two tasks: configure Cisco ICS to send syslog messages to the MARS Appliance, and add the Cisco ICS management server to the MARS web interface as a reporting device.

This chapter contains the following topics:

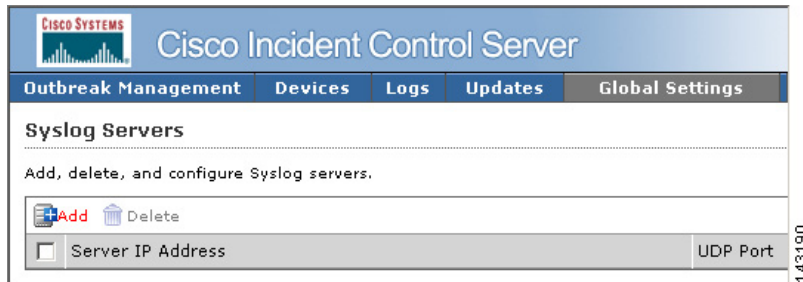
- [Configure Cisco ICS to Send Syslogs to MARS, page 31-1](#)
- [Add the Cisco ICS Device to MARS, page 31-2](#)
- [Define Rules and Reports for Cisco ICS Events, page 31-3](#)

Configure Cisco ICS to Send Syslogs to MARS

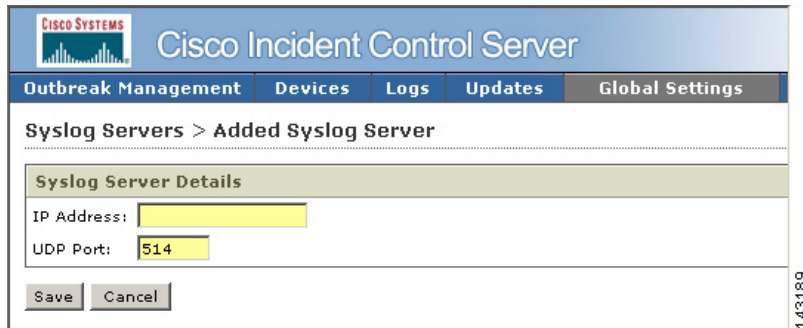
Cisco ICS publishes syslog messages to MARS. To configure Cisco ICS, you simply define a syslog server with the IP address of the MARS Appliance. You do not need to enable any special logs, and you cannot tune the messages that are sent to MARS. The Cisco ICS events for which syslog messages are generated have been selected to provide the most benefit to your Security Threat Mitigation (STM) system.

To prepare Cisco ICS to publish events to MARS, follow these steps:

-
- Step 1** Log in to the Cisco ICS Management Console.
 - Step 2** Click **Global Settings > Syslog Servers**.



Step 3 Click **Add**.



Step 4 In the IP Address field, enter the address of the MARS Appliance to which the Cisco ICS will publish syslog messages.

Step 5 Click **Save**.

Cisco ICS now publishes syslog message to MARS. For MARS to be aware of this device, you must add the Cisco ICS device as a software application running on a host and you must click **Activate** in the web interface.

Add the Cisco ICS Device to MARS

Before MARS can be processing the syslog messages as Cisco ICS messages, you must define the Cisco ICS management server as a software application running on a host. After Cisco ICS is defined as a reporting device, MARS can process any inspection rules that you have defined using Cisco ICS event types.

To add a Cisco ICS server to MARS, follow these steps:

Step 1 Click **Admin > Security and Monitor Devices > Add**.

Step 2 From the Device Type list, select **Add SW Security apps on a new host**.

You can also select **Add SW Security apps on an existing host** if you have already defined the host within MARS, perhaps as part of the Management > IP Management settings or if you are running another application on the host, such as Microsoft Internet Information Services.

Step 3 In the Device Name field, enter the hostname of the server.

- Step 4** In the Reporting IP field, enter the IP address of the interface in Cisco ICS server from which the syslog messages will originate.
- Step 5** Under Enter interface information, enter the interface name, IP address, and netmask value of the interface in Cisco ICS server from which the syslog messages will originate.
This address is the same value as the Reporting IP address.
- Step 6** Click **Apply**.
- Step 7** Click **Next** to move the Reporting Applications tab.
- Step 8** In the Select Application field, select **Cisco ICS 1.x**, then click **Add**.

Cisco ICS

Submit if you want to add Cisco ICS to this host

Cancel

Submit

143191

- Step 9** Click **Select** to add the Cisco ICS application to this host.
- Step 10** Click **Done** to save the changes.
- Step 11** To activate the device, click **Activate**.

Define Rules and Reports for Cisco ICS Events

From Cisco ICS, MARS receives syslog messages that allow it to identify outbreaks, successful OPACL and OPSig deployments, and failed attempts to deploy. MARS stays abreast of when the OPACLs and OPSigs fire on Cisco IPS devices. MARS also monitors the Cisco ICS server for system issues, such as database failures.

These events assist MARS in providing an accurate, holistic assessment of your network. OPACL and OPSig matching events provide five-tuple correlation, which MARS uses to perform attack path analysis and verify the containment of threats. You can use the events to define inspection rules that help you perform manual mitigation on devices that cannot use OPACLs and OPSigs.

For example, an inspection rule could be written to match the OPACL event. Your mitigation team can respond by investigating the OPACL that was pushed to the reporting device, from which they can determine the five tuple (source address and port, destination address and port and network service). Using that information, they could push equivalent ACLs to devices not managed by Cisco ICS.

When defining inspection rules or reports, you can access the list of Cisco ICS-specific events by entering *Cisco ICS* in the Description / CVE: field and clicking Search on the Management > Event Management page of the web interface.

There are four predefined system inspection rules for Cisco ICS:

- New Malware Discovered
- New Malware Prevention Deployed
- New Malware Prevention Deployment Failed
- New Malware Traffic Match

In addition, there are five predefined reports:

- Activity: New Malware Discovered - All Events
- Activity: New Malware Prevention Deployment Failure - All Events
- Activity: New Malware Prevention Deployment Success - All Events
- Activity: New Malware Traffic Match - All Events
- Activity: New Malware Traffic Match - Top Sources