

## LOCATING A MISSING ASSET

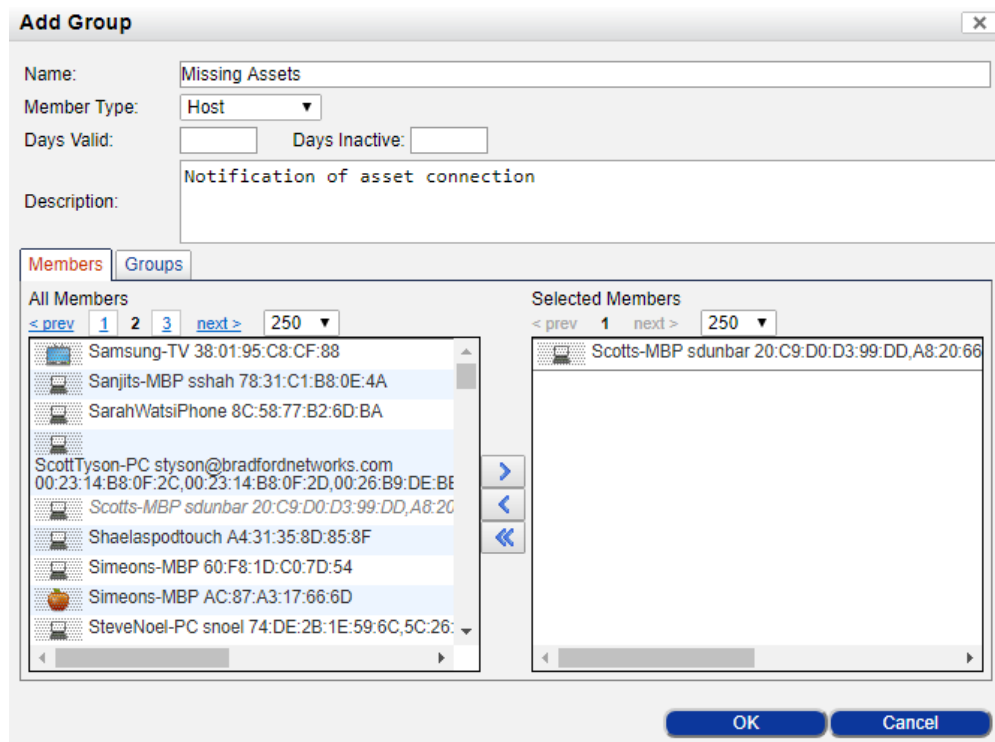
**DATE:** 01.07.2013

**REVISED:** 08.28.2018

If an asset, such as a laptop, is stolen or missing, you can monitor the network in case it later connects to the network. When it does, you will have the means to locate it.

### Section 1. Create a Group for Missing Assets

1. From the Admin UI, navigate to **System -> Groups**.
2. **Add** a new group and fill in the fields. Member Type should be Host.
3. Select the host deemed as the “missing asset” on the left in the All Members section and press the → to add the host to the Selected Members section on the right, then click **OK**. Note that only registered hosts will appear in this list.



## Section 2. Enable the Event

1. Navigate to **Logs -> Event Management**.
2. Locate the **Host Connected** event.
3. Set the Log to **Internal** or **Internal & External**. Any host that connects to the network will trigger a "Host Connected" event.

The screenshot shows the Fortinet Event Management interface. At the top, there is a navigation bar with 'Event Management' and 'NETWORK SENTRY / RTR'. Below this is a menu bar with 'Bookmarks', 'Users', 'Hosts', 'Network Devices', 'Logs', 'Policy', 'System', and 'Help'. The main content area is titled 'Event Management - Displayed: 439 Total: 439'. It features a table with columns: Log, Event Name, Group, Group Type, Last Modified By, and Last Modified Date. A 'Modify Group' dialog box is open over the table, showing a dropdown menu with 'Missing Assets' selected. The dialog has 'OK' and 'Cancel' buttons. The table row for 'Host Connected' is highlighted in blue, with 'Missing Assets' in the Group column, 'adonaldson' in the Last Modified By column, and '09/01/17 03:27 PM EDT' in the Last Modified Date column. At the bottom, there are 'Export to' options (CSV, PDF, RTF) and 'Options' and 'Modify Group' buttons.

Log	Event Name	Group	Group Type	Last Modified By	Last Modified Date
Internal	Gaming Device Registration	All Groups	Host		
Internal	Group Does Not Exist For Scan				
Internal	Guest / Contractor Pre-allocation Critical				
Internal	Guest / Contractor Pre-allocation Warning				
Internal & External	Guest Account Created	All Groups	Host		
Internal & External	Guest Account Deleted	All Groups	Host		
Internal	HTTP Rate Limiting Disabled				
Internal	HTTP Rate Limiting Enabled				
Internal	Hard Disk Usage Critical				
Internal	Hard Disk Usage Warning				
Internal & External	Host Aged Out				
Internal & External	Host Application Violation				
Internal & External	Host Application Violation Re				
Internal & External	Host At Risk				
Internal & External	Host At Risk Failure	All Groups	Host		
Internal & External	Host At Risk Success	All Groups	Host		
Disabled	Host At-Risk Status Not Enforced	All Groups	Host		
Internal	Host CLI Task Failure	All Groups	Port		
Internal	Host CLI Task Success	All Groups	Port		
Internal	Host Connected	Missing Assets	Host	adonaldson	09/01/17 03:27 PM EDT
Internal	Host Copied from NCS	All Groups	Host		
Disabled	Host Created	All Groups	Host		
Internal	Host Destroyed	All Groups	Host		
Internal & External	Host Disassociated	All Groups	Device		
Internal & External	Host Disconnected	All Groups	Host		
Internal	Host Has Multiple Adapters Connected	All Groups	Host		
Internal	Host Identity Changed	All Groups	Host		
Internal & External	Host Passed Security Test	All Groups	Host		
Internal	Host Pending At Risk	All Groups	Host		

### Section 3. Mapping the Event to an Alarm

To notify administrations as soon as the missing device has reconnected to the network, map an alarm to the event.

1. Navigate to **Logs -> Event to Alarm Mappings**.
2. Locate and Modify the **Host Connected** event. If no **Host Connected** event exists, then use the **Add** button.
3. Modify the alarm mapping so that it only applies to the **Missing Assets** group. Also select **Notify Users** and select the **All Management Group** or another applicable user group. Click the **Send Email** box, and click **OK**. Members of the All Management Group will receive an email when a host in the Missing Assets group connects to the network.

**Modify Event to Alarm Mapping**

Enabled

Trigger Event: Host Connected

Alarm To Assert: Host Connected

Severity: Critical

Clear on Event: 17.6.1.3.6.1.4.1.776.102.6.0.3

Send Alarm to External Log Hosts

Send Alarm to Custom Script: AgentlessScanRegisterClient

Apply To: Group Missing Assets

Notify Users: All Management Group

Send Email  Send SMS

Trigger Rule: One Event to One Alarm

Action: Command Line Script Action

OK Cancel

### Section 4. Validate the Configuration

1. Connect the “missing asset” to the network.
2. Navigate to **Logs -> Events** and verify that an event has been triggered. An easy way to find the event is to filter for only the Host Connected event and press **Update**.
3. The Message field indicates the location of the missing asset.
4. Members of the All Management Group should also receive an email regarding the Host Connected event. This assumes that Email Settings are configured and functioning properly. Navigate to **System -> Settings -> Email Settings** to verify.