

Rogue Device Detection

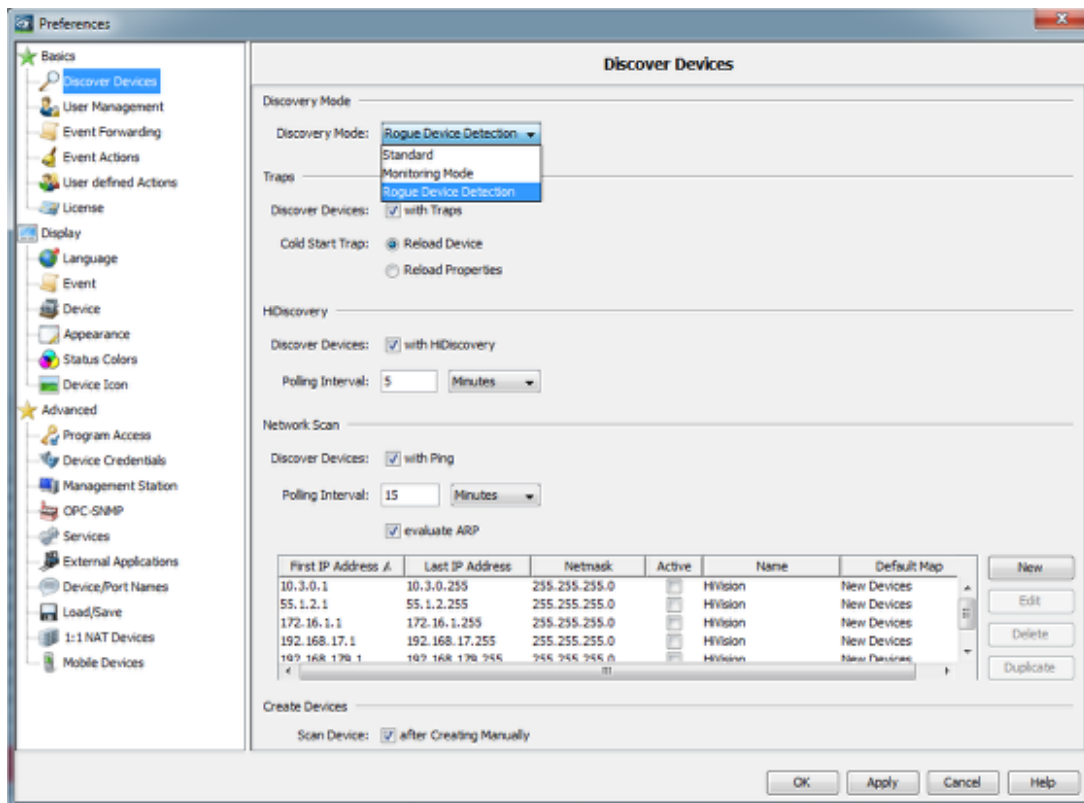
- 2018-02-21 - Industrial HiVision

Rogue Device Detection is available as of IHV v6.0 and can be selected in the preferences dialog.

This discovery mode will detect devices using the selected discovery options but place discovered devices in a separate folder named Rogue Devices.

This feature allows to find devices which do not belong to the monitored network.

Discovery Mode



In the preferences you can select from 3 different discovery modes.

Standard: IHV uses the selected options to discover devices

Monitoring Mode: no automatic scanning but Network Scan, HiDiscovery Scan or add device manually are available

Rogue Device Detection: selected options will be used (at least one option must be selected). Discovered devices will be placed in folder Rogue Devices

Rogue Devices

The screenshot shows the Hirschmann Industrial HiVision software interface. The top menu includes File, Edit, View, Configuration, Tools, and Help. The main window displays a network map with a 'Rogue Devices' folder highlighted in red. Below the map is a table of 'Unacknowledged Events'.

ID	Act.	Type	Category	Time	User	Source	Component	Message
535			Device Managed	2015-04-27 13:22:13	DEPSTAR@	Industrial HiVision Service		Device Added to Topology 172.16.1.226, 00:80:63:2F:6E:08
534			Device Managed	2015-04-27 13:22:08	DEPSTAR@	Industrial HiVision Service		Compatible Class Found for Device: IP Address: 172.16.1.220, 00:80:63:2F:6E:08. Device Class: CooperRail, Mach 4000, ...
533			Device Managed	2015-04-27 13:23:07	DEPSTAR@	Industrial HiVision Service		SNMP Access Established 172.16.1.220
532			Device Discovered	2015-04-27 13:23:07	DEPSTAR@	Industrial HiVision Service		New Rogue Device Detected by SNMP Trap 172.16.1.220
531			Device Discovered	2015-04-27 13:23:07	DEPSTAR@	Industrial HiVision Service		New Rogue Device Detected by SNMP Trap 172.16.1.220
530			User Intervention	2015-04-27 13:22:26	superuser	Industrial HiVision		Privileged Mode Entered
529			User Intervention	2015-04-27 13:22:12	superuser	Industrial HiVision		Industrial HiVision is Switched to Edit Mode! superuser/Operator
528			User Intervention	2015-04-27 13:22:12	superuser	Industrial HiVision		Industrial HiVision is Switched to Run Mode! superuser/Operator
527			Device Removed	2015-04-27 13:22:07	DEPSTAR@	Industrial HiVision Service		Device Removed: 172.16.1.226, 00:80:63:2F:6E:08
526			User Intervention	2015-04-27 13:22:05	DEPSTAR@	Industrial HiVision		Refresh Device (F5), Device: 172.16.1.220, 00:80:63:2F:6E:08
525			Domain	2015-04-27 13:21:47	DEPSTAR@	Industrial HiVision Service		Connected to subdomain 172.16.1.225
524			SNMP Trap	2015-04-27 13:21:40	DEPSTAR@	172.16.1.220	172.16.1.220	Device was Switched ON
523			Status Better	2015-04-27 13:21:38	DEPSTAR@	172.16.1.220	Protocol/Protocol ON	Status Improvement: OK (Reachability=Yes)
522			Status Worse	2015-04-27 13:20:44	DEPSTAR@	172.16.1.220	Protocol/Protocol ON	Status Impairment: Error (Reachability=No)
521			Status Worse	2015-04-27 13:20:34	DEPSTAR@	172.16.1.220	Protocol/Protocol ON	Status Impairment: Error (Reachability=No)
520			Event Acknowledge	2015-04-27 13:20:25	superuser	Industrial HiVision		Severe Events Acknowledged by User: 181,187,194,196,198-203,210-211,214,216-221,258,269,308,309,311,317,323,...

Log entries for discovered rogue devices are generated