infraray

Network Security Management

For IT and industrial Networks

Monitor, Control, and Secure all Switches,
Routers, Gateways, Servers, Ports, and Endpoints

www.infraray.com

Contents

Purpose of This Document

This document is a high-level introduction to the Security capabilities and features of Infraray Business Infrastructure Control Solution (BICS) for IT and industrial control networks.

It provides prospective BICS customers with an understanding of the overall integration, approach, and capabilities of BICS, including features that are unique to BICS.

This document is not a tutorial and does not replace the BICS technical documentation. We recommend that prospective customers contact Infraray to arrange a live demonstration via Web. A detailed live demonstration is recommended. Please contact Infraray to arrange a presentation and Q&A for your team.

BICS Network Security Management for IT & Industrial Networks

BICS for IT Security and its counterpart, BICS for Industrial Security, overcome key challenges of securing complex, heterogeneous IT and industrial control networks. BICS enables discovery, monitoring, and control of IT and industrial network endpoint devices and the ability to “speak with” their command sets. These capabilities scale to networks with a million or more ports or connected endpoints, and to over 4,000 tenant networks in BICS multi-tenant mode.

Monitor, Control, and Secure all Switches, Routers, Gateways, Servers, Ports, and Endpoints

For convenience and brevity, this document refers to the Infraray Business Infrastructure Control Solution (BICS) as “BICS for IT Security” or “BICS for Industrial Security” or “Infraray BICS for Security”, or simply “BICS.” Please note that Infraray BICS is a comprehensive platform that can include other modules, in addition to Security, to handle Asset Management, Network Monitoring, and a range of other key enterprise network functions.

Infraray BICS can monitor, control, and secure the network centrally, automatically querying switches and gateways in a heterogeneous infrastructure (for both IT and operational infrastructure) and identify connected endpoints, ports, and uplinks. Because its discovery, monitoring, and control are comprehensive and able to communicate with thousands of device types, makes, and models, BICS supports vendor independence and device heterogeneity.

To manage Network Security Management for industrial networks, operators of the BICS platform use interfaces and screens that are identical to those use in BICS to manage IT networks. Infraray BICS for Security works in both **multi-instance and multi-tenant modes**.

1. BICS Network Security Management Features

- Verification and administration of network devices and ports for Information Technology (IT) and Operational Technology (OT) control, management, and security.
- Supports IEEE 802.1X, MAC, and PWA authentication.
- Vendor-independent solution.
- Designed to secure heterogeneous networks of any size, from medium-scale to very large scale, including those with hundreds of thousands of endpoints.
- Single-Pane-Of-Glass, intuitive user interface for centralized monitoring and control. Visual depiction of the entire network infrastructure, with real-time / dynamic topological, geographical, and organizational views. Drill down from high-level dashboard to discrete endpoint.
- Automated recognition and pinpoint localization, including alarms and alerts.
- Analysis of data flows throughout the entire network.
- Interfaces for integration of existing security software (e.g. Splunk).

2. Key BICS Tasks for Network Security Management

Unambiguously identify devices using MAC Layer 2, and automatically allocate roles for these devices. If the device supports IEEE 802.1X, BICS can also identify the end user and identify specific authorizations that each user holds, such as VLAN permissions and restrictions.

1 Graphical dashboard combining granular alarm updates and current summaries of port status and security metrics.

With 802.1X implemented, the BICS Policy Editor enables operators to manage and prepare individual policies and roles for various user or device groups.

BICS for Security provides for less detailed policy setting in MAC Layer 2 implementations.

- Automatically comply with security requirements, e.g. White List, 802.1x certificate
- Enforce established security requirements in real time, such as limiting or completely blocking an unknown device from entering the network.
- Detect and report on the connection location, port, and switch used by each endpoint.
- Issue alarms as necessary.

INFRARAY BICS for Security divides the successful performance

2.1 Recognition, localization, and authentication

- BICS automatically recognizes and pinpoints the switch and port connection point of every network component in real time, including wireless networks (WLANs). This functionality is independent of the place of access.

- Unambiguous authentication of users and devices for guaranteeing the identity of each, in accordance with the IEEE 802.1X standard.

2.2 Assessment

- BICS assesses whether the MAC address, username (related to 802.1x), password, and/or certificate are valid, in real time, during the login process.

2.3 Authorization

- Access control for users and devices, correctly granting access to areas as defined by security requirements (guest, quarantine, or production areas), based on the preceding checks.

- Automatic alarm procedure in the event of unauthorized network access or faulty or suspicious behavior by an endpoint device.

- Reaction in real time: BICS can immediately and automatically disconnect a device from the network and – if policy so instructs – isolate it within a guest network.

Figure 2 Example of a "CIO" single-pane-of-glass dashboard in BICS.

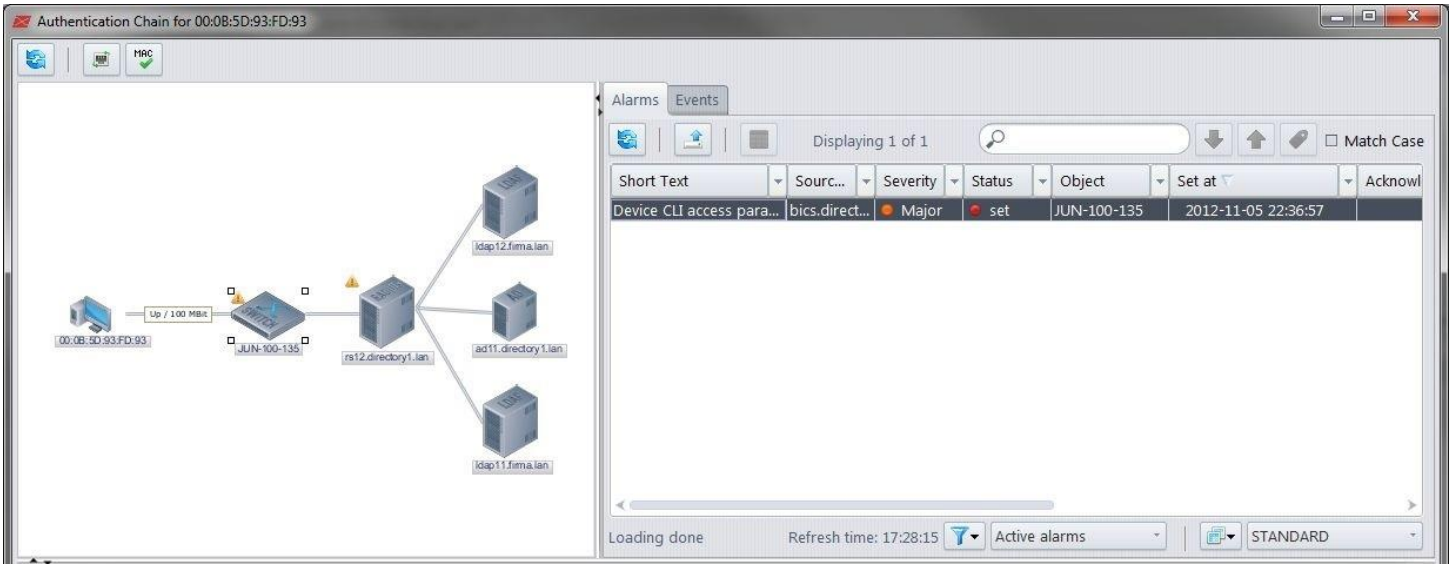
2.4 Single-Pane-of-Glass Monitoring and Control

- Single-Pane-of-Glass, simplified, intuitive user interface for centralized monitoring and control of networks and endpoints.

  (i) Visual depiction of the entire network infrastructure.

  (ii) Real-time / dynamic drill-down from high-level dashboard to discrete endpoint.

  (iii) Customizable views based on roles or company policy.



3 BICS displays the security authentication chain for any device in the network.

BICS for Security can also depict in real time the authentication chain of any endpoint in the IT or OT-linked infrastructure.

Single-Day Deployment Can Meet Requirements of Imminent-Threat Scenarios

BICS for Security can be deployed and implemented very quickly. For MAC Layer 2 implementations, this can be as short as a few hours. This can be important in an imminent-threat situation. The time required for 802.1X implementations is faster with BICS for Security than competing products, and depends on such factors as customer requirements, clarity, and complexity of network structure, and other configuration-related issues.

Once implemented, BICS can discover hundreds of thousands of ports within one day, and begin to monitor them persistently. It provides automated, full virtualization of entire IT environments down to the port level and shows the physical condition and state of every device.

In addition to the array of equipment that BICS discovers and controls in an IT network – Cisco, HP, Dell, Extreme, and other common makes of devices – in industrial OT networks, BICS discovers and recognizes IP-addressable industrial devices, equipment brands, and models, including: MOXA, Phoenix, Hirschmann, Siemens, Belden, Schneider, and associated endpoint devices. As with IT Networks, BICS communicates with these industrial devices in their native command sets. BICS provides the operator a common set of BICS commands for controlling groups of devices and/or individual devices from a central location, all from a customizable “single pane of glass” dashboard.

3. Network-Port Security Management

Port security is delivered in INFRARAY BICS for Security as a key component named Port Security Management. It enables network access control for organizations of any size, and for multiple entities.

BICS enables security for each network port by working through the associated Ethernet switch and permanently linking every port interface with one or more MAC addresses. The devices with these MAC addresses are restricted to communication with the network via this interface, thereby preventing access to the network by unauthorized endpoint devices, and blocking certain attacks from within the company's own network.

In addition, Infraray BICS supports the IEEE 802.1X standard to further enhance network-port security. Instead of the MAC address "sticking" to the port (as it does when 802.1X is not possible), it is stored on a RADIUS server and accessed by 802.1X. IEEE 802.1X authentication enables the worldwide administration of a MAC address on a LAN or VLAN, supporting high levels of user mobility.

Infraray BICS manages Security for Network Ports

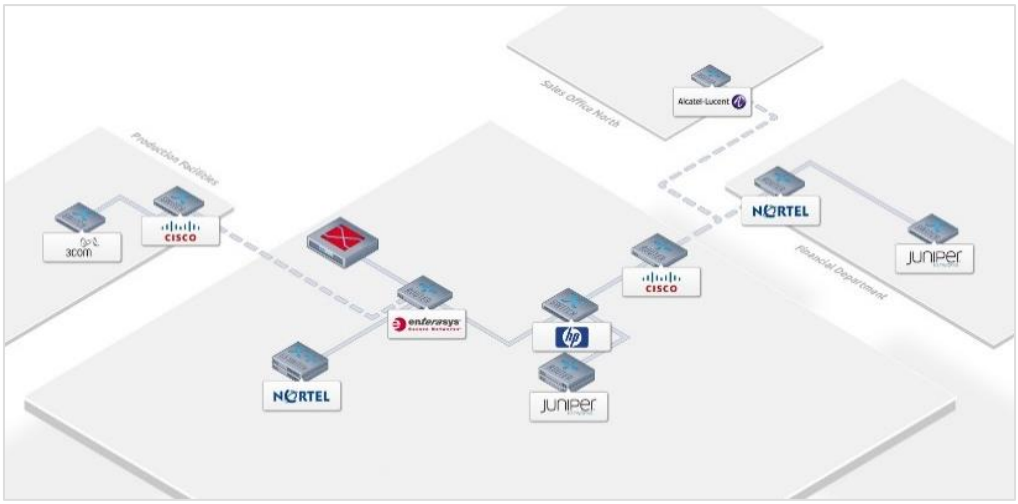
Infraray BICS' network-port security can automatically detect whether or not a user attempting to log on has the correct authorization from the system or device assigned to him or her. If these parameters match up and comply with requirements, the user is granted access to corporate resources – within the scope of the access rights granted to him or her (Precondition: IEEE 802.1X, User Certificates, VLAN steering). If a user attempts unauthorized logon, BICS automatically triggers an alarm and acts in accordance with the preset security policies – for example, automatically blocking the port.

4. Device Control Library and Vendor Independence

Infraray facilitates vendor independence for comprehensive network security. Cisco, HP, Allied Telesis, Nortel, Juniper, Dell, and Enterasys are among the long list of manufacturers that BICS can monitor and control at the command-line level to manage, control and secure IT Networks. For industrial networks, BICS monitors and controls a broad range of devices from manufacturers including: MOXA, Phoenix, Hirschmann, Siemens, Belden, Schneider, and associated endpoint devices.

The Infraray BICS Device Control Library is extensive, and makes BICS effectively vendor-independent. It enables network management and Port Security Management with BICS to encompass the entire network, even if it contains equipment from numerous different manufacturers. Onboarding a new

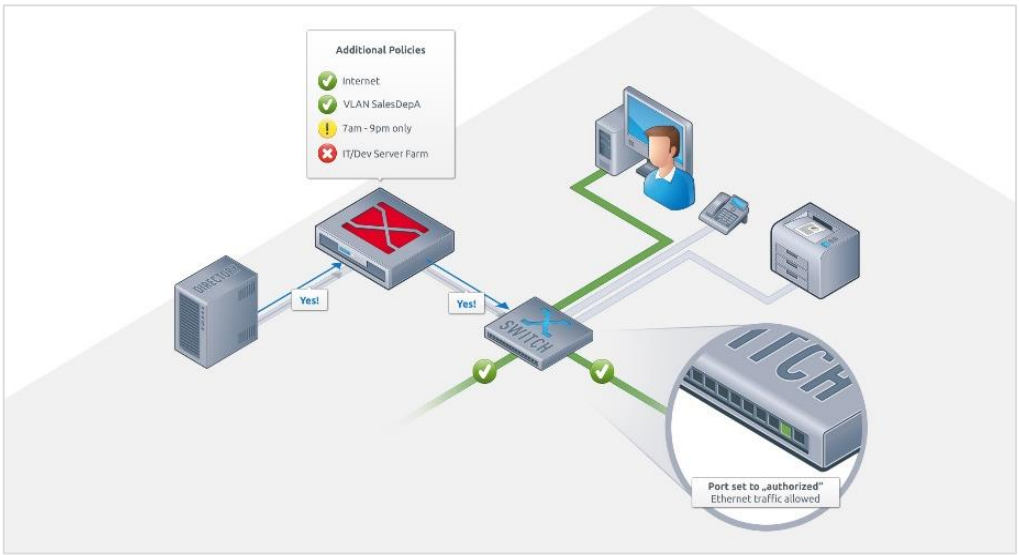
device into the Device Control Library usually takes about three days – executed swiftly be a dedicated Integration Team.



4 The Infraray Device Control Library enables full vendor independence. Integrating a new network device into the Device Control Library typically takes two days.

5. Blocking Unauthorized Access to the Network

BICS enables network switches to block unwanted LAN access by unauthorized endpoint devices, and manages the security settings of each device and port.



5 BICS enables automated control of all ports, groups of ports, and individual ports.

5.1 Feature Description

- **BICS secures the LAN to prevent the connection of unknown devices.** Only devices with known MAC addresses, stored on a white list, are allowed to use the LAN. BICS will issue an alarm to a designated operator, and / or shut down any port where an unknown MAC addressed device attempts access.

- **Inspects (in Learning mode) the network to determine which MAC addresses are used by every connected endpoint device.** BICS will detect the connected endpoints and store their MAC address in the Infraray BICS database (CMDB).

- **Detects and stores the connection time and port location for each endpoint.**
  BICS maintains and continually updates a database of the connection history of every endpoint.

- **Monitors (Events & Alarms) endpoint connection events and device movements from port to port on the network.** Every successful and unsuccessful connection is stored in the BICS database of connection history.

- **Detects MAC spoofing.**
  BICS throws alarm if it suspects duplicate MAC addresses, and new MAC addresses that attempt access via multiple ports.

- **Prevents use of MAC addresses in different locations, or contrary to security policy.**
  BICS allows the operator to bind any MAC address, or group of MAC addresses, to specific locations and ports.

- **Helps resolved blocked situations.**
  Provides suggestions to the network operator to quickly resolve block situations.

This excerpt from a BICS for Security screen shows one example of “repair hints” and Recommended Actions that BICS displays for the network operator in the event of an access error for a device

6 BICS for Security recommends corrective actions that reduce the impact of human omission and errors.

5.2 Control of Switches

- BICS Configure automatically sets any discovered switch to be controlled by Infraray network-port security management.

- The operator can also designate switches individually and in groups to operate under the control of BICS.

- BICS recognizes the following five states for every port, and lets the operator configure them manually or automatically on every switch, for each port. On a switch that is under BICS control, every port will have one of the following states at all times (but never more than one state):

  Learn: Learns the MAC address and stores it in the BICS CMDB. This signifies that the MAC address is authorized.

  Secure: Immediately shuts down a port where an unauthorized MAC address attempts access, or overrides other settings and immediately assigns the endpoint device to a quarantine VLAN. This action also stores the MAC address in a “black list.”

  Watch: Monitors an unauthorized MAC address, storing it in a black list, and issues an alarm, but does not shut down the port.

  Uplink: An automatic process that recognizes the port is used as an uplink to another switch or a router, not as an access point for an endpoint device.

  Ignore: Operator can designate a port as an exception to these processes/ actions by putting it into the Ignore state.

- Bind endpoints to ports.
- The MAC address of the endpoint can be tied to a specific port.
- Define and monitor security events and alarms.
- In the BICS Configurator, the operator can select from predefined alarms, and / or define and add new alarms.

6. IEEE 802.1X Support

Infraray BICS uses IEEE 802.1X, and enables the Extensible Authentication Protocol. BICS improves the management of the device and port-based settings of this authentication method and allows them to be embedded into an existing 802.1X structure.

6.1 Feature Description

- **LAN secured to prevent the connection of unknown devices (device certificate) and users (user certificate) to the network.**
  When a supplicant requests access to the network, BICS manages the authorization process and sets the access rights on the network component.
- **Secure the LAN for use with non-supplicant devices with MAC authentication bypass.**
  This method can be used for non-supplicant devices, such as printers.
- **Secure the LAN with Port Web-based Authentication (PWA) or Captive Portal.**
  BICS can provide this common method to grant access to the LAN.
- **Determine whether network devices are capable of using the IEEE 802.1X authentication method.**
  BICS will audit the device during the discovery process to determine whether it is capable of using 802.1X. BICS determines which method can be used. It will not allow setting an unsupported method for authenticating a device.

6.2 BICS Functionality supporting 802.1X

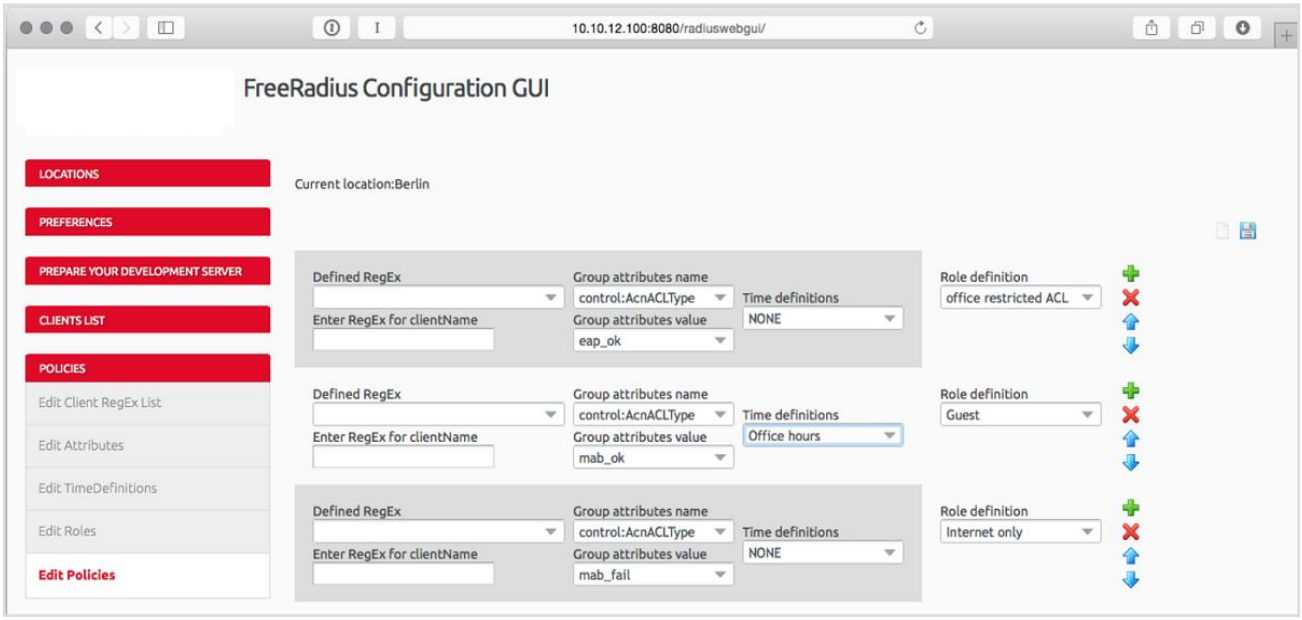
- **Enables 802.1X support for switches.**
  In the Port Security Manager, the switch will be enabled.
- **Set the authentication method**.
  Set UserAuth; MACAuth; PWAAuth (multi-select).

- **Configure RADIUS.**

The administrator can configure the BICS Radius server via the graphical user interface.

7. Network Security Management Policy Support

Infraray BICS allows operators to set management policies. With access granted by the RADIUS server, admins can set additional rights.



7 BICS enables simple, menu-driven operation of the Radius server.

7.1 Access control

- **Operators can set rules and policies to prevent unwanted access to the LAN.**
  Operators can configure detailed, flexible rules to easily establish and guide the authentication process.

7.2 Functionality supporting network port security

- **Define Resources**
  Group devices, ports, and resources in resource groups.

- **Define Time Rules**
  Define time definitions on an hourly, daily, weekly, and monthly basis.

- **Define Roles (accept, reject, assign to VLAN x)**
  Define the authentication actions.

- **Combine all the above functions in a policy definition.**
  Combine the defined policy parameters to a policy that will be executed on the connected endpoint.

8. VLAN Management

VLAN management enhances INFRARAY Security with the capability to configure and assign designated ports to specific VLANs.

8.1 Feature Description

- **Set port VLANs for authorized endpoints.**

Assigns endpoints automatically to a specific VLAN, according to defined policies.

- **Set port VLANs for unauthorized endpoints.**

An unknown endpoint can be assigned to, and confined to, a “Guest” or “Quarantine” VLAN.

- **Manage VLAN-IDs and VLAN-names.**

A central view and operational interface to create, manage, and if necessary delete VLANs.

8.2 Functionality supporting this feature

- **The operator can predefine VLANs.**

Define any number of VLANs in the management interface.

- **The operator can preset policies so that the following functions are carried out automatically, in real time, by BICS.**

Set the switch / port VLAN settings

For a MAC address that is unknown, BICS will set the port status to Unauthorized (shutting down the port) or assign the port to a quarantine VLAN.

Set the VLAN for authorized, unauthorized, and unused ports.

- **BICS allows the operator to designate specific VLAN IDs for specific MAC addresses, and to preset the VLAN assignment policies that BICS will automatically follow and enforce in real time.**

The operator can define the VLAN to which MAC addresses and ranges of MAC addresses will be automatically assigned upon login of an endpoint to the network. In other words, if the device attempting logon has a known MAC

address, BICS can immediately assign that device to a predefined VLAN and, at the same time, authorize the port that the new device is utilizing. When any device logs on to the network, BICS will look up the MAC address in its MAC / VLAN table to check whether that address has been pre-assigned to a specific VLAN. If so, BICS automatically assigns the port being used to the appropriate one.

www.infraray.com

About Infraray

Infraray was founded in 1998 by a German engineering team with deep expertise in IT Operation Management. The company provides information technology solutions and offers network management, network security, IT infrastructure management, cloud, network automation, and business infrastructure control solutions.

Infraray BICS is the Next-Generation ITOM platform to control large & heterogeneous enterprise networks. BICS not only provides network infrastructure management for all vendors' devices and endpoints, but also serves as the foundation for a new generation of IT infrastructure management.

Auconet became part of Beta Systems Group in early 2018.

infraray

Infraray GmbH
Stromstr. 5
10555 Berlin / Germany

Tel. +49 (0) 30 254 690-0
Fax: +49 (0) 30 254 690-199
hello@auconet-it.com