INC – Intelbras Network Center

Overview

INC is a comprehensive, modular platform with the flexibility and scalability to meet the network needs of small-to-medium-sized businesses as well as global enterprises. It consolidates many traditionally separate management tools, including those for managing the network infrastructure, its services and users.

Based on years of accumulation and in-depth understanding of the network, INC platform provides customer with practical and easy to use network management functions. Based on centralized network resource management, the topology, fault, performance, configuration, and security of INTELBRAS are realized.

For the network with large equipment, wide distribution and relatively centralized, the INC platform provides hierarchical management, conducive to the clear division of power management and load balance for the whole network. The management platform's integrated toolset covers the entire network, from the data center to the edge, even if it is geographically dispersed.

And it supports the management of all Intelbras network equipment as well as over 8,000 third-party devices from multi vendors. INC provides visibility across entire networks, enabling complete management of resources, services, and users. The management platform unifies management of wired, wireless, physical, and virtual resources—and their users—leading to increased performance, enhanced security, and reduced infrastructure complexity and costs.

Features

Single platform management

The single platform management feature of INC enables you to get the information you need at a glance, including a display of both physical and virtual assets as well as wired and wireless elements. Convenient color-coded displays, topology overlays, and focused zooming make it easy for you to view the entire network or to concentrate on an area of interest.

Unified resource management of network and servers

More management equipment types: besides the traditional routers and switches, INC can manage the wireless, security, voice, storage, monitoring, server, printer, UPS and other equipment in the network to realize the centralized management of the network resources.

Supporting the batch configuration and verification of equipment access parameters, providing the function of searching, modifying, deleting and importing / exporting of network equipment resources, and also providing user batch management functions, including batch modification of user additional information, batch cancellation of users, and batch user import functions to save operator's time. - Flexible and fast automatic discovery algorithm:

Based on Intelbras patent algorithm, INC platform not only provides rapid automatic discovery, but also provides five advanced automatic discovery methods, including routing, ARP, IPsec VPN, network segment, PPP, and so on, which can quickly and accurately find network resources. Support panel management, which displays the composition and running state of the device via WYSIWYG.

Unified control of virtual and physical worlds

Unifies physical and virtual network management and helps IT overcome the challenges of administering the new virtual server edge. It maps the topology of the entire network, making it clear which devices are virtual and which are physical. Management focus and policies remain linked to virtual assets, even if those assets are on moving

Unified management of wired and wireless networks

INC provides a unified view of wired, wireless networks and stations with enhanced network performance monitoring and management. From access points (AP) to edge routers, administrators can manage these devices in a consistent manner using policies. INC delivers role-based access and centralized policy enforcement for users and their devices. Identity-based access helps ensure that the appropriate security measures and policies are applied consistently to users, whether each user connects through a wired or wireless LAN

Flexible centralized reporting

INC receives and logs SNMP traps and syslog reports, and it can generate online and historical network performance information in highly adaptable report formats. The reports enable powerful fault finding and event generation. In addition, flexible historical reports provide the information you need for network trend analysis and capacity planning. You can also easily create inventory reports that show network device details, such as model, firmware, available memory, IP address, and serial number. The reports can be run with a mouse click or scheduled to run regularly. And you can view reports in a few formats, including pdf,.csv,.rtf and .xls, and send them automatically via email.

Hierarchical management

The standard version of INC offers distributed management capabilities that allow multiple servers with different installed modules to retain the appearance of a single UI. The professional version provides the greatest span of control, with a hierarchical deployment mode that can extend visibility across multiple networks, multiple countries, and even multiple continents. For greater flexibility and convenience, you can combine the distributed and hierarchical modes of deployment. INC provides hierarchical rights management which enables the hierarchical authorization on device or user or operation.

High Availability

Redundancy configuration of servers with single or shared remote database allowing high availability.
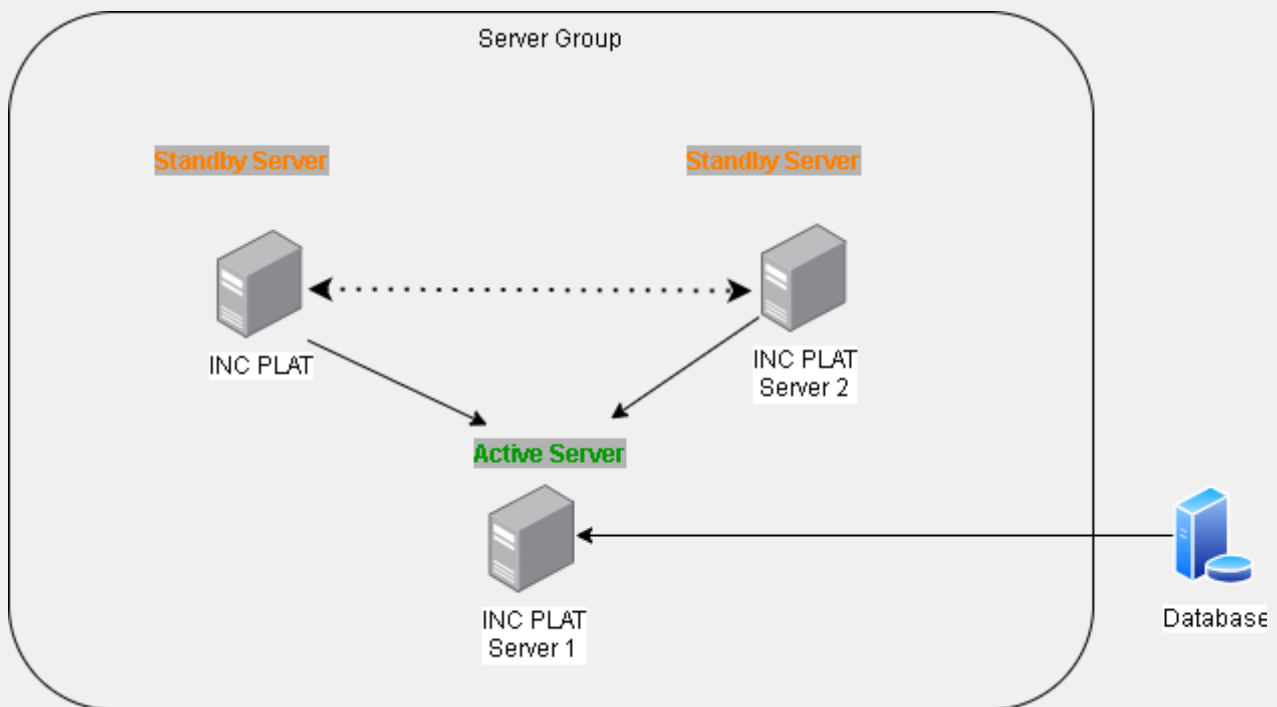
INC On-premises Standard Edition module

Fault	Local server process management
	Distributed deployment process management
	Checking detailed INC process information and their running status
	Alerting the exception of INC process
	Launch or terminate one or more INC processes
	Setting startup mode for INC processes

Configuration	Distributed deployment
	Distributed installation
	Typical installation
	Distributed service Portal
	SOAP based SOA
	REST based SOA
	Operator rights (ADMIN, Maintenancer, Viewer)
	Operator Group
	Adding, removing, and modifying operator information
	Online operator management
	Password Strategy
	Operator access control
	System logon and logoff
	Adding pages to the favorite folder
	Pre-defined service links
	Local command or any URL link
	Querying operation logs and displaying detailed operation information
	Password display in Device access parameter
	System Web access mode
	System ping timeout
	Internet Connection Configuration
	Periodical mass data exporting
	Dump condition setting
	Manual exporting
	Mail server configuration
	Short message service center configuration
	Download Device software files from the Intelbras website
	SSH device communication
	Download INC upgrading version files from the Intelbras website
Accounting	Reporting the user's information and his device information to the 3Com's website for device warranty
	Device data gathering
	INC data gathering
Performance	Monitoring servers
	Synchronizing and refreshing device status

Security	
	Creating an account
	Batch importing accounts
	Maintaining user information
	Cancel an account
	Batch user operation
	Additional user information management
	Multi-device type support
	Multi-protocol support to access device
	Device models customizable
	Multi-vendor devices support
	Adding vendors manually
	Identifying INC server automatically
	Adding/removing devices manually
	Additional device information management
	Auto-discovery
	Monitoring servers
	Synchronizing and refreshing device status
	Modifying device classification
	Searching, fast locating devices, interfaces, and users
	User group management
	Device group management
	IP view
	Device view
	Customized view
	Port Group
	Faulty device display view
	Resources in different statuses are displayed in different colors
	Device panel management
	Device basic configuration
	Device configuration
	Panel Project management
	Device management web client
	IP Address allocation
	IP/MAC binding
	Terminal Access binding

Switch Access binding
Illegal Access Processing Policy
Illegal Access Log
History Access Log
Real-time Location
IP/MAC learning
Terminal name parsing
IP topology
Layer 2 topology
SNS topology
Neighbor topology
LLDP-MED topology
Customized topology
Data center topology
Data center room topology
Data center rack topology
IRF topology
Converged topology
Display, bubble display device\link information
Adding\deleting cloud
Saving the current topological view
Export to VISIO format
Set Default Topology View
Editing and zooming topology, layout, and displaying grids
Hiding\displaying topology objects
Setting device label display mode
Setting link label display mode
Overview
Searching and locating devices in the current topology
Switching to subnet topology\upper layer topology
Viewing path topology
Viewing STP topology
Viewing MSTP topology
Viewing Ping topology
Topology integrality diagnosis

Ping, Telnet, and traceroute devices

Device Web-based NMS

Online user-associated operations

Setup the assets

Extendable properties of assets

Querying the assets

Auditing the assets' changing

Assets management options

Receiving SNMP v1/v2c/v3 traps

Alarm resolution

Alarm browsing

Root alarm

Alarm statistics

Acknowledging, recovering and deleting alarms

Audible and visual alarm prompts

Forwarding alarms to other NMSs

Email reminding

Short message reminding

System provides default maintenance suggestion, and can be modified

Browsing the original traps

Filtering repeated events

Filtering Intermittent failure events

Filtering unknown events

Filtering events generated by unmanaged devices

Customizing event filtering rules

System pre-defined alarm generating rules

Customizing alarm generating rules

Trap definition

Import/add/edit trap definition

Alarm correlation analysis based on category

Alarm correlation analysis based on multi-source

Alarm root cause based on topology

Display of the alarm correlation analysis

Alarm correlation analysis and impact report

Core devices configuration

Receiving syslogs

Filtering syslogs

Querying syslogs

Syslog parsing template

Analyzing and aggregating syslogs

Basic performance indices

Extended performance indices

Customized performance indices

Unified performance configuration and management

Batch add/cancel performance monitoring instance

Global indices' threshold and sample interval configuration

Instance threshold and sample interval configuration

Default Monitoring Indices

Overall monitoring statistics report

User-defined organization and display of performance views

Support to RFC 3164 (Syslog)

Query/add/delete/modify the performance views

User-defined view formats of data in performance view

Default view formats for performance view

Default performance view

Organize the performance views in folders

Performance view report

Performance detailed report

Extend performance data in device details page

Extend performance data in topology

Performance display options

Monitor Option

Real-time monitoring

Monitor Item	Description
Input Bandwidth Utilization of Highspeed Interface(%)	The number of bits received on the interface per unit time/interface rate
Output Bandwidth Utilization of Highspeed Interface(%)	The number of bits sent on the interface per unit time/interface rate
Input Bandwidth Utilization of Lowspeed Interface(%)	The number of bits received on the interface per unit time/interface rate
Output Bandwidth Utilization of Lowspeed Interface(%)	The number of bits sent on the interface per unit time/interface rate

Input Packets Error Rate(%)	The number of input error packets/the total number of input packets
Output Packets Error Rate(%)	The number of output error packets/the total number of output packets
Proportion of Discarded Input Packets(%)	The number of discarded input packets/the total number of input packets
Proportion of Discarded Output Packets(%)	The number of discarded output packets/the total number of output packets
Proportion of Received Packets With Unknown Protocol(%)	The number of input unknown protocol packets/the total number of input packets
Packets Received	The total number of packets received on the interface
Packets Sent	The total number of packets sent by the interface
Discarded Input Packets	The number of discarded input packets on the interface
Discarded Output Packets	The number of discarded output packets on the interface
Received Error Packets	The number of error packets received on the interface
Sent Error Packets	The number of error packets sent by the interface
Received Packets With Unknown Protocol	The number of unknown protocol packets received on the interface
Unicast Packets Received	The number of unicast packets received on the interface
Unicast Packets Sent	The number of unicast packets sent by the interface
Multicast Packets Received	The number of multicast packets received on the interface
Multicast Packets Sent	The number of multicast packets sent by the interface
Broadcast Packets Received	The number of broadcast packets received on the interface
Broadcast Packets Sent	The number of broadcast packets sent by the interface
Octets Received	The number of bytes received on the interface
Octets Sent	The number of bytes sent by the interface

Custom report homepage

Predefined report templates

Report right control

Viewing real-time report

Creating\deleting\modified periodic report

Suspending\Resuming periodic report

Viewing historical report

Sending report by Email

Rapid report customizing

Building reports using the data of downstream NMS

Multi-format exporting

Modifying report's customized information

Centralized task management

Displaying/modifying/duplicating/deleting/starting/suspending/resuming a task

Generic configuration deployment capacity

Configuration adaptability for 3-party device

By default, the system provides common configuration segments.

Viewing/adding/modifying/removing/duplicating/importing/exporting/deploying configuration files (segments, CLI script)

Dynamic parameter

Unified management of device software, including common software, Boot ROM, ONU software, ONU algorithm, and OSM software.

Deploy any file to device, including Web APP.

Viewing the list of software installed, importing software from files/devices, modifying/removing software, exporting software to clients, and deploying software

Device space management

Software baseline

Uniform device deployment wizard portal

Deploying device configuration

Deploying device software

Completing deployment by task

Automatic deployment plan (Zero Touch provisioning)

Configuration and software list

Viewing the current software version and available software in software library/updating software

Viewing the configuration time of the latest backup/manually backing up the configuration files of a device

Viewing whether automatic backup is enabled on a device/adding a device to the list supporting automatic backup/setting an automatic backup period

Viewing the latest startup configuration file and the run configuration file on a device

Viewing the detailed configuration management information of a device

Default start configuration for Intelbras serial

View the basic configuration of the device

Browse/Modify/Restore/Compare/Delete configuration files, make configuration files baseline

Browse/Restore/Delete software upgrade history

Device software history

Extendable 3-party configuration backup and update management

Adding/deleting/modifying auto-backup plan

Resuming/suspending auto-backup plan

Viewing the backup history

Viewing/deleting backup history report

Exporting backup configuration files

Repeat executing the failed backup operation

FTP mode for a specific device

Maximum number of backup configuration files

Defining compliance checking rules

Define compliance policy

Adding/deleting/modifying checking task

Enable/disable/executing checking task

Querying/deleting checking result

Repair incompliance devices

Alarm when incompliance

Check task history

CLI return segment

Supporting standard rules, extended rules, Layer 2 rules, and customized rules

Browsing all ACL resources in the network, and ACL applications in device view

Adding, removing, and modifying ACL resources

Rule set in ACL resources and browsing, adding, removing, and modifying rules

Removing overridden rules

Merging the address ranges by the mask

Merging rule port ranges

Removing redundant rules

Removing repeated rules

Moving up the most frequently hit rules

Browsing, adding, removing, and modifying ACL on devices

Browsing and configuring ACL applications on devices

Browsing and configuring ACL application time range on devices

History of ACL configuration changes, application configuration changes, time range configuration changes, and configuration history management
Synchronizing ACL configuration on devices
Batch configuring ACLs for multiple devices by task
Deploying ACL configuration wizard
Removing ACL configuration wizard on devices
Removing time range configuration wizard on devices
Deploying ACL application wizard
Removing ACL application wizard on devices
Creating/removing/modifying ACL template and its rules
Creating/removing/modifying ACL parameter template and its rules
Exporting templates to ACL resources
QoS based on ACL
Network address management
Creating/removing/modifying the global VLAN
Removing members of global VLAN
VLAN Device Configuration
VLAN Interface Configuration
Access Interface Configuration
Trunk Interface Configuration
Hybrid Interface Configuration
Batch Deploy Access Interface
Batch Deploy Trunk Interface
Batch Deploy Hybrid Interface
VLAN topology
Generic VLAN configuration

End-user Intelligent Access (EIA) module

The EIA component includes User Access Manager (UAM) and TACACS+ Authentication Manager (TAM). UAM provides policy-based Authentication, Authorization and Accounting (AAA) services. UAM software extends management to wired, wireless and remote network users and enables the integration of network device, user, guest and terminal management on a single unified platform. TAM provides basic AAA functions for network

devices or IT users for network device management security. TAM can assign users with 2 different privileges, monitor login and command execution operations, and simplify user management.

Fault	Trouble report management
	Notifying third-party devices of user logon/logoff events
	Process monitoring
	ARP attack protection
Configuration	Automatic synchronization of LDAP users
	Synchronizing users from OUs
	Synchronizing users from groups
	On-demand synchronization of LDAP users
	Synchronizing users periodically
	Manual synchronization of users
	Support for binding users with LDAP server and unbinding them manually
	LDAP user batch export
	Automatic cancelling LDAP user synchronization
	LDAP user transfer OU function
	LDAP service group management
	Transferring LDAP users between user groups
	Bulk setting a password for all LDAP administrators
	Applying for services based on the user group
	Synchronizing user groups based on OUs
	Allowing online AD users to change their passwords
	Immediate/scheduled password sending
	Account registration by guests
	Guest password SMS message
	Guest registration approval notification
	Guest preregistration
	Lifetime for a guest account
	Lifetime for a guest account password
	Guest manager
	Guest service management
	User group based policy control
	Online guest number limit
	Guest policy
	Approving guest registration by scanning a QR code
	Quick configuration of the guest service
	Customization develop interface

Customization query interface

RESTful APIs

User self-service of touch version

User information query

User information modification

User password modification

User pre-registration

Changing pre-registered users to formal users

Second confirmation for pre-registered users

Device management users

Query of the user operation log

Customizing self-service center logo

Query online user list

Enforce to offline user in self-service center

Automatic password acquisition

Custom pre-registration pages

Custom attributes of pre-registration pages

Previewing pre-registration pages

Applying pre-registration pages

Custom the self-service center homepage

Custom links

Access device management

Adding access devices by using IP subnets

Adding access devices from the device list in the platform

Support for access devices of multiple vendors

ACL assignment to the access device

Integration with the network topology

Assigning messages to users on the basis of an access device

Logging out users on the basis of an access device

Deleting online records on the basis of an access device

Access device group management

Access topology view management

Device management in access topology view

Terminal topology displaying

Monitoring a specified user

Monitoring users of an access device

Logging out users in the access topology

Deleting online records in the access topology

	Support access service statistic reports
	Service policy group management
	Service policy management right
	Flexible service parameter configuration
	Trouble report management
	Notifying third-party devices of user logon/logoff events
	Providing an AAA configuration page for access devices
	Providing an 802.1X and MAC authentication configuration page for access devices
	Providing a portal authentication configuration page for access devices
	Batch deploying configurations to access devices
	Viewing access device configurations
	Quickly enabling 802.1X and portal authentication on access devices for users
	Providing unified authentication
	Displaying nodes permitted by the EIA license on the home page
	Configuring email contents
	Unified SMS gateway configuration
	Endpoint aging time settings
	EAP certificate upload
	CRL check on certificates
	Synchronizing CRL periodically
	Manual synchronization of CRL
	Manual import of CRL
	Hot backup
	Cold backup
	Escape solution
	UAM distribution deployment
	Support for Windows+SQL Server platform
	Support for centralized deployment and distributed deployment
	Process monitoring
	Integration of upgrading and installation disks
	Tomcat+Apache integration
	Automatically detection of the availability of RADIUS authentication and accounting ports
	Deployment of multiple portal servers
	Support database and component separated
	Support IPv6
Accounting	Lifetime for a guest account
	Lifetime for a guest account password
	User group based policy control

Online guest number limit

Guest policy

Approving guest registration by scanning a QR code

Quick configuration of the guest service

Customization develop interface

Customization query interface

RESTful APIs

User self-service of touch version

User information query

User information modification

User password modification

User pre-registration

Changing pre-registered users to formal users

Second confirmation for pre-registered users

Device management users

Query of the user operation log

Customizing self-service center logo

Query online user list

Enforce to offline user in self-service center

Automatic password acquisition

Custom pre-registration pages

Custom attributes of pre-registration pages

Previewing pre-registration pages

Applying pre-registration pages

Custom the self-service center homepage

Custom links

Access device management

Adding access devices by using IP subnets

Adding access devices from the device list in the platform

Support for access devices of multiple vendors

ACL assignment to the access device

Integration with the network topology

Assigning messages to users on the basis of an access device

Logging out users on the basis of an access device

Deleting online records on the basis of an access device

ARP attack protection

Access device group management

Access topology view management

	Device management in access topology view
	Terminal topology displaying
	Monitoring a specified user
	Monitoring users of an access device
	Logging out users in the access topology
	Deleting online records in the access topology
	Support access service statistic reports
	Service policy group management
	Service policy management right
	Flexible service parameter configuration
Performance	Process monitoring
	Access device group management
	Access topology view management
	Device management in access topology view
	Terminal topology displaying
	Monitoring a specified user
	Monitoring users of an access device
	Logging out users in the access topology
	Deleting online records in the access topology
	Support access service statistic reports
	Service policy group management
	Service policy management right
	Flexible service parameter configuration
	Trouble report management
	Notifying third-party devices of user logon/logoff events
	Security (Segurança):
	ARP attack protection
	Access device group management
	Access topology view management
	Device management in access topology view
	Terminal topology displaying
	Monitoring a specified user
	Monitoring users of an access device
	Logging out users in the access topology
	Deleting online records in the access topology
	Support access service statistic reports
	Service policy group management
	Service policy management right

	Flexible service parameter configuration
	Trouble report management
	Notifying third-party devices of user logon/logoff events
	Hot backup
	Cold backup
	Escape solution
	UAM distribution deployment
	Support for Windows+SQL Server platform
	Support for centralized deployment and distributed deployment
	Process monitoring
	Integration of upgrading and installation disks
	Tomcat+Apache integration
	Automatically detection of the availability
	ARP attack protection
	Access device group management
	Access topology view management
	Device management in access topology view
	Terminal topology displaying
	Monitoring a specified user
	Monitoring users of an access device
	Logging out users in the access topology
	Deleting online records in the access topology
	Support access service statistic reports
	Service policy group management
	Service policy management right
Security	Flexible service parameter configuration
	Trouble report management
	Notifying third-party devices of user logon/logoff events
	Hot backup
	Cold backup
	Escape solution
	UAM distribution deployment
	Support for Windows+SQL Server platform
	Support for centralized deployment and distributed deployment
	Process monitoring
	Integration of upgrading and installation disks
	Tomcat+Apache integration
	Automatically detection of the availability

Wireless Service Manager (WSM) module

The WSM module provides unified management of wired and wireless networks. With this module, you can add wireless network management functions to your existing wired network management system, instead of establishing a new IT management platform, safeguarding your legacy network investment from obsolescence and reducing maintenance costs. WSM software offers wireless LAN (WLAN) device configuration, topology, performance monitoring, RF heat mapping, and WLAN service reports.

Fault	AC management
	Fit AP management
	Client management
	Realtime monitor
	Displaying AP channel quality information
	Synchronize AP label
	AC configuration wizard
	Fit AP information management
	Location view topology
	Physical connection between Fit APs and ACs in the Fit AP topology
	RF coverage
	Query basic information of device
	Local Service Report
	Distributed wireless performance collecting
	Energy Policy Management
	AP Model Management
	Displaying history information for ACs
	Displaying history information for Fit APs
	Displaying history information based on SSIDs
	Displaying history information in location views
Configuration	AC configuration wizard
	Exporting Fit AP templates
	Importing Fit AP templates
	Fit AP information management
	Fit AP Templates management
	Synchronize AP label
	Service Policy Management
	View and configure Radio information
	Location view
	AC Group

	Fit AP group
	Energy Policy Management
	AP Model Management
Accounting	Local Service Report
Performance	Realtime monitor
	Displaying AP channel quality information
	Service Policy Management
	Supports modify radio power
	Energy Policy Management
	Exporting Fit AP templates
	Importing Fit AP templates
	Fit AP information management
	Fit AP Templates management
	AP Model Management
	Distributed wireless performance collecting
Security	AC configuration wizard
	Exporting Fit AP templates
	Importing Fit AP templates
	Fit AP information management
	Fit AP Templates management
	Realtime monitor
	Service Policy Management
	View and configure Radio information
	Location view
	AC Group
	Fit AP group
	Energy Policy Management
	Supports modify radio power
	Supports start or stop SSID
	Supports start or stop radio
	Supports start or stop AP
	AP Model Management

Network Traffic Analyzer Component (NTA) module

	Realtime monitor
Performance	Displaying AP channel quality information
	Service Policy Management

Supports modify radio power
Energy Policy Management
Exporting Fit AP templates
Importing Fit AP templates
Fit AP information management
Fit AP Templates management
AP Model Management
Distributed wireless performance collecting

Installation requirements

Operating system requirements (x86-64-bit preferred)

Windows

- Windows Server 2012 with KB2836988 (64bit)

- Windows Server 2012 R2 (64bit)

- Windows Server 2016 (64bit)

- Windows Server 2019 (64 bit)

Database requirements

INC embedded database

INC provides an embedded SQL Server 2016 Express database with a size limit of 10 GB. You can use this embedded database only if you use the following INC settings:

- Default data retention settings.

- Fewer than 20K performance collecting units.

- Fewer than 100K alarms.

- Fewer than 1K managed device nodes.

SQL Server

The following are supported SQL Servers:

- SQL Server 2012 Enterprise SP4 (64 bit)

- SQL Server 2014 Enterprise SP3(64 bit).

- SQL Server 2016 Enterprise SP2(64 bit).

- SQL Server 2017 Enterprise (64 bit).

- SQL Server 2019 Enterprise (64 bit).

Typically, you must use SQL Server Enterprise Edition. However, you may choose to use SQL Server Workgroup

Edition if you are using the following INC settings:

- Default data retention settings.

- Fewer than 100K performance collecting units.

- Fewer than 500K alarms.

- Fewer than 2K managed device nodes.

MySQL

The following are supported MySQL databases:

- MySQL Enterprise Server 5.5.

- MySQL Community Server 5.5.

- MySQL Enterprise Server 5.6.

- MySQL Community Server 5.6.

- MySQL Enterprise Server 5.7.

- MySQL Community Server 5.7.

- MySQL Enterprise Server 8.0.

- MySQL Community Server 8.0.

Mariadb

- Mariadb 5.5.x.

- Mariadb10.3.x.

- Mariadb10.5.x.

VMware

- VMware ESXi 5.5

- VMware ESXi 6.0

- VMware ESXi 6.5

- VMware ESXi 6.7

CAS

- CAS 2.0

- CAS 3.0

- CAS 5.0

Hyper-V

- Hyper-V 2008R2

- Hyper-V 2012

- Hyper-V 2012R2

Nutanix

- AHV 2019

- AHV 2020

Ordering Information:

Product ID	Product Description
SW-INC-ST	Software INC On-premises Standard Edition Foundation
SW-INC-STA-25	Software INC On-premises Standard Edition, 25 Licenses
SW-INC-STB-50	Software INC On-premises Standard Edition, 50 Licenses
SW-INC-STC-100	Software INC On-premises Standard Edition, 100 Licenses
SW-INC-STD-200	Software INC On-premises Standard Edition, 200 Licenses
SW-INC-STE-500	Software INC On-premises Standard Edition, 500 Licenses
SW-INC-STF-1K	Software INC On-premises Standard Edition, 1000 Licenses
SW-INC-WSM	Software INC On-premises, Wireless Service Manager Foundation
SW-INC-WSMA-50	Software INC On-premises, Wireless Service Manager, 50 Licenses
SW-INC-WSMB-100	Software INC On-premises, Wireless Service Manager, 100 Licenses
SW-INC-WSMC-200	Software INC On-premises, Wireless Service Manager, 200 Licenses
SW-INC-WSMD-500	Software INC On-premises, Wireless Service Manager, 500 Licenses
SW-INC-WSME-1K	Software INC On-premises, Wireless Service Manager, 1000 Licenses
SW-INC-WSMF-2K	Software INC On-premises, Wireless Service Manager, 2000 Licenses
SW-INC-WSMG-5K	Software INC On-premises, Wireless Service Manager, 5000 Licenses
SW-INC-EIA	Software INC On-premises End-user Intelligent Access Foundation
SW-INC-EIAA-50	Software INC On-premises End-user Intelligent Access, 50 Licenses
SW-INC-EIAB-200	Software INC On-premises End-user Intelligent Access, 200 Licenses
SW-INC-EIAC-500	Software INC On-premises End-user Intelligent Access, 500 Licenses
SW-INC-EIAD-2K	Software INC On-premises End-user Intelligent Access, 2000 Licenses

All licenses described above do not have an expiration date.