Firmware Feature List

Generation 6 Ethernet Switches

Firmware Version: 10.7.9a, 03.06.2022

General Architecture

Linux OS	Das Linux basierende System stellt State-of-the-Art Technology sicher. Auf Grund der Open-Source Technology ist langfristige Verfügbarkeit und der schnelle Zugriff auf neue Protokolle und Methoden gewährleistet.	Seit Version: 10.1.0, 31.08.2012
Advanced G6 Architecture	Modernste Softwarearchitektur basiert auf einem zentralen Datenmodell. Große Teile der Managementschnittstellen inklusive des Handbuchs werden automatisch generiert und sind somit immer aktuell.	Seit Version: 10.1.0, 31.08.2012
SD Memory Card	Speicherung sämtlicher Firmware- und Konfigurationsdateien auf einer microSD Speicherkarte. Mit dem Wechsel der Speicherkarte werden die Dateien von einem zum anderen Gerät übertragen. Geräte-spezifische Daten wie MAC-Adresse sowie Artikel-/Seriennummer sind in einem Geräteinternen Speicher festgehalten. Die Geräte der Industrial Reihe verwenden die robustere SD Speicherkarte.	Seit Version: 10.1.0, 31.08.2012
Internal Memory Option	Bei Geräten mit internem Speicher werden die Firmware- und Konfigurationsdateien komplett intern gespeichert. Die microSD Karte kann alternative Software halten oder aus Sicherheitsaspekten gesperrt werden.	Seit Version: 10.3.3, 18.11.2013
Mirror SD card	Die auf einer SD Karte laufende Software kann auf den internen Speicher eines G+ Gerätes kopiert werden.	Seit Version: 10.5.4, 19.06.2015

Factory Information

Inventory and Factory information	Jedes Gerät verfügt über permanente Identitäts-Informationen (Seriennummer, MAC-Adresse und erweiterte Hardwaredetails). Diese Daten sind nicht auf der wechselbaren SD-Karte gespeichert.	Seit Version: 10.1.6, 13.11.2012
Custom Device Info	Kundenspezifische permanent in der Hardware gespeicherte Daten, welche auch bei SD Kartenwechsel erhalten bleiben. Von Kunden selbst durchführbar oder bei der Bestellung im Werk individuell vorkonfigurierbar.	Seit Version: 10.3.3, 18.11.2013

System

Custom MAC address	Die MAC-Adresse wird in der Produktion zugewiesen und in einem permanenten Speicher im Gerät abgelegt. Es ist jedoch möglich diese MAC per Konfiguration zu überschreiben.	Seit Version: 10.1.6, 13.11.2012
Custom Inventory Data	Kundenspezifische Inventurdaten können auf der SD Karte abgelegt werden. Im Gegensatz zu den (kundenspezifischen) Factory Daten, wandern diese mit der SD Karte. Hierzu gehören u.a.: Port alias Namen (64 Zeichen), Lokation (255 Zeichen) und Inventurtexte (bis 512 Zeichen).	Seit Version: 10.2.0, 14.12.2012
Temperature Control	Die interne Gerätetemperatur wird überwacht, gegebenenfalls werden Aktionen ausgelöst: Warnnachrichten (Syslog, Trap) in mehreren Schritten sowie Reduzierung von Portgeschwindigkeiten bzw. Power down (PoE) zur Verringerung der Verlustleistung.	Seit Version: 10.1.6, 13.11.2012

Hardware

Function	Lüfterloser Layer 2+ Switch, gesteuert durch Highspeed 1GHz ARM CPU.	Seit Version: 10.1.0, 31.08.2012
Green IT	Neueste Chiptechnologie zur Unterstützung von Energy Efficient Ethernet. Normen: IEEE 802.3az	Seit Version: 10.1.0, 31.08.2012
Jumbo Frames	Unterstützung von Jumbo-Frames mit bis zu 10kByte Länge.	Seit Version: 10.1.0, 31.08.2012
Modular Hardware Design *(Nur Industrie Switch)*	Modulare, im Feld erweiterbare Hardware in stabilem Edelstahlgehäuse. Besonders kompakte Bauform.	Seit Version: 10.3.0, 04.06.2013
RGB LED	Vollfarbige LED-Anzeigen ermöglichen ein leichtes Erkennen des Betriebsstatus. Verschiedene Modi (Dynamic, Static, Quiet, Off) ermöglichen - wenn gewünscht - ein unauffälliges Betreiben des Switches. Zur schnellen Identifizierung einzelner Geräte wird ein Lightshow-Modus angeboten.	Seit Version: 10.1.6, 13.11.2012
Input / Output Pins *(Nur Industrie Switch)*	Im Industrieswitch sind zwei unabhängige Eingänge, sowie zwei steuerbare Relais-Ausgänge verfügbar. Die Eingänge lösen Alarme aus und können darüber hinaus per Script beinahe beliebige Funktionen steuern. Die Relais schalten bei Netzteil- oder thermischen Problemen bzw. sind per Script frei programmierbar.	Seit Version: 10.3.0, 04.06.2013

IP Stack

Dual Stack	Parallele Handhabung des IPv4 und IPv6 Protokolls.	Seit Version: 10.2.2, 21.03.2013
IPv4 Stack	IPv4 Handhabung mit IPv4, ARP, DHCP, ICMP Unterstützung. Normen: RFC 791 (IPv4), RFC 826 (ARP), RFC 792 (ICMP), RFC 793 (TCP), RFC 768 (UDP), RFC 2131 (DHCP)	Seit Version: 10.1.0, 31.08.2012
DHCP Options 66/67	Gerätekonfiguration oder Softwareupdates können über DHCP-Optionen 66/67 automatisch durchgeführt werden. Zudem können Konfigurationsänderungen oder Downloads per CLI-Script geladen werden. Normen: RFC 2131 (DHCP), RFC 2132 (DHCP Options), RFC 951 (BOOTP)	Seit Version: 10.2.1, 08.02.2013
Ping, Trace Route	Die standard IP Testfunktionen PING und Trace Route sthen zur Verfügung. Seit 10.6.1d kann zudem Packet size und Anzahl der Pings eingestellt werden. Normen: RFC 792 (PING), RFC 1393 (Trace Route)	Seit Version: 10.2.0, 14.12.2012
IPv6 Management Access	IPv6 Handhabung mit IPv6, DHCPv6, ICMPv6, NDP Unterstützung. IPv6 Zugriff via WEB, CLI , SNMP und NMP-Software. Normen: RFC 2460/2464/3484/3513 (IPv6), RFC 2462 (Address Configuration), RFC 2463 (ICMPv6), RFC 2461 (Neighbor Discovery Protocol), RFC 3315 (DHCPv6)	Seit Version: 10.2.2, 21.03.2013
IPv6 Transport	IPv6-Traffic kann mit dem Switch übertragen werden. Filteroptionen für ein erweitertes Security-Set sind verfügbar.	Seit Version: 10.2.0, 14.12.2012
Dynamic ARP Inspection *Nicht verfügbar mit Hardware 1.5 / Nur verfügbar auf Ports [2/*] mit Hardware 1.6.*	Überprüft ARP Pakete auf valide MAC/IP Zuordnungen. Dazu wird die automatisch per DHCP snooping erstellte Datenbank sowie eine manuell erstellbare Zugangsliste verwendet. Bei ARP Attacken wird der Port geblockt.	Seit Version: 10.5.1, 11.12.2014
Secondary IPv4 Address	Das Gerät kann wahlweise unter einer zweiten IP Adresse angesprochen werden.	Seit Version: 10.5.4, 19.06.2015
Secondary static DNS Address	Eine zweite DNS Adresse kann konfiguriert werden.	Seit Version: 10.7.9, 10.12.2021

Ethernet Port Features

Administration	Die Abschaltung einzelener Ports ist möglich. Jeder Anschluss kann mit einem 64 Byte langem, individuellen Alias-Namen versehen werden.	Seit Version: 10.1.6, 13.11.2012
Ethernet Twisted-Pair	Auto-Negotiation von Geschwindigkeit, Duplexmode, Flow-Control, Auto MDI/MDI-X Normen: 802.3u, 802.3z	Seit Version: 10.1.6, 13.11.2012
Cable Tester	Der integrierte Kabeltester hilft dabei Kabelbrüche zu finden, hierbei findet die Zeitbereichsreflektometrie (TDR - Time Domain Reflectometry) Verwendung. Für jedes Kabelpaar wird der Status erfaßt und ggf. der Abstand zum Kurzschluß ermittelt.	Seit Version: 10.4.0, 20.12.2013
Ethernet Fixed Fiber	100/1000, Duplexmode, Flow-Control, 10G Ethernet in bestimmten Produkten	Seit Version: 10.2.0, 14.12.2012
Wire Speed MACSEC Encryption	Ausgewählte 10G Ethernet fähige Geräte bieten "wire speed"MACSEC AES256 Verschlüsselung. Dabei können Teile des IP Headers unverschlüsselt bleiben um eine Übertragung durch andere Netze hindurch zu ermöglichen.	Seit Version: 10.7.9, 10.12.2021
Ethernet SFP	Unterstützung von steckbaren Transceivern (SFP) für flexible Verwendung unterschiedlicher optischer Parameter (Wellenlänge, Glasfasertyp, Geschwindigkeit und Kabellänge). Gerätevarianten mit zwei SFPs (FTTO) oder bis zu 8 SFPs (Industrieswitch) sind verfügbar. Die SFP Anschlüsse sind nicht kodiert, es können alle am Markt verfügbaren SFPs eingesetzt werden.	Seit Version: 10.2.0, 14.12.2012
Dual Media Ports	Dual Media Ports können mit Kupfer- oder Glasfaserkabeln angeschlossen werden. Präferenzen und Prioritäten können hierfür festgelegt werden.	Seit Version: 10.2.1, 08.02.2013
Loop Protection	Lokale Loop Protection zur Erkennung und Deaktivierung parallel geschalteter Verbindungen zum gleichen Switch oder Schleifen zwischen lokalen Anschlüssen.	Seit Version: 10.3.2a, 04.11.2013
SFP Auto Speed	Die Portgeschwindigkeit wird automatisch der maximalen Datenrate des eingesteckten SFP angepasst. Diese Funktion ist nur mit MICROSENS SFPs verfügbar.	Seit Version: 10.5.2, 11.02.2015

SFP

SFP Management	Automatische Erkennung und Anzeige von SFPs, Unterstützung von Digital Diagnostik Funktionen (DDM). Einsetzen und Entfernen generiert automatische Meldungen (Traps/Syslog).	Seit Version: 10.1.7, 19.11.2012
Power Monitoring	Die optische Sende- und Empfangsleistung werden permanent überwacht. Bei Leistungsabfall können automatische Alarmmeldungen generiert werden, wodurch wärend der Installation nicht jeder Anschluß manuell konfiguriert und gemessen werden muß.	Seit Version: 10.1.7, 19.11.2012
CSFP Support	Einige Switch Ausführungen unterstützen so genannte Compact SFPs (CSFPs). Ein CSFP kann zwei unabhängige Ethernet Verbindungen übertragen (2x Simplex, über Port 5 und 6).	Seit Version: 10.2.1, 08.02.2013
micro OTDR Support	Unterstützt SFP basierte OTDR Messungen(Reflektometer) um Veränderungen oderBrüche in Glasfaserkabel zu erkennen. Diese Funktion ist besonders für das NM3 Modul im MSP1000 geeignet.	Seit Version: 10.7.4a, 13.06.2019

Power-over-Ethernet (PoE)

PoE and PoE+ support	Bis zu 30W pro angeschlossenem Endgerät (PoE+). Die Gesamtleistung pro Switch ist abhängig vom Netzteil und Gerätetyp. Normen: 802.3af (PoE) 802.3at (PoE+)	Seit Version: 10.1.6, 13.11.2012
PoE Control	PoE / PoE+ werden nur aktiv, wenn ein PD-Gerät (Powered Device) erkannt wird. Die Ausgangsspannung und –strom werden überwacht. Werden Limits überschritten, wird an dem Port PoE abgeschaltet. Via Syslog/Traps können Warnmeldungen generiert werden.	Seit Version: 10.1.6, 13.11.2012
PoE+ Enable	PoE+ sollte nur automatisch mittels LLDP-MED Protokoll aktiviert werden, sofern Endgeräte dies nicht unterstützen, kann die Aktivierung manuell übers Management erfolgen.	Seit Version: 10.2.1, 08.02.2013
Emergency Port	Einzelne Anschlüsse können eine entsprechende Priorität erhalten. Sollte die PoE-Power Limitierung greifen, werden diese (emergency) Ports nicht abgeschaltet.	Seit Version: 10.1.6, 13.11.2012
PD Operation	Bestimmte Switch Versionen können als Powered Device (PD) per PoE betrieben werden. In diesem Modus wird kein Netzteil benötigt. Bei Switches welche zusätzliche externe Netzteile vorsehen, kann der PoE Eingang als zusätzliches Backup verwendet werden.	Seit Version: 10.3.0, 04.06.2013
PoE Watchdog	Die Erreichbarkeit eines PoE versorgten Endgerätes kann überwacht werden. Wird ein Ausfall erkannt, wird automatisch die PoE Versorgung für kurze Zeit unterbrochen um eines Reset auszulösen.	Seit Version: 10.7.9a, 03.06.2022

Switch / MAC

MAC Table	Unterstützung von bis zu 8192 MAC-Adressen. MAC-Adressen werden automatisch gelernt, können aber auch manuell konfiguriert werden	Seit Version: 10.1.0, 31.08.2012
MAC Filter	Über verschiedene Anzeigenfilter kann auf die MAC-Adresstabelle zugegriffen werden. Für die Suche werden vordefinierte sowie individuelle Filter zur Verfügung gestellt.	Seit Version: 10.2.0, 14.12.2012
SNMP Access	D-BRIDGE und Q-BRIDGE MIBs werden unterstützt Normen: RFC1493 (obsoletes RFC1286)	Seit Version: 10.2.2, 21.03.2013
MAC Limit	Limitierung der zugriffsberechtigten MAC-Adressen pro Port ist möglich. Siehe auch Abschnitt PAC (Port Access Control)!	Seit Version: 10.5.1, 11.12.2014
MAC Limit per VLAN	Limitierung der zugriffsberechtigten MAC-Adressen pro Port und VLAN ist möglich. Siehe auch Abschnitt PAC (Port Access Control)!	Seit Version: 10.7.1, 14.03.2018
Configurable MAC Aging Time	Die MAC-aging-Time kann zwischen 15s und 1h eingestellt werden (Vorgabe: 5min)	Seit Version: 10.4.0, 20.12.2013

RMON Statistics

RMON counters	35 integrierte Zähler pro Anschluß sind hilfreich für die Netzwerkanalyse und bei der Fehlerbehebung. Normen: RMON: RFC 2819 (obsoletes RFC 1757, RFC 1271), Etherlike: RFC 2665 (obsoletes RFC 1643, RFC 1623, RFC 1398), RFC 2233 (obsoletes RFC 1573, RFC 1213)	Seit Version: 10.1.7, 19.11.2012
Port Utilization	Für jeden einzelnen Port ist die Auslastung in % pro Übertragungsrichtung sichtbar. Angezeigt werden die aktuelle Auslastung sowie ein Durchschnitt über 30 Sekunden sowie 5 Minuten.	Seit Version: 10.2.3, 28.04.2013
Port Mirroring	Daten eines oder mehrerer Ports können auf einen anderen Port kopiert werden. Auf diese Weise können die Daten auf einem externen Analyzer angesehen werden.	Seit Version: 10.6.1, 22.07.2016

MSP 1000

Forward Migration	Das neue NM3 Management Modul erweitert alle Vorteile des G6 Systems auf die MSP1000 Optische WDM Plattform. Alle Funktionen der vorherigen Generationen wurden erhalten und sogar ältere TeraMile und LastMile System können aufgerüstet werden.	Seit Version: 10.6.0, 22.12.2015
Inventory	Automatische Erkennung der eingesteckten Module. Übersichtliche Darstellung aller relevanten Kenndaten.	Seit Version: 10.6.0, 22.12.2015
Configuration and Status	Alle MSP 1000 Module sowie fast alle Module der TeraMile und LastMile können vollständig konfiguriert und überwacht werden. All dies ist über alle verfügbaren Management Schnittstellen wie SNMP, Web, CLI und NMP Manager möglich.	Seit Version: 10.6.0, 22.12.2015
Alarm Correlation	In Kombination mit NMP wird eine Liste aller aktiven Störungen angezeigt.Ist ein Problem gelöst verschwindet es aus der Liste.	Seit Version: 10.7.4a, 13.06.2019
Active and Passive mode	Im passiven Mode lernt die NM3 die aktuellen Einstellungen aller anderen Module. Im aktiven Mode erzwingt die NM3 ihre lokalen Einstellungen auf die anderen Module.	Seit Version: 10.6.0, 22.12.2015

SmartOffice

General Features	SmartOffice is complete room automation system designed to measure and control office environment. This includes lighting, temperature, outlets, blinds, air condition and other facilities. Sensor and actors from MICROSENS or various third parties can be combined for a customized decentralized solutiuon. Such rooms can in turn be managed centrally from a Building Mangement System.	Seit Version: 10.7.0, 07.04.2017
PoE based LED Lighting	LED panels replace traditional neon tubes. The MICROSENS SmartLightController acts as an intelligent power supply that converts PoE energy to dimmable LED complatible power.	Seit Version: 10.7.0, 07.04.2017
Room Sensors	The MICROSENS SmartLightController includes sensors to detect ambient temperature, brightness, motion. These sensor data act as inputs to the room automation.	Seit Version: 10.7.0, 07.04.2017
Automatic Room	A SmartOffice can operate fully automated, based on motion and time. After a programmable idle time the room is shut down. What exactly shuts down, and what not can be configured.	Seit Version: 10.7.0, 07.04.2017
Configurable Graphical User Interface	A SmartOffice can also be operated very conviently via a tablet or mobile phone. The graphical user interface (GUI) is fully configurable and customizable to meet any customer requirements.	Seit Version: 10.7.0, 07.04.2017
Scene Based	All actions are grouped in scenes. A scene may affect every as little or as much of the parameter as desired. A scene can be global, room specific or even remotely accessed (if enabled) to be engaged from a third party.	Seit Version: 10.7.0, 07.04.2017
Hardware Buttons	A SmartOffice can interface to many types of physical switches. Any switch can be mapped to any scene.	Seit Version: 10.7.0, 07.04.2017
Scripting Language	A key feature of the SmartOffice solution is the powerful scripting engine The script incorporates the decision logic as what to do based on sensor input. Most scripts are preinstalled during installation of the SmartDirector App, but additional custom scripts may be added to perform a wide range of features such as SNMP, HTTP or FTP operations, special office functions, etc.	Seit Version: 10.7.0, 07.04.2017
SmartDirector App	The SmartOffice framework offers great flexibility. In fact so much that it is sensible to offer a default functionality and graphical user interface. This interface is created by installation the SmartDirector App. For special applications, other variations of the App can be created, without affecting the general firmware of the underlying switch.	Seit Version: 10.7.0, 07.04.2017
microPLC	Das SmartOffice system bietet eine Soft-SPS Funktio. Damit können neben der üblichen Event basierendenLogik auch strikt zeitgesteuerte Regleralgorithmen wie ein PID regler einfach realisiert werden. Die micoPLC benötigt keinen Compiler kann direkt in microScript programmiert werden. IEC Programmiersprachen wie ST werden nicht unterstützt.	Seit Version: 10.7.2, 02.10.2018
Remote Control Interface	A SmartOffice comes with a local graphical interface. To operate the system remotely it possible to simulate operation via an HTTPS REST API interface. When enabled, for each element indiviually, it is possile to expose a well defined set of functions, which can be controlled. Likewise,it is possible to read information from the system.	Seit Version: 10.7.0, 07.04.2017
enOcean support	SmartOffice support wireless automation devices using the enOcean protocol. This includes switches, relays to switch outlets, blinds and some sensors. Energy consumption monitoring is available.	Seit Version: 10.7.0, 07.04.2017
Homematic support	SmartOffice support wireless automation devices using the Homematic protocol. This includes switches, relays to switch outlets temperature control and other devices.	Seit Version: 10.7.0, 07.04.2017
Modbus/RTU support	Modbus is a standard automation bus. SmartOffice supports local serial wiring to Modbus enabled devices. Custom scripts are required for integration as there is no standard on how to interpret the data.	Seit Version: 10.7.0, 07.04.2017

Modbus/IP support	Modbus/IP ist ein Standard Automation Protokoll. Beliebige Modbus Daten können auf SmartOffice Sensoren oder Aktoren lesend bzw. schreibend abgebildet werden. Dabei können Datentyp und Einheit definiert werden. Normen: IEC 61158 CPF15/1	Seit Version: 10.7.2, 02.10.2018
IP500 support	IP500 ist ein neue Funkschnittstelle welche durch parallele Verwendung zweier Frequenzen erhöhte Zuverlässigkeit bietet. Je nach Gerät wird eine zusätzliche Hardware benötigt, welche die Funkelektronik beinhaltet. Normen: IEC 61158 CPF15/1	Seit Version: 10.7.9, 10.12.2021

Controller

Smart Light Controller	Über die universelle Konfiguration eines standart SmartOffice Device hinaus, können die SmartLight Controller hiermit einfacher und umfangreicher eingestellt werden.	Seit Version: 10.7.1c, 17.07.2018
Smart IO Controller	Über die universelle Konfiguration eines standart SmartOffice Device hinaus, können die digitalen und analogen Schnittstellen parametrisiert werden und SmartOffice Sensor oder Actor Gruppen zugefügt werden.	Seit Version: 10.7.1c, 17.07.2018
CSLC	Der kompakte CSLC ermöglicht die direkte Ansteuerung von 24 LED Leuchten über twisted pair Verkabelung.	Seit Version: 10.7.7, 28.05.2020

Virtual LANs (VLANs)

VLAN Filter	Bis zu 256 VIDs (Virtual LAN IDs) sind konfigurierbar Normen: IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p	Seit Version: 10.2.0, 14.12.2012
Access Mode	Für die Verbindung von nicht VLAN-fähigen Endgeräten (z.B. PCs). Hier werden ausgehende Datenpakete ohne VID zum Endgerät gesendet. Eingehende Datenpakete erhalten die PVID (Port-Default-VLAN ID).	Seit Version: 10.2.0, 14.12.2012
Trunk Mode	Für die Verbindung zu VLAN-fähigen Netzwerkgeräten. Hierbei werden alle ausgehenden Datenpakete mit VID versehen und eingehende werden mit VID empfangen. Eingehende ohne 'VLAN Tag' erhalten die PVID.	Seit Version: 10.2.0, 14.12.2012
Hybrid Mode	Für den Verbindung von VLAN-fähigen und nicht VLAN-fähigen Endgeräten am selben Anschluß (Bsp. VoIP-Telefon und PC). Eingehende Datenpakete ohne VID werden mit der PVID versehen. Bei Paketen mit VID erfolgt keine Umsetzung. Entsprechend wird in der Gegenrichtung verfahren.	Seit Version: 10.2.0, 14.12.2012
Multiple VLAN Reservation Protocol (MVRP)	Multiple VLAN Registration Protocol (MVRP) automatisiert die VLAN Konfiguration. Normen: IEEE 802.1ak	Seit Version: 10.5.0, 22.08.2014
Extreme Auto Attach (former Avaya Fabric Attach)	Ermöglich Anschluß an ein SPB basieren Netzwerk wie Avaya Fabric. Dabei werden lokale VLANs auf SPB I-SIDs abgebildet.	Seit Version: 10.6.1, 22.07.2016
Extreme (Avaya) Zero Touch	Bei Anschluss an ein SPB basierendes Netzwerk werden die lokale VLAN automatisch über das Netz angelegt. Hinweis: Der Authentifizierungsschlüssel des Netzes muss dafür voreingestellt sein.	Seit Version: 10.7.5, 31.08.2019
Stacked VLANs (Q-in-Q)	Stacked (gestapelte) VLANs werden von Netzbetreibern genutzt um bereits VLAN getaggte Kundendaten durch das eigene VLAN basierede Netz zu transportieren. Normen: IEEE 802.1ad	Seit Version: 10.7.0, 07.04.2017
Priority Override	Die Priorität im vorhandenen VLAN-Tag (Trunk- oder Hybrid-Modus) kann durch eine selbst definierte Priorität überschrieben werden.	Seit Version: 10.1.7, 19.11.2012
Voice VLAN	Die Voice VLAN-ID wird per LLDP/CDP einem VOIP Telefon zugewiesen.	Seit Version: 10.1.7, 19.11.2012
RSTP VLAN	Das RSTP VLAN wird vom Spanning Tree für die Übertragung der BPDU-Pakete verwendet.	Seit Version: 10.1.7, 19.11.2012
Unauthorized VLAN	Die Unauthorized VLAN-ID wird in Verbindung mit Port Access Control (PACC) für abgewiesene Endgeräte verwendet (Gast VLAN)	Seit Version: 10.1.7, 19.11.2012
Management VLAN	VLAN ID welche der Management Agent (interner Port) verwendet.	Seit Version: 10.1.7, 19.11.2012

Quality of Service (QoS)

Priority Queues	4 Warteschlangen pro Port.	Seit Version: 10.1.6, 13.11.2012
Prioritization Scheme	Unterstützt zwei mögliche Abarbeitungsschemen: Strikte Priorität (höhere Priorität immer zuerst) oder gewichtete (8:4:2:1 hoch zu niedrig).	Seit Version: 10.1.6, 13.11.2012
Layer1 Priority	Statische Priorität, Zuordnung pro Port	Seit Version: 10.1.6, 13.11.2012
Layer2 Priority (802.1p)	Ankommende Pakete werden anhand der Priorität im VLAN-Tag den Warteschlangen zugeordnet. Die 8 VLAN Prioritäten Codes können individuell den 4 Warteschlangen zugeordnet werden. Normen: IEEE 802.1p (VLAN priority code point)	Seit Version: 10.1.6, 13.11.2012
Layer3 Priority (IPv4 / IPv6)	Ankommende Pakete werden anhand des DiffServ-Wertes (IPv4) bzw. Traffic-Klasse (IPv6) gewichtet. Unterstützt werden 64 Codepoints, wobei jeder individuell einer Warteschlange zugeordnet werden kann. Normen: RFC 2474/3260 (IPv4 DiffServ/IPv6 Traffic Class)	Seit Version: 10.1.6, 13.11.2012
Egress Rate Shaping	Begrenzung der ausgehenden Daten. Sie werden gepuffert um einen gleichmäßigen Datenfluß zu erzielen. (Bandbreitenbegrenzung)	Seit Version: 10.5.0, 22.08.2014
Ingress Rate Shaping	Begrenzung der Datenmenge die ein Anschluß empfangen kann.(Bandbreitenbegrenzung)	Seit Version: 10.6.1, 22.07.2016

Spanning Tree Protocols

Spanning Tree (STP)	Automatische Erkennung von Loops (Schleifen) sowie redundanten Netzwerkpfaden, auch in Kombination mit VLANs	Seit Version: 10.2.0, 14.12.2012
Rapid Spanning Tree (RSTP)	Automatische Erkennung von Loops (Schleifen) sowie redundanten Netzwerkpfaden, auch in Kombination mit VLANs. RSTP ist rückwärts kompatibel zu STP, verwendet aber einen schnelleren Algorithmus. Normen: IEEE 802.1D-1998 IEEE 802.1D-2004 IEEE 802.1w	Seit Version: 10.2.0, 14.12.2012
Multiple Spanning Tree (MSTP)	Bis zu 64 STP-Instanzen laufen in konfigurierbaren VLAN Gruppen. Normen: IEEE 802.1s IEEE 802.1Q	Seit Version: 10.3.2a, 04.11.2013
BPDU Guard	BPDU Guard zeigt die Aktivität von STP an, wenn durch STP Pakete entfernt werden. Der betroffene Port kann zur Sicherheit abgeschaltet werden oder nur ein Event (Syslog/ Trap) erzeugt werden.	Seit Version: 10.3.0, 04.06.2013
Bridge Assurance	Erkennung unidirektionaler Linkfehler, die bei Glasfaserverbindungen entstehen, wenn nur die Faser einer Richtung gestört ist.	Seit Version: 10.3.2a, 04.11.2013

Port Access Control

IEEE 802.1X Authentication	Mehrere Nutzer können über einen zentralen RADIUS Server/ Dienst mit Hilfe von Username/Passwort oder Zertifikat authentifiziert werden. Normen: EAP-PEAP/MSCHAPv2, EAP-PEAP/TLS, EAP-PEAP/ MD5, EAP-TTLS/EAP-MD5, EAP-TTLS/EAP-MSCHAPv2, EAP-TTLS/MSCHAPv2, EAP-TTLS/EAP-TLS, EAP-TTLS/PAP,EAP-FAST	Seit Version: 10.2.1, 08.02.2013
IEEE 802.1X Supplicant *Nicht verfügbar mit Hardware 1.5 / Nur verfügbar auf Ports [2/*] mit Hardware 1.6.*	Ein IEEE 802.1X Supplicant übernimmt die authentifizierung lokal angeschloser Geräte. Lokaler Nutzername und Passwort oder Zertifikate können verwendet werden.(EAP-MD5, PEAP) Normen: EAP-MD5, PEAP	Seit Version: 10.7.0, 07.04.2017
RADIUS MAC Authentication	Mehrere Netzwerkgeräte können über einen zentralen RADIUS Server/Dienst aufgrund der MAC-Adresse authentifiziert werden. Normen: EAPOL, RADIUS	Seit Version: 10.2.1, 08.02.2013
MAC locking	Mehrere Netzwerkgeräte können mit Hilfe der MAC-Adresse authentifiziert werden. Dabei können beliebig viele MAC-Adressen manuell oder automatisch konfiguriert werden. Spezifische MAC-Adressen und Hersteller-MACs können kombiniert werden.	Seit Version: 10.2.1, 08.02.2013
MAC learning	Pro Port können bis zu 9 MAC-Adressen gelernt werden. Die gelernten Adressen werden in der Konfiguration gespeichert (permanent). Das MAC-learning kann manuell angestoßen werden, die ersten „n" Geräte werden automatisch gelernt.	Seit Version: 10.2.1, 08.02.2013
Limited number of MACs	Ports können individuell konfiguriert werden nur zwischen 1 - 255 MACs zuzulassen. Weitere hereinkommende MACs werden im Hardware Layer verworfen.	Seit Version: 10.5.1, 11.12.2014
Limited number of MACs per VLAN	Ports können individuell konfiguriert werden nur zwischen 1 - 255 MACs pro VLAN zuzulassen.	Seit Version: 10.7.0, 07.04.2017
Learned MAC time out	Die Gültigkeit gelernter MAC-Adressen kann zeitlich begrenzt werden, um weitere Computer über die MAC-Adresse verbinden zu können.	Seit Version: 10.4.0, 20.12.2013
Dynamic VLAN	Über RADIUS kann pro Nutzer eine spezifische VLAN-ID übergeben werden („tunnel-attribute in accept message"). Am Port wird das VLAN automatisch eingestellt. Im Fall einer Abweisung (nicht Authentifizierung) kann der ganze Port geblockt oder der Nutzer einem hierfür spezifischem VLAN (Gast-VLAN) zugewiesen werden.	Seit Version: 10.2.1, 08.02.2013
Allowed Outgoing Port (Port based VLANs)	Diese Funktion beschränkt den Datenfluss zwischen bestimmten Ports auf dem gleichen Switch.	Seit Version: 10.7.0, 07.04.2017
IP Address Logging	Die im Netz auftretenden IP Adressen werden durch Mitlesen der ARP und DHCP Nachrichten erlernt	Seit Version: 10.5.1, 11.12.2014
Wake-on-Lan support	Die Funktion erlaubt das senden von Wake-On-Lan Paketen durch einen geblockten Port. Auch bekannt als Unidirectional Controlled Port oder Admin Controlled Directions in der IEEE 802.1X-2004 Spezifikation.	Seit Version: 10.6.1d, 11.11.2016
Network Edge Authentication	Die network edge authentication Funktion wird verwendet einen Authentication Switch zu authentifizieren. Dies entspricht der Cisco NEAT Funktion.	Seit Version: 10.7.0, 07.04.2017
Authentication Fail Retry Timer	Wenn eine Authentifizierung fehlgeschlagen ist, wird diese nach eingestellter Zeit automatisch wiederholt, auch wenn es das Endgerät nicht selbst einleitet.	Seit Version: 10.7.0d, 10.11.2017
Change of Authorization	CoA ermöglicht De-Authentifizierung gefolgt von einer Re-Authentifizierung von einer bestehenden Sitzung eingeleitet durch den Authentifizierungs Server über das RADIUS Protokoll. Normen: RFC 3576 (CoA)	Seit Version: 10.7.9, 10.12.2021

IGMP

IGMP Snooping	„Snooping of Internet Group Management Protocol" (IGMPv1/v2/v3) für IPv4. Automatisches Erkennen und Weiterleiten von IPv4 Multicast-Strömen. Nicht registrierte Pakete können geflutet oder geblockt werden. Multicast Router werden automatisch oder mittels Abfrage erkannt. Normen: RFC 4541 (IGMP)	Seit Version: 10.2.0, 14.12.2012
IGMP Snooping per VLAN	IGMP-Funktion unabhängig von konfigurierten VLANs	Seit Version: 10.3.0, 04.06.2013
MLD Snooping	„Snooping of Multicast Listener Discovery (MLDv1/v2)" für IPv6. Automatisches Erkennen und Weiterleiten von IPv6 Multicast-Strömen. Multicast Router werden automatisch oder mittels Abfrage erkannt. Normen: RFC 3810/4604 (MLD), RFC4541	Seit Version: 10.3.2a, 04.11.2013

DHCP

DHCP Snooping *Nicht verfügbar mit Hardware 1.5 / Nur verfügbar auf Ports [2/*] mit Hardware 1.6.*	Durch Mitlesen aller DHCP Nachrichten erlernt das Gerät die gültigen MAC/IP Beziehungen. Zusätzlich werden DHCP Pakete von nicht vertrauenswürdigen Ports verworfen.	Seit Version: 10.5.1, 11.12.2014
IP-MAC Binding Table *Nicht verfügbar mit Hardware 1.5 / Nur verfügbar auf Ports [2/*] mit Hardware 1.6.*	Durch DHCP Snooping gelernte MAC-IP Beziehungen werden in einer Tabelle bereitgestellt.	Seit Version: 10.5.1, 11.12.2014
DHCP Filtering *Nicht verfügbar mit Hardware 1.5 / Nur verfügbar auf Ports [2/*] mit Hardware 1.6.*	DHCP Filterung zur Prävention gegen bösartige Nutzer. Dieses Feature funktioniert unter IPv4 und IPv6 gleichermaßen.	Seit Version: 10.5.0, 22.08.2014
DHCP Flooding Detection *Nicht verfügbar mit Hardware 1.5 / Nur verfügbar auf Ports [2/*] mit Hardware 1.6.*	Versucht DHCP Attacken durch zu viele herein kommende DHCP Meldungen zu erkennen und blockiert gegebenfalls den lokalen Port.	Seit Version: 10.5.0, 22.08.2014
DHCP relay agent with option 82	DHCP-Anfrage von Endgeräten, die über einen Accessport/ Userport hereinkommen, werden vom Switch um sogenannte Lokationsinformationen (z. Bsp. Switch- und Portnummer) ergänzt. Vom DHCP-Dienst/Server können so qualifiziertere Zuweisungen der IP-Einstellungen erfolgen.	Seit Version: 10.5.1, 11.12.2014
DHCP Options 66/67	Per DHCP (Option 66/67) können Gerätekonfiguration und/ oder Firmware-Updates gesteuert werden. Durch Download eines CLI-Scriptes können Aktionen wie weitere Downloads (Firmware) oder Konfigurationsänderungen angestoßen werden. Normen: RFC 2131 (DHCP)	Seit Version: 10.2.1, 08.02.2013
Dynamic ARP Inspection *Nicht verfügbar mit Hardware 1.5 / Nur verfügbar auf Ports [2/*] mit Hardware 1.6.*	Überprüft ARP Pakete auf valide MAC/IP Zuordnungen. Dazu wird die automatisch per DHCP snooping erstellte Datenbank sowie eine manuell erstellbare Zugangsliste verwendet. Bei ARP Attacken wird der Port geblockt.	Seit Version: 10.5.1, 11.12.2014
PPPoE Snooping	PPP over Ethernet wird von Carriern genutzt um eindeutig das Gerät und den Port zu identifizieren an dem ein Login statt findet. Normen: RFC 2516	Seit Version: 10.7.0, 07.04.2017
PPPoE variable Remote and Circuit Ids	PPPoE kann vom Netzbetreiber flexibel voreingestellt werden. Normen: RFC 2516	Seit Version: 10.7.0d, 10.11.2017
RADIUS controlled dynamic IP-Address provisioning with DHCP	DHCP Anfragen werden lokal mit IP Address und Netmask beantwortet, welche per RADIUS vom zentralen Server übermittelt werden, sobald sich das Endgerät erfolgreich authentifiziert hat.	Seit Version: 10.7.6, 22.01.2020
DHCP Server	Ein lokaler DHCP Server kann eingeschaltet werden. Dabei sind Adressbereich und Laufzeit einstellbar.	Seit Version: 10.7.9, 10.12.2021

Network Time Protocol (NTP)

NTP Client	Die Netzwerkzeit kann durch einen NTP-Dienst automatisch empfangen werden. Es ist möglich bis zu 2 NTP-Server zu konfigurieren oder bis zu 4 server per DHCP zu erhalten. Die Agent-Zeit kann auch manuell konfiguriert werden. Normen: RFC 4330 (SNTP)	Seit Version: 10.1.7, 19.11.2012

Redundant Ring Protocol

MICROSENS Ring Protocol	MICROSENS Ring Redundanz Protokoll. Ein Gerät kann hierbei in zwei unabhängigen Ringen gleichzeitig Teilnehmer sein. Typische Ringwiederherstellungszeit liegt unter 50ms.	Seit Version: 10.4.1, 21.02.2014

Link Layer Discovery Protocols (LLDP, CDP)

LLDP reception	Empfangen von LLDP-Information vom Nachbargerät am Netzwerkanschluss. Anzeigen der empfangenen Informationen inkl. geografischer Koordinaten und Lokationsinformationen. Normen: IEEE 802.1AB (LLDP)	Seit Version: 10.2.1, 08.02.2013
LLDP transmission	Eigene geografische Koordinaten und Lokationsinformationen für das Aussenden können definiert werden.	Seit Version: 10.2.1, 08.02.2013
LLDP-MED	„Media Endpoint Discovery" für die automatische Erkennung von LAN-Policies. Unterstützung der VLAN–Zuweisung und PoE+ Steuerung. Normen: ANSI/TIA-1057 (LLDP-MED)	Seit Version: 10.2.2, 21.03.2013
LLDP/CDP preference	Gerät bevorzugt den LLDP-Standard, reagiert und akzeptiert aber auch CDP.	Seit Version: 10.2.0, 14.12.2012
CDP operation	Unterstützung des Cisco Discovery Protocol CDP v1, v2 für die automatische Erkennung von CDP-fähigen Nachbargeräten.	Seit Version: 10.2.0, 14.12.2012
CDP Voice VLAN	Unterstützung der automatischen Voice-VLAN Zuweisung bei Anschluss eines Cisco VoIP-Gerätes.	Seit Version: 10.2.0, 14.12.2012

Link Aggregation Control Protocol (LACP)

Static Link Aggregation	Vervielfältigt die verfügbare Bandbreite zwischen zwei Endpunkten. Die Konfiguration erfolgt manuell. Normen: IEEE 802.1ax, IEEE 802.3ad	Seit Version: 10.3.2a, 04.11.2013
Dynamic Link Aggregation	Vervielfältigt die verfügbare Bandbreite zwischen zwei Endpunkten. Die Konfiguration erfolgt dynamisch und automatisch mit allen verfügbaren Ports eine Gruppe. Normen: IEEE 802.1ax, IEEE 802.3ad	Seit Version: 10.3.2a, 04.11.2013
Load Balancing and Trunking	Lastverteilung findet zwischen den LACP Endpunkten statt. Bei Ausfall eines Port des Bündels wird auf den übrigen Ports weiter gearbeitet. So ist auch ein Backup realisiert. Diese Funktion wird auch EtherChannel genannt.	Seit Version: 10.3.2a, 04.11.2013
IEEE 802.1X Supplicant should authenticate on every port of a LACP trunk	Wenn der Uplink Port eines Switches per LACP aggregiert wird, so kann IEEE 802.1X Supplicant zur Authentifizierung verwendet werden.	Seit Version: 10.7.6, 22.01.2020

Access Control Lists (ACL)

Access Control Lists (ACL) *Nicht verfügbar mit Hardware 1.5 / Nur verfügbar auf Ports [2/*] mit Hardware 1.6.*	ACL filltern eingehende Pakete mit voller Datenrate um unerwünschte oder gefährliche Daten daran zu hindern in das Netz zu gelangen.	Seit Version: 10.6.1, 22.07.2016
Dynamic ACL via RADIUS *Nicht verfügbar mit Hardware 1.5 / Nur verfügbar auf Ports [2/*] mit Hardware 1.6.*	Zentralisiert das Konfigurieren der ACL. Während der 802.1X Port-Authentifizierung werden die gültigen ACL Regeln übermittelt und automatisch angewendet.	Seit Version: 10.7.1, 14.03.2018

IoT Protocol MQTT

Auto publish actor, sensor and GUI data	Alle Änderungen von Sensoren oder Aktoren können publiziert werden. Ebenso können alle Bedienungen der GUI ausgesendet werden. Diese Funktionen können individuell eingeschaltet werden. Normen: MQTT V3.1.1	Seit Version: 10.7.1c, 17.07.2018
Auto subscribe actor, sensor and GUI data	Sensoren oder Aktoren können per MQTT gesetzt werden.Auch die Bedienungen des GUI kann aus der Ferne erfolgen. Die Funktionsgruppen können individuell eingeschaltet werden. Normen: MQTT V3.1.1	Seit Version: 10.7.4, 31.01.2019
Topic Map	Einzelne MQTT Topics können abonniert werden und auf interne Sensoren abgebildet werden. Ebenso können einzelne Daten selektiv publiziert werden.	Seit Version: 10.7.1c, 17.07.2018
Configuration via MQTT	Die Systemkonfiguration kann per MQTT gelesen und geschrieben werden. Schreiben kann Grundsätzlch abgeschaltet werden. Die Zugriffsrechte können aber auch Feingranular auf einen MQTT user zugeschnitten werden.	Seit Version: 10.7.7, 28.05.2020
Script Execution via MQTT	Auf dem System befindliche MicroScripts können per MQTT gestarted werden. Dabei werden sowohl die MQTT Daten wie auch das Topic als Parameter übergeben.Die erlaubten Scripte können präzise eingeschränkt werden.	Seit Version: 10.7.7, 28.05.2020
Local broker	Normalerweise wird ein zentraler Broker zur MQTT Kommunikation genutzt. Alternativ kann ein inter Broker eingeschaltet werden.	Seit Version: 10.7.1c, 17.07.2018
Data Transformation	Oft liegen die gleichartige Daten unterschiedlicher Hersteller in verschiedenen Formaten oder Einheiten vor. Durch Transformation kann dies vereinheitlicht werden.	Seit Version: 10.7.2, 02.10.2018

Automation Protocol Modbus

Element Map	Daten von Modbus-fähigen Geräten könnenauf lokale SmartOffice Sensoren und Aktoren umgesetzt werden.	Seit Version: 10.7.2, 02.10.2018
Data Formatting	Modbus Daten kommen ohne jegliche Kennzeichung des Datentyps oder deren Bedeutung. Mit Format-Einstellungen können die Daten gekennzeichnet und verständlich im SmartOffice eingebunden werden.	Seit Version: 10.7.2, 02.10.2018
Data Transformation	Oft liegen die gleichartige Daten unterschiedlicher Hersteller in verschiedenen Formaten oder Einheiten vor. Durch Transformation kann dies vereinheitlicht werden.	Seit Version: 10.7.2, 02.10.2018

Command Line Interface (CLI)

Base Features	Intuitives Command Line Interface für das Management jedes einzelnen Aspektes des Geräts. Unterstützung von Wildcards und Portnamen sowie Variablen. Schnelle Befehlseingabe durch Auto-Vervollständigung und Befehlswiederholungsspeicher. Unterstützung von individuellem Consolen-Prompt, automatischem Timeout bei Inaktivität und automatischem Logout bei Verbindungsabbruch sowie Farbanzeigen, integrierte Hilfe für sämtliche Parameter und Befehle.	Seit Version: 10.1.6, 13.11.2012
Context Sensitive Help	Eingabe eines „?" (Fragezeichens) während der Eingabe listet die zum Befehl spezifischen Parameter und Optionen sowie einen kurzen Hilfetext auf. Alle optionen werden detailiert aufgelistet.	Seit Version: 10.1.6, 13.11.2012
Offline Configuration	Die Offline-Konfiguration erlaubt das Schreiben von beliebig vielen Konfigurationen / Befehlen. Diese können per Dateitransfer kopiert, geladen und gespeichert werden. Offline-Konfigurationen können online zu jeder Zeit durchgeführt werden.	Seit Version: 10.1.6, 13.11.2012
Comprehensive Editing	Alle Parameter werden immer in der gleichen Syntax angezeigt und geschrieben. Für den Umgang ist kein separates Handbuch notwendig. Befehle können gescrollt, Wertebereiche entsprechend angezeigt, Parameter können per Bereich oder * „Wildcard") geschrieben werden.	Seit Version: 10.1.6, 13.11.2012
Scripting	Vollständige Script Unterstützung. Ein Script kann sämtliche CLI-Befehle beinhalten. Die Bearbeitung kann sowohl lokal im CLI als auch Remote mit einem späteren Up-/Download erfolgen. Die Script-Funktion ist ebenso mit der DHCP/BOOTP-Funktion anwendbar. Per Script kann ein Gerät konfiguriert, weitere Scripte geladen oder Software-Updates ausgelöst werden.	Seit Version: 10.1.7, 19.11.2012
microScript Language	Umfangreiche und mächte Scriptsprache erlaubt kundenspezifische Funktionserweiterungen, ohne dass die Systemsoftware angepasst werden muss.	Seit Version: 10.3.1, 30.08.2013
Timer Controlled Scripting	Vereinfacht den Entwurf von komplexen Scripten und zeitgesteuerten Abläufen.	Seit Version: 10.6.1, 22.07.2016
Show All Config	Mit dem Befehl „ShowAllConfig" wird die gesamte Konfiguration des Gerätes angezeigt und simultan eine Script Datei erstellt. Das Script kann so direkt als Backup oder zur gleichen Konfiguration weiterer Geräte dienen. Mit diesem Befehl können zudem auch Unterschiede zwischen Konfigurationen (zum Bsp. zu bereits gespeicherten oder Standard Konfigurationen angezeigt werden.	Seit Version: 10.2.1, 08.02.2013
Show All Status	Mit dem Befehl „ShowAllStatus" wird der gesamte Status aller Parameter des Gerätes angezeigt und simultan eine Script Datei erstellt. Das Script kann für spätere Vergleiche aufbewahrt werden oder als Grundlage für ein automatisiertes Testsystem genutzt werden.	Seit Version: 10.4.1, 21.02.2014
Create Snapshot	Erzeugt eine einzige gepackte Datei, welche die gesamte Konfiguration, allen Status sowie diverse systeminterne relevante Parameter auflistet.	Seit Version: 10.4.1, 21.02.2014
Live Syslog	Syslog-Events können unmittelbar auf allen aktiven Consolen angezeigt werden. Normen: RFC3164	Seit Version: 10.2.0, 14.12.2012
Telnet	Das Gerät kann per Telnet erreicht werden. Telnet kann vollständig oder per Anwender deaktiviert werden. Normen: RFC 854 (Telnet) via TCP/IP port 23.	Seit Version: 10.1.7, 19.11.2012
Secure Shell (SSH)	Eine SSH-Session wird automatisch mit dem CLI Verbunden. SSH kann global oder per Anwender deaktiviert werden. Normen: SSH via TCP/IP port 22. Authentication methods: RSA, Diffie-Hellman Key Exchange. Encryption protocols: 3DES-CBC, HMAC-SHA1.	Seit Version: 10.1.6, 13.11.2012

SSH CLI-Commands	Es ist möglich direkt in einem SSH-Verbindungsaufbau ein CLI Kommando zu übergeben. Dieses wird dann ausgeführt und die Verbindung danach sofort getrennt.	Seit Version: 10.7.9a, 03.06.2022
Welcome Message	Eine frei definierbare Nachricht wird bei jedem einloggen angezeigt. Diese kann auch mehrzeilig sein.	Seit Version: 10.3.2a, 04.11.2013
Umlaut Support	Umlaute und andere Europäische Sonderzeichen können in beschreibenden Parametern verwendet werden. Es wird die ISO 8859-1 Zeichenkodierung verwendet.	Seit Version: 10.4.1, 21.02.2014
Favorites	Häufig benötigte CLI Kommandos können als Favoriten abgespeichert werden und mit einer Taste aufgerufen werden. Normen: RFC 854 (Telnet) via TCP/IP port 23.	Seit Version: 10.6.0, 22.12.2015

Login Access Protection

Unlimited number of Users	Mit Auslieferung sind 3 Standardnutzer definiert. Es können unbegrenzt weitere Nutzer definiert werden.	Seit Version: 10.1.6, 13.11.2012
View Based Access Model	Zugriffsrechte können dediziert pro Nutzer definiert werden. Das Rechtemodell deckt sich dabei mit dem Modell für SNMPv3. Im CLI stehen dann die gleichen Nutzer (mit deren Rechten) zur Verfügung.	Seit Version: 10.1.6, 13.11.2012
General access rights	Für ein einfaches und schnelles Nutzermanagement können generelle Lese- und Schreibrechte definiert werden	Seit Version: 10.1.6, 13.11.2012
Disable Insecure Interfaces	Es ist möglich den Managementzugriff ausschließlich für sichere Interfaces wie HTPPS, SSH bzw. SNMPv3 zu erlauben. Diese Auswahl kann pro Nutzer definiert werden.	Seit Version: 10.1.6, 13.11.2012
Interface Restrictions	Für jeden Anwender können die freigegeben Managementschnittstellen individuell definiert werden.	Seit Version: 10.1.6, 13.11.2012
Public key encrypted passwords	Jeder Nutzer erhält dediziert ein Passwort. Für SNMPv3 wird ein eigenes Passwort vergeben. Die Speicherung erfolgt nach AES256 verschlüsselt.	Seit Version: 10.1.6, 13.11.2012
View Model for SNMP V1,V2c	Das Zugriffsrechtemodell kann auch für den SNMPv1 oder v2c Zugriff angewendet werden. Somit unterliegt SNMPv1/v2c-Zugriff praktisch den gleichen Sicherheitsbeschränkungen wie SNMPv3, ohne dessen Komplexität zu benötigen.	Seit Version: 10.1.7, 19.11.2012
Firewall with Black and White List	Um den Managementzugriff zu beschränken kann eine IP-Adressliste erstellt werden. Diese Black/White Liste ist mit Firewall-Funktionen kombiniert.	Seit Version: 10.3.1, 30.08.2013
TACACS+ Authentication	Anwender können zentral per TACACS+ authentifiziert werden. Der jeweils gelieferte Zugangslevel wird dabei auf die Rechte eines frei definierbaren lokalen Nutzers übersetzt	Seit Version: 10.4.0, 20.12.2013
RADIUS access verification	Anwender können zentral per RADIUS authentifiziert werden. Es können zwei Server angegeben werden sowie ggf. ein Rückfall auf die lokalen Nutzerdefinitionen.	Seit Version: 10.3.1, 30.08.2013

Web Interface (WEB)

Base Features	Das Gerät verfügt über einen modernen integrierten Web-Manager. Der Zugriff erfolgt mit einem Standardbrowser. Hier stehen die gleichen, definierten Nutzer des CLIs zur Verfügung, es können sämtliche Aspekte des Gerätes konfiguriert werden. Normen: HTML v4.01,HTTP, HTTPS, Java Script	Seit Version: 10.1.7, 19.11.2012
Web Authentication	Der Web-Zugriff erfolgt über eine Login/Passwort-Sequenz. Das Nutzermodell wird durchgängig entsprechend dem CLI auch beim Web angewendet.	Seit Version: 10.2.0, 14.12.2012
RADIUS access verification	Web Zugriff kann per zentralen RADIUS Server zur Authentifizierung geschützt werden.	Seit Version: 10.3.1, 30.08.2013
HTTPS	Mit HTTPS wird für das Web ein sicherer Zugriff mit verschlüsseltem Datentransport unterstützt. Als Alternative wird auch der Standard HTTP-Zugriff unterstützt. Wird HTTPS konfiguriert (Standard), wird nur noch TLS1.2 Verschlüsselung akzeptiert. Normen: TLS1.2	Seit Version: 10.1.7, 19.11.2012
Less Secure HTTPS	Ermöglicht HTTPS Zugriff auch von Geräten die nicht TLS1.2 unterstützen. Wir diese Funktion ausgeschaltet (standard) werden automatisch die weniger sicheren Zugriffsmethoden ausgeschaltet und somit die Sicherheit erhöht Normen: TSL1.0, TSL1.1, SSLv2, SSLv3	Seit Version: 10.7.7, 28.05.2020
Custom SSL Certificates	Es können eigene SSL Zertifikate geladen und gespeichert werden. Dadurch können firmenspezifische Zertifikate einfach und sicher genutzt werden.	Seit Version: 10.5.1, 11.12.2014
Full Functional Support	Sämtliche Funktionen des Gerätes stehen im Web-Interface zur Verfügung, inkl. aller "Action" Kommandos.	Seit Version: 10.2.3, 28.04.2013
Animated Device Graphics	Die Gerätegrafik zeigt die genaue Anordnung aller Buchsen und LED. Farbige Markierungen zeigen den Zustand der Ports und die LED leuchten entsprechend dem realen Gerät.	Seit Version: 10.1.7, 19.11.2012
Firmware Update	Alle Gerätefunktionen sind verfügbar, auch ein Firmware-Update ist unkompliziert durchführbar.	Seit Version: 10.2.0, 14.12.2012
Online Documentation	Das automatisch erstellte, und dadurch immer zum Softwarestand kompatible Handbuch, ist über das Web-Interface abzurufen.	Seit Version: 10.2.0, 14.12.2012
SNMP MIB download	Sämtliche MICROSENS spezifische SNMP MIB-Dateien können vom Web-Interface geladen werden. Die MIBs sind auch per FTP zugänglich.	Seit Version: 10.2.1, 08.02.2013
Event Display	Die letzen 20 Alarmmeldungen können angezeigt werden. Ein Filter kann gesetzt werden, welche Alarme (Events) dort angezeigt werden.	Seit Version: 10.7.2, 02.10.2018
REST API interface	Alle Konfigurations-, Status oder SmartOffice-Daten können gelesen oder geschrieben werden. Optional kann JSON verwendet werden. Sämtliche Zugangsbeschränkungen gelten und die Daten werden gesichert über SSH versendet.	Seit Version: 10.7.4, 31.01.2019
Configurable Web GUI	Zusätzlich zum normal Web Interface gibt es eine vollständig durch Configuration erstellte Web Oberfläche welche z.B. zur Steuerung von SmartOffice Lösungen genutzt werden kann.	Seit Version: 10.7.0, 07.04.2017
Responsive Web GUI	Die konfigurierbare Web Oberfläche passt sich der Bildschirmgröße an und kann auf Handy wie PC gleichermaßen gut genutzt werden.	Seit Version: 10.7.9a, 03.06.2022
Web GUI Styles	Die konfigurierbare Web Oberfläche unterstützt Styling Vorlagen welche auf einfache Weise den Look der Anwendung verändern.	Seit Version: 10.7.9a, 03.06.2022

Simple Network Management Protocol (SNMP)

SNMP V1/V2c	Vollständige Unterstützung von SNMPv1/v2c für den Zugriff auf Geräteinformationen. Grundlegender SNMP Schutz durch "Community Strings". Normen: RFC 1155 (SMIv1), RFC 1156/1157 (SNMPv1), RFC 1901/1905/1906 (SNMPv2)	Seit Version: 10.1.6, 13.11.2012
SNMP V1/2c Security	SNMP v1/v2c unterstützt vom Standard her keinen sicheren Zugriffschutz. Um einen zusätzlichen Schutz bei SNMPv1/v2c zu realisieren, ist es möglich das CLI/WEB Zugriffsmodell auch für SNMPv1/v2 anzuwenden. Dazu werden die Rechte eines beliebigen Nutzers zugeordnet. Grundsätzlich kann zudem das SET Kommando ganz gesperrt werden.	Seit Version: 10.1.7, 19.11.2012
SNMP V3	SNMPv3 für sicheren Zugriff auf Geräteinformationen. SNMPv3 beinhaltet die Verschlüsselung von übertragenen Informationen. Dem zu Grunde liegt ein User-based Security Model (USM) sowie View-based Access Control Model (VACM). Normen: RFC 3411/3412/3584 (SNMPv3), RFC 2574/3414 (USM), RFC 2575/3415 (VACM)	Seit Version: 10.2.0, 14.12.2012
SNMP TSM	Bei SNMPv3 mit TSM werden die SNMP v3 Daten über einen mit Zertifikaten abgesicherten SSH Tunnel geschickt. Normen: RFC 5591/5592	Seit Version: 10.7.4, 31.01.2019
Traps (SNMP V1/V2c/ V3)	Traps, Benachrichtigungen und Informationen können an eine beliebige Anzahl, frei zu konfigurierende Empfängerstationen versendet werden. Dabei können jedem Ziel verschiedene Formate zugewiesen werden. (Syslog, TRAP, INFORM,..)	Seit Version: 10.1.6, 13.11.2012
Private Traps	Jedem wichtigen Vorgang im Gerät ist ein "Event" zugeordnet. Diese können als private Traps (MICROSENS G6-TRAP-MIB) versandt werden. Events, welche in der MIB-II definiert sind, können zusätzlich oder alternativ im Standardformat versandt werden. Private Traps sind beispielsweise für Konfigurationsänderungen oder Nutzer-Logins definiert. (Ca. 80 Alarm Typen)	Seit Version: 10.1.6, 13.11.2012
Private and Public MIBs	Das Gerät unterstützt Private MIBs mit denen sämtliche Funktionen bedient werden können. Zudem wird eine Reihe von Standard-MIBs unterstützt (z. B. Bridge-MIB oder QBridge-MIB). Die Private MIBs können per Web oder FTP geladen werden. Normen: MIB-2, BRIDGE_MIB, Q-BRIDGE-MIB, RMON-MIB, EtherLike-MIB, POWER-ETHERNET-MIB, IGMP-STD-MIB, RADIUS-AUTH-MIB, LLDP-MIB (SMIv2), LLDP-EXT-MED-MIB, IEEE8023-DOT3-LLDP-EXT-V2-MIB	Seit Version: 10.1.7, 19.11.2012
ARP-Guard Compliance	Kompatibel und geprüft mit der Netzsicherheitssofttware ARP-Guard der Firma ISL GmbH.	Seit Version: 10.5.4c, 22.07.2015
MACMON Compliance	Kompatibel und geprüft mit der Netzsicherheitssofttware MACMON der Firma MIKADO AG.	Seit Version: 10.3.0, 04.06.2013
Integrated SNMP Browser	Integrierter Text-basierender SNMP Browser unterstützt GET, GETNEXT, SET und WALK. SNMP Version v1,v2c und v3 sind dabei verfügbar. Der Browser versteht die private G6 MIB sowie einige Standard MIBs.	Seit Version: 10.4.1, 21.02.2014

RADIUS Client

Access	Integrierter RADIUS-Client (via UDP/IP Ports 1812 (Access)) erlaubt zentralisierte Authentifizierung. Normen: RFC 2865 (RADIUS), RFC 2868 (Tunnel Attributes)	Seit Version: 10.2.0, 14.12.2012
Accounting	Integrierte RADIUS-Client Funktion (via UDP/IP Port 1813 (Accounting)) für Logging der Nutzer Accounting Information Normen: RFC 2866 (Accounting)	Seit Version: 10.2.0, 14.12.2012
Redundancy	Für jede RADIUS Anwendung kann ein Primär und Sekundär Server spezifiziert werden. Insgesamt können bis zu 8 RADIUS-Server konfiguriert werden.	Seit Version: 10.2.0, 14.12.2012
Tunnel Attributes	Wenn 802.1X, RADIUS und VLAN gemeinsamgenutzt werden, besitzt das RADIUS ACCESS-REQUEST Paket zusätzliche Attribute. Normen: RFC 3580, RFC2868	Seit Version: 10.7.0a, 10.07.2017

File Management

File Transfer Protocols	Der Dateitransfer kann verwendet werden um die Firmware zu aktualisieren oder um Konfigurations-Scripte auszutauschen. Das Gerät unterstützt TFTP, FTP, SFTP, HTTP, HTTPS Transferprotokolle. Weiterhin können per DHCP-Optionen Dateien zugewiesen werden. Das Gerät kann für die Dienste FTP, SFTP und TFTP sowohl als Client als auch als Server dienen Normen: TFTP, FTP, SFTP, HTTP, HTTPS	Seit Version: 10.1.6, 13.11.2012
Firmware Download	Der Download von Software kann vollständig oder auch inkrementell erfolgen. Auf der SD-Speicherkarte können beliebig viele Firmware-Stände gespeichert werden. Das Speichern der Firmware ist unabhängig von deren Aktivierung.	Seit Version: 10.1.6, 13.11.2012
Secure Firmware Update	Es können individuelle Softwaremodule geändert werden, in der Regel ohne Neustart des Gerätes. Ein flexibler Vorgang ermöglicht nach Bedarf angepasste Upgrades	Seit Version: 10.3.1, 30.08.2013
Firmware and Configuration Export and Import *(Nur Industrie Switch)*	Firmware updates und Konfigurationsdaten können per USB Stick zwischen Geräten ausgetauscht werden.	Seit Version: 10.4.0, 20.12.2013
Script Files	Es können CLI-Scripte sowie andere Dateien geladen und gespeichert werden. Auf diesem Weg kann eine netzwerkweite Konfiguration verteilt werden.	Seit Version: 10.1.6, 13.11.2012
Configuration Files	Sämtliche Gerätekonfigurationen werden in XML-Dateien gespeichert. Die Dateien können auch über andere Geräte verteilt sowie als Backup bzw. Sicherheitskopie verwendet werden. Diese können auch Offline bearbeitet werden. Dafür bietet das CLI einen so genannten Offlinemodus an.	Seit Version: 10.1.6, 13.11.2012
Compare Config and create Transformation Scripts	Gerätekonfigurationen können verglichen und Unterschiede angezeigt werden. Dabei werden automatisch CLI-Scripte erzeugt, mit dem die jeweils andere Konfiguration erreicht werden kann (für beide Richtungen).	Seit Version: 10.2.2, 21.03.2013
Temporary Configuration	Normalerweise soll die Gerätekonfiguration permanent gespeichert sein. Für bestimmte Anwendungen im öffentlichen Raum kann es sicherer sein das das niemand, auch illegal, die Einstellungen verändern kann. Nach einen Neustart steht auf jeden Fall die urprüngliche Konfiguration wieder zur Verfügung.	Seit Version: 10.7.0a, 10.07.2017

Event Logging

Function	Über das Syslog-Protokoll für UDP/IPv4 und UDP/IPv6 können Meldungen, die vom System generiert werden an eine beliebige Anzahl von Syslog-Servern gesendet werden. Normen: RFC 5424, RFC 3164	Seit Version: 10.1.6, 13.11.2012
Syslog to CLI	Der Standardempfänger von Syslog-Meldungen ist das CLI-Interface. Ein angemeldeter Nutzer empfängt die Meldungen in Abhängigkeit der selbst definierbaren Wichtigkeit.	Seit Version: 10.2.0, 14.12.2012
Local Logfile	Sämtliche Meldungen, unabhängig davon ob sie weitergeleitet wurden, werden auch in einem lokalen Logfile gesichert. Dabei werden zwei Dateien wechselweise rotiert, so dass der benötige Speicherplatz festgelegt ist.	Seit Version: 10.2.0, 14.12.2012
Log Filters	Die Meldungen können je nach Benachrichtigungsziel unterschiedlich gefiltert und formatiert werden.	Seit Version: 10.1.6, 13.11.2012
Recent Logs	Die letzen 15 Meldungen werden in einer tabelle gehalten und zwar mit dem neuses evetn immer an erster Stelle. So können dile letzten Meldungen noch einmal nachgelesen werden, ohne das ein Logfile bemüht werden muss.	Seit Version: 10.7.0, 07.04.2017
Log to MQTT topic	Meldungen können als MQTT topic gesendet werden.Es steht ein festes topic oder ein dynamisches topic format zur Verfügung.	Seit Version: 10.7.5, 31.08.2019
Long Term History	Bit zu 15 beliebige system status variablen können automatisch im Sekundenintervall eingelesen und aufgezeichnet werden.Direkt im Status verfügbar sind die Werte der letzten Minute, Stunde und Tage. Zusätzlich werden die Daten auch in Excel kompatiblen csv Dateien abgespeichert.	Seit Version: 10.7.0, 07.04.2017

Event Defintions

Event Scheme	Die modulare Softwarestruktur nutzt Meldungen zwischen den internen Prozessen. Eine Vielzahl dieser Meldungen kann direkt für die Generierung von SNMP Traps und Syslogs verwendet werden.	Seit Version: 10.1.6, 13.11.2012
Customizable events	Die Wichtigkeit des bzw. das Alarmlevel sind für jedes einzelne Event frei konfigurierbar. Zudem sind sogar die Eventinhalte über das User Interface frei definierbar. So können Beispielsweise andere Sprachen definiert werden.	Seit Version: 10.1.6, 13.11.2012
Configuration Changes	Jede einzelne Änderung eines Parameters (egal durch welches User Interface) wird registriert mit Zeitstempel, Operatornamen, User Interface, alter und neuer Wert. So kann jede Veränderung rückverfolgt werden. Jede solche Konfigurationsänderung kann Syslogs und/oder Traps erzeugen.	Seit Version: 10.1.6, 13.11.2012
Debug Information	Es ist möglich interne Debug-Informationen in Events für Syslog und/oder Traps zu wandeln. Dadurch kann ein Remote-Debugging ermöglicht werden. Diese Funktionen sind durch das definierte Zugriffsschema geschützt und stellen somit kein Risiko dar.	Seit Version: 10.1.6, 13.11.2012
Run Scripts on Event	Jeder Meldung können microScripts zugeordnet werden. Diese vielseitge Funktion ermöglicht eine Vielzahl von anwendungsspezifischen Sonderfunktionen.	Seit Version: 10.3.1, 30.08.2013

Test Functions

Ping, Trace Route	Klassische IP Testfunktionen wie PING, DNS lookup und Traceroute sind verfügbar. Dabei sind umfangreiche Optionen vorhanden.	Seit Version: 10.1.6, 13.11.2012
Port Mirroring	Die übertragenen Daten eines Anschlusses können auf einen weiteren, nicht verwendeten Anschluss gespiegelt/kopiert werden.	Seit Version: 10.3.0, 04.06.2013
Test Trap	Mittels Testfunktion kann eine Testmeldung ausgelöst werden um das korrekte Versenden an die gewünschten Trap- und Syslog Empfänger zu prüfen.	Seit Version: 10.1.6, 13.11.2012
Led Test	Schaltet alle LEDs der Reihe nach in allen verfügbaren Farben ein. Neben dem LED Test ist diese Option auch hilfreich um einen bestimmten Switch zu identifizieren.	Seit Version: 10.1.6, 13.11.2012
ARP Cache	Das ARP Cache listet MAC/IP Beziehungen von Verbindungen, welche auf das Management zugreifen oder über die CPU kontrolliert werden.	Seit Version: 10.4.3, 07.04.2014

Script Data

Custom Parameter	Selbst geschriebene microScripts können private Parameter registrieren. Diese sind dann über alle Managmentschnittstellen konfigurierbar. Somit kann ein parametrisiertes Script erstellt werden.	Seit Version: 10.3.2a, 04.11.2013
Custom Variables	Selbst geschriebene microScripts können private Variablen registrieren. Diese sind dann über alle Managmentschnittstellen lesbar. Somit kann ein Script einen eigenen Status erstellen.	Seit Version: 10.3.2a, 04.11.2013

Misc

Terminal Server	Der serielle Port kann verwendet werden um ein anderes Produkt, welches nicht über Ethernet verfügt, anzusteuern. Der serielle Port ist über Telnet oder SSH erreichbar. Ebenfalls ist the serielle zu serielle Verbindung über Ethernet möglich. Auch eine PC COM Port emulation ist möglich.	Seit Version: 10.6.0, 22.12.2015
Loudspeaker support	Besondere Situationen können per Lautsprecher angesagt werden. Bei SmartOffice Anwendungen kann Musik über das Netzwerk gespielt werden.	Seit Version: 10.6.0, 22.12.2015