



Access Manager

Access Manager

Abgesicherte und normengerechte Remote-Verbindungen

Konzernübergreifend stehen Anlagenbetreiber durch alle Branchen hindurch zunehmend vor der Herausforderung, ihre technische IT und Automatisierungsumgebungen nachhaltig gegen interne und externe Bedrohungen abzusichern.

Industrial Defender, als führender Hersteller von IT-Security für kritische Infrastrukturen, bietet auf Basis einer konsequenten Defense-in-Depth™ Security-Strategie ein skalierbares Lösungskonzept an.

Als Teil davon ist der Access Manager die Komponente für sichere Zugangslösungen und Authentifizierungsverfahren zu Anlagen bzw. Anlagenteilen. Konzipiert nach den Anforderungen nationaler und internationaler Empfehlungen und Standards zum Schutz kritischer Infrastrukturen, ist er die Grundlage zur Erfüllung betreiberseitiger Compliance-Verpflichtungen:

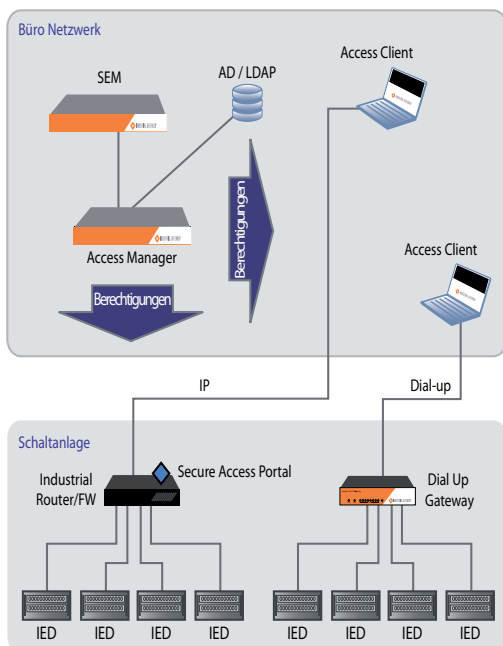
- Authentifikation, Autorisierung und Rechteverwaltung, zugeschnitten auf nationale und internationale Normen, wie IEC62443, ISA99, NERC CIP usw.
- Sichere IP-, Serial-over-IP und Dial-up-Kommunikation
- Zentrale Verwaltung der Benutzerautorisierung und der zu kontaktierenden Komponenten
- Individuelle Zugangsberechtigungen (digitale Zertifikate, Handshake-Authentifizierung)
- Erstellung elektronischer Sicherheitsperimeter
- Active Directory Integration für einfache Administration und Gruppenverwaltung
- Umfassende Ereignismeldungen inklusive, One-Click AutoAudit™ Meldung
- Schnittstellen- und hardwareunabhängige Zugangslösung

Entstanden aus dem Teltone Gauntlet System für sicheren Zugang in Schaltanlagen, ist der Access Manager jetzt als flexible und normengerechte Zugangslösung in das Industrial Defender Security-Konzept integriert.

Systemarchitektur

Durch das Zusammenspiel der Software- und Hardwarekomponenten des Access Managers wird der Zugang zu kritischen Geräten überwacht und verwaltet. Die Access Manager Webanwendung/Datenbank bietet eine Vielzahl von Tools zur Verwaltung von Benutzerberechtigungen, Konfiguration von Gateways und Secure Access Portalen, Kennzeichnung kritischer Anlagen und schnellen Änderungen der Sicherheitsfreigaben für Benutzer. Die Access Client Software bietet Benutzerauthentifizierung und stellt einen sicheren Zugang zu autorisierten Geräten und Ports her. Das Dial-up Gateway (nur für Nordamerika verfügbar) ist ein speziell für Schaltanlagen entwickelter Switch für die gemeinsame Nutzung von Telefonleitungen. Die Secure Access Portal Software läuft auf sicheren industriellen Netzwerkkomponenten und kontrolliert den Zugang zu geschützten IP-Geräten während sie die Zugriffsaktivität protokolliert.

Der Access Manager unterstützt eine „dezentralisierte“ Topologie, das heißt, Benutzer mit aktueller Berechtigung werden direkt mit der Anlage bzw. dem Anlagenteil verbunden. Dabei besteht keine aktive Serververbindung, es werden lediglich in festgelegten Zeitintervallen neue Berechtigungen heruntergeladen. Selbst wenn das WAN durch einen Ausfall oder andere Gründe nicht verfügbar ist, können autorisierte Benutzer, die für sie freigeschalteten Geräte sicher über den Remote-Zugriff erreichen, solange das Berechtigungsticket aktiv ist.



Dezentraler IP- / Dial-up-Zugang am Beispiel einer elektr. Schaltanlage

IP: Der Access Manager bietet individualisierte Sicherheitsberechtigungen zum Secure Access Portal der Access Client Schaltanlage, wobei der Client die Verbindung zum Portal über einen sicheren SSL-VPN-Tunnel herstellt. Dabei laden die Benutzer des Clients in regelmäßigen Abständen aktuelle, individualisierte Berechtigungen vom Access Manager herunter, die vom Portal verifiziert werden. Gleichzeitig überwacht das Portal den IP-basierten Remote-Zugriff auf geschützte Geräte.

Dial-up: Der Access Manager bietet zu jedem Dial-up Gateway eindeutige Berechtigungen für jeden geschützten Port. Die Benutzer des Access Clients laden in regelmäßigen Abständen aktuelle, individualisierte Berechtigungen vom Access Manager herunter. Der Access Client wählt sich über das Dial-up Gateway ein, das autorisierten Benutzern portspezifischen Zugang gewährt.

Access Manager Leistungspakete

Um unterschiedliche Anlagengrößen und -anforderungen zu bedienen, wird der Access Manager in den Ausführungen „Standard“ und „Plus“ angeboten. „Standard“ adressiert Konzerne, die geringere Verwaltungs- und Zugangsanforderungen haben. Für Situationen mit vielen (Teil-)Anlagen und zahlreichen fernzugreifenden Benutzern, empfiehlt sich die Version „Plus“. Sie bietet u.a. Server- Redundanz, Active Directory Integration, sowie maßgeschneiderte Gerätehierarchie und -typen:

Merkmale	Standard	Plus
Zentralisierte Administration	x	x
Individuelle Accounts und Berechtigungen für Benutzer	x	x
Active Directory Integration für Benutzer und Gruppen		x
Starke Passwörter und Handshake-Authentifizierung	x	x
Auflistung kritischer Cyber Assets	x	x
Maßgeschneiderte Geräteklassifizierung		x
Hierarchische Gruppierung/ Organisation der Geräte		x
Detaillierte Protokolle und Meldungen der Zugriffe	x	x
AutoAudit Berichterstattung	x	x
Entspricht Normenanforderungen für Remotezugriffe	x	x
Redundante Hardware (RAID, doppelte Netzteile, etc.)		x
redundante Datenbanken / Hot-Stand-by-Komponente	x	x

Integration mit minimalem Aufwand

Der Access Manager ist mit minimalem Aufwand in Netzwerke installier- und konfigurierbar und beherrscht gängige Kommunikationsprotokolle (wie DNP3, UCA, Modbus, Probus, IEC870-5, IEC 16850, IEC 60870-5-104, ODVA Ethernet/IP usw.). Die nahtlose Integration in bestehende Infrastrukturen erlaubt die Nutzung bestehender Hardwarekomponenten und Softwareapplikationen, ohne diese separat anpassen zu müssen.

KORAMIS GmbH

Kompetenzzentrum

Automatisierungstechnik & IT-Sicherheit

Neumühler Weg 32.1

D - 66130 Saarbrücken-Güdingen

Tel. +49 (0)681 - 968 191 - 30

Fax +49 (0)681 - 968 191 - 930

KORAMIS – Ihr Partner für IT-Security

Als innovatives Unternehmen adressiert KORAMIS seit 1985 die Prozess- und Versorgungsindustrie und bietet Lösungen und Tools im technischen Umfeld von kritischen Infrastrukturen an. Im Bereich IT-Security ist KORAMIS Partner von Industrial Defender und bietet von der Risiko-Analyse über Lösungsimplementierung bis zum Support komplette Sicherheitslösungen aus einer Hand.