



Security Tech Germany

TECTIQ IT- ADMINISTRATION

Information & Checkliste

PROJEKT

Objekt/Projekt: _____

Ansprechpartner IT: _____

Datum Inbetriebnahme: _____

Fachhandelspartner: _____

Ansprechpartner Fachpartner: _____

Vorabinformationen für IT-Ansprechpartner

TECTIQ ist ein digitales Schließsystem. Es nutzt die Technologie Data on Card, dabei werden die Zutrittsberechtigungen auf die Transponder der Mitarbeiter geschrieben. Für eine höhere Sicherheit haben die Transponder eine einstellbare Gültigkeit (z. B. 24 Stunden). Das Update der Berechtigungen und die Verlängerung der Gültigkeit des Transponders erfolgt durch die Mitarbeiter an sogenannten Update Terminals.

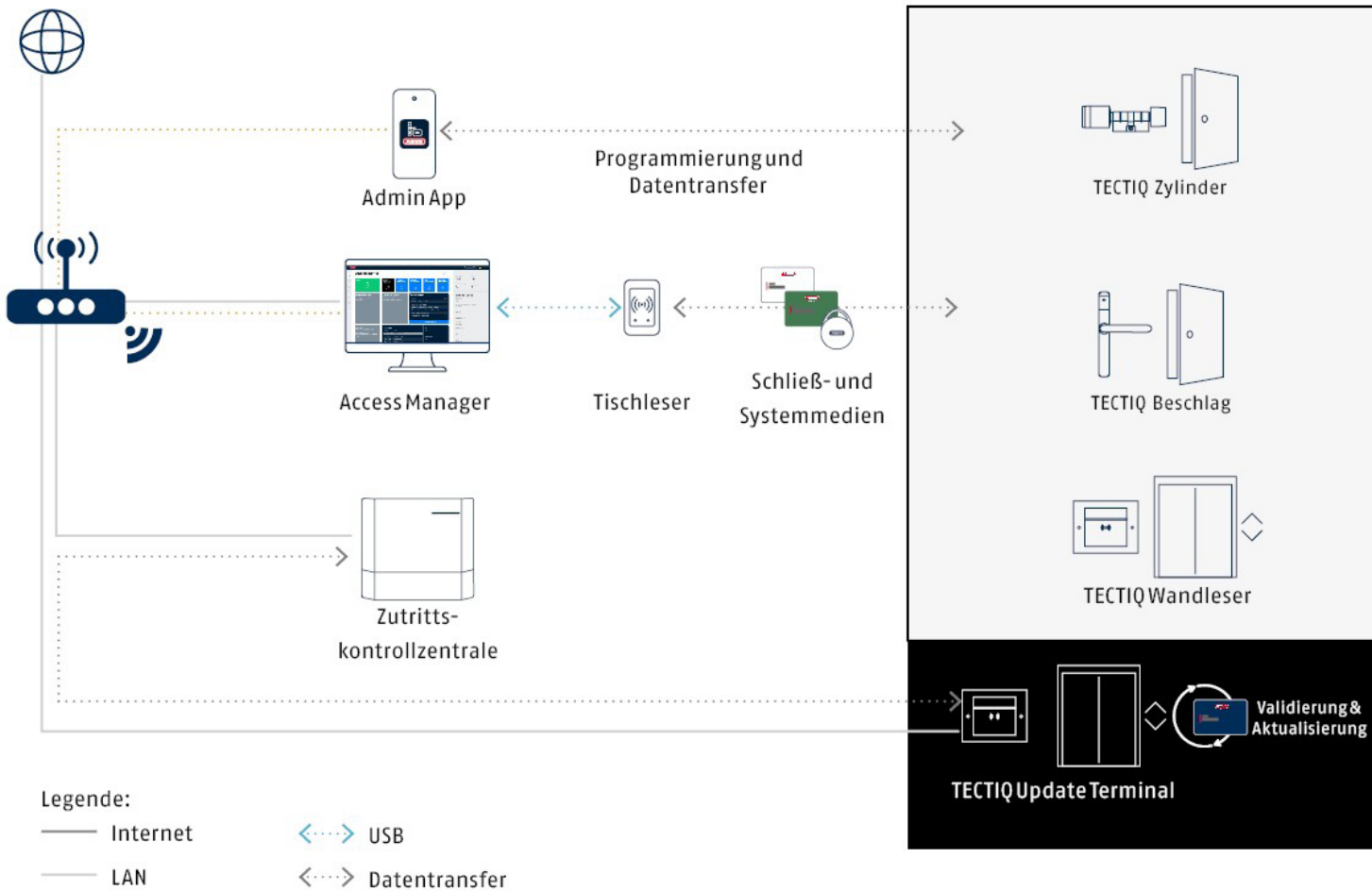
Als Steuerungseinheit und Datenbank des TECTIQ Systems dient die Zutrittskontrollzentrale.
Die Administration erfolgt mithilfe der Software Access Manager.

Für den Zugriff auf die Zutrittskontrollzentrale mithilfe des Access Managers und für die Anbindung der Update Terminals ist eine Netzwerkverbindung erforderlich. Das System kann sowohl offline, d. h. nur im lokalen Netzwerk als auch Online (Zugriff über das Internet) betrieben werden*.

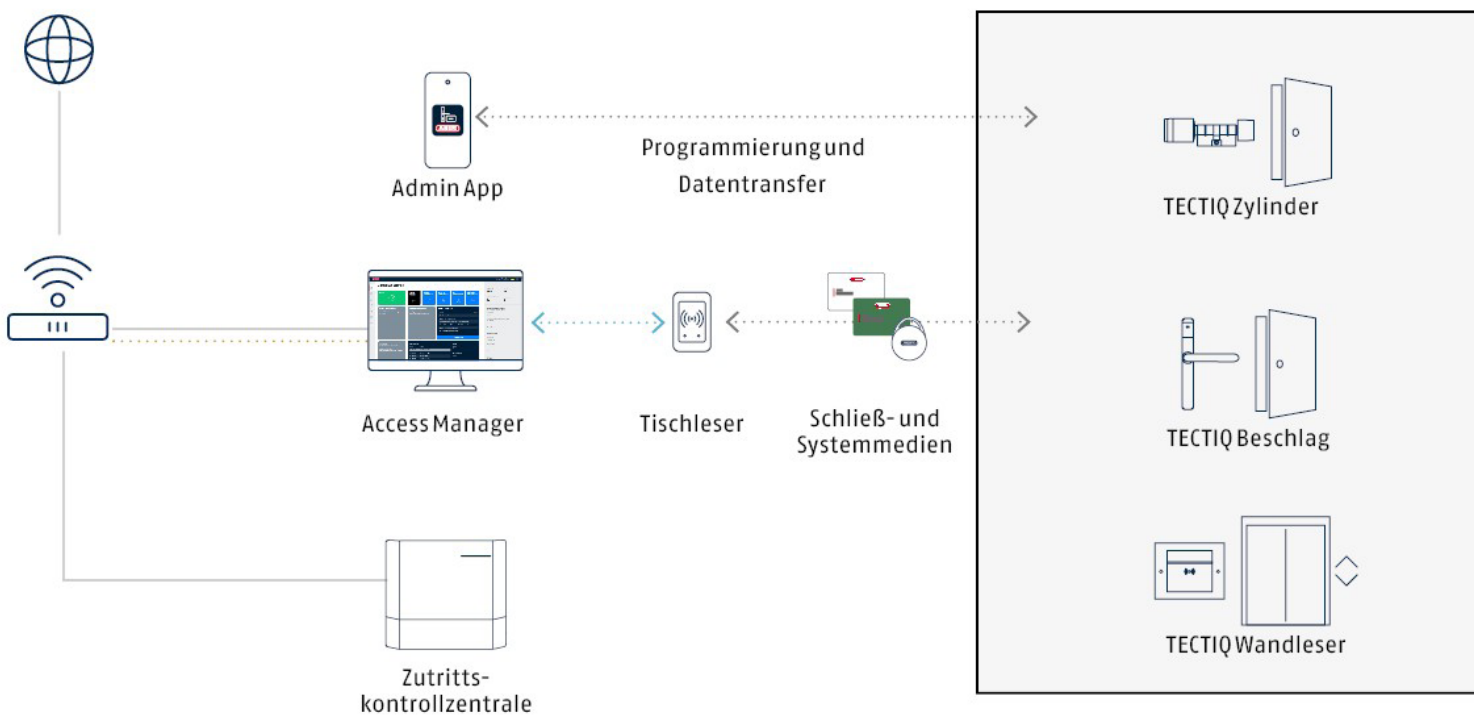
Alle Informationen sowie die Systemanleitung und die Installationsdatei des „Access Managers“ (Desktop-Software) finden Sie online unter: abus.com/product/TTC010000

*Der volle Leistungsumfang von TECTIQ steht nur mit einer Online-Netzwerkverbindung zur Verfügung.

SYSTEMAUFBAU MIT UPDATE TERMINAL (lokal)



SYSTEMAUFBAU OHNE UPDATE TERMINAL



NETZWERKINTEGRATION TECTIQ SYSTEM

Zur Ersteinrichtung und zur späteren Wartung wird empfohlen die Konfiguration der IP-Adressen sowie der entsprechenden MAC-Adressen zu dokumentieren. Die folgende Übersicht sollte daher mit der für die IT zuständige/n Fachperson/en abgestimmt werden.

Empfehlung: Nach der Ersteinrichtung wird empfohlen, wenn möglich fixe IP-Adressen zu verwenden. Sollte DHCP zum Einsatz kommen, wird zu einer DHCP-Adressreservierung geraten.

Option 1: Betrieb mit Update Terminal

Zutrittskontrollzentrale

Installationsort: _____
MAC-Adresse: 8C:11:CB:30: _____
Fixe IP: _____ DHCP _____

Update Terminals

Installationsort: _____
MAC-Adresse: 8C:11:CB:30: _____
Fixe IP: _____ DHCP _____

Installationsort: _____
MAC-Adresse: 8C:11:CB:30: _____
Fixe IP: _____ DHCP _____

Installationsort: _____
MAC-Adresse: 8C:11:CB:30: _____
Fixe IP: _____ DHCP _____

Installationsort: _____
MAC-Adresse: 8C:11:CB:30: _____
Fixe IP: _____ DHCP _____

Installationsort: _____
MAC-Adresse: 8C:11:CB:30: _____
Fixe IP: _____ DHCP _____

Option 2: Betrieb ohne Update Terminal

Zutrittskontrollzentrale

Installationsort: _____
MAC-Adresse: _____
Fixe IP: _____ DHCP _____

TECTIQ ERSTEINRICHTUNG

Um bei der Ersteinrichtung im Netzwerk Ihre Zutrittskontrollzentrale und vorhandene neue Update Terminals über den Access Manager einfach finden zu können, wurde ein sog. Discovery-Service integriert.

Empfehlung für Ersteinrichtung

1. Für eine einfache und schnelle Ersteinrichtung und Betrieb empfehlen wir die Zutrittskontrollzentrale, Update Terminals und den PC mit dem Access Manager im gleichen Subnetz zu betreiben. Nur im gleichen Subnetz funktioniert der Discovery Service ohne weitere Konfigurationen an der Netzwerkinfrastruktur. Dies gilt auch für das Hinzufügen der Update Terminals im Access Manager.
2. Alternativ können Zutrittskontrollzentrale und Update Terminals manuell über die Eingabe der IP-Adresse hinzugefügt werden.

Wichtige Hinweise:

Sollten sich die Zentrale, Update Terminals oder der PC mit Access Manager Software bei der Ersteinrichtung nicht im selben Subnetz befinden, sind folgende Hinweise zu beachten:

- Der Discovery Service des Access Managers nutzt in lokalen Netzwerken die mDNS-Technologie. Mittels mDNS-Discovery werden im Netzwerk vorhandene Geräte erkannt, sowie deren IP-Adresse ermittelt. Um mDNS-Anfragen in andere Subnetze (bzw. auch in andere VLANs) weiterzuleiten, muss darauf geachtet werden, dass "mDNS-Weiterleitung" in der Konfiguration der entsprechenden Router/Switches aktiviert ist.
- Die Konfiguration der "mDNS-Weiterleitung" ist abhängig vom Hersteller der eingesetzten Switches (Layer 3 routing-fähig). Die meisten "managed" Router/Switches (z. B. viele Modelle von Juniper, Cisco, Aruba, ...) unterstützen diese Funktion.
- Nach erfolgreicher Discovery wird grundsätzlich keine mDNS-Weiterleitung mehr benötigt. Werden Geräte entfernt oder neue hinzugefügt, muss sichergestellt werden, dass die mDNS-Weiterleitung aktiv ist.
- Bitte beachten Sie zusätzlich die Portfreigaben (s.u.) für die Konfiguration der Firewall. Alternativ ist das Hinzufügen über die Eingabe der IP-Adresse möglich.

TECTIQ SYSTEM Online FUNKTIONALITÄT

Das TECTIQ System kann im lokalen Netzwerk betrieben werden. Durch die Online Anbindung können weitere Funktionen genutzt werden. Das sind z. B.:

- Systemverwaltung aus der Ferne, durch Fernzugriff mithilfe des Access Managers auf die Zutrittskontrollzentrale.
- Standortübergreifende Einbindung von Update Terminals in die Zutrittskontrollzentrale. Dies ermöglicht die Ausstattung mehrerer Standorte mit einem TECTIQ System.
- Administration und Wartung des Systems mit der Admin App, auch wenn sich das Smartphone in einem anderen Netzwerk befindet.
- Kommunikation zur ABUS Cloud, z. B. zur Bereitstellung von Firmware- und Softwareupdates.

Wichtige Hinweise:

- **Fernzugriff Access Manager:** Wurden Zutrittskontrollzentrale und PC mit Access Manager Software bei der Ersteinrichtung bekannt gemacht (z. B. im gleichen Subnetz) und sind die entsprechenden Einstellungen in der Firewall konfiguriert (s.u. P2P Vermittlungsserver), dann können ab diesem Zeitpunkt PCs mit Access Manager die Zentrale auch unabhängig vom Subnetz/VLAN sehr einfach vom öffentlichen Netz (WAN) aus erreichen.

- **Standortübergreifendes System:** Update Terminals die sich in einem anderen Netzwerk/Standort als die Zutrittskontrollzentrale befinden, können über eine sichere Peer-to-Peer-Verbindung eingebunden werden. Dazu muss das Update Terminal zunächst im selben Netzwerk mit der Zutrittskontrollzentrale verbunden werden. Anschließend kann es im entfernten Netzwerk/Standort verbaut werden. Der Verbindungsaufbau zur Zutrittskontrollzentrale erfolgt dann automatisch. Für eine bessere Performance sollten Standortübergreifende Systeme durch eine V-Lan Verbindung virtuell in das gleiche Netzwerk gebracht werden. Diese Verbindung verhält sich dann wie eine lokale Verbindung. Bitte Ports beachten.
- **Fernzugriff Admin App:** Die Admin App kommuniziert über eine sichere Peer-to-Peer-Verbindung mit der Zentrale. Dazu muss das Smartphone einmalig im Access Manager hinzugefügt werden. Es kann anschließend im lokalen Netzwerk oder über mobile Daten auf die Zentrale zugreifen.

FIREWALL-EINSTELLUNGEN FÜR FUNKTIONEN MIT ONLINE KONNEKTIVITÄT

Je nach Netzwerk sind Firewall-Einstellungen für die Online-Funktionen notwendig.

Im Folgenden finden Sie alle Informationen:

1. NTP-SERVER

Zur Synchronisation der Systemzeit wird dringend geraten einen NTP-Server auszuwählen.

Für diese Verbindung zum Zeitserver im Internet muss der Port 123 (TCP/UDP) freigeschaltet werden.

2. ABUS Cloud

Um Verbindung zur ABUS Cloud und die Funktionen wie dem Download der neuesten Firmware, der Anzeige von Gerätedaten im Portal, den Benachrichtigungen im Eventfall u.v.m. nutzen zu können, sind folgende Ports und Adressen in der Firewall freizuschalten.

- **Port 443 (TCP):** cdn.abus-cloud.com (Download Firmware)
- **Port 443 (TCP):** azure-devices-provisioning.net (Geräteregistrierung an der Cloud)
- **Port 8883 (TCP):** azure-devices.net (Telemetriedaten und Benachrichtigungen)

3. PEER-TO-PEER VERMITTLUNGSSERVER

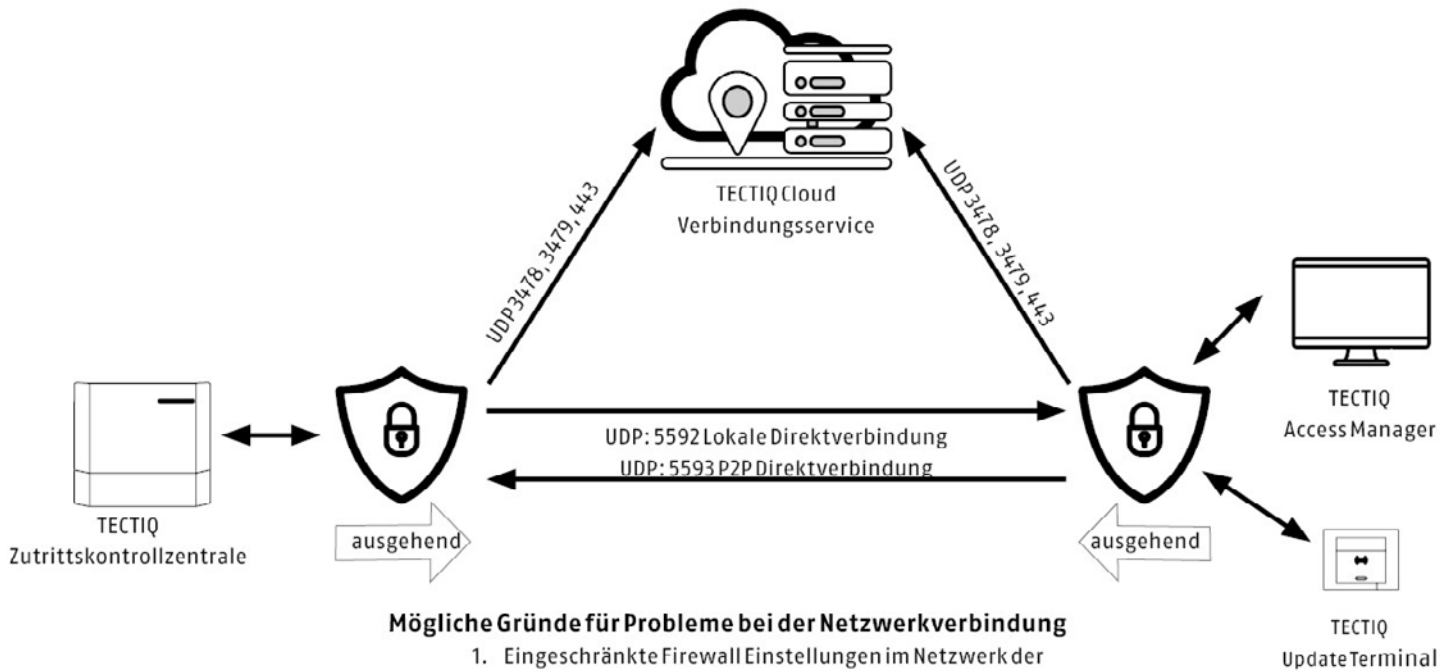
Um (auch von außerhalb des internen Netzwerks) mittels der TECTIQ Access Manager Software auf die Zutrittskontrollzentrale zugreifen zu können oder um entfernte Update Terminals einbinden zu können, wurde ein Peer-to-Peer-Dienst integriert. Dieser ermöglicht sowohl ein Höchstmaß an Komfort und Einfachheit als auch an Sicherheit bei Remote-Verbindungen zur TECTIQ Zutrittskontrollzentrale.

Folgende **ausgehende** Firewall- und Porteeinstellungen sind für die ordnungsgemäße Funktion sowohl für die Zutrittskontrollzentrale als auch für die PCs mit der Access Manager Software zu konfigurieren (eingehende Ports sind nicht notwendig):

Dringend erforderlich:

Port 53 (UDP):	DNS Service
Port 443 (UDP/TCP):	TECTIQ Cloud Verbindungsservice
Port 3478 (UDP):	Server Verbindung
Port 3479 (UDP):	Server Verbindung
Port 5592 (UDP):	Lokale Direktverbindung
Port 5593 (UDP):	P2P Direktverbindung

Direkte P2P oder Lokale Verbindung wird empfohlen da dies eine verbesserte Performance bietet.



Mögliche Gründe für Probleme bei der Netzwerkverbindung

1. Eingeschränkte Firewall Einstellungen im Netzwerk der TECTIQ Zutrittskontrollzentrale
2. Eingeschränkte Firewall Einstellungen auf Client Seite bei Fernzugriff
3. Standard DNS Lookup für den UDP Port 53 ist blockiert oder DNS Server befindet sich in einem anderen V-LAN und ist nicht erreichbar.

Relevante Produktdatenblätter

Bitte beachten Sie die PC-Voraussetzungen für die Verwendung des TECTIQ Access Managers, sowie die Anforderungen zur Installation von Zutrittskontrollzentrale und Update Terminals. Die Datenblätter sind jeweils in den Downloads der untenstehenden Produktseiten abrufbar:

Access Manager

abus.com/product/TTAM10000

TECTIQ Zutrittskontrollzentrale

abus.com/product/TTC010000

TECTIQ Update Terminal

abus.com/product/TTSG10000 (Steuereinheit Update Terminal)

abus.com/product/TTWL100675 (Leseinheiten)