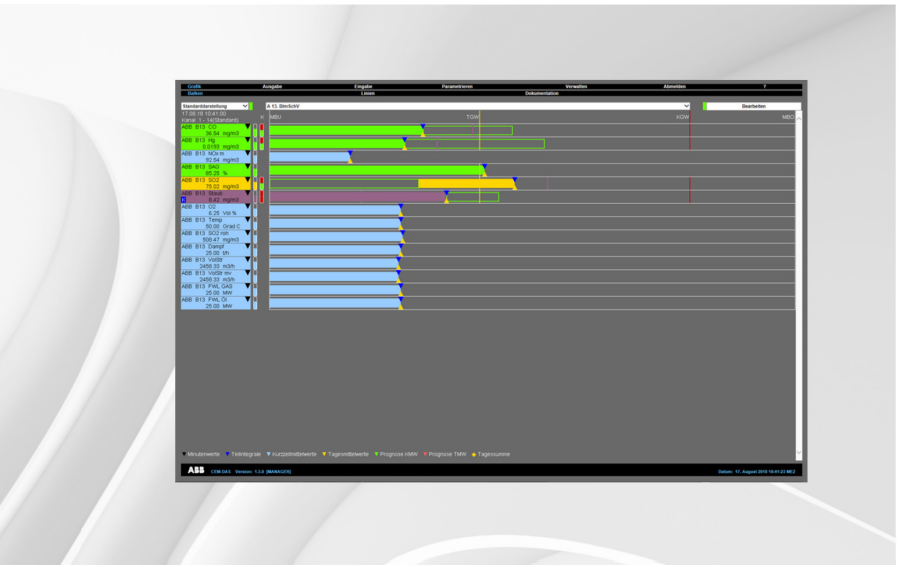
ABB MEASUREMENT & ANALYTICS | SYSTEMHANDBUCH

CEM-DAS Connect

Sicherer Zugang zu CEM-DAS Systemen über ein öffentliches Netzwerk



Measurement made easy

CEM-DAS Connect

Einführung

CEM-DAS Connect Softwareversion 1.0 stellt Anwendern den gesicherten Zugriff auf CEM-DAS Systeme über das Internet bereit.

CEM-DAS ist ein komplettes, vernetzbares IT System für die kontinuierliche Aufzeichnung und Auswertung von Emissionsdaten, geeignet für alle Industrien.

CEM-DAS Connect erlaubt beispielsweise das Abrufen von behördenrelevanten Informationen wie Wertelisten oder Protokollen.

Weitere Informationen

Zusätzliche Dokumentation zum CEM-DAS-System steht kostenlos unter www.abb.de/analysentechnik zum Download zur Verfügung.
Alternativ einfach diesen Code scannen:

Inhaltsverzeichnis

1 Einleitung 3
Beschreibung 3
Internetdresse 3

2 Systemaufbau 4
Übersicht 4
Betreiber 5
Connect Server 5
Behörde 5

3 Anmeldung 5

4 Sicherheit 6
Konzept 6
Implementierung 6

5 Weitere Dokumente 7

1 Einleitung

Beschreibung

Das Produkt CEM-DAS Connect stellt Anwendern den gesicherten Zugriff auf CEM-DAS Systeme (siehe **Weitere Dokumente** auf Seite 7) über das Internet bereit.
CEM-DAS Connect erlaubt beispielsweise das Abrufen von behördenrelevanten Informationen wie Wertelisten oder Protokolle. Typische Anwender von CEM-DAS Connect sind Behörden oder Betreiber.

Über CEM-DAS Connect kann der Anwender über einen Webbrowser indirekt auf CEM-DAS Betreibersystemdaten zugreifen, diese ansehen und abrufen.

Auch wenn mehrere Betreiber einer Behörde zugeordnet sind, erfolgt der Zugriff der Behörde immer über den zentralen CEM-DAS Connect Server. Die Behörde benötigt folglich nur die Internetadresse dieses zentralen Servers.

Auf dem zentralen Server wird hinterlegt, welche Betreibersystemdaten der Behörde zur Verfügung gestellt werden.

Das Betreibersystem muss nicht aus dem Internet erreichbar sein. Es benötigt nur den Zugriff auf den zentralen CEM-DAS Connect Server.

Internetdresse

Der zentrale CEM-DAS Connect Server ist unter der folgenden Adresse aus dem Internet erreichbar:

https://www.cemdas.eu

2 Systemaufbau

Übersicht

In der folgenden **Abbildung 1** ist der Aufbau von CEM-DAS Connect schematisch dargestellt.

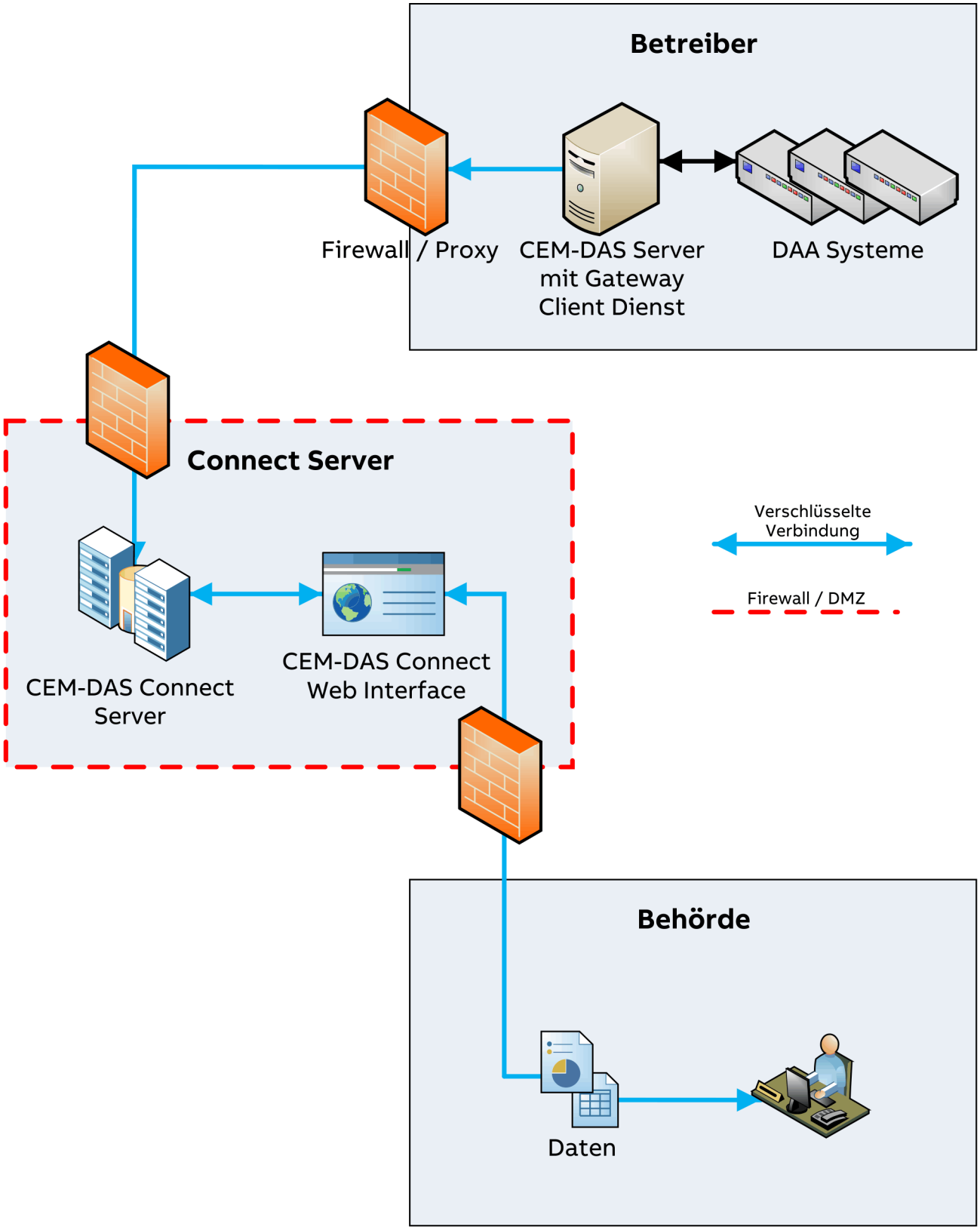


Abbildung 1: Systemübersicht

Betreiber

Auf dem CEM-DAS Server des Betreibers wird das Programm „Gateway Client“ als Windows Dienst installiert. Dieser baut eine Verbindung zum CEM-DAS Connect Server auf, ruft dort Anfragen der Behörde ab und bearbeitet und beantwortet diese.

Connect Server

Der zentrale CEM-DAS Connect Server stellt Anfragen der Behörde für den entsprechenden CEM-DAS Server des Betreibers bereit. Der Gateway Client holt die Anfragen ab und bearbeitet diese, wofür dieser wiederum entsprechende Anfragen an den CEM-DAS Server stellt. Die bearbeiteten Anfragen werden vom CEM-DAS Connect Server zurück an die Behörde weitergeleitet.

Der CEM-DAS Connect Server verfügt über eine Zugangsliste, in der festgelegt ist, welche CEM-DAS Serverdaten für die Behörde zugänglich sind.

Behörde

Über einen Webbrowser meldet sich die Behörde am CEM-DAS Connect Web-Interface an. Nach erfolgreicher Anmeldung kann die Behörde die benötigten Daten abrufen.

3 Anmeldung

Zur Anmeldung am CEM-DAS Connect Web-Interface werden vom Betreiber für die Behörde Benutzername und Passwort vergeben.

Die Anmeldung erfolgt auf der Webseite mit der Adresse https://www.cemdas.eu.



Abbildung 2: Anmeldung

Nach der erfolgreichen Anmeldung wird die Web-Oberfläche des CEM-DAS Betreibersystems dargestellt.
Zum Zugriff auf die benötigten Daten das CEM-DAS Bedienhandbuch „OI/CEM-DAS“ beachten.

4 Sicherheit

Konzept

CEM-DAS Connect wurde von Grund auf mit den aktuell empfohlenen besten Sicherheitspraxen entwickelt.

Das Produkt ist darauf ausgelegt, die beste Kombination von Sicherheit und Funktionalität zu ermöglichen. Dabei hat die Sicherheit der Integrität und Verfügbarkeit des CEM-DAS Betreibersystems den höchsten Stellenwert.

Insofern ist das zentrale CEM-DAS Connect Server Konzept so ausgelegt, dass selbst bei einem Angriff mit den ungünstigsten Randbedingungen (ein Angreifer bekommt kompletten administrativen Zugriff auf den zentralen Server) die Betreibersysteme bestmöglich geschützt sind.

Dieser Schutz wird dadurch erreicht, dass der Gateway Client Dienst außerhalb des Betreibersystems nicht sichtbar ist. Es kann keine Verbindung zu ihm aufgebaut werden. Die Kommunikation zwischen Gateway Client Dienst und CEM-DAS Connect Server wird ausschließlich vom Gateway Client Dienst initiiert und aufgebaut. Dadurch werden Angriffe auf das Betreibersystem, z.B. über den CEM-DAS Connect Server oder das Internet, unterbunden.

Da der CEM-DAS Connect Server nur als Vermittler zwischen Betreiber und Behörde dient, werden die Daten des CEM-DAS Servers nicht gespeichert, sondern nur durchgereicht.

Implementierung

Bei der Implementierung wurden folgende sicherheitsrelevante Konzepte und Aspekte verfolgt bzw. umgesetzt:

- Durchgehende TLS 1.2 Standard basierende Verschlüsselung von allen per Netzwerk ausgetauschten Daten.
- Begrenzung der Angriffsfläche durch die bewusste Minimierung der verfügbaren Funktionalitäten.
- Das Betreibersystem darf nicht dem Internet ausgesetzt sein. Der betreiberseitige Gateway Client Dienst nimmt keine Verbindungen an, weder vom Internet noch anderweitig.
- Der betreiberseitige Gateway Client Dienst enthält und speichert keine Zugangsdaten.
- Nur der CEM-DAS Connect Server akzeptiert eingehende Verbindungen. Dadurch werden Betreibersysteme von allen internetseitigen Angriffen (wie z.B. Schwachstellenausnutzung und DDoS) isoliert.
- Der CEM-DAS Connect Server läuft auf einer gehärteten Minimalinstallation von Debian Linux, das zyklisch mit Sicherheitsupdates aktualisiert wird.
- Der CEM-DAS Connect Server läuft als Gast in einem VMware ESXi Cluster innerhalb von einem mit einer Firewall gesicherten DMZ-Netz.
- Der CEM-DAS Connect Server wird zusätzlich mit einer Firewall gesichert (Ferm, Konfiguration für iptables).
- Der betreiberseitige Gateway Client Dienst benötigt keinen direkten Zugang zum Internet, er kann über einen oder mehrere Proxy Server (HTTP, SOCKS und Proprietär) auf das Internet zugreifen.
- Die Standardeinstellungen des betreiberseitigen CEM-DAS Servers müssen nicht angepasst werden (es muss keine eingehende Verbindung freigegeben sein).
- Der CEM-DAS Connect Server wurde mit .Net Core 2.2 implementiert. Dadurch werden die meisten Angriffsvektoren (z.B. Buffer Overflow) schon vor der Ausführung unterbunden.
- Zudem wurde eine umfassende Protokollierung realisiert, die eine ausführliche Nachforschung von Ereignissen erlaubt.
- Die Anmeldeinformationen und die Zugangsliste werden per individuell gesalzenem SH512 Hash irreversible verschlüsselt gespeichert.

5 Weitere Dokumente

Nr.	Doc-ID	Titel
1	TD/CEM-DAS-DE	CEM-DAS Systemhandbuch
2	OI/CEM-DAS-DE	CEM-DAS Bedienhandbuch

Hinweis
Alle Dokumentationen, Konformitätserklärungen und Zertifikate stehen im Download-Bereich von ABB zur Verfügung.
www.abb.de/analysentechnik

ABB Automation Products GmbH
Measurement & Analytics
Analytical Sales
Oberhausener Str. 33
40472 Ratingen
Deutschland
Tel: +49 2102 12-1919
Fax: +49 2102 12-1487
Email: analytical.sales@de.abb.com

abb.de/analysentechnik

ABB AG
Measurement & Analytics
Brown-Boveri-Str. 3
2351 Wr. Neudorf
Österreich
Tel: +43 1 60109 0
Email: instr.at@at.abb.com

Technische Änderungen sowie Inhaltsänderungen dieses Dokuments behalten wir uns jederzeit ohne Vorankündigung vor.
Bei Bestellungen gelten die vereinbarten detaillierten Angaben. ABB übernimmt keinerlei Verantwortung für eventuelle Fehler oder Unvollständigkeiten in diesem Dokument.

Wir behalten uns alle Rechte an diesem Dokument und den darin enthaltenen Themen und Abbildungen vor. Vervielfältigung, Bekanntgabe an Dritte oder Verwendung des Inhaltes, auch auszugsweise, ist ohne vorherige schriftliche Zustimmung durch ABB verboten.

© ABB 2019

3KXG141104R2903

TD/CEM-DAS-CONNECT-DE Rev. B 08.2019