Servicebeschreibung

Fernwartung

www.aeb.com

AEB

Rechtliche Hinweise

Bestimmte Funktionalitäten, die in diesem oder anderen Produktdokumenten beschrieben werden, sind nur verfügbar, wenn die Software entsprechend eingerichtet ist. Das Einrichten geschieht je nach Produktreihe entweder in Abstimmung mit Ihrer Ansprechperson bei AEB oder anhand eines entsprechenden Dokumentes, das Sie von Ihrer Ansprechperson bei AEB erhalten. Details regelt der Vertrag, den Sie mit AEB abgeschlossen haben.

"AEB" bezieht sich grundsätzlich auf das Unternehmen, mit dem Sie als Kunde den jeweiligen Vertrag abgeschlossen haben. In Betracht kommen die AEB SE oder die von ihr mehrheitlich kontrollierten verbundenen Unternehmen. Eine Übersicht dieser Unternehmen finden Sie auf unseren Webseiten www.aeb.com bzw. www.aeb.com/de. Ausnahmen davon werden durch spezifische Nennung des Unternehmens kenntlich gemacht.

Die Benutzung des Programms erfolgt ausschließlich gemäß den vertraglichen Lizenzbestimmungen.

Marken

In dieser Produktinformation sind Marken nicht explizit als solche gekennzeichnet – wie dies in technischen Dokumentationen üblich ist:

- Adobe, Acrobat, Reader, Experience Manager Forms und AcroForms sind Warenzeichen oder eingetragene Marken von Adobe Systems Inc.
- HTML und XML sind Warenzeichen oder eingetragene Marken des W3C, World Wide Web Consortium, Massachusetts Institute of Technology.
- TIBCO Jaspersoft Business Intelligence Suite ist eine Marke der TIBCO SOFTWARE INC.
- Java und Oracle sind eingetragene Marken der Oracle Corporation.
- Microsoft Windows, MS Word, MS Excel und MS SQL sind eingetragene Marken der Microsoft Corporation.
- NiceLabel, Designer Pro und Designer Express sind Warenzeichen oder eingetragene Marken von NiceLabel / Euro Plus d.o.o.
- Salesforce, Sales Cloud und weitere sind Marken von salesforce.com, inc.
- SAP und SAP S/4HANA sind Warenzeichen oder eingetragene Marken der SAP SE.

Alle anderen Produktnamen werden als eingetragene Marken der jeweiligen Firma angenommen. Alle Marken sind anerkannt.

Alle Angaben in diesem Dokument sind unverbindlich und dienen lediglich zu Informationszwecken.

Urheberrechte

AEB Add-ons für SAP®: Verwendung von produktinternem Code von AEB

Im Rahmen der Wartung und Weiterentwicklung ist jederzeit mit Änderungen der internen Programmierung des Standardsystems zu rechnen. Funktionalitäten der internen Programmierung (z. B. im SAP®-Objektcode) dürfen deshalb vom Kunden nicht über eigene Programmierungen angesprochen werden. Zum Zweck der Nutzung durch den Kunden dokumentierter Code, wie beispielsweise eine Übergabeschnittstelle zum Aufruf von Funktionalitäten des Produkts, ist hiervon ausgenommen.

Stand: 07.01.2025

Inhaltsverzeichnis

1 Einleitung

Sowohl für die Implementierungsphase der AEB-Lösung bei Ihnen als auch für den anschließenden reibungslosen Betrieb ist eine funktionierende Fernwartungsanbindung ein wichtiger Baustein. Für kurze Projektlaufzeiten und eine schnelle Lösungsfindung im Problemfall sowie für die Einhaltung von abgeschlossenen SLAs ist sie außerdem notwendig.

2 Sicherheit und berechtigte Personen bei AEB

Generell gilt, dass sich alle Mitarbeitenden von AEB persönlich zur Geheimhaltung verpflichtet haben. Diese Verpflichtung gilt sowohl gegenüber AEB als auch gegenüber allen AEB-Kunden.

Die eingegangene Verpflichtung kann vom AEB-Mitarbeitenden nur dem Arbeitgeber gegenüber erbracht werden, nicht gegenüber Dritten (Dienstherrenprinzip). Zudem hat AEB auch ihren Mitarbeitenden gegenüber den Datenschutz zu wahren.

Aus diesem Grunde sichert AEB folgende Verfahrensweise und -sicherheit für Kunden-Fernwartungen zu:

- Für den Zugriff auf ein Kundensystem muss immer ein Grund vorliegen. Diese Notwendigkeit im Regelbetrieb wird in einem Ticket innerhalb eines AEBTicketsystems dokumentiert. Projektbezogene Fernwartungszugriffe erfolgen in Absprache mit dem Projektleiter oder dem Projekt-Team.
- AEB verwaltet Passwörter oder andere sicherheitskritische Fernwartungsdaten mit Hilfe eines Passwort-Tools, das Zugriffe für AEB-Mitarbeitende reglementiert und nur berechtigten Personen protokolliert Zugriff darauf erteilt.
- Passwortdaten und andere sicherheitskritische Fernwartungsdaten werden nicht im Klartext gespeichert.
- Zugriffe auf Kundensysteme erfolgen ausschließlich aus gesicherten Netzwerken von AEB. Im Einsatz befindliche Next-Generation-Firewalls und -Virenscanner werden ständig durch AEB überprüft und auf Basis aktueller Bedrohungsszenarien permanent optimiert und gewartet.

Im Bedarfsfall kann AEB die durchgeführten Zugriffe inklusive beteiligten AEB-Mitarbeitenden, Tickets und Dauern auflisten und auf Nachfrage zur Verfügung stellen.

Im Regelbetrieb erbringen eine Vielzahl von Mitarbeitenden Service und Support, teilweise auch im Mehrschichtbetrieb und von unterschiedlichen Standorten aus. Alle diese Mitarbeitenden unterstehen ausnahmslos den oben genannten Verschwiegenheits- und Datenschutzerklärungen.

3 Technische Verbindung

AEB bietet die folgenden Varianten für die Fernwartungsverbindung zu Kunden an. Die zuerst genannten Varianten passen aus AEB-Sicht insgesamt erfahrungsgemäß am besten bezüglich dem initialen und dem laufenden Aufwand und verursachen somit die geringsten Verzögerungen im Projekt und bei Support-Fällen.

» Aus jahrelanger Erfahrung empfiehlt AEB im Betrieb und bei Kundenprojekten die Einrichtung einer Site-2-Site-VPN-Verbindung zum Zugriff per RDP oder SAP®-GUI auf Kundenserver mit AEB-Komponenten, siehe auch Abschnitt Site-2-Site VPN (LAN-LAN-Kopplung) (▸ Seite 2).
Um auch bei Supportfällen in Randzeiten die Reaktionszeit möglichst gering zu halten, wird zur Authentifizierung ein nicht-personalisierter Zugangsuser bevorzugt, der im AEB-Passwort- Tool hinterlegt werden kann.

3.1 TeamViewer

Webbasierte Standard-Anwendung für Fernwartungen über das Internet:

- Für die Ad-Hoc-Variante ist keine Installation notwendig, der Client wird im Bedarfsfall im Browser von einem Mitarbeitenden des Kunden aufgerufen.
- Für die „TeamViewer – Host"-Variante ist die Installation eines Dienstes auf (mindestens) einem der fernzuwartenden Kundenserver notwendig.

Vorteile

- Keine Einrichtung notwendig (außer bei der Variante „TeamViewer – Host")
- Schnelle Verbindung über das Internet nach Freigabe durch den Benutzer

Nachteile

Die folgenden Nachteile gelten **nicht** für die Variante "TeamViewer – Host":

- Der Anwender muss die Fernwartung aktiv öffnen und den Prozess der Analyse und Fehlerbehebung begleiten. Arbeiten an diesem Fernwartungsrechner sind während dieser Zeit nicht möglich.
- Längere Analysen können unter Umständen auch mehrere Zugriffe benötigen, die dann gemeinsam geplant werden müssen.
- Servicefallbearbeitung zu Randzeiten oder mit Analyse-Unterbrechungen (z. B. durch interne Rückfragen) werden erschwert bzw. sind nicht möglich.
- Übergabe der Fernwartung an einen Entwickler oder ein Produkt-Team zur weiteren Analyse ist nicht oder nur sehr schwer möglich.

3.2 Site-2-Site VPN (LAN-LAN-Kopplung)

Netzwerkkopplung über eine abgesicherte VPN-Anbindung auf Router-Ebene, die einen Zugriff per RDP, SAP®-GUI o. ä. (je nach Bedarf) aus dem AEB-Netz auf die fernzuwartenden Kundenserver ermöglicht.

Vorteile

- Schneller Zugriff auf die installierten AEB-Systeme beim Kunden
- Bessere Lösungs- und Supportzeiten bei komplexen Problemen, ggf. auch in Rand- und Sonderzeiten hinein
- Kein aktives Eingreifen auf Kundenseite zur Öffnung der Fernwartung erforderlich
- Sichere, getunnelte Lösung ohne Einsatz von Fremdsoftware
- Schnelles Teamworking mit Produkt- und Entwicklungskollegen bei komplexen Fehlersituationen

Nachteile

- Initial geringfügig höherer Aufwand bei der Einrichtung

3.3 Terminal-Server-basierter Zugang

Dieser Zugang basiert z. B. auf Citrix oder RDP zu gepublishten Anwendungen oder Desktops, die eine Fernwartung ermöglichen, z. B. Web-Browser, SAP®-GUI, RDP-Verbindungen.

Vorteile

- Ggf. kein aktives Eingreifen auf Kundenseite zur Öffnung der Fernwartung erforderlich
- Zwei-Faktor-Authentifizierung möglich, wenn gewünscht

Nachteile

- Initialer Einrichtungsaufwand
- Laufender Pflegeaufwand auf Kundenseite
- Ggf. initiale und/oder laufende Kosten für Lizenzen und/oder Tokens
- Ggf. keine Datenübertragung möglich, dadurch erschwerte Analyse von Logs durch Produkt- oder Entwicklungsteams

3.4 VPN-Client in einer Fernwartungs-DMZ bei AEB

Einsatz eines VPN-Clients, der eine verschlüsselte VPN-Verbindung zum Kundennetz aufbaut.

Voraussetzungen

Split-Tunneling muss auf Kundenseite zwingend erlaubt sein

Für die Fernwartung können ausschließlich die folgenden von *AEB* freigegebenen VPN-Clients verwendet werden:

- GlobalProtect
- Cisco AnyConnect
- Cisco Secure Client
- Checkpoint SecuRemote
- Juniper Pulse Secure
- Ivanti Secure Access
- OpenVPN
- Barracuda Network Access Client
- FortiClient VPN
- SonicWall VPN
- BIG-IP Edge Client
- Sophos VPN Client
- Watchguard VPN
- SoftEther VPN Client

Die Nutzung des VPN-Zugangs erfolgt ausschließlich über anonyme Benutzerkonten. Named User (persönlich identifizierbare Benutzerkonten) sind für den VPN-Zugang nicht zulässig, um Sicherheits- und Datenschutzanforderungen zu erfüllen.

Falls Sie als Kunde einen eigenen VPN-Client verwenden möchten, bedarf dies einer Prüfung durch AEB. Die Prüfung kann zusätzliche technische Anforderungen umfassen, muss vor der Einrichtung abgeschlossen sein und ist kostenpflichtig. AEB behält sich das Recht vor, die Verwendung des kundeneigenen VPN-Clients abzulehnen, falls Sicherheits- oder Kompatibilitätsprobleme festgestellt werden.

Vorteile

- Ggf. kein aktives Eingreifen auf Kundenseite zur Öffnung der Fernwartung erforderlich
- Zwei-Faktor-Authentifizierung möglich, wenn gewünscht

Nachteile

- Nutzung einer speziellen Fernwartungs-DMZ auf AEB-Seite aus Kompatibilitäts- und Sicherheitsgründen
- Deutlich erhöhter initialer Einrichtungsaufwand
- Erhöhter laufender Pflegeaufwand auf Kunden- und AEB-Seite
- Erhöhte Reaktionszeit im Projekt und bei Support-Fällen durch aufwändigeren und fehleranfälligeren Verbindungsaufbau
- Ggf. initiale und/oder laufende Kosten für Lizenzen und/oder Tokens
- Ggf. keine Datenübertragung möglich, dadurch erschwerte Analyse von Logs durch Produkt- oder Entwicklungsteams

4 Authentifizierung

Für die Verbindungs-Authentifizierung bei den Fernwartungsvarianten Terminal-Server-basierter Zugang (▸ Seite 3) und VPN-Client in einer Fernwartungs-DMZ bei AEB (▸ Seite 3) gibt es drei gängige Varianten.

Authentifizierung über Benutzername und Passwort

Zugangsdaten werden in einem Passwort-Tool bei AEB hinterlegt und im Bedarfsfall verwendet, siehe auch Abschnitt Sicherheit und berechtigte Personen bei AEB (▸ Seite 1). Der Zugriff auf die Zugangsdaten in diesem Passwort-Tool ist dabei auf berechtigte Personen eingeschränkt.

Zwei-Faktor-Authentifizierung über Hardware-Token

Der Kunde überlässt AEB einen Hardware-Token, der von AEB zur Authentifizierung verwendet wird.

Zwei-Faktor-Authentifizierung über Soft-Token oder Spezial-App

Auf Kundenwunsch kann ergänzend zu Benutzerdaten und Passwörtern ein zweiter Faktor über einen Soft-Token oder eine Spezial-App generiert werden. Entsprechende Token-Generatoren und Spezial-Apps müssen von der AEB vorab auf Kompatibilität überprüft werden.

» Eine Zwei-Faktor-Authentifizierung über einen Telefonanruf oder eine SMS ist nicht möglich und wird von AEB daher nicht unterstützt. FIDO2-Varianten (z. B. Yubi-Key) müssen vorab von AEB geprüft werden.

AEB

AEB SE
Hauptsitz . Sigmaringer Straße 109 . 70567 Stuttgart . Deutschland . +49 711 72842 0 . www.aeb.com . info.de@aeb.com
Registergericht: Amtsgericht Stuttgart . HRB 767 414 . Geschäftsführende Direktoren: Matthias Kieß, Markus Meißner
Vorsitzende des Verwaltungsrats: Maria Lobe