20.10.2026 – Console, Sicherheit, Aufnahmen, Gateway und TANSS

Die wichtigsten Ergänzungen und Korrekturen seit dem Changelog vom 19.10.2026 für die tägliche Arbeit mit der ERP Austria Remote Console, dem Agenten, Gateway und TANSS. Bereits im vorherigen Eintrag beschriebene Funktionen werden hier nur aufgeführt, wenn sich ihr Verhalten seitdem geändert hat. Stand: 20.10.2026.

Anwendung	Lokal bereitgestellter Stand
ERP Austria Remote Console – Windows und macOS ARM64	1.00.599
Gateway – Windows	1.00.592
ERP Austria Remote Agent – Windows	1.00.459
QuickSupport – Standard und Full, Windows	1.00.328
TANSS Session Tracker	1.2.14 – unverändert

Die Windows-Versionen wurden an den vorhandenen EXE-Dateien in den bisherigen Ausgabeordnern abgelesen; für macOS liegt das Console-Paket 1.00.599 vor. Die QuickSupport-Versionsdatei im Quellstand nennt bereits 1.00.336, die vorhandenen EXE-Dateien dagegen noch 1.00.328. Ein höherer Quellstand ist deshalb nicht als bereits ausgeliefertes Programm ausgewiesen. Installierte Programme und der PHX-Updatekatalog können abweichen.

Remote Console

Sitzungen bedienen und die Console beenden

- **Behoben – Escape bleibt für den entfernten Rechner verfügbar:** Die Escape-Taste beendet bei RDP und QuickSupport nicht mehr den Vollbildmodus und dockt keine Sitzungsfenster an. In einer fokussierten Fernwartung kann sie damit für Dialoge und Aktionen am Ziel verwendet werden. Vollbild und Andocken werden über die vorgesehenen Schaltflächen bedient.
- **NEU – Rückfrage vor dem Beenden:** Bei offenen oder gerade startenden RDP-, QuickSupport-, Agent-, SSH-/Web- oder Dateiverbindungen fragt die Console nach. Erst „Verbindungen trennen und beenden“ schließt die Verbindungen. „Abbrechen“, Escape oder das Schließen des Rückfragedialogs lassen die Sitzungen einschließlich ausgelagerter Fenster bestehen.

- **ERWEITERT – Schutz beim Programmende und Update:** Die Rückfrage gilt auch für das native Beenden-Menü. Untergeordnete Sitzungsfenster werden nicht vor der Entscheidung geschlossen. Bei offenen Verbindungen startet LiveUpdate keinen Installationshelfer.

Verständlichere RDP-Anmeldefehler

- **Behoben – Verbindungsfehler sind keine Kennwortfehler:** Ein abgebrochener FreeRDP-Aufbau und Transportfehler erhalten passende Meldungen. Nur eindeutige Kennwortfehler werden als solche bezeichnet. Allgemeine Anmeldeablehnungen fordern zur Prüfung von Benutzername und Anmeldedaten auf.
- **ERWEITERT – Hinweise während der Anmeldung:** Integriertes Windows-RDP zeigt bekannte Anmeldefehler über der Sitzung und im Protokoll. Gesperrte oder deaktivierte Konten und abgelaufene Kennwörter werden unterschieden. Integriertes Mac-RDP meldet fehlende gespeicherte Zugangsdaten vor dem Start; externe RDP-Programme verwenden ihre eigenen Dialoge.

Sicherheitsüberprüfung gespeicherter Kennwörter

NEU – Kennwörter auf Auffälligkeiten prüfen

- **Für Administratoren:** Unter „Administration → Rechtsklick → Sicherheitsüberprüfung“ können alle am Gateway gespeicherten RDP-/SSH-Verbindungen geprüft werden, einschließlich privater Verbindungen. Dieses Berichtsrecht erlaubt nicht das Öffnen oder Bearbeiten fremder privater Verbindungen.
- **Für Mitarbeiter:** Unter „Verbindungen → Rechtsklick → Sicherheitsüberprüfung“ werden die berechtigten Verbindungen der aktuellen Baumansicht mit ihren Unterordnern geprüft. Suchfilter und Firmenabonnements begrenzen den Umfang.
- **Konkrete Prüfgründe:** Die Prüfung berücksichtigt Mindestlänge, einfache Wiederholungen, bekannte Kennwort-/Tastaturmuster, Ziffernfolgen und enthaltene Benutzernamen. Regulär gelten mindestens 12 Zeichen; für „admin“ und „administrator“ mindestens 16 Zeichen und zwei Sonderzeichen. Mehrere Verstöße werden gemeinsam angezeigt.
- **Mehrfach verwendete Kennwörter:** Identische Kennwörter auf verschiedenen Geräteeinträgen werden innerhalb des jeweiligen Prüfumfangs gekennzeichnet. Mehrere Profile desselben Geräteeintrags lösen allein keine Mehrfachverwendungswarnung aus.

- **Hinweis direkt in RDP:** Bei einem auffälligen gespeicherten Kennwort erscheint in der Sitzungsleiste „Kennwort unsicher“. Die Verbindung bleibt möglich. Das Kennwort muss am Zielrechner beziehungsweise in der Domäne geändert und danach im gespeicherten Profil aktualisiert werden.
- **Übersicht und Fehlerkorrektur:** Ein eigener Reiter zeigt betroffene Computer, Profile, Benutzer und Eigentümer. „Info“ öffnet die vollständigen Gründe und Zusatzangaben. Scrollen und die Behandlung freigegebener Listenelemente wurden korrigiert.

Prüfumfang: Es werden gespeicherte Verbindungskennwörter ausgewertet, keine Windows-Kennwörter ausgelesen oder Anmeldeversuche durchgeführt. Der Bericht überträgt keine Kennwörter oder Kennworthashes an die Console und verwendet keinen externen Prüfdienst. Leere Kennwortfelder gelten als nicht prüfbar. Ein unauffälliges Ergebnis ist keine Sicherheitsgarantie.

Webseiten und SSH

NEU – Webseiten-Zugangsdaten und Auto-Fill

- **Zugangsdaten hinterlegen:** Webseitenverbindungen können Benutzername und Kennwort im bestehenden geschützten Gateway-Speicher halten. Unter „Auto-Fill“ lassen sich typische Anmeldefelder oder eigene CSS-Selektoren zuordnen.
- **Automatisch oder auf Knopfdruck ausfüllen:** Auto-Fill ist zunächst ausgeschaltet. Nach Aktivierung werden passende leere Felder nach dem Laden ausgefüllt. „Zugangsdaten ausfüllen“ in der Browserleiste führt die Zuordnung bei Bedarf erneut aus. Die Anmeldung selbst wird weiterhin bewusst abgesendet.
- **Auf die richtige Webseite begrenzt:** Zugangsdaten werden ausschließlich auf HTTPS-Seiten mit exakt dem hinterlegten Protokoll, Host und Port ausgefüllt. Fremde Weiterleitungen, Frames und abweichende Formularziele erhalten keine Zugangsdaten. Bereits ausgefüllte Felder werden nicht überschrieben; ein anderer eingetragener Benutzer verhindert das zugehörige Kennwort-Auto-Fill.

NEU – SSH und Webseiten über den Gateway erreichen

- **Optionaler Verbindungsweg:** In den Verbindungseigenschaften lässt sich „Verbindung über unseren Gatewayserver leiten“ einschalten. Zusätzlich muss die Weiterleitung im Gateway unter „Verbindungen über Gateway“ aktiviert sein. Das Zielnetz muss vom Gateway aus erreichbar sein, beispielsweise über VPN.

- **Browser und Terminal bleiben in der Console:** Der Gateway stellt die Verbindung zum Ziel her. Bei Webseiten bleibt die ursprüngliche URL erhalten; HTTPS-Zertifikate und SSH-Hostschlüssel werden weiter für das tatsächliche Ziel geprüft.
- **Zusätzliche Webziele ausdrücklich erlauben:** Benötigte Anmelde-, Weiterleitungs- oder Inhaltsserver werden als zusätzliche Web-Ursprünge hinterlegt. Ihre Erreichbarkeit über den Gateway erweitert nicht den erlaubten Auto-Fill-Ursprung.
- **Eigenes Browserprofil:** Gateway-Webseiten verwenden pro Öffnung einen temporären Browserspeicher. Eine Anmeldung muss nach erneutem Öffnen gegebenenfalls wiederholt werden. Bei fehlgeschlagenem Gateway-Verbindungsaufbau erfolgt kein automatischer Wechsel auf eine Direktverbindung.

Für diese Erweiterungen Console und Gateway gemeinsam aktualisieren. Die Weiterleitung erfolgt über den Gateway, nicht über einen Kunden-Agenten.

Fernwartungen lokal aufzeichnen

NEU – Aufnahme für eingebettetes RDP

- **„Aufnahme…“ in der Sitzungsleiste:** Nach dem Verbindungsaufbau öffnet sich ein Aufnahmefenster mit Vorschau, „Aufzeichnung starten“ und optionalem Techniker-Mikrofon. Die Videodatei wird lokal am Techniker-PC gespeichert. Schließen der Sitzung oder des Aufnahmefensters schließt die Datei ab.
- **Nur die betreffende RDP-Ansicht:** Aufgenommen wird mit maximal 1280 × 720 Pixeln und fünf Bildern pro Sekunde. Die entfernte Auflösung wird nicht geändert. Externe RDP-Programme werden nicht erfasst. Unter Windows pausiert das Bild bei ausgeblendetem oder minimiertem RDP-Fenster; ein eingeschaltetes Mikrofon kann weiterlaufen.
- **Anzeige bei RDP:** Die Aufnahmeanzeige befindet sich in der Techniker-Console. Eine zusätzliche Kundenanzeige wie bei QuickSupport gehört bei normalen RDP-Verbindungen nicht zu diesem Ablauf.

ERWEITERT – Aufnahme bei Agent-Benutzerunterstützung

- **„Aufzeichnen“ im Agent-Viewer:** Bei „Benutzersitzung unterstützen“ kann jetzt die bereits empfangene Bildschirmansicht gespeichert werden. Der unterstützte Mitarbeiter erhält eine native Aufnahmeanzeige mit „Aufzeichnung beenden“. Der Start wartet auf die technische Bestätigung, dass diese Anzeige bereitsteht.
- **Kontrolle beim unterstützten Mitarbeiter:** Dessen Stopptaste beendet nur die Aufnahme; die Fernwartung bleibt bestehen. Nach diesem Stopp ist eine weitere Aufnahme in derselben Sitzung gesperrt. Ältere Agenten und der lokale Konsolenmodus

ohne Benutzerfreigabe bieten diese Aufnahmefunktion nicht an.

Wie bei der bereits beschriebenen QuickSupport-Aufnahme ist ausschließlich das Techniker-Mikrofon optional. Kundenmikrofon, Kamera und eine zusätzliche Systemtonaufnahme werden nicht verwendet. Das verfügbare lokale Videoformat ist WebM oder MP4.

Agent und Agentinformationen

- **Behoben – Freigabefenster besser sichtbar:** Bei der Benutzerunterstützung wird der Kundendialog aktiviert und bleibt bis zur Entscheidung über normalen Anwendungen sichtbar. Der anfängliche Fokus liegt auf „Ablehnen“, damit laufende Tastatureingaben nicht versehentlich eine Freigabe bestätigen. Das Fenster erscheint weiterhin nicht über dem Windows-Sperr- oder UAC-Desktop.
- **ERWEITERT – Dienste übersichtlich darstellen:** Agentinformationen verwenden Karten und eine Dienstetabelle mit Dienstname, Starttyp und Status. Beendete automatische Dienste stehen oben und sind rot markiert, beendete manuelle orange, laufende grün und deaktivierte grau. Text ergänzt die Farben.
- **Behoben – Mehrere Softwarefunde:** Für Actian und gotomaxx PDFMAILER wird pro Produkt die neueste numerisch verglichene Version angezeigt. Die Console verdichtet auch Meldungen älterer Agenten. Unvollständig ermittelte Informationen bleiben gekennzeichnet.
- **ERWEITERT – Updateangebot aktuell prüfen:** Jede Agentinformationsabfrage prüft das verfügbare Agent-LiveUpdate erneut und zeigt installierte sowie angebotene Version mit Prüfzeitpunkt. Fehler ergeben einen unbekannten Status. Frühere automatische Updateereignisse werden getrennt mit ihrem damaligen Zeitpunkt angezeigt. Die reine Informationsabfrage installiert kein Update.

TANSS: Zeiteingabe und Sitzungsabschluss

- **Behoben – Uhrzeiten einfacher ersetzen:** Bei manueller TANSS-Erfassung werden die Uhrzeitfelder beim Betreten für eine neue Eingabe geleert.
- **ERWEITERT – Rundung auch bei der Übertragung:** Die im letzten Changelog beschriebene Anzeige ganzer Minuten wird für Console-Zeiten nun auch beim TANSS-Abgleich, Anlegen und Verlängern einheitlich verwendet. Der Beginn bleibt erhalten, das übertragene Ende liegt eine aufgerundete Anzahl ganzer Minuten danach. Gemessene Originalzeiten bleiben im Verlauf erhalten; RoyalTS-Zeitkorrekturen sind hiervon unabhängig.

- **Behoben – Abschluss persönlicher RDP-Verbindungen:** Beim Schließen werden TANSS-Einstellungen erneut geladen, auch wenn der Gateway beim Sitzungsstart nicht erreichbar oder TANSS damals deaktiviert war. Fehlende Zeitdaten oder eine fehlgeschlagene Abfrage gelten nicht mehr vorschnell als erledigter Abschluss.
- **Behoben – Nachholen ohne doppelte Dialoge:** Direkte Sitzungsberichte werden nach Ende des Listeners nochmals synchronisiert und ausstehende Abschlüsse erneut versucht. Bereits gezeigte oder bewusst abgebrochene Dialoge werden nicht doppelt geöffnet. Bei längerem Gateway-Ausfall bleibt die Sitzung lokal vorgemerkt und kann später im Verlauf bearbeitet werden.
- **ERWEITERT – Abschluss für Agent-Fernwartungen:** Auch Benutzerunterstützung und lokaler Agent-Desktop öffnen nach einer tatsächlich aufgebauten Sitzung den TANSS-Abschluss mit Firma und Computer. Eine abgelehnte Freigabe oder ein Viewer ohne empfangenes Desktopbild löst keinen Abschluss aus. Die bestehende Mindestdauer von 15 Sekunden gilt weiter.

Hinweis zur Aktualisierung und Prüfung

Für Sicherheitsüberprüfung, Webseiten-Auto-Fill, Gateway-Weiterleitung und die angepasste TANSS-Übertragung Console und Gateway gemeinsam aktualisieren. Die neue Agent-Aufnahmeanzeige und die überarbeitete Freigabemaske benötigen einen passenden aktuellen Agenten. Das macOS-ARM64-Console-Paket 1.00.599 liegt im bisherigen Setup-Ordner; die native Mac-Ausführung muss praktisch geprüft werden.

Die Versionsübersicht beschreibt vorhandene lokale Pakete und bestätigt keine Installation beim Kunden oder Freigabe im PHX-Updatekatalog. Bestehende Einstellungen, Zugangsdaten und Gateway-Daten beim Übernehmen der Programme erhalten. Für diesen Changelog wurden keine produktiven Programme oder Dienste beendet und keine neuen Releases erstellt.

Prüfstand und Grenzen: Der vollständige Solution-Build wurde bei der Zusammenstellung erfolgreich mit null Warnungen und null Fehlern ausgeführt. Automatisierte Prüfungen der neuen Funktionen sind im Projekt enthalten. Echte RDP-Bildaufnahme auf dem Zielsystem, SSH-Anmeldung am Kundenziel, die Freigabeanzeige in einer Kunden-/RDS-Sitzung sowie native macOS-WebViews benötigen zusätzlich praktische Prüfungen. Die Zusammenstellung umfasst eingecheckte und lokal vorhandene Implementierungen seit dem letzten Changelog; die obige Versionsübersicht grenzt diese vom tatsächlich vorhandenen Paketstand ab.

Der zusätzlich gestartete vollständige .NET-Testlauf meldete Fehler unter anderem in Registrierungs-, Verzeichnis- und nativen Fenstertests und wurde abgebrochen. Ein erfolgreicher Gesamttest wird für diese Zusammenstellung daher nicht bestätigt; die Ursachen der Testfehler wurden im Rahmen der Changelog-Erstellung nicht untersucht.

Created 2026-10-20 21:53:53 CEST by Access System API
Updated 2026-10-20 21:55:54 CEST by Access System API