ESTOS
Communication Solutions

ProCall Enterprise

Best Practise

Betriebsrat

Informationen für Partner und verantwortliche beim Kunden, wenn der Betriebsrat „Überwachungsfunktion“ beim Einsatz von ESTOS ProCall Enterprise befürchtet.

Rechtliche Hinweise / Impressum

Die Angaben in diesem Dokument entsprechen dem Kenntnisstand zum Zeitpunkt der Erstellung. Irrtümer und spätere Änderungen sind vorbehalten.

Die ESTOS GmbH schließt jegliche Haftung für Schäden aus, die direkt oder indirekt aus der Verwendung dieses Dokumentes entstehen.

Alle genannten Marken- und Produktbezeichnungen sind Warenzeichen oder Eigentum der entsprechenden Inhaber.

Die derzeit gültigen Allgemeinen Geschäftsbedingungen finden Sie auf unserer Webseite unter http://www.estos.de/agb.

ESTOS GmbH
Petersbrunner Str. 3a
D-82319 Starnberg
info@estos.de
www.estos.de

Dokumenthistorie

Version	Datum	Autor	Änderungen
1.0	22.02.2011	Thomas Pecher-Wagner	Initial
1.1	14.10.2011	Thomas Pecher-Wagner	Verbesserungen
2.0	08.10.2014	Thomas Pecher-Wagner	Update/Überarbeitung

Inhalt

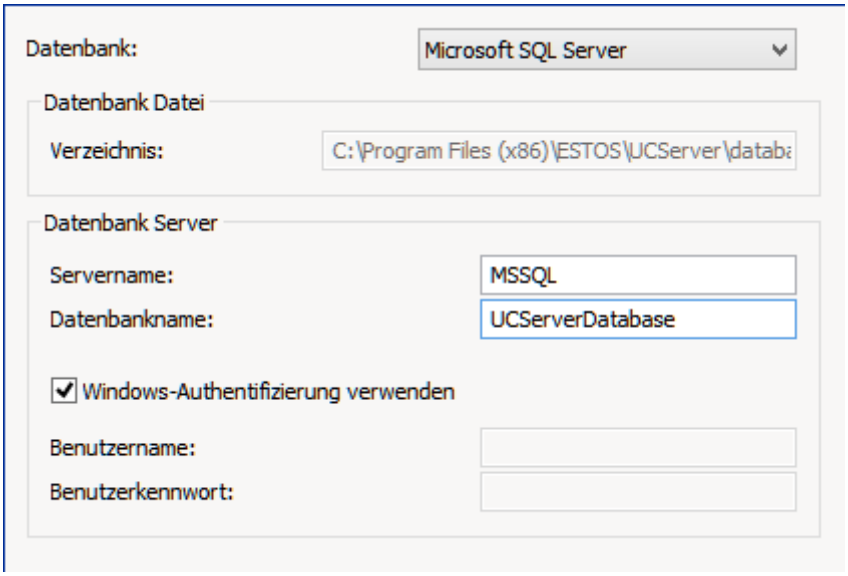
Einleitung

Im Rahmen von Projekten, bei denen die Einführung von ESTOS ProCall 4.0 Enterprise auch mit dem Betriebsrat besprochen wird, kommt es bisweilen zu Fragen der neu einzuführenden Lösung. Vor allem zu den Themen *Journal* und *Präsenzmanagement* herrschen bisweilen Vorbehalte, zu denen mangels Information nicht ausreichen Stellung genommen werden kann. Um Bedenken auszuräumen und über den tatsächlichen Sachverhalt zu informieren wurde ein Schreiben verfasst, das nach Bedarf angepasst, Partnern und verantwortlichen Kunden bereitgestellt werden kann. Sollte darüber hinaus weiterer Informationsbedarf herrschen, bitte den direkten Kontakt mit dem Produktmanagement herstellen.

1 Zugriffskontrolle

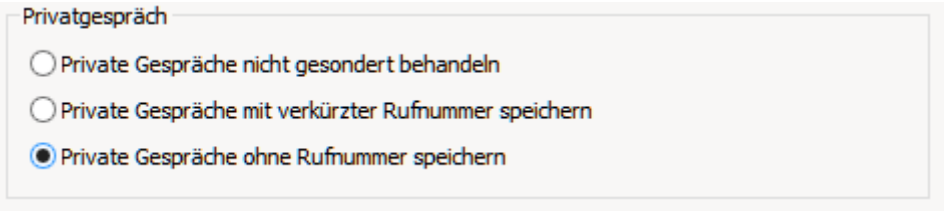
1.1 Administration, Administrator Konsole

Der Zugriff auf die Administrationskonsole ist zum einem über das MS Windows Rechte System beschränkt und zusätzlich mit einem speziellen Administrator-Login geschützt. Der Zugriff auf die Informationen in den Journaldatenbanken ist zusätzlich über das MS Windows Rechte System beschränkt oder mit einem speziellen Administrator-Login geschützt.



1.2 Journal

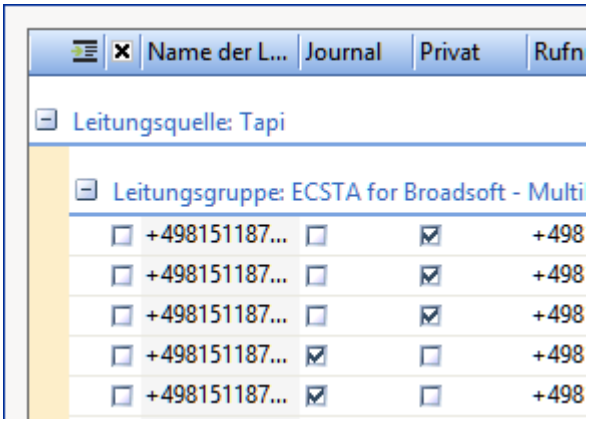
Die Daten in den Journal-Datenbanken sind ähnlich wie bei einem Groupware-System, z.B. MS Exchange, ausschließlich für den Administrator einsehbar. Der Zugang für den Administrator ist zur Analyse bei Problemen und für statistische Auswertung notwendig. Die Protokollierung von Daten für Privatgespräche erfolgt nach Regeln, die konfiguriert werden können.



Der Nutzer kann Gespräche einfach als privat markieren.
Leitungen können generell als privat gekennzeichnet.

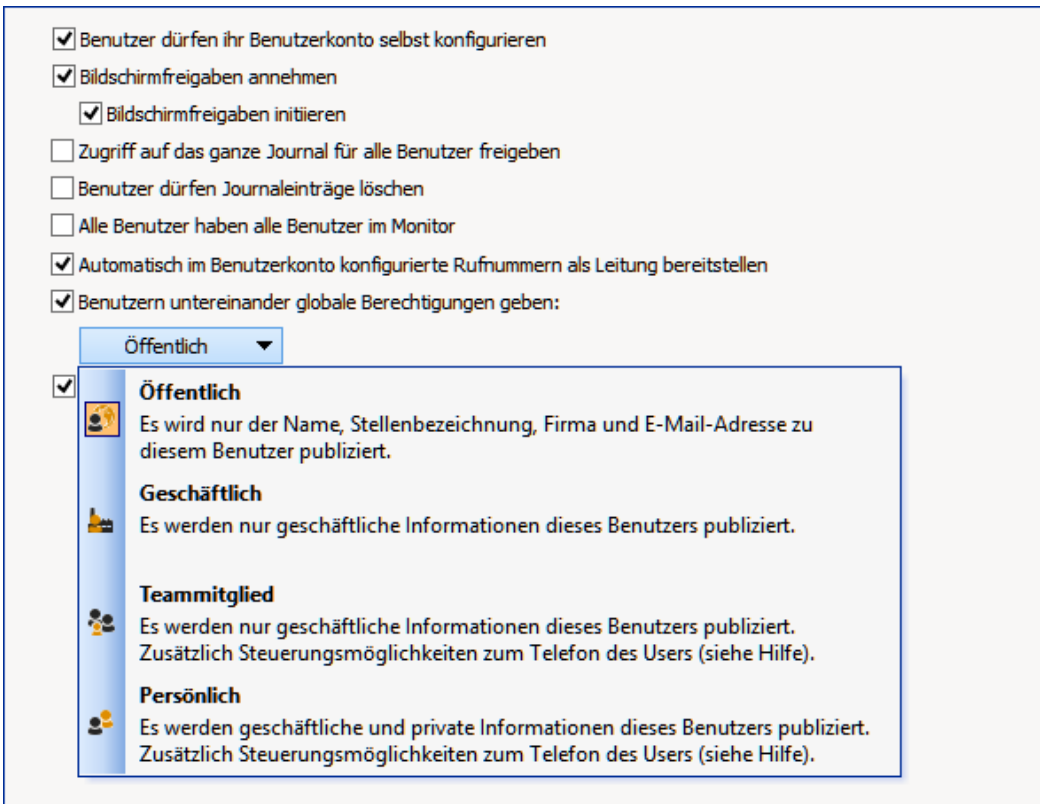
1.3 Leitungen

Spezielle Telefonleitungen, z.B. Telefone des Betriebsratsbüros können von einer Journalisierung generell ausgenommen werden.

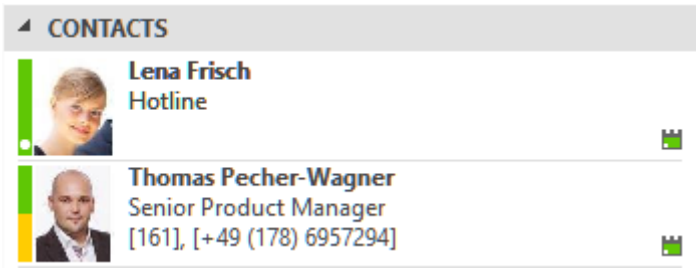


1.4 Präsenz

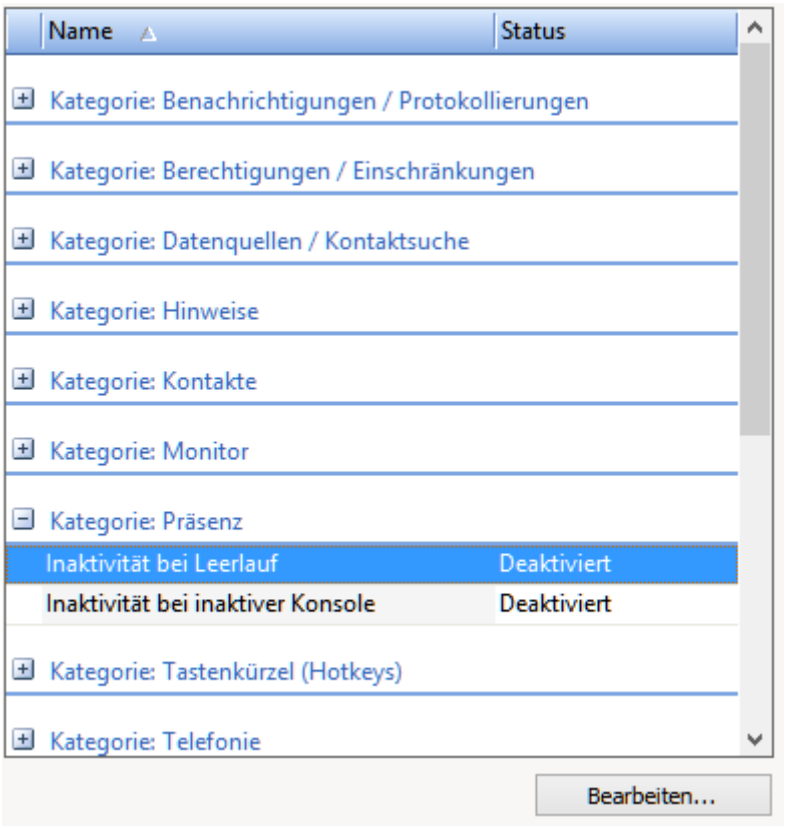
Präsenzzustände bzw. eine Änderungshistorie von Präsenzzuständen werden nicht protokolliert. Eine Möglichkeit zur statistischen Auswertung von Präsenzzuständen ist nicht vorgesehen. Im Sinne einer Umsetzung von individuellen Betriebsvereinbarungen kann der Austausch von Präsenz-relevanten Informationen differenziert konfiguriert werden. Die Einrichtung des kleinsten gemeinsamen Nenners zum Thema Präsenz innerhalb einer Unternehmung oder Institution kann auf den Stufen Global, Gruppenebene und Nutzerebene geschehen. Das Rechtsystem ist additiv, d.h. erwirbt man auf einer Stufe ein Recht, kann es nicht auf einer anderen weggenommen werden.



Bisweilen ist gewünscht, dass keine Anzeige der Änderung des Präsenzzustandes (=>zweigeteiltes Icon - inaktiv) auf Grund eines "Leerlaufs" (aka Idle Zustand) erfolgt.



Es gibt eine Möglichkeit, die Präsenzzustand-Anzeige auf Grund von sogenannten „Leerlauf"-Zuständen Zentral/serverseitig zu konfigurieren bzw. zu deaktivieren. Sie finden die Konfiguration am UCServer in den Einstellungen im Bereich Benutzerverwaltung→Profile.



1.5 Leistungsmerkmal Freisprechmodus

Anlagen mit CSTA LM „Freisprechmodus“ und ESTOS ECSTA Middleware:

Stellt die CSTA Schnittstelle einer Anlage die Funktion „in Freisprechmodus schalten" bereit, kann dieses Leistungsmerkmal ggf. über eine kompatiblen ESTOS ECSTA Middleware (ab inkl. Version 3.0) ausgeschalten werden. "Aufschaltfunktionen" von PBX Systemen werden durch die ESTOS ECSTA Middleware generell **NICHT** unterstützt

2 Informationsberechtigung

Welche Informationen ein Benutzer von anderen Usern einsehen darf wird mit dem Berechtigungsmanagement geregelt. Dabei kann u.a. jeder Benutzer einstellen, welcher andere Benutzer Informationen einholen darf, bzw. welcher Benutzer dies nicht darf:

2.1 Berechtigungs-Layer

Globale Rechte.
Ist eine Berechtigung in den Globalen Rechten erteilt, so gilt diese für alle Benutzer des Systems. Diese Rechte werden ausschließlich vom Administrator konfiguriert.

Gruppen-Rechte.
Ist eine Berechtigung in den Gruppen-Rechten erteilt, so gilt diese für alle Benutzer, die Mitglied dieser Gruppe sind. Diese Rechte werden ausschließlich vom Administrator konfiguriert.

Benutzer-Berechtigungen.
Jeder Benutzer kann anderen Benutzern individuell Rechte an sich selbst vergeben. Diese Rechte können auch vom Administrator eingesehen und konfiguriert werden

2.2 Berechtigungsstufen

Präsenz sehen	Der andere Benutzer darf die Präsenz (Anwesend, Abwesend...) sehen.
Präsenz setzen	Der andere Benutzer darf die Präsenz ändern. Dieses Recht sollte nur bei besonderen Vertrauensstellungen gesetzt werden.
Private Termine sehen	Der andere Benutzer darf die als Privat markierten Termine aus dem Kalender sehen.Dieses Recht sollte nur bei besonderen Vertrauensstellungen gesetzt werden.
Öffentliche Termine sehen	Der andere Benutzer darf öffentliche Termine aus dem Kalender sehen.
Abgehende Rufnummern sehen (primäre/zweite Leitung)	Der andere Benutzer darf sehen, wen der Benutzer mit seinem primären/zweiten Telefon gerade anruft. Dieses Recht sollte nur bei besonderen Vertrauensstellungen gesetzt werden.
Ankommende Rufnummern sehen (primäre/zweite Leitung)	Der andere Benutzer darf sehen, von wem der Benutzer mit seinem primären/zweiten Telefon gerade angerufen wird.
Nummer einer gesetzten Rufumleitung sehen (primäre/zweite Leitung)	Der andere Benutzer darf sehen, zu welcher Zielrufnummer eine Rufumleitung am Telefon eingeschaltet ist. Dieses Recht sollte nur bei besonderen Vertrauensstellungen gesetzt werden.
Rufumleitung sehen (primäre/zweite Leitung)	Der andere Benutzer darf sehen, dass eine Rufumleitung am Telefon eingeschaltet ist.
Anrufe an den Benutzer zu sich heranholen (primäre/zweite Leitung)	Der andere Benutzer darf an der primären/zweiten Leitung ankommende Anrufe zu sich heranholen. Dieses Recht sollte nur bei besonderen Vertrauensstellungen gesetzt werden.