ProCall Enterprise

Explanation for works councils

[Comments]

Legal Information/Imprint

The information contained in this document reflects the state of knowledge at the time the document was created. Errors and subsequent alterations are reserved.

estos GmbH rejects any liability for damage caused by the direct or indirect use of this document. All brand and product names quoted are trademarks or property of their respective owners.

Our current General Terms and Conditions can be found on our website at http://www.estos.com/about-us/imprint.html

estos GmbH,Petersbrunner Str. 3a,82319 Starnberg, Germany
info@estos.de
www.estos.de

Template 12/5/2015

Document history

Version	Date	Author	Amendments
1	8/10/2014	RBO	Initial version
1.1	6/2/2018	SHE	Minimal textual amendments made

Contents

1. Introduction

Projects that discuss the introduction of ProCall Enterprise with the works council sometimes raise questions about the new solution to be implemented. Sometimes, there are reservations about the subjects of call logging and presence management, which cannot be adequately explained due to a lack of information. In order to dispel concerns and provide information about the facts, a letter has been prepared that can be adapted as needed and provided to partners and responsible customers. Should there be any further need for information, please contact estos product management directly.

2. Access control

2.1. Administration, administrator console

Access to the administration console is restricted via the Microsoft Windows rights system and additionally protected by a special administrator login. Access to the information in the call log databases is additionally restricted via the MS Windows rights system or protected by a special administrator login.

2.2. Journal/call logging

The data in the call log databases is similar to a groupware system, e.g. Microsoft Exchange, available only to the administrator. Access for the administrator is required for analysis in case of problems and for statistical evaluation. The logging of data for personal calls is carried out according to rules which can be configured.
The user can mark conversations as private. Lines can generally be marked as private.

2.3. Lines

Special telephone lines, e.g. the works council office telephones, can generally be exempted from call logging.

2.4. Presence

Presence states or a change in history of presence states are not logged. It's not possible to statistically evaluate presence states. In terms of implementation of individual company agreements, the exchange of presence-relevant information can be configured differentially.
The establishment of the lowest common denominator regarding presence within a company or institution can be done at the global level, group level and user level. The rights management system is additive, which means that if you acquire a right at one stage, it cannot be removed at another.

Sometimes, when “idle” (no/few calls), it is desirable that no indication in the change of presence status (=> split icon – inactive) is made.

There is a possibility to configure/deactivate the presence status display centrally/on the server side due to so-called "idle" states. You can find the configuration in the ProCall Enterprise UCServer Administration in the settings of the User Management Profiles area.

2.5. Hands-free mode feature

If the CSTA interface of a telephone system provides the function "switch to hands-free mode", this feature may be switched off via a compatible estos ECSTA middleware driver. estos ECSTA middleware drivers generally do not support the "override function" of telephone systems.

3. Information permissions

What information a user may see from other users is regulated by authorization management. Each user can adjust what information is available about themselves and what can be obtained by other users.

3.1. Authorization layers

- **Global rights:**

  If authorization is granted in global rights, this applies to all users of the system. These rights are only configured by the administrator

- **Group rights:**

  If authorization is granted in group rights, this applies to all users who are members of this group. These rights are only configured by the administrator

- **User permissions:**

  Each user may grant other users individual rights themselves. These rights can also be viewed and configured by the administrator

3.2. Authorization levels

View presence	The other user is allowed to view presence (present, absent ...).
Set presence	The other user is allowed to change the presence. This authorization should only be set for special trusted users.
View private appointments	The other user is allowed to view events marked as private from the calendar. This authorization should only be set for special trusted users.
View public appointments	The other user is allowed to view public appointments from the calendar.
View outgoing numbers (primary/secondary line)	The other user can view who the user is calling with his/her primary/secondary telephone. This authorization should only be set for special trusted users.

View incoming numbers (primary/secondary line)	The other user can view who is currently calling the user with their primary/secondary phone.
View number of a set call diversion (primary/secondary line)	The other user is allowed to view the destination number a call is diverted to, if enabled on the phone. This authorization should only be set for special trusted users.
View call diversion (primary/secondary line)	The other user is allowed to view that call diversion on the phone is switched on.
Pick up other user's calls (primary/secondary line)	The other user is allowed to pick up incoming calls on the primary/secondary line. This authorization should only be set for special trusted users.