

Smart Connect

Программное решение, позволяющее использовать карту-чип или биометрические данные для более быстрого доступа сотрудника в систему. Оперативность аутентификации позволит сократить расходы операционного времени, сохраняя при этом высочайший уровень безопасности авторизованного доступа.



В современном, динамично меняющемся мире, сотрудник компании может использовать любое рабочее место. Для этого он должен залогиниться на своем рабочем месте, ввести пароли для входа в систему, зарегистрировать свой телефон, получить от администратора те или иные права для доступа к сетевым ресурсам, и только после этих обязательных процедур приступить непосредственно к выполнению своих задач. В конечном итоге, все эти манипуляции занимают определенное количество операционного времени, что сказывается на эффективности работы сотрудников.

В поиске путей для оптимизации рабочего процесса в офисе, мы разработали решение, позволяющее сократить время на выполнение таких рутинных операций, как аутентификация и сегментация доступа к сетевым ресурсам. Решение **Smiddle Smart Connect (SC)** предназначено для автоматической аутентификации сотрудника на рабочем месте и предоставления ему прав доступа к сетевым ресурсам в зависимости от его профиля. Функционал данного программного решения позволяет использовать различные известные способы авторизации для быстрой регистрации сотрудника в системе. Чем это полезно? Благодаря возможностям **SC**, сотрудники могут получать доступ к своему персонализированному рабочему месту и настройкам системы посредством подтверждения личности при помощи, например, карты-чипа, отпечатка ладони или рисунка радужки глаза. Данный способ авторизации позволяет не только сократить время на подготовку операторов к рабочему процессу, но и предоставляет больший уровень безопасности данных через возможность персонализированного контроля над операторами.

На сегодняшний день, вопрос безопасности становится одним из наиболее важных и актуальных вопросов на любом предприятии. Особенно ключевым, по ряду причин, этот вопрос становится в разрезе современных офисов с открытым рабочим пространством, учитывая специфику их использования и мобильность рабочего места.

Функциональные возможности Smiddle SC:

1. Отслеживание авторизаций пользователя через CISCO ISE.
2. Автоматическая авторизация пользователя на телефоне через CUCM.
3. Контроль уже авторизованных пользователей.
4. Применение на портах коммутаторов доступа Dinamyc Access Control List в зависимости от значений тех или иных полей Active Directory, характеризующих сотрудника.
5. Автоматическое разлогинивание пользователя на CUCM на предыдущем РМ при авторизации на другом РМ.
6. WEB - интерфейс пользователя для внесения настроек.
7. Логирование.

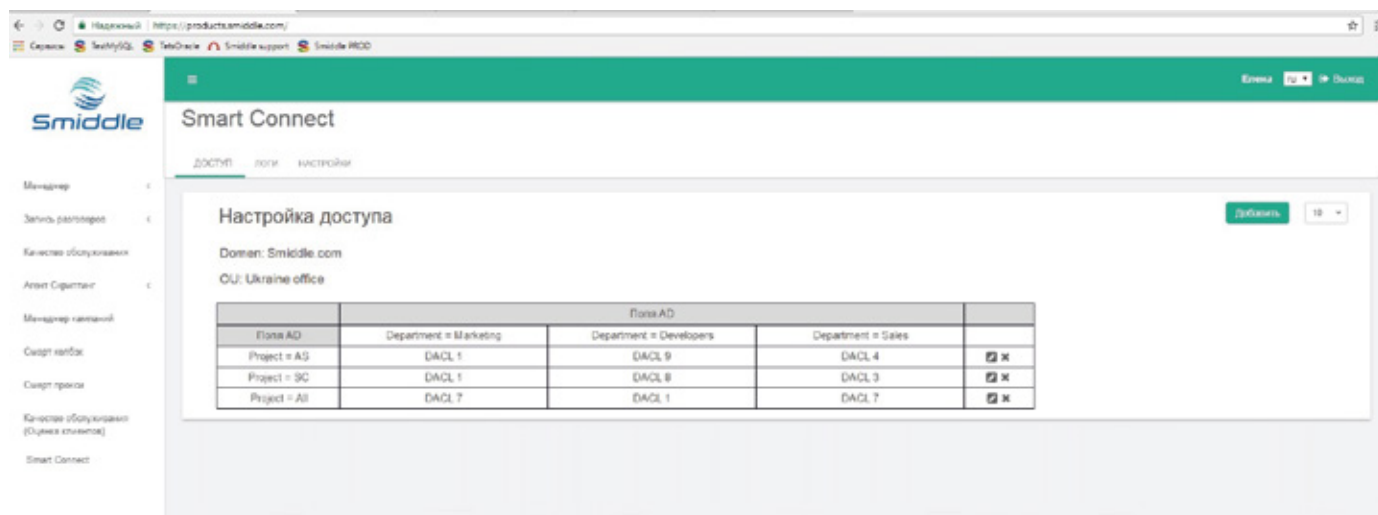




Как это работает?

Принцип работы данного решения довольно простой. При наличии необходимых инструментов для бесконтактной авторизации сотрудника в системе, процесс аутентификации можно сократить до секунды! Все, что нужно сделать – приложить магнитную карту с чипом, где прописаны предварительные настройки пользователя, к считывающему устройству, которое автоматически авторизует сотрудника в системе, где он получит возможность сразу приступить к работе.

Если же сотруднику, по каким-либо причинам, необходимо сменить рабочее место, он может авторизоваться на другом компьютере, подтянув через персональную карточку свои настройки на другую физическую машину. При этом, система автоматически разлогинит данного пользователя с предыдущего рабочего места, соблюдая правила безопасности доступа.



Чем это件озно:

Функциональные возможности **Smiddle SC** позволяют использовать современные инструменты авторизации для более быстрого и безопасного доступа в систему. Оперативность аутентификации при помощи карты-чипа или биометрических данных позволит сократить расходы операционного времени, сохраняя при этом высочайший уровень безопасности авторизованного доступа.

Повышение уровня безопасности сетевого взаимодействия сотрудников благодаря:

- программному определению дробных сегментов сети для повышения гибкости (например, для предотвращения горизонтального распространения угрозы или помещения в карантин потенциально скомпрометированной оконечной точки обширной системы);
- программной автоматизации управления сегментами и политиками.

Кроме того, **SC** отслеживает входы и выходы пользователей на рабочее место в Cisco Identity Services Engine (CISCO ISE) и автоматически авторизует их на телефоне в Extension Mobility, закрепленном за этим рабочим местом.

В базе данных за пользователем также сохраняются настройки и записи журнала событий.

Свяжитесь с нами, чтобы узнать о решении больше
и оценить все выгоды для Вашего бизнеса!
e-mail: sales@smiddle.com www.smiddle.com