
myTrace
powered by JST

Bisher bedeutete zusätzliche Flexibilität im Kontrollraum immer eine Einschränkung der Sicherheit.

Mit *my***Trace**® erhöhen Sie die Sicherheit, steigern die Flexibilität und beschleunigen die Prozesse in Ihrem Kontrollraum.

my**Trace**® erfüllt die Vorgaben des BSI

Was ist myTrace®?

Die englische Vokabel „trace“ bedeutet „eine Spur nachverfolgen“, „nachzeichnen“ oder auch „ausfindig machen“. Dieser Begriff beschreibt exakt die Funktion, welche my**Trace**® in Ihrem Kontrollraum leisten wird: das revisionssichere „tracing“ von Rechner und Konsolen.

Mit my**Trace**® können Sie im Kontrollraum …

- … Ihrem Team einen blitzschnellen An- und Abmeldeprozess an allen Arbeitsplätzen und allen Konsolen ermöglichen. Kurzzeitiges Sperren oder Wechseln des Arbeitsplatzes, Schichtwechsel etc. erfolgen im Handumdrehen
- … nachvollziehen, welche Rechner zu welchem Zeitpunkt von welchem Mitarbeiter am Arbeitsplatz oder auf dem Großbildsystem bedient wurden
- … Tastatur- und Mausbedienung unterbinden, während der Monitorinhalt am Arbeitsplatz und auf dem Großbildsystem in Echtzeit dargestellt wird
- … bewusst nicht nachvollziehen, welche Tastatureingaben vom Mitarbeiter getätigt wurden
- … vorhandene Gruppenaccounts, technische User und Sammelaccounts bewusst beibehalten
- … auf Sicherheit zählen. Alle auf myTrace basierenden Authentifizierungs-Vorgänge sind mind. mit einem 128-Bit AES Schlüssel gesichert
- … vollkommen fexibel arbeiten, obwohl im Optimalfall alle im Kontrollraum stattfindenden Authentifizierungen kryptografisch gesichert sind
- … ein „free-seating“ Konzept umsetzen, welches auch höchste Sicherheits-Anforderungen erfüllt
- … einen Grafik-Controller oder eine MultiConsoling-Anlage einbinden
- … die Security-Compliance gemäß ISO 27001 und des BSI erfüllen

Blitzschneller Benutzerwechsel mit myTrace®

Mit myTrace® können beliebig viele Rechner unterschiedlichster Nutzer auf diverse Konsolen (Keyboard/Video/Mouse) nachvollziehbar geschaltet werden.

Ohne Authentifizierung ist das Bild der Konsole zwar sichtbar, über Tastatur und Maus jedoch nicht zu bedienen; dies gilt auch für Remote-Verbindungen. Das bedeutet, dass der Benutzer jederzeit den Arbeitsplatz verlassen kann und seine Teamkollegen dennoch die Tastatur und Maus mittels Ihrer eigenen Anmeldung wieder frei schalten können.

Sollte sich ein Mitarbeiter nicht abgemeldet haben und ein anderer meldet sich an der Konsole an, wird automatisch der vorherige Benutzer abgemeldet. Aufwendige und zeitintensive Zwangsabmeldungen entfallen komplett.

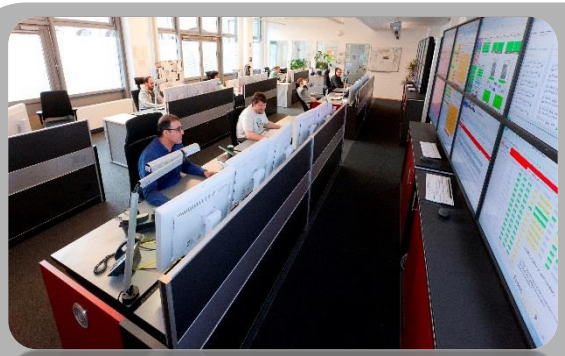
Vergessene Passwörter gehören der Vergangenheit an, da der An- und Abmeldevorgang mittels Karte erfolgt.

Die myTrace© Technologie:

- Die gesamte myTrace® Systemarchitektur ist mit 128 bit-aes extrem sicher verschlüsselt. Dazu zählt auch die „Luft-Schnittstelle“ zwischen Authentifizierungsmedium (die Karte) und dem Empfänger am Arbeitsplatz (das Lesegerät).
- Es ist keinerlei Software-Installation auf Ihren Rechnern nötig und somit kompatibel zu jedem Betriebssystem.
- Es erfolgt keine Speicherung biometrischer Merkmale der Mitarbeiter; myTrace® ist somit betriebsratkonform.
- Es werden keine Eingaben der Mitarbeiter ausgelesen, gespeichert oder verarbeitet; myTrace® ist somit datenschutzkonform.
- Als Authentifizierungsmedium ist die myTrace® RFID-Karte oder ein vorhandener kundenseitiger RFID-Träger einsetzbar (z.B. Chipkarte, Mitarbeiterausweis, …).
- Die Administrations-Oberfläche ist mit jedem aktuellen Web-Browser bedienbar; myTrace® ist somit höchst flexibel.


Der myTrace® Bedienkomfort & die Nachvollziehbarkeit:

- Die Anmeldung am Arbeitsplatz erfolgt blitzschnell und die „Default“-Konsolen (*) werden unmittelbar aufgeschaltet.
- Nach der Abmeldung bleiben die Bildinhalte am Arbeitsplatz und auf dem Großbildsystem weiterhin sichtbar – aber nicht mehr bedienbar!
- Beim Wechsel an einen anderen Arbeitsplatz „folgen“ die Default-Konsolen automatisch.
- Flexibles „free-seating“-Konzept mit absoluter Sicherheit & Nachvollziehbarkeit.
- Beim Holen, Wechseln oder Verschieben der Konsolen, werden diese Aktionen im Logbuch dokumentiert.
- Das Logbuch ist nur über eine 4-Augen-Authentifizierung einsehbar.



(*) Default-Konsolen: Konsolen, welche sich der Mitarbeiter als „Standard“ definiert. Dieses sollten die Konsolen sein, mit welchen die meiste Zeit gearbeitet wird.

Ambientlight

Das ereignisgesteuerte Ambientlight am optionalen StratosX11-Kontrollraumtisch signalisiert den my**Trace**®-Anmeldezustand.
Dies erfordert den Einsatz von Ambientlight-AlarmLichtband und Ambientlight-AlarmController.

Rotes RGB-LED-Lichtband

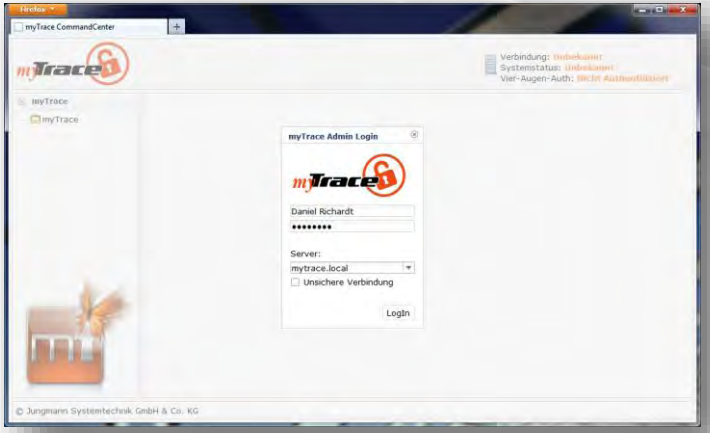
Arbeitsplatz wird nicht verwendet
(Mitarbeiter ist abgemeldet)

Grünes RGB-LED-Lichtband

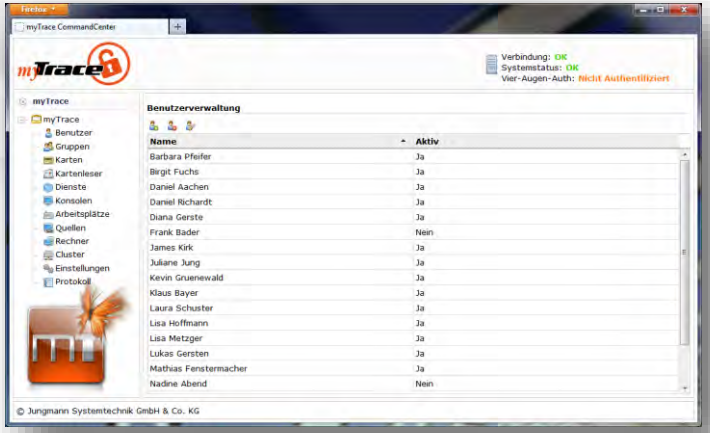
Arbeitsplatz wird aktiv verwendet
(Mitarbeiter ist angemeldet)

<u>Übersichtlich – das myTrace®-Logbuch:</u>
Welcher Rechner war zu welchem Zeitpunkt, an welchem Arbeitsplatz bei welchem Mitarbeiter im Zugriff?

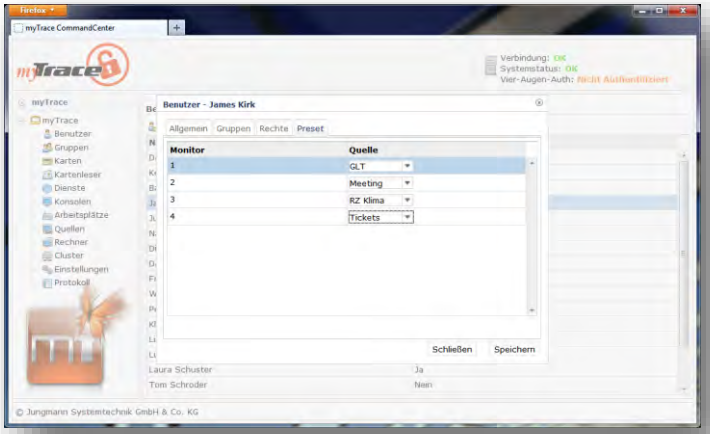
myTrace® unterscheidet dabei zwischen „Beobachten“ = nur ansehen (blauer Balken) oder „Vollzugriff“ = ansehen und bedienen (grüner Balken). Das Logbuch kann nur mit der 4-Augen-Authentifizierung eingesehen werden. Beispielsweise sind die dafür notwendigen Zugangskarten beim Abteilungsleiter und beim Betriebsrat hinterlegt. Das Logbuch kann NICHT allein durch ein Passwort eingesehen werden.



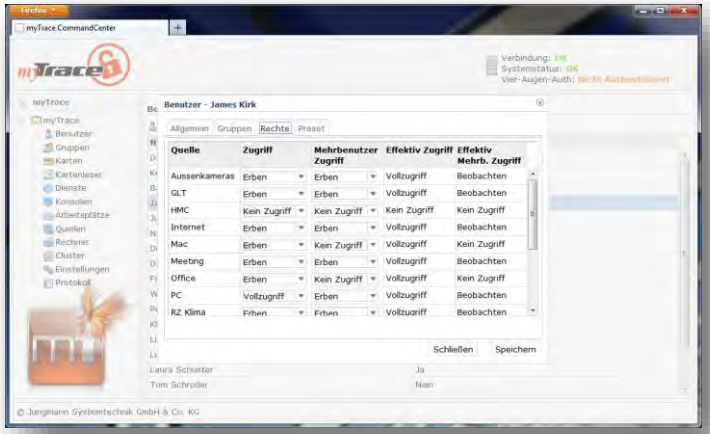
Login in die Admin-Bedienoberfläche mit Passwort und RFID-Karte



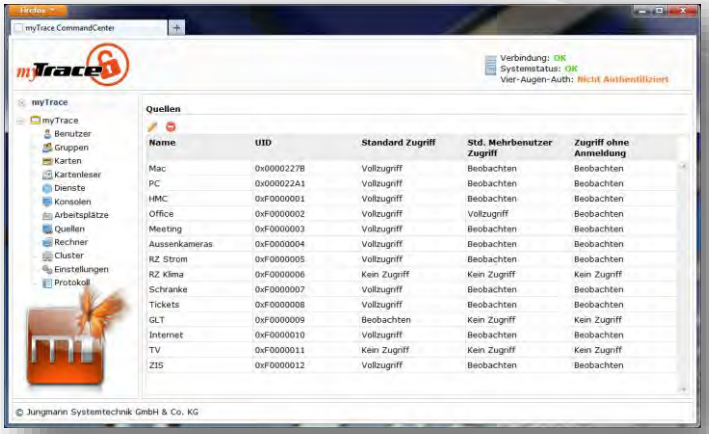
Links – Übersichtliche Navigation aller Bereiche
Rechts aufgeschlagen - Benutzerverwaltung



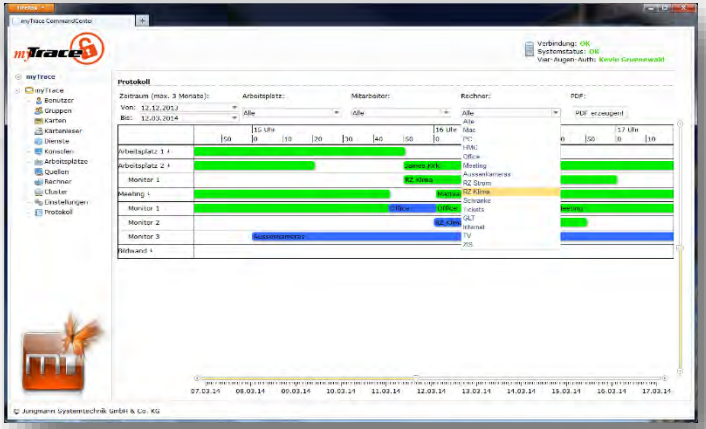
Default-Einstellung der Standard-Rechner
Welche Rechner sollen nach dem Login angezeigt werden?



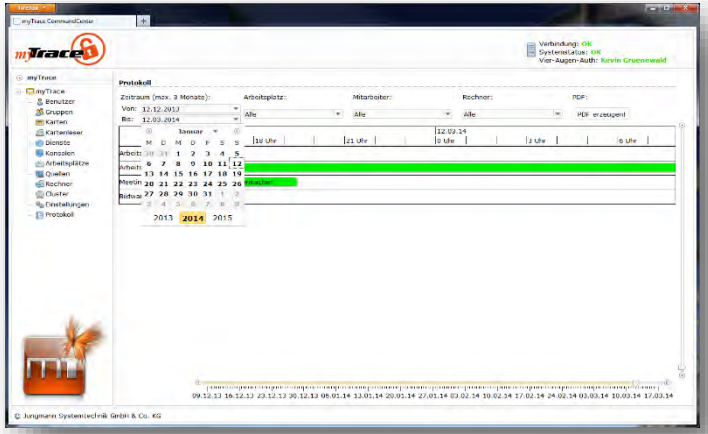
Detaillierte Rechtevergabe
Jeder Benutzer kann individuelle Rechte erhalten, damit Fehlbedienungen erst gar nicht möglich sind



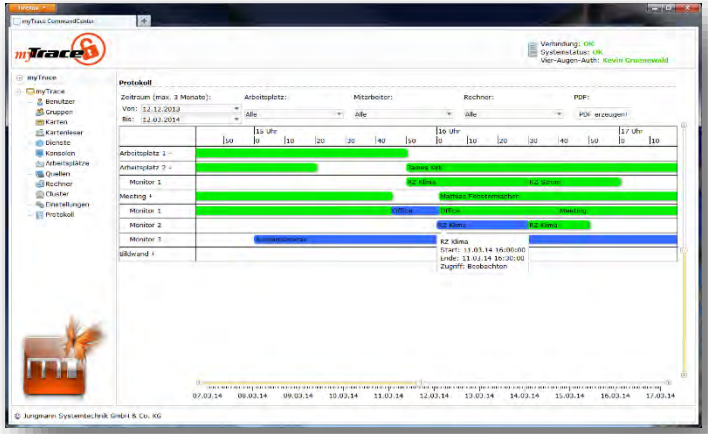
Standard-Rechtevergabe für jeden Rechner



Nach erfolgter 4 Augen Authentifizierung kann das Logbuch eingesehen werden



Auswahl des Zeitfensters Monat & Tag.



Ansicht im Detail: welche Mitarbeiter hatten den Rechner „Klima“ von 16.00 bis 16.30h bedient?

Made in Germany

Ein eingespieltes Team: Die Hard- und Softwarelösungen von JST!

Die my**Trace**® -Funktionen sind nahtlos in **Multi**Consoling®, **Cockpit**View® und **Pixel**Detection® integriert! Sämtliche Einstellungen in Bezug auf die Rechtevergabe wirken sich in **Multi**Consoling® und **Cockpit**View® aus.

Sie möchten myTrace vergleichen oder Sie benötigen Ausschreibungstexte?

Hier finden Sie die entsprechenden Textbausteine:

Im Projekt xxxxxxxx ist es geplant, ein neues Rechte-Management-System, nachfolgend mit RMS benannt, zu installieren. Große Teile der Signalquellen sind Rechner, auf denen die verschiedensten Monitoring-, Interventions- oder Kamerasysteme installiert sind, die von allen Mitarbeitern genutzt werden. Ein ständiger Benutzerwechsel (An- und Abmeldevorgang) ist sehr aufwändig und zeitintensiv. Ein allgemeines technisches User-Passwort, mit dem viele User auf einem Rechner ohne Benutzerwechsel arbeiten, ist verboten. Mit dieser Arbeitsweise würde eine erhebliche Sicherheitslücke entstehen. Es muss also stets nachvollziehbar sein, welcher Mitarbeiter hat zu welchem Zeitpunkt an welchem Rechner gearbeitet.

Ein neues RMS soll nun ein Höchstmaß an Sicherheit, Schnelligkeit und Benutzerfreundlichkeit bieten. In Verbindung mit einem „free-seating“-Konzept soll gleichzeitig die Flexibilität beim Arbeitsplatzwechsel gesteigert werden. Das RMS muss die Konsolen (Keyboard/Video/Mouse) an den Arbeitsplätzen oder, sofern im Einsatz, an den Großbildwänden schnell an- und abmelden sowie protokollieren können.

Das System ist mit den nachstehend aufgeführten Eigenschaften und Funktionen betriebsfertig zu implementieren. Sollten nachstehende Produkteigenschaften und Funktionen nicht eingehalten werden können bzw. nur geringfügig abweichen, führt dies zum Ausschluss des Bieters.

1. Damit die Mitarbeiter keine neuen Benutzerkennungen lernen bzw. sich Passwörter merken müssen, erhält jeder Mitarbeiter seine eigene RFID-Karte, die als Identifizierungsmerkmal gegenüber dem Schutzsystem dient. Diese Karten befinden sich im Lieferumfang des Bieters.
2. Ein Anmeldvorgang (Auflegen der RFID-Karte auf das Lesegerät) darf vom Zeitpunkt des Kartenauflegens bis zur Freischaltung der Konsole nicht länger als 10 Sekunden dauern. Sobald sich die RFID-Karte auf einem Kartenleser befindet, soll der Mitarbeiter Eingaben an den für Ihn freigeschalteten Rechnern vornehmen können. Die Lesegeräte befinden sich im Lieferumfang des Bieters.
3. Nach der Abmeldung (Entnahme der RFID-Karte vom Lesegerät) dürfen keine Eingaben mit Tastatur und Maus möglich sein – der Bildschirm muss jedoch immer in Echtzeit sichtbar bleiben und darf nicht eingefroren werden, damit die Teamkollegen auch ein abgemeldeten Rechner weiterhin überwachen können.
4. Das Sperren der Konsole erfolgt ohne Zeitverzögerung, d. h. direkt mit dem Entnehmen der RFID-Karte.
5. Über ein integriertes Logbuch muss lückenlos nachvollziehbar sein, welcher Mitarbeiter zu welchem Zeitpunkt welchen Rechner bedient hat. Eine Aufzeichnung der Tastatureingaben darf auf keinen Fall erfolgen.
6. Das Rechte-Management-System muss lückenlos in das MultiConsoling-Konzept der Arbeitsplätze und, sofern im Einsatz, der Großbildwand integriert werden.

7. Aus Sicherheitsgründen und aus Gründen der größtmöglichen Flexibilität und Stabilität ist die Installation von Software jeder Art auf den zu schützenden Rechnern nicht erlaubt! Der An- und Abmeldevorgang darf nicht im Betriebssystem des jeweiligen Rechners, sondern muss durch das übergeordnete RMS erfolgen. Durch diese System-Architektur muss zwingend gewährleistet sein, das Rechner mit verschiedensten Betriebssystemen in dieses Konzept eingebunden werden können. Ein späteres Update auf höhere Betriebssysteme darf keine Auswirkungen auf das RMS haben.
8. Es ist eine so genannte „free-seating“-Funktion zu installieren. Damit muss es möglich sein, dass nach der Anmeldung mittels RFID-Karte die Rechner, welche der Mitarbeiter als Favoriten angelegt hat, automatisch am Arbeitsplatz aufgeschaltet werden, an dem sich der Mitarbeiter nun befindet. Die Rechner müssen also dem Mitarbeiter folgen und nicht umgekehrt.
9. Es muss durch das Auflegen und Abnehmen der RFID-Karte möglich sein, dass eine Beleuchtung an den Arbeitsplatzmöbeln in z. B. grün/rot zu schalten. Hierdurch soll gewährleistet werden, dass jeder Mitarbeiter erkennt, ob ein Arbeitsplatz besetzt oder unbesetzt ist. Ebenfalls soll erkannt werden, dass ein Alarm an einem Platz dargestellt wird, der aller Voraussicht nach längere Zeit nicht besetzt sein wird.
10. Es ist zu berücksichtigen, dass nicht alle Signalquellen schützenswert sind. Das Schutzsystem muss entsprechend konfigurierbar sein. Nur bei zu schützenden Systemen ist ein Mehrfachzugriff mit Eingaberechten (schreibend) nicht gestattet.
11. Für einen schreibenden Mehrfachzugriff eines schützenswerten Rechners ist eine Queue zu führen. Wird der Schreibzugriff von einem Arbeitsplatz abgegeben, so erhält der nächste Arbeitsplatz in der Queue den Schreibzugriff. Lesend kann ein Mehrfachzugriff erfolgen.
12. Pro Mitarbeiter (resp. RFID-Karte) ist festzulegen, auf welche Rechner welcher Zugriff besteht (keiner, lesend, schreibend). Es ist festzulegen auf welche Rechner der Mitarbeiter Zugriff hat und in welcher Form, also lesend oder schreibend.
13. Sofern eine Großbildwand im Einsatz ist, ist diese in geeigneter Weise ebenfalls einzubinden, so dass über diesen Weg kein schreibender Mehrfachzugriff auf schützenswerte Rechner durchgeführt werden kann.
14. Die Konfiguration und das Anzeigen der Protokolle erfolgen webbasiert. Hierbei soll ein aktueller Browser (Internet Explorer, Firefox) genutzt werden.
15. Die komplette Datenkommunikation (inkl. der Luftschnittstelle zwischen RFID-Karte und Kartenleser) muss mind. 128-Bit AES verschlüsselt sein. Die gespeicherten Daten befinden sich in einer gesicherten Datenbank. Hierbei sind folgende Mindestvorgaben einzuhalten: Jegliche Kommunikation über das Netzwerk ist kryptografisch gesichert (verschlüsselt). Die hierzu nötigen Schlüssel werden mit einem asymmetrischen 4096-Bit RSA Schlüssel gesichert ausgehandelt. Die Identität des Partners wird hierbei fälschungssicher überprüft. Die anschließende Kommunikation ist mit einem 256-Bit AES Schlüssel verschlüsselt.
16. Die Logdateien sind nur nach dem 4-Augen-Prinzip einsehbar. So wird Datenmissbrauch vorgebeugt. Das 4-Augen-Prinzip muss wie folgt arbeiten: Erst nachdem zwei voneinander unterschiedlich Berechtigte, die beide über das Recht zum Einsehen der Protokolle verfügen, sich nacheinander mit Ihrer RFID-Karte identifiziert haben, ist der Zugriff auf diese Protokolle gestattet.