LÖSUNG IM ÜBERBLICK
CA IDENTITY SUITE

Mit Identity Management und Governance Anwender in Unternehmen unterstützen

Die Lücke zwischen der IT und Anwendern in Unternehmen schließen

ca technologies

Kurzfassung

Ausgangssituation

Als IT- oder Security-Führungskraft oder Geschäftsbereichsleiter leben Sie in bewegten Zeiten, die voller Herausforderungen stecken. IT-Umgebungen werden immer verteilter, komplexer und heterogener. Zu entscheiden, wer auf was zugreifen darf, und diese Richtlinien zuverlässig zu erzwingen, ist jedoch eine vielschichtige Herausforderung, die alle drei Gruppen gemeinsam angehen müssen: die IT, die Security und die Geschäftsbereiche.

Zugleich werden der IT häufig Budgets gekürzt und Ressourcen gestrichen, mit denen sie ihrer Verantwortung nachkommen kann. Sie benötigen also eine zuverlässige und kosteneffiziente Möglichkeit, die folgenden wichtigen Herausforderungen bei der Identität zu bewältigen:

- schnelles Onboarding neuer Anwender, damit sie so schnell wie möglich produktiv arbeiten können
- Sicherstellung, dass alle Anwender ausschließlich über die passenden Zugriffsberechtigungen für ihre aktuelle(n) Rolle(n) verfügen
- Automatisierung wichtiger Identitätsprozesse zur Erhöhung der Effizienz und Senkung von Kosten
- Erkennung und Verhinderung potenzieller Richtlinienverstöße (verwaiste Accounts, unangemessene Berechtigungen usw.), bevor sie auftreten
- Erfüllen von Auditing-Anforderungen, indem bekannt ist, wer auf was zugreifen kann

Einer der wichtigsten Faktoren in Umgebungen von heute ist zudem folgender:

- Bereitstellung einer einfachen und intuitiven Experience, damit Anwender in Unternehmen leicht und unkompliziert auf wesentliche Identitätsservices zugreifen können

Chance

Die stärkere Ausrichtung auf die Unterstützung von Anwendern in Unternehmen bringt viele Herausforderungen für die Anwender der meisten heute erhältlichen Identity-Management-Lösungen mit sich. Den sehr wenigen Lösungen, die eine akzeptable User Experience bieten, fehlen im Allgemeinen die Breite der Provisionierungs-, Rollenmanagement- und Governance-Funktionen und die nötige Skalierbarkeit zur Unterstützung des Identity Management im erweiterten Unternehmen. Dies zwingt Sie dazu, zwischen umfangreicher Funktionalität und Anwenderfreundlichkeit zu wählen.

CA Identity Suite hilft Ihnen auf einzigartige Weise, die Kluft zwischen aktuellen IAM-Technologien und Anwendern in Unternehmen zu überwinden. Diese integrierte Suite von Identity-Management- und -Governance-Funktionen kombiniert robuste Funktionalität mit einer intuitiven, unkomplizierten und Business-orientierten User Experience. Sie vereinfacht die Identity-Management-Prozesse, verbessert die Anwenderzufriedenheit, unterstützt On-Premise- und Cloud-Anwendungen und bietet Skalierbarkeit auf Verbraucherlevel. Und sie ist unkompliziert und schnell bereitgestellt.

Kritische Punkte für den Erfolg von Identity Management und Governance

In diesem White Paper werden einige wichtige Identity-Management-Herausforderungen der offenen Unternehmen von heute benannt und die Gründe beschrieben, aus denen diese Herausforderungen Ihr Unternehmen weiterbringen oder behindern können. Sie erhalten einen Überblick darüber, wie CA Identity Suite Ihrem Unternehmen helfen kann, diesen Herausforderungen erfolgreich zu begegnen.

Jede der folgenden Herausforderungen umfasst einen Business- und einen IT-Aspekt. In der Vergangenheit wurde der Schwerpunkt bei der User Experience für Identitätsservices vor allem auf die IT gelegt. Dies führte zu schwierigen Benutzeroberflächen und geringerer Zufriedenheit. Die heutige Umgebung erfordert eine Brücke zwischen der IT und den Anwendern in Unternehmen, um die Verwendung von Identitätsservices zu erweitern und die User Experience insgesamt zu verbessern. In diesem Beitrag werden die geschäftliche wie die technische Seite dieser Herausforderungen beleuchtet.

Die folgenden Aspekte setzen umfassende Planung voraus und sollten Teil jedes Implementierungsplans sein:

- **Anwenderakzeptanz** – Verbesserung und Vereinfachung der allgemeinen User Experience, um die Anwenderakzeptanz von Identitätsprozessen zu erhöhen
- **Zugriffsanfragen** – Vereinfachung des Prozesses, mit dem Anwender notwendigen Zugriff auf Anwendungen erhalten
- **Risikomanagement für Berechtigungen** – Verhinderung von Verstößen gegen Berechtigungsrichtlinien
- **Zugriffszertifizierungen** – Erhöhung der Produktivität von Managern
- **Zugriff auf Anwendersoftware** – Bereitstellung einer unkomplizierten Möglichkeit für Anwender für den Zugriff auf die wichtigsten Anwendungen
- **Identity-Echtzeitanalysen** – Gewährleistung effizienter grundlegender Identitätsservices
- **Probleme bei der Bereitstellung** – Verbesserung von ROI und Time-to-Value

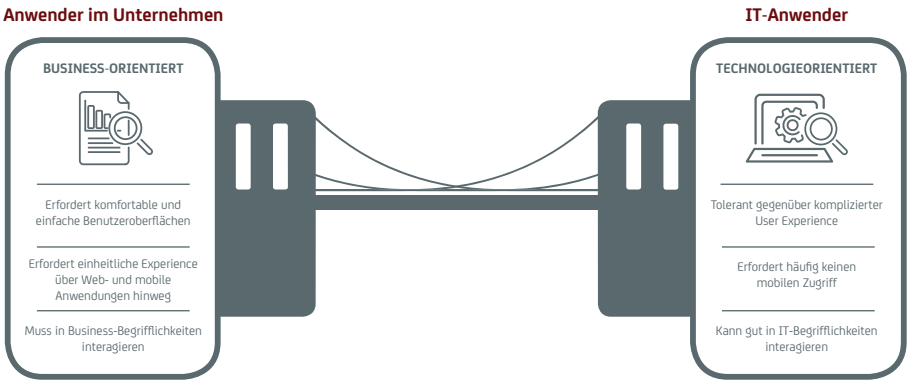
Herausforderung Anwenderakzeptanz

„Meine Anwender sind durch die komplizierte Benutzeroberfläche frustriert, die sie für viele nötige Identitätsfunktionen nutzen müssen. Dies begrenzt unsere Möglichkeiten wesentlich, diese Services für eine größere Anwendergruppe in meinem Unternehmen zu implementieren.“

Eine der größten Herausforderungen für erfolgreiche Identity-Management-Bereitstellungen besteht darin, dass die User Experience für Identitätsservices im Allgemeinen klar an der IT orientiert ist. Früher war dies vielleicht akzeptabel. Sobald jedoch das Identity Management über den Bereich der reinen IT-Anwender hinausgeht, ist dieser Ansatz nicht mehr effektiv. Begrifflichkeiten und Prozesse, die für IT-Anwender selbstverständlich sein mögen, führen bei den meisten Anwendern in Unternehmen zu Verwirrung und Frustration. Dies führt zu geringerer Akzeptanz von Identitätsprozessen, höherer Belastung der IT, fehlender Einhaltung von Vorschriften und Frustration der Anwender. Anwender benötigen leichte, schnelle Unternehmensanwendungen, die keine Schulung erfordern und auf dem Gerät ihrer Wahl zur Verfügung stehen. Sie müssen an die grundlegenden Identitätsprozesse herangeführt werden. Dies ist jedoch nur möglich, wenn die Experience für sie einfach, intuitiv und vor allem an Anwendern in Unternehmen statt an IT-Anwendern ausgerichtet ist.

CA Identity Suite

CA Identity Suite hilft Ihnen auf einzigartige Weise, die Kluft zwischen aktuellen IAM-Technologien und Anwendern in Unternehmen zu überwinden. Diese integrierte Suite von Identity-Management- und -Governance-Funktionen kombiniert robuste Funktionalität mit einer intuitiven, unkomplizierten und Business-orientierten User Experience. Durch die verbesserte Produktivität und Zufriedenheit von Anwendern in Unternehmen kann die User Experience von CA Identity Suite das Nutzenpotenzial der IAM-Lösung für große Unternehmen enorm steigern und der IT-Abteilung beträchtlichen Verwaltungsaufwand ersparen.



Einige der zahlreichen wichtigen Vorteile der Suite für die User Experience sind folgende:

- Berechtigungskatalog in Business-Begrifflichkeiten
- Dashboard und Launchpad für Webanwendungen und mobile Anwendungen
- alles an einem Ort – zentraler, müheloser Zugriff auf alle Identitätsservices für Anwender in Unternehmen
- warenkorbähnliche Experience für Zugriffsanfragen und Verfolgung
- Social-Network-ähnliche Experience für die Verfolgung von Zugriffsanfragen
- proaktive Vorschlagstools
- mobile Anwendung, mit der Anwender Identitäten jederzeit und überall verwalten können

CA Identity Suite erleichtert außerdem die Erzeugung individueller, kundenspezifischer Dashboards für die Anforderungen einzelner Rollen, wie Führungskräfte, Security-Beauftragte und Unternehmenspartner. Administratoren können eine Benutzeroberfläche anhand der Anwenderrolle und der Services konfigurieren, auf die der Anwender zugreifen kann. Die Benutzeroberfläche der Suite kann zudem mit Firmenlogos, Farbschemas, Schriftarten, ausgewählten Hintergrundbildern und mehr vollständig an das Branding Ihres Unternehmens angepasst werden. So gibt Ihr Portal die Unternehmensidentität klar wieder.

„Bei der Umfrage einer externen Analystenfirma gaben 97 % der befragten Kunden an, dass die User Experience mit CA Identity Suite andere Anbieter übertraf."

Quelle: TechValidate-Umfrage

Herausforderung Zugriffsanfragen

„Es ist für meine Anwender kaum möglich, den Zugriff auf Anwendungen und Systeme, die sie für ihre Arbeit brauchen, mühelos anzufordern. Der Prozess ist langwierig, und die Ressourcenbezeichnungen sind für die Mitarbeiter häufig verwirrend."

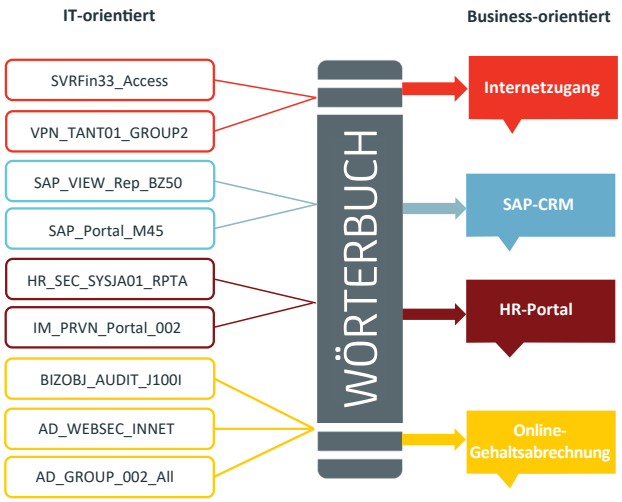
Anwender müssen Zugriff auf Anwendungen und Daten, die sie benötigen, schnell und leicht erhalten. Dabei müssen auch die geltenden Vorschriften eingehalten werden. Zugriffsanfragesysteme basierten bisher jedoch im Allgemeinen auf einem Satz von Berechtigungen, die für Administratoren entworfen wurden, die ihre Bedeutung kannten, und Anwendern aufgebürdet wurden, die die Terminologie der IT praktisch wie eine neue Sprache lernen mussten. Da immer mehr Anwender in Unternehmen mit den Identitätsprozessen des Unternehmens zu tun haben, behindert diese unintuitive Experience die Akzeptanz, verringert die Zufriedenheit und führt häufig dazu, dass die IT-Mitarbeiter doch helfen müssen, weil nur sie die Fragen der verwirrten Anwender beantworten können.

Eine neue Art der Interaktion mit Anwendern in Unternehmen ist erforderlich, und der Bereich der Zugriffsanfragen ist ein hervorragendes Beispiel für die Vorteile dieses neuen Ansatzes. Auch die IT hat jedoch in diesem Bereich berechtigte Anforderungen, wie die Automatisierung grundlegender Prozesse für Zugriffsanfragen und das mühelose Auditing von Anfragen und Genehmigungen. Funktionen, die die Automatisierungsanforderungen der IT erfüllen, aber auch leicht durch Anwender in Unternehmen genutzt werden können, sind also unerlässlich.

CA Identity Suite

CA Identity Suite bietet eine intuitive, einfache „Warenkorb"-Experience, die den Prozess für Zugriffsanfragen drastisch vereinfacht. Wie in dem Prozess, den sie von Einzelhandelswebseiten kennen, können Anwender unkompliziert Rollen und Berechtigungen, die sie für ihre Arbeit benötigen, in ihren Warenkorb legen, aktuelle Zugriffsberechtigungen anzeigen und den Status früherer Anfragen überprüfen.

Den Kern der einfachen, Business-orientierten User Experience von CA Identity Suite bildet der anwenderfreundliche Unternehmens-berechtigungskatalog. Er übersetzt kryptische Ressourcenbezeichnungen wie „TSS_MNG_per_view" in intuitivere Namen wie „Online-Gehaltsabrechnung", sodass Anwender in Unternehmen die benötigten Ressourcen leichter finden. Außerdem können Sie Anwendungen in logische Kategorien gruppieren, um den Zugriff weiter zu erleichtern, beispielsweise, indem Sie eine Gruppe „SRM-Zugriff" erstellen, die die SAP-Anwendungen, Oracle-Anwendungen und SalesForce-Funktionen enthält, die Anwender in Unternehmen im Allgemeinen benötigen – definiert in Begriffen, die diesen Anwendern vertraut sind. Die folgende Grafik zeigt die Zuordnung zwischen IT- und Business-Begriffen, die der Katalog bereitstellt.



CA Identity Suite umfasst proaktive Vorschlagstools, die den Zugriffsanfrageprozess wesentlich vereinfachen. Der Anwender kann Rollen und Zugriffsrechte anzeigen, die anhand seiner Eigenschaften vorgeschlagen werden. Diese proaktiven Vorschläge helfen dem Anwender, den richtigen Zugriff anzufordern. Außerdem stellen sie einen Risikowert bereit, der auf dem angeforderten Zugriff und den Risiken basiert, die dieses Zugriffsrecht bedeuten kann. Der Anwender kann dann eine fundiertere Entscheidung dazu treffen, welche Zugriffsanfrage für ihn geeignet ist.

Herausforderung Risikomanagement

„Manchmal werden Anwendern versehentlich Berechtigungen zugewiesen, die gegen unsere Security-Richtlinie verstoßen. Ich möchte, dass solche Verstöße verhindert werden, bevor sie auftreten."

Unpassende Anwenderberechtigungen sind die eigentliche Ursache einer Reihe in letzter Zeit an die Öffentlichkeit gedrungener Verstöße. Dies gilt vor allem für privilegierte Anwender, weil sie im Allgemeinen über sehr umfangreiche Berechtigungen verfügen. Das Prinzip ist jedoch für alle Anwender gleich: Unpassende Berechtigungen, die gegen die Security-Richtlinien verstoßen, müssen korrigiert werden, bevor sie erteilt werden („vorbeugende Kontrolle"). Wenn sie in der Vergangenheit bereits erteilt wurden, müssen sie widerrufen werden („reaktive Kontrolle"). Ohne effektive Kontrollen für beide Fälle steigt das Risiko, und Audits zur Einhaltung von Vorschriften werden problematischer.

Außerdem werden Richtlinien manchmal geändert, und Zugriffsrechte, die vor langer Zeit gewährt wurden, verstoßen dann gegen die neue Richtlinie. Bei regelmäßigen Zugriffszertifizierungen muss dies für den Manager transparent sein, damit dieser dem Anwender die Zertifizierung für diese Zugriffsberechtigung entziehen kann.

CA Identity Suite

Mit CA Identity Suite können Sie Sätze von Unternehmensprozessregeln (Business Process Rules, BPRs) formulieren, erzwingen und überprüfen, um die Aufgabentrennung und andere logische Einschränkungen für die Beziehungen zwischen Anwendern, Rollen und Berechtigungen zu implementieren. Beispielsweise kann mit einer Unternehmensprozessregel eine Einschränkung „Personen mit Zugriffsberechtigung für X dürfen keine Zugriffsberechtigung für Y erhalten" oder eine Abhängigkeitsbeziehung wie „nur Personen mit Zugriff für A dürfen auf B zugreifen" modelliert werden. So können Fälle, die gegen diese Security-Richtlinien verstoßen, verhindert werden, bevor sie auftreten.

Die Suite warnt Sie zudem, wenn Rechte angefordert werden, die miteinander in Konflikt stehen (mithilfe der oben beschriebenen vorbeugenden Kontrollen). Sie weist der Anfrage einen Risikowert zu, der auf dem angeforderten Zugriff und der zugehörigen Richtlinie basiert. Der Risikowert basiert auf dem Anwender, seinen sonstigen Berechtigungen und allen gegebenenfalls relevanten Kontextfaktoren. Dieser Risikolevel wird dem Anforderer mitgeteilt, wenn die Genehmigungsanfrage gestellt wird, um ihn bei potenziell unpassenden Anfragen zu warnen. Auch der Genehmiger sieht diesen Risikowert vollständig transparent im Genehmigungsprozess, sodass die Erteilung risikoreicher Zugriffsrechte verhindert werden kann.

Die Suite stellt außerdem reaktive Kontrollen bereit, um unpassende Zugriffsrechte aufzuheben, die bereits erteilt wurden. Die Suite führt bei der Zertifizierung Richtlinienprüfungen für den Zugriff aus und teilt Ihnen mit, ob der gegebene Anwender über unpassende Zugriffsrechte verfügt, die gegen Richtlinien verstoßen. Dem Manager werden Verstöße für jeden Anwender deutlich gekennzeichnet angezeigt, damit sofort Abhilfe geschaffen werden kann. Beide Arten von Kontrollen können das Risiko wesentlich reduzieren, dass unpassende Berechtigungen erteilt werden bzw. unerkannt bleiben.

Herausforderung Zugriffszertifizierung

„Ich möchte Zertifizierungen einfach und intuitiv gestalten, damit ich die Produktivität meiner Manager erhöhen und meine Compliance Audits vereinfachen kann."

Wie wichtig eine automatisierte Funktion ist, die Informationen zum Anwenderzugriff in die passende Sprache und das passende Format für jede Ihrer Zertifizierungskampagnen übersetzt, wurde bereits deutlich. Wenn Zugriffsnamen intuitiv und Business-orientiert sind, flexible Workflows für individuelle Anforderungen entworfen werden können und Verfolgung und Status jeder Kampagne leicht abrufbar sind, steigen die Erfolgschancen Ihres Zertifizierungsprogramms.

CA Identity Suite

Die Zertifizierungsfunktionen in CA Identity Suite basieren auf dem Unternehmensberechtigungskatalog, mit dem Manager die Zugriffsrechte jedes Mitarbeiters sehr leicht verstehen und die Zugriffsrechte jedes Anwenders leicht genehmigen, verweigern oder delegieren können. Außerdem steht Managern ein Risikowert zur Verfügung, wenn ein bestimmtes Zugriffsrecht oder eine Kombination von Rechten besonders risikoreich ist. Dank der transparenten Risikobewertungen ist die Zertifizierung nicht mehr nur eine Ja-Nein-Entscheidung, sondern es können Risiken hervorgehoben werden, die sonst nicht sichtbar wären.

CA Identity Suite ist so flexibel, dass sie viele unterschiedliche Arten von Zertifizierungskampagnen unterstützen kann, wie die folgenden:

- **Entitätszertifizierung**: wird verwendet, um die bestimmten Anwender-, Rollen- oder Ressourcenentitäten zugeordneten Zugriffsrechte durch Manager, Rollenverantwortliche oder Rollenverwalter zu zertifizieren.
- **Erneute Zertifizierung**: ermöglicht es Ihnen, die Zertifizierung basierend auf einer früheren Kampagne zu wiederholen.
- **Differenzielles Vorgehen**: startet eine Zertifizierungskampagne, die ausschließlich auf den Berechtigungen basiert, die seit einer früheren Kampagne geändert wurden.
- **Selbstbescheinigung**: ermöglicht es Anwendern – und nicht nur Managern oder Ressourcenverantwortlichen – ihre eigenen Berechtigungen zu zertifizieren. Diese Art von Kampagne kann eine Reihe juristischer Anforderungen an die Security-Zertifizierung für Daten erfüllen.

Zertifizierungskampagnen können mühsam, zeitaufwendig und im Endeffekt zur Risikosenkung ineffektiv sein. CA Identity Suite erhöht nicht nur die Effektivität dieses Prozesses aus Security- und Compliance-Sicht, sondern bietet auch eine einfache, sehr intuitive Experience, die Managern gefällt.

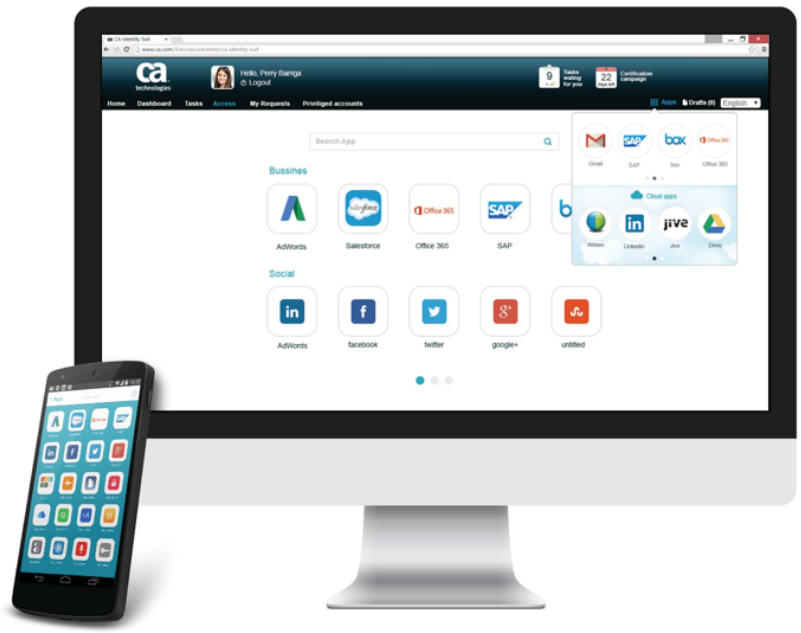
Herausforderung unkomplizierter Anwendungszugriff

„Ich möchte, dass meine Anwender sehr leicht auf ihre Anwendungen zugreifen können – in der Cloud und on-premise –, aber nur auf die, für die sie die passenden Zugriffsrechte besitzen. Außerdem möchte ich ihnen mühelosen Zugriff für alle ihre Geräte bereitstellen."

Anwender sind schnell frustriert, wenn sie mühsame Schritte durchführen müssen, um auf eine ihrer vielen Anwendungen zuzugreifen. Häufig beklagen sie, dass sie sich mehrmals anmelden müssen und Anwendungen nicht direkt starten können. Mit zunehmender Mobilität gewöhnen Anwender sich an den Komfort dieser Gerätebenutzeroberflächen, sodass die Frustration und die Herausforderungen für die Produktivität zunehmen. Benötigt wird eine unkomplizierte Methode für den schnellen und leichten Zugriff auf die Anwendungen jedes Anwenders, die Single Sign-On für alle diese Anwendungen bietet und den Zugriff auf die Anwendungen beschränkt, für die der jeweilige Anwender befugt ist.

CA Identity Suite

CA Identity Suite umfasst ein Launchpad für Web- und Mobilanwendungen, das Anwendern ein zentrales Dashboard bereitstellt, über das sie leicht und schnell auf alle autorisierten Web-, Cloud- und Mobilanwendungen zugreifen können. Das Launchpad ist über jedes Gerät zugänglich und bietet erweiterte Suchfunktionen. Nach der Anmeldung am CA Identity Portal kann der Anwender jede Webanwendung mit einem Mausklick öffnen. Außerdem stehen alle Anwendungen, auf die Anwender über ihren Desktop zugreifen, stets auch über CA Identity Portal Mobile zur Verfügung. Mit diesem Launchpad können Mitarbeiter unterwegs produktiv sein, da es ein vollständiges Single Sign-On für mobile Webanwendungen in einem mobilitätsfreundlichen Format bietet.



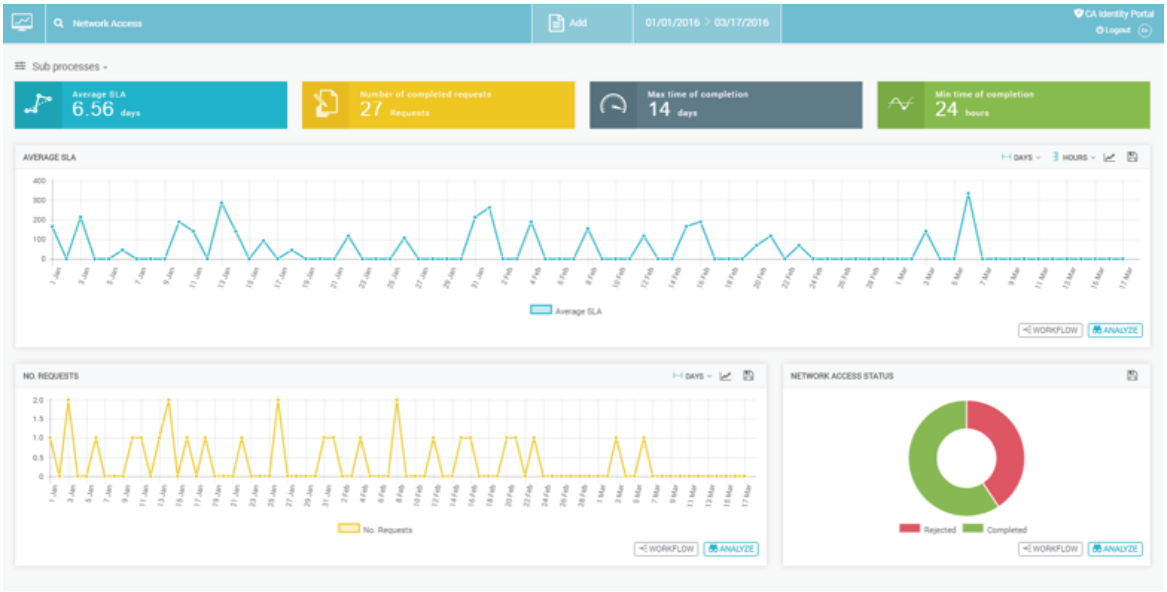
Herausforderung Prozesseffizienz zur Erfüllung von SLAs

„Einige Identitätsprozesse funktionieren nicht reibungslos, sodass sich andere Manager bei mir über die bereitgestellten Service Levels beschweren. Aber mir fehlen einfach Informationen zu den Engpassstellen, sodass ich sie auch nicht beseitigen kann."

Identitätsprozesse sind häufig komplex und können Workflowschritte in mehreren Phasen beinhalten. Laufen diese Prozesse nicht effizient ab, beispielsweise, wenn eine bestimmte Anwendergruppe ihre Aufgabe schlicht nicht fristgemäß erledigt, kann dies das gesamte System zum Erliegen bringen, sodass die Service-Level-Vorgaben nicht eingehalten werden können. Werden grundlegende Prozesse wie beispielsweise Zugriffszertifizierungen nicht gemäß den vereinbarten Servicezielen ausgeführt, folgen daraus Schwachstellen bei Audits oder auch einfach ein höherer Grad an Ineffizienz. Ohne ausreichend transparenten Einblick in die Details zum Ablauf dieser Prozesse lassen sich die Ursachen dieser Probleme nicht ermitteln, geschweige denn schnell beseitigen.

CA Identity Suite

Mit CA Identity Suite verfügen Sie über erweiterte Echtzeitanalysen, anhand derer Sie die Abläufe zu grundlegenden Identitätsprozessen wesentlich besser nachvollziehen und optimieren können. Auf diese Weise lassen sich Engpässe erkennen und wichtige SLAs erfüllen. Die folgende Abbildung illustriert ein einfaches Beispiel. Dargestellt ist eine zeitbasierte Ansicht aktueller SLAs im Vormonat sowie eine Reihe von Kennzahlen wie Durchschnitt, Maximum und Minimum zu den SLAs für einen gegebenen Prozess. Daneben ist die tägliche Zahl neuer Anforderungen im Vormonat sowie eine Dispositionsübersicht (abgeschlossen, abgelehnt) zu allen Anforderungen dargestellt. Mit dieser Funktion verfügen Manager über deutlich mehr Informationen, sodass sich Prozesse optimieren und der Gesamtstatus für alle Prozesse unkompliziert anzeigen lassen.



Herausforderung Bereitstellungsprobleme

„Es ist zeitintensiv und sehr aufwendig, die Identity-Management-Lösung bereitzustellen. Allein die Lösung zu installieren und zu konfigurieren, dauert Tage, und einige grundlegende Anwendungsfälle zum Laufen zu bringen, kann Wochen beanspruchen, weil ich eigenen Code entwickeln und Workflows, Richtlinien und die Benutzeroberfläche definieren muss."

Die Bereitstellung einer robusten Identity-Management-Lösung kann aufwendig und teuer sein. Bis einige grundlegende Funktionen betriebsfähig sind, können leicht Wochen vergehen. Zudem können Anforderungen wie Konnektoren für firmenspezifische Anwendungen Ressourcen und die verfügbare Zeit stark strapazieren.

CA Identity Suite

Mit folgenden Funktionen in CA Identity Suite lässt sich die Zeit bis zum einwandfreien Betrieb *erheblich* verkürzen:

- **Virtuelle Appliance (vApp).** Mit vApp entfällt die traditionelle Installationsphase, weil ein vorinstalliertes und vorkonfiguriertes Image einer virtuellen Maschine bereitgestellt wird, das sofort mit Produktionskonfigurationen auf gängigen Virtualisierungsplattformen eingesetzt werden kann. Die virtuelle Appliance umfasst ein gehärtetes Betriebssystem, einen Anwendungsserver und CA Identity Suite. Sie beinhaltet darüber hinaus integrierte Unterstützung für gängige DevOps-Verfahren wie Hochverfügbarkeitskonfigurationen, Kapazitätsanpassungen, Protokollaggregierungen, Plattform-Patches und Lösungsupdates.

  Zur Bereitstellung von Identitätsservices ziehen Sie den Servicenamen einfach auf den Namen der entsprechenden Maschine. Die Installation erfolgt dann automatisch. Wird ein Service auf mehreren Maschinen abgelegt, werden sämtliche Kommunikationsmechanismen für Hochverfügbarkeit (Lastverteilung, Failover usw.) automatisch übernommen. Zeitaufwendige und fehleranfällige manuelle Konfigurationsarbeiten entfallen. So sparen Sie enorm viel Zeit.

  Mit diesem Konzept lassen sich Time-to-Value und TCO umfassend reduzieren, sodass Sie bei unverändertem Team und Budget mehr erreichen. Mit diesem Verfahren lassen sich zudem jährlich Tausende Euro an Lösungslizenzkosten einsparen, weil sämtliche zentralen Systemkomponenten ohne Bedarf an weiteren Lizenzen nach Belieben bereitgestellt werden können.
- **Deployment Xpress (Depx).** DepX sorgt für grundlegende Verbesserungen bei der Bereitstellung von Identity-Management-Lösungen. Die Funktion umfasst eine Reihe vorkonfigurierter Anwenderszenarien für häufige Anwendungsfälle, die in den meisten Unternehmen benötigt werden, wie Anwender-Onboarding, Passwortzurücksetzung, Zugriffszertifizierungen, Partner-Onboarding usw. Jedes Szenario umfasst alle nötigen Elemente für die unkomplizierte Bereitstellung, wie Vorlagen für Benutzeroberflächen, Workflows und Richtliniendefinitionen. Manager wählen einfach die benötigten Szenarien aus, legen diese in den Warenkorb und gehen zur Kasse. Damit werden alle grundlegenden Elemente automatisch in Identity Suite geladen und bereitgestellt. Diese Elemente sind anpassbar (z. B. mit Corporate Branding für die Schnittstelle), ohne dass eigener Code programmiert werden muss. Die Szenarien beschleunigen den Bereitstellungsprozess und können die Time-to-Value bei der Bereitstellung typischer Identitätsservices deutlich verkürzen.
- **Sonstige Xpress-Tools.** Identity Suite umfasst noch weitere Tools, die die Verwaltung von Bereitstellungsumgebungen optimieren:
  - Connector Xpress vereinfacht die Erstellung von Konnektoren für selbst entwickelte Anwendungen und erleichtert den Aufbau von Verbindungen mit Systemen, für die keine sofort einsatzfähigen Konnektoren vorhanden sind.
  - Mit Config Xpress können Sie Komponenten schneller und leichter zwischen Staging-Umgebungen verschieben und so das Konfigurationsmanagement vereinfachen, damit mehr Zeit für funktionales Testing bleibt.
  - Mit Policy Xpress lassen sich Richtlinien für die Durchführung Ihrer individuellen, komplexen Unternehmensprozesse konfigurieren. Im Allgemeinen wird zu diesem Zweck firmenspezifischer Code entwickelt. Mit diesem assistentenbasierten Tool können Sie Richtlinien dagegen innerhalb von Stunden intern erstellen, statt Wochen mit Programmierarbeiten zu verbringen.

Schlüsselfunktionen

CA Identity Suite stellt die folgenden wichtigen Funktionen bereit:

- Self-Service-Identity-Portal („alles an einem Ort"): zentralisiert Berechtigungsdaten und bietet einen intuitiven Warenkorb für Zugriffsanfragen.
- Erheblich verkürzte Bereitstellungszeiten: von Tagen auf Minuten!
- Für Unternehmen optimierter Berechtigungskatalog: macht Zugriffsanfragen und die Berechtigungszertifizierung für Business-Mitarbeiter verständlicher.
- Proaktive Analysen: bieten Anwendern in Unternehmen Hinweise und Warnungen zu möglichen Richtlinienverletzungen und verhindern diese.
- Anwenderprovisionierung: für eine Vielzahl von On-Premise-Apps, SaaS-Services und nicht verbundenen Systemen möglich.
- Anwender-Self-Service: ermöglicht es Anwendern, ihre Informationen selbst zu verwalten, um die Belastung der IT zu verringern.
- Deployment Xpress: vereinfacht mit vorkonfigurierten Anwendungsfallvorlagen die Erstbereitstellung und die nachfolgende Verwaltung erheblich.
- Anpassung ohne firmenspezifischen Code: sorgt dank leistungsstarker Funktionen wie ConfigXpress, PolicyXpress und ConnectorXpress für die unkomplizierte Anpassung von Identity-Management-Infrastrukturen.
- Berechtigungsbereinigung: ermittelt vorhandene Systemberechtigungen und markiert übermäßige oder überflüssige Berechtigungen.
- Rollen-Modeling mit moderner, zum Patent angemeldeter Analyse-Engine: ermöglicht die effiziente Filterung auch großer Anwendergruppen und großer Mengen an Berechtigungsinformationen, um potenzielle Rollen zu erkennen.

ca technologies

Kontaktieren Sie CA Technologies unter ca.com/de.

CA Technologies (NASDAQ: CA) entwickelt Software, die Unternehmen bei der Umstellung auf die Application Economy unterstützt. Software steht in allen Branchen und in allen Unternehmen im Mittelpunkt. Von der Planung über die Entwicklung bis hin zu Management und Security arbeitet CA Technologies weltweit mit Unternehmen zusammen, um die Art, wie wir leben, Transaktionen durchführen und kommunizieren, neu zu gestalten – ob mobil, in der privaten oder öffentlichen Cloud oder in verteilten Systemen oder Mainframe-Umgebungen. Weitere Informationen finden Sie unter **ca.com/de**.

CS200-230014_1016