Unica Platform Version 12.1.1 Administratorhandbuch

Inhalt

Kapitel 1. Administratorhandbuch..... 1

Unica Platform features..... 1

Informationen zu Sicherheitsfunktionen in Unica Platform..... 1

Konfigurationsmanagement..... 4

Lokalisierung in Unica..... 4

Die gemeinsame Benutzeroberfläche..... 5

Anmelden bei Unica..... 6

Dokumentation und Hilfe zu Unica Platform..... 7

Lizenzierung - Übersicht..... 8

Lizenzierungsportal..... 9

Unica-Benutzerkontomanagement..... 13

Arten Benutzerkonten: intern und extern..... 13

Eigenschaften interner Benutzerkonten..... 14

Hinzufügen von internen Benutzerkonten..... 15

Löschen von internen Benutzerkonten..... 16

Ändern des Ablaufdatums für das Kennwort eines internen Benutzers..... 16

Zurücksetzen von internen Benutzerkennwörtern..... 17

Ändern der Eigenschaften von internen Benutzerkonten..... 17

Ändern des Systemstatus interner Benutzer..... 18

Hinzufügen von Datenquellen interner Benutzer..... 18

Ändern von Datenquellen interner Benutzer..... 19

Löschen von Datenquellen interner Benutzer..... 19

Seiten für Benutzermanagement..... 19

Ländereinstellung....24
Synchronisation externer Benutzer....25
Sicherheitsmanagement....25
Berechtigungen und Aufgaben des Sicherheitsadministrators in Unica Platform....26
Sonderzeichen in Rollen- und Richtliniennamen....27
Rollen und Berechtigungen in Unica Platform und Unica Campaign....28
Übersicht über Verwaltung des Benutzerzugriffs auf Anwendungen in Unica Platform....29
Arten von Grupen: intern und extern....29
Partitions- und Sicherheitsmanagement....30
Vorkonfigurierte Benutzer und Rollen....31
Partitionsübergreifende Administratorberechtigungen....34
Hinzufügen einer internen Gruppe....34
Hinzufügen einer Untergruppe....35
Löschen einer Gruppe oder Untergruppe....36
Ändern der Beschreibung einer Gruppe oder Untergruppe....36
Zuweisen einer Gruppe zu einer Partition....37
Hinzufügen eines Benutzers zu einer Gruppe oder Untergruppe....37
Entfernen eines Benutzers aus einer Gruppe oder Untergruppe....38
Seiten für Benutzergruppenmanagement....39
Erstellen einer Rolle....41
Ändern von Rollenberechtigungen....42
Entfernen einer Rolle aus dem System....42
Zuordnen einer Rolle zu einer Gruppe oder Entfernen einer Rolle aus einer Gruppe....43

Zuweisen einer Rolle zu einem Benutzer und Entfernen einer Rolle..... 44
Definitionen von Berechtigungsstatus..... 44
Berechtigungen für Produkte, die nur Basisrollen verwenden..... 45
Berechtigungen für Unica Platform..... 48
Berechtigungen für Opportunity Detect..... 49
Konfigurationsmanagement..... 51
Eigenschaftskategorien..... 52
Eigenschaftsbeschreibungen..... 54
Aktualisierungsfunktion..... 54
Standardbenutzervorgabe für die Ländereinstellung..... 55
Navigieren zu einer Kategorie..... 55
Bearbeiten von Eigenschaftswerten..... 56
Erstellen einer Kategorie aus einer Vorlage..... 56
Löschen einer Kategorie..... 57
Dashboard-Management..... 58
Planung von Dashboards..... 58
Dashboardzielgruppen..... 58
Erforderliche Benutzerberechtigungen zum Anzeigen von Dashboards..... 59
Vordefinierte Portlets..... 59
Vorgefertigte Dashboards..... 69
IBM® Cognos® Bericht Leistungsaspekte..... 72
Dashboardkonfiguration..... 74
Quick Link-Portlets..... 82
Benutzerdefinierte Portlets..... 84
Verwalten der Dashboardzugehörigkeit..... 92

Unica-Scheduler..... 93

Scheduler-Trigger, die bei Erfolg oder Fehler von Ausführungen gesendet werden..... 95

Vom Abschluss mehrerer Ausführungen abhängige Zeitpläne..... 96

Planen der von externem Script gesendeten Trigger..... 98

Scheduler-Wiederholungsstruktur..... 99

Zeitzonenunterstützung..... 100

Schedulerrichtwerte..... 101

Whitelist-Voraussetzung für externe Aufgaben (nur mit FixPack 10.0.0.1)..... 103

Bewährte Verfahren zur Konfiguration von Zeitplänen..... 106

Um Assistent „Zeitplan erstellen“..... 106

Ausführen von Ausschlüssen..... 114

Aspekte bei der Verwendung des Schedulers mit Unica Campaign..... 121

Zeitplanbenachrichtigungen..... 127

Zeitplanmanagement..... 130

Auf SAML 2.0 basierende föderierte Authentifizierung..... 141

Implementieren der föderierten Authentifizierung..... 144

Zugehörige Konzepte..... 157

Einmalige Anmeldung (Single Sign-on) zwischen Unica und IBM Digital Analytics aktivieren..... 158

Konfigurieren der einmaligen Anmeldung (Single Sign-on; SSO) zwischen Unica und Digital Analytics mit automatischer Benutzerkontenerstellung..... 160

Konfigurieren der einmaligen Anmeldung zwischen Unica und Digital Analytics mit manueller Benutzerkontenerstellung..... 163

Konfigurieren von WebLogic für einmalige Anmeldung zwischen Digital Analytics und Unica..... 165

Konfigurieren von WebSphere® für einmalige Anmeldung zwischen Digital Analytics und Unica....166

Digital Analytics-Integration mit Websense mithilfe eines angepassten Proxys....166

Integration zwischen Unica und Windows™indows Active Directory....171

Funktionen bei der Integration in Active Directory....171

Voraussetzungen für die Integration in Active Directory....175

Roadmap für den Konfigurationsprozess: Integration in Active Directory....175

Integration zwischen Unica und LDAP-Servern....188

Funktionen bei der Integration in LDAP....189

Voraussetzungen für die LDAP-Integration....193

Roadmap für den Konfigurationsprozess: LDAP-Integration....193

Integration mit Plattformen zur Webzugriffskontrolle....204

Informationen zu Kontextstammverzeichnissen....207

Voraussetzungen für die SiteMinder-Integration....207

Integrationsvoraussetzungen für IBM Security Access Manager....213

Roadmap für den Konfigurationsprozess: Unica mit einer Webzugriffssteuerung integrieren....223

Konfigurieren der Integration mit SSL-Typ „WebSEAL-Junction“....227

Alert- und Benachrichtigungsmanagement....228

Alert- und Benachrichtigungsabonnements....229

Konfigurieren von E-Mail-Benachrichtigungen in Unica....230

Implementierung von unidirektionalem SSL....231

Übersicht über SSL-Zertifikate....232

Client- und Serverrollen in Unica....233

SSL in Unica....234

Roadmap für den Konfigurationsprozess: SSL implementieren in Unica..... 236
Zertifikate für SSL.....237
Konfigurieren Sie Ihren Webanwendungsserver für SSL..... 247
HCL Unica für SSL konfigurieren.....248
Überprüfen der SSL-Konfiguration.....263
Nützliche SSL-Links.....263
Datenschutzniveau-Einstellungen für WebLogic..... 264
Datenschutzniveau-Einstellungen für WebSphere.....264
Sicherheitsframework für Unica-APIs.....265
Erzeugung und Management von Datenfiltern.....269
Übersicht über das Erstellen von Datenfiltern..... 269
Roadmap für den Konfigurationsprozess: Datenfilter erstellen.....272
XML-Datenfilterreferenz.....280
Beispiel: Manuelles Angeben von Datenfiltern..... 291
Beispiel: Gruppe von Datenfiltern automatisch generieren..... 299
Informationen zum Zuweisen von Benutzern und Gruppen in der XML..... 310
Informationen zum Zuweisen von Benutzern und Gruppen über die Benutzerschnittstelle..... 320
Hinzufügen von Datenfiltern nach Erstellung des ersten Satzes..... 323
Prüfereignisüberwachung in Unica..... 324
Einschränkungen bei der Prüfereignisüberwachung.....325
Traditionelle Prüfereignisse..... 325
Rückwirkende Änderungen..... 326
Berechtigungen zum Anzeigen des Prüfereignisberichts in Umgebungen mit mehreren Partitionen.....326
Aktivieren und Inaktivieren der Ereignisprüfung.....327

Die Prüfereignisse konfigurieren, die im Bericht erscheinen sollen..... 327
Inhalt und Anzeige des Prüfberichts ändern..... 328
Felder im Fenster „Berichtsparameter“..... 329
Felder und Schaltflächen im Prüfereignisbericht..... 330
Archivierte Prüfereignisse..... 332
Konfigurieren der Benachrichtigungen über die Sicherung von Prüfereignissen..... 333
Exportieren des Prüfereignisberichts..... 334
Optimieren des Exports des Prüfereignisberichts für große Ereignisvolumen..... 334
Unica Platform-Systemprotokoll..... 335
Konfiguration des Systemprotokolls..... 337
Aktivieren der Protokollierung für einzelne Benutzer..... 339
Unica Platform-Dienstprogramme..... 344
So richten Sie Platform-Dienstprogramme auf zusätzlichen Maschinen ein..... 347
Dienstleistungen..... 349
Unica Platform-SQL-Scripts..... 373
ManagerSchema_DeleteAll.sql..... 373
ManagerSchema_PurgeDataFiltering.sql..... 374
ManagerSchema_DropAll.sql..... 374
SQL-Scripts für die Erstellung von Systemtabellen..... 375
Unica-Konfigurationseigenschaften..... 377
Unica Platform-Konfigurationseigenschaften..... 377
Digital Analytics-Konfigurationseigenschaften..... 484
Berichtskonfigurationseigenschaften..... 486
Unica Plan Konfigurationseinstellungen..... 486

Unica Campaign Konfigurationseigenschaften..... 486

Unica Deliver Konfigurationseigenschaften.....487

Unica Interact Konfigurationseigenschaften..... 487

Konfigurationseigenschaften von Unica Journey.....487

Konfigurationseigenschaften von Unica Content Integration.....487

Unica Collaborate Konfigurationseigenschaften.....487

IBM SPSS Modeler Advantage Enterprise Marketing Management Edition-Konfigurationseigenschaften..... 488

Opportunity Detect und Unica Interact Advanced Patterns - Konfigurationseigenschaften..... 491

Anpassung von Style-Sheets und Bildern in Unica-Benutzeroberfläche.....500

Vorbereiten des Corporate Theme..... 501

Anwenden des Corporate Theme.....502

Index.....

Kapitel 1. Administratorhandbuch

Unica Platform features

Unica Platform stellt Sicherheits-, Konfigurations-, Benachrichtigungs- und Dashboardfunktionen für Unica Produkte bereit.

Unica Platform stellt eine anwendungsübergreifende Benutzeroberfläche für Unica Produkte sowie die Infrastruktur für die folgenden Funktionen bereit.

- Unterstützung für Berichterstellung in vielen Produkten von Unica.
- Unterstützung für Sicherheit in Anwendungen, einschließlich Authentifizierung und Autorisierung.
- Konfigurationsverwaltung, beispielsweise das Festlegen der Ländereinstellungen des Benutzers und eine Benutzeroberfläche zum Bearbeiten von Konfigurationseigenschaften für einige Unica-Anwendungen.
- Ein Scheduler, mit dem Sie einen Vorgang konfigurieren können, der in bestimmten Zeitabständen ausgeführt werden soll.
- Dashboardseiten, die so konfiguriert werden können, dass für Benutzergruppen mit unterschiedlichen Rollen im Unternehmen nützliche Informationen darin enthalten sind.
- Unterstützung und Benutzeroberfläche für Alerts und Benachrichtigungen.
- Sicherheitsprüfungsberichte.

Informationen zu Sicherheitsfunktionen in Unica Platform

Die Sicherheitsfunktionen in Unica Platform setzen sich aus einem zentralen Repository und einer webbasierten Schnittstelle zusammen, in denen Unica-interne Benutzer definiert und Benutzern verschiedene Zugriffsebenen auf die Funktionen innerhalb der Unica-Anwendungen zugewiesen werden.

Unica-Anwendungen nutzen die Unica Platform-Sicherheitsfunktionen, um Benutzer zu authentifizieren, die Benutzerzugriffsrechte auf Anwendungen zu überprüfen und Datenbankanmeldeinformationen sowie andere erforderliche Berechtigungsnachweise zu speichern.

In Unica Platform verwendete Sicherheitstechnologien

In Unica Platform werden standardisierte Verschlüsselungsmethoden verwendet, um die Authentifizierung durchzuführen und die Sicherheit in sämtlichen Unica-Anwendungen durchzusetzen. Benutzer- und Datenbank-Kennwörter werden über unterschiedliche Verschlüsselungstechnologien geschützt.

Berechtigungsverwaltung über Rollen

Unica Platform definiert den Basiszugriff eines Benutzers auf Funktionen in den meisten Unica-Anwendungen. Zudem können Sie für Unica Campaign und Unica Platform den Benutzerzugriff auf Funktionen und Objekte innerhalb der Anwendung steuern.

Sie können Rollen mehrere Berechtigungen zuordnen. Danach haben Sie folgende Möglichkeiten zur Verwaltung der Benutzerberechtigungen:

- Zuweisen von Rollen an einzelne Benutzer
- Zuweisen von Rollen an Gruppen und Zuordnen des Benutzers zu dieser Gruppe

Informationen zu Partitionen in Unica Campaign

Unica Platform unterstützt Partitionen in der Unica Campaign-Produktfamilie. Partitionen stellen eine Möglichkeit dar, Daten in Verbindung mit unterschiedlichen Benutzergruppen zu sichern. Wenn Sie Unica Campaign oder eine zugehörige Unica-Anwendung für die Funktion mit mehreren Partitionen konfigurieren, wird den Anwendungsbenutzern jede Partition als separate Instanz der Anwendung und ohne Anzeichen dafür, dass andere Partitionen auf demselben System vorhanden sind, angezeigt.

Informationen über Gruppen

Eine Untergruppe übernimmt die Rollen, die den übergeordneten Gruppen zugeordnet wurden. Ein Administrator kann eine unbegrenzte Anzahl von Gruppen definieren, und ein Benutzer kann mehreren Gruppen angehören. Auf diese Weise können problemlos unterschiedliche Rollenkombinationen erstellt werden. Ein Benutzer kann z. B. ein Unica Deliver-Administrator und ein Unica Campaign-Benutzer ohne Administratorberechtigungen sein.

Eine Gruppe kann nur einer Partition zugeordnet sein.

Verwalten der Berechtigungsnachweise für Datenquellen

Sowohl Benutzer als auch Administratoren können die Berechtigungsnachweise für die Datenquelle eines Benutzers vorab festlegen, damit der Benutzer diese nicht eingeben muss, wenn er mit einer Anwendung arbeitet, für die Zugriffsberechtigungen auf die Datenquelle erforderlich sind.

Integration mit externen Benutzer- und Gruppenverwaltungssystemen

Unica Platform kann für die Integration mit externen Systemen konfiguriert werden, mit denen Benutzer und Ressourcen zentral verwaltet werden. Dazu zählen der Windows™ Active Directory Server, andere unterstützte LDAP-Verzeichnisserver und Plattformen zur Webzugriffskontrolle wie Netegrity SiteMinder und IBM® Security Access Manager. Dadurch werden Fehler vermieden und Supportkosten reduziert, und es wird weniger Zeit für die Bereitstellung einer Produktionsanwendung benötigt.

Unterstützung für SAML 2.0

Unica Platform unterstützt SAML (Security Assertion Markup Language) 2.0 in folgenden Bereichen.

- Föderierte SAML 2.0-Authentifizierung. Diese Funktion ermöglicht die einmalige Anmeldung (SSO = Single Sign-on) für verschiedene Anwendungen.

  Sie können die föderierte Authentifizierung verwenden, um Single Sign-on zwischen Unica Anwendungen und anderen Anwendungen oder Anwendungen eines anderen Anbieters zu implementieren.

  Die Unica Platform-Installation enthält die folgenden Komponenten, die eine föderierte Authentifizierung unterstützen.

  - Die WAR-Datei eines Identitätsprovider-Servers.
  - Eine Client-JAR-Datei, die Sie mit Java™-Anwendungen verwenden können, um SAML 2.0-Zusicherungen zu generieren und zu analysieren. Die Java™-Produkte, die Sie mit Unica verknüpfen, verwenden die Zusicherungen, um mit dem Identitätsproviderserver zu kommunizieren.
- Single Sign-on mit SAML 2.0

Für diese Integration ist ein SAML 2.0-IdP-Server mit vollem Funktionsumfang erforderlich.

Nachdem Sie die erforderlichen Konfigurationseigenschaften und eine Metadatendatei eingerichtet haben, werden Benutzer, die versuchen, sich über die Unica Platform-Anmeldeseite anzumelden, über den SAML 2.0.IdP-Server (Identitätsprovider) Ihres Unternehmens authentifiziert.

Benutzer, die bei einer Anwendung angemeldet sind, die den IdP-Server für die Authentifizierung verwendet, können auf HCL Unica zugreifen, ohne sich nochmals anmelden zu müssen.

Datenfilter

Unica Platform unterstützt konfigurierbare Datenfilter, mit denen Sie Einschränkungen für den Datenzugriff in Unica-Produkten festlegen können. Datenfilter ermöglichen es, die Kundendaten zu beschränken, die ein Unica-Benutzer in Anwendungen anzeigen und bearbeiten kann.

Konfigurationsmanagement

Die Seite „Konfiguration“ bietet Zugriff auf die zentralen Konfigurationseigenschaften für Unica-Anwendungen.

Benutzer mit Admin-Berechtigungen in Unica Platform können die Seite „Konfiguration“ verwenden, um Folgendes durchzuführen:

- Suchen nach Konfigurationseigenschaften, die in einer Hierarchie aus Kategorien und Unterkategorien nach Produkt angeordnet sind
- Bearbeiten der Werte von Konfigurationseigenschaften
- Löschen bestimmter Kategorien (bei Kategorien, die gelöscht werden können, wird auf der Seite „Einstellungen“ der Link **Kategorie löschen** angezeigt)

Mithilfe des Dienstprogramms configTool, das in Unica Platform bereitgestellt wird, können Sie zusätzliche Änderungen auf der Seite „Konfiguration“ vornehmen.

Lokalisierung in Unica

Unica Platform unterstützt die Lokalisierung durch die Zeichensatzcodierung und dadurch, dass ein Administrator Ländereinstellungen für einzelne Benutzer oder alle Benutzer festlegen kann. Benutzer können zudem ihre eigenen Ländereinstellungen festlegen.

Sie können die Ländereinstellungen für interne und externe Benutzer, für jeden Benutzer einzeln oder für alle Anwendungen festlegen, die diese Funktion unterstützen. Diese Voreinstellung wirkt sich auf die Ansicht der Sprache, Uhrzeit, Zahlen und Datumsangaben in Unica-Anwendungen aus.

Unica Platform unterstützt UTF-8 als Standard-Zeichensatzcodierung. Damit können Benutzer Daten in allen Sprachen eingeben (z. B. Chinesisch oder Japanisch). Beachten Sie jedoch, dass die vollständige Unterstützung aller Zeichensätze in Unica Platform auch von der Konfiguration folgender Komponenten abhängt:

- Die Datenbank der Unica Platform-Systemtabellen.
- Die Clientmaschinen und Browser, über die der Zugriff auf Unica erfolgt.

Die gemeinsame Benutzeroberfläche

Unica Platform stellt einen gemeinsamen Zugriffspunkt und eine Benutzeroberfläche für Unica-Anwendungen bereit.

Die gemeinsame Benutzeroberfläche stellt die folgenden Funktionen bereit.

- Wenn mehrere Unica-Produkte installiert sind, können Sie zwischen den Produkten navigieren, ohne neue Fenster zu öffnen.
- Sie können eine Auflistung der zuletzt besuchten Seiten anzeigen und über das Menü **Zuletzt besucht** zurück zu einer dieser Seiten navigieren.
- Sie können eine Unica-Seite als Startseite festlegen (die erste Seite, die nach der Anmeldung angezeigt wird) und jederzeit zu dieser Seite zurückkehren, indem Sie auf das Symbol für die Startseite klicken.
- Über das Feld **Suchen** können Sie auf die Suchfunktionen aller installierten Produkte zugreifen. Der Kontext dieser Suchfunktion ist die Seite, die Sie anzeigen. Wenn Sie z. B. eine Liste von Kampagnen in Unica Campaign anzeigen, werden bei einem

Suchlauf alle Kampagnen durchsucht. Wenn Sie nach einem Unica Plan-Projekt suchen möchten, müssen Sie die Suche ausführen, während Sie eine Liste von Unica Plan-Projekten anzeigen.

Anmelden bei Unica

Verwenden Sie diese Prozedur, um sich bei Unica anzumelden.

Sie benötigen das Folgende.

- Eine Intranet-(Netz-)Verbindung, um auf den Unica-Server zuzugreifen.
- Einen auf dem Computer installierten Browser, der auch unterstützt wird.
- Benutzername und Kennwort, damit Sie sich bei Unica anmelden können.
- Die URL, um im Netz auf Unica zuzugreifen.

Die URL ist:

`http://host.domain.com:port/unica`

Wo

`host` ist das System, auf dem Unica Platform installiert ist.

`domain.com` ist die Domäne, in der sich die Hostmaschine befindet.

`port` ist die Portnummer, auf welcher der Unica Platform-Anwendungsserver empfangsbereit ist.

Anmerkung: Für das folgende Verfahren wird vorausgesetzt, dass Sie mit einem Konto angemeldet sind, das über Administratorzugriff für Unica Platform verfügt.

Greifen Sie über den Browser auf die Unica-URL zu.

- Falls Unica für die Integration mit Windows™ Active Directory oder mit einer Plattform zur Webzugriffssteuerung konfiguriert ist und Sie bei diesem System angemeldet sind, wird die Standarddashboardseite angezeigt. Ihre Anmeldung ist abgeschlossen.
- Wenn die Anmeldeanzeige angezeigt wird, melden Sie sich mit den Standardberechtigungsnachweisen für Administratoren an. Verwenden Sie in einer

Umgebung mit nur einer Partition `asm_admin` mit `password` als Kennwort. Verwenden Sie in einer Umgebung mit mehreren Partitionen `platform_admin` mit `password` als Kennwort.

Sie werden aufgefordert, das Kennwort zu ändern. Sie können das vorhandene Kennwort eingeben. Aus Sicherheitsgründen sollten Sie jedoch ein neues Kennwort verwenden.

- Falls Unica für die Verwendung mit SSL konfiguriert ist, werden Sie bei der erstmaligen Anmeldung eventuell aufgefordert, ein digitales Sicherheitszertifikat anzunehmen. Klicken Sie auf **Ja**, um das Zertifikat anzunehmen.

War die Anmeldung erfolgreich, zeigt Unica die Standarddashboardseite an.

Mit den Unica Platform-Administratorkonten zugeordneten Standardberechtigungen können Sie mithilfe der im Menü **Einstellungen** aufgeführten Optionen Benutzerkonten und Sicherheitsaspekte verwalten. Wenn Sie für Unica-Dashboards Administrationsaufgaben auf der höchsten Ebene ausführen möchten, müssen Sie sich als **platform_admin** anmelden.

Dokumentation und Hilfe zu Unica Platform

Unica Platform stellt Dokumentation und Hilfe für Benutzer, Administratoren und Entwickler bereit.

Tabelle 1. Installation und Aktualisierung

Task	Dokumentation
Eine Liste mit neuen Funktionen, bekannten Problemen und Problemumgehungen anzeigen	*Unica Platform Freigeben Notes®*
Informationen zur Struktur der Unica Platform-Datenbank	*Unica Platform Handbuch für Systemtabellen*
Installation oder Upgrade von Unica Platform und Bereitstellung der Unica Platform-Webanwendung	Eines der folgenden Handbücher:

Tabelle 1. Installation und Aktualisierung (Fortsetzung)

Task	Dokumentation
	• *Unica PlatformInstallationshandbuch* • *Unica Platform Aktualisierungshandbuch*
Implementieren Sie die mit Cognos® bereitgestellten Berichte in Unica	UnicaInstallations- und Konfigurationshandbuch für -Berichte

Tabelle 2. Unica Platform konfigurieren und verwenden

Task	Dokumentation
• Konfigurations- und Sicherheitseinstellungen für Produkte anpassen • Integration mit externen Systemen wie beispielsweise LDAP und Webzugriffskontrolle • Einmalige Anmeldung (SSO = Single Sign-on) mit verschiedenen Anwendungen mithilfe der auf SAML 2.0 basierenden föderierten Authentifizierung oder Single Sign-on implementieren • Dienstprogramme ausführen, um Produkte zu warten • Prüfereignisüberwachung konfigurieren und verwenden • Zeitplanausführung von Unica-Objekten	*Unica PlatformAdministratorhandbuch*

Lizenzierung - Übersicht

HCL Unica Produkte sind lizenzbasiert und die Benutzer müssen erforderliche Lizenzen mit den Produkten konfigurieren, damit sie beginnen können.

Im folgenden finden Sie eine Auflistung der Unica-Produkte, für die eine Lizenz obligatorisch ist:

- Unica Platform
- Unica Campaign
- Unica Interact
- Unica Deliver
- Unica Journey

Nachdem Benutzer eine saubere Installation oder ein Upgrade von 12.1-Version von Unica-Produkten durchgeführt und Unica-Produkte bereitgestellt haben, müssen Benutzer die Lizenz konfigurieren. Während der Benutzer die Unica Platform URL besucht, leitet er die Anzeige auf den Bildschirm für die Lizenzdetails um. Benutzer müssen die Lizenzen so konfigurieren, dass Sie mit den Unica-Produkten gestartet werden. Erst nach Angabe gültiger Lizenzinformationen werden Benutzer an die Unica Platform-Anmeldeseite umgeleitet.

Lizenzierungsportal

Das Lizenzportal bietet sowohl Softwareverteilung als auch Verwaltung Ihrer Softwareberechtigungen, die Sie von HCL Products and Platforms erworben haben. Die Portal bietet Ihnen Kontrolle und Flexibilität darüber, wie Sie Ihre Lizenzen verbrauchen können. Außerdem können Sie die Lizenzen registrieren. In der Regel wird in einer Organisation jemand als Lizenzmanager identifiziert, der über eine Vertrautheit mit der Sprache der Lizenzen verfügt, und wahrscheinlich möchten Sie ihn als Benutzer hinzufügen. Falls nicht, sind diese Anweisungen ausreichend dafür, um mit der Nutzung Ihrer HCL Software loszulegen.

Lizenzen und Verbrauchsdetails

Benutzer können die Details des Lizenzverbrauchs über das Häkchen der Lizenzen sowie über die Unica Platform Lizenzdetails-Seite durch Navigieren auf der Seite Einstellungen > Lizenzierungsdetails aktivieren. Wenn Sie auf die Seite Lizenzdetails anzeigen klicken, wird die Anzahl der Lizenzverbrauchsanzahl für alle berechtigten Produkte angezeigt. Falls es keine Verbindung mit dem Lizenzserver gibt, kann der Lizenzverbrauch heruntergeladen und mit Unica geteilt werden.

Produktname	HCL Unica-Produktnamen, für den die Berechtigung zugewiesen ist

Lizenztyp	Zeitspanne/Ewig
Startdatum	Beginn des Nutzungsrechts
Ablaufdatum	Verfallsdatum der Berechtigung (nicht anwendbar für die ewige Lizenz)
Verfügbare Berechtigungen	Die Gesamtzahl der Berechtigungen, die für ein Gerät oder einen Server bereitgestellt werden.
Verbrauchte Berechtigungen	Die bis jetzt verbrauchten Berechtigungen
Berechtigungen für Überziehungen	Verwendetes Lizenzierungsmodell, aktuelles Modell unterstützt unbegrenzte Überziehungen. (Nicht zutreffend für die ewige Lizenz)
Verbrauchte Überziehungen	Unterschied zwischen verfügbaren und überzogenen Berechtigungen. (Nicht zutreffend für die ewige Lizenz)

Weitere Informationen zur Lizenzierung finden Sie im HCL Unica Lizenzhandbuch.

Lizenzkonfiguration

Benutzer müssen die Lizenz mit HCL Unica-Produkten konfigurieren, bevor Sie mit der Verwendung beginnen. Wenn Benutzer auf die Unica Platform URL zugreifen, werden Sie auf die Seite "Lizenzkonfiguration" umgeleitet. Benutzer müssen die Lizenzdetails auf dieser Seite konfigurieren. Unica Marketing Platform validiert die Lizenz und bei einer erfolgreichen Lizenzkonfiguration werden Benutzer an den Unica Marketing Platform Anmeldebildschirm weitergeleitet.

Lizenzserver	URL der Lizenzserver-API, der Benutzer kann die URL des Lizenzservers vom HCL Lizenzportal abrufen.
Benutzer	HCL Lizenzserver – für jedes Gerät, wird standardmäßig der Benutzer "admin" unterstützt.
Kennwort	Kennwort für das Gerät festgelegt

Unica Umgebungstyp	Der Benutzer kann angeben, ob es sich um eine "Produktions-" oder um eine "Nicht-Produktions-"Umgebung handelt.
Proxy	Verwenden Sie den Proxy-Server, um eine Verbindung zum HCL Lizenzportal herzustellen. Verwenden Sie den Proxy-Server, wenn Sie nicht über abgehende Zugriffsrechte für das HCL Lizenzportal verfügen.
Proxy-Host	Der Hostname oder die IP-Adresse des Proxy-Servers.
Proxy-Port	Proxyserver-Port
Proxy-Benutzer	Proxy-Server
Proxy Password (Proxy-Kennwort)	Kennwort für Proxy-Server-Benutzer.

Alle diese Lizenzserverdetails werden in Unica Platform gespeichert. Benutzer können zur Seite Einstellungen > Lizenzierungsdetails navigieren, wenn die Lizenzdetails geändert werden müssen.

Verfügbarkeit des Lizenzservers

HCL Unica-Produkte müssen immer mit der HCL License Portal verbunden sein. HCL Unica-Produkte werden unzugänglich, wenn zwischen HCL Unica Products und HCL License Portal Server seit 5 Stunden keine Konnektivität mehr vorhanden ist. Benutzer werden zur Seite "Lizenzdetails" weitergeleitet. Sobald die Konnektivität zwischen HCL Unica und HCL License Server etabliert ist, können Benutzer auf die Anwendung zugreifen. HCL Unica-Produkte aktualisieren die Verbrauchsdetails im HCL Lizenzportal alle 10 Minuten. Im Falle eines Konnektivitätssproblems hilft den Wert des-Contributs, die Unica Platform und sobald die Konnektivität hergestellt ist, wird der Verbrauch auf dem Portal der Lizenz aktualisiert

Lizenzverbrauchsdetails

Benutzer können die Details des Lizenzverbrauchs über das Häkchen der Lizenzen sowie über die Seite Unica Platform Lizenzierungsdetails aktivieren. Der Benutzer kann zur Seite Einstellungen > Lizenzierungsdetails navigieren. Wenn Sie auf die Seite Lizenzdetails anzeigen klicken, werden die Lizenzverbrauchsanzahl für alle berechtigten Produkte angezeigt.

Produktname	HCL Unica-Produktnamen, für den die Berechtigung zugewiesen ist
Lizenztyp	Zeitspanne/Ewig
Startdatum	Beginn des Nutzungsrechts
Ablaufdatum	Verfallsdatum der Berechtigung (nicht anwendbar für die ewige Lizenz)
Verfügbare Berechtigungen	Die Gesamtzahl der Berechtigungen, die für ein Gerät oder einen Server bereitgestellt werden.
Verbrauchte Berechtigungen	Die bis jetzt verbrauchten Berechtigungen
Berechtigungen für Überziehungen	Verwendetes Lizenzierungsmodell, aktuelles Modell unterstützt unbegrenzte Überziehungen. (Nicht zutreffend für die ewige Lizenz)
Verbrauchte Überziehungen	Unterschied zwischen verfügbaren und überzogenen Berechtigungen. (Nicht zutreffend für die ewige Lizenz)

Auf der Seite Lizenzdetails wird die Nachricht angezeigt, dass "keine Lizenzen für diese Umgebung konfiguriert sind, da diese Umgebung nicht Produktionsumgebung ist". Wenn Sie die-Umgebung als nicht Produktionsumgebung ausgewählt haben, während Sie Lizenzdetails angeben.

Wenn Sie eine nicht Produktionsumgebung als Produktionsumgebung vornehmen müssen. Sie können die Lizenzdetails ändern und den Umgebungstyp als "Produktion" markieren. Wenn Sie diese Umgebung als Produktionsumgebung markieren, müssen Sie alle Lizenzdetails eingeben.

Anmerkung: Auf der Seite "Lizenzdetails" werden nur die aktiven Berechtigungen von HCL Unica-Produkten angezeigt.

Ausführliche Informationen hierzu finden Sie im Unica Lizenzierungsdokument.

Unica-Benutzerkontomanagement

Sie können die Attribute von Benutzerkonten, die über die Unica Platform-Benutzeroberfläche erstellt wurden, verwalten. Diese Konten werden als interne Konten bezeichnet. Sie werden durch diese Bezeichnung von externen Benutzerkonten abgegrenzt, die aus einem externen System importiert werden, z. B. aus einem LDAP-Server oder einem System für die Webzugriffskontrolle.

Externe Konten werden über das externe System verwaltet.

Arten Benutzerkonten: intern und extern

Wenn Unica mit einen externen Server integriert ist (beispielsweise mit einem unterstützten LDAP-Server oder einem System zur Webzugriffskontrolle), werden zwei Arten von Benutzerkonten (interne und externe Gruppen) unterstützt: intern und extern

- **Intern** - Benutzerkonten, die über die Unica-Sicherheitsbenutzeroberfläche in erstellt wurden. Diese Benutzer werden über Unica authentifiziert.
- **Extern** - Benutzerkonten, die durch Synchronisation mit einem externen Server in Unica importiert wurden. Diese Synchronisation geschieht nur dann, wenn Unica für die Integration in den externen Server konfiguriert wurde. Diese Benutzer werden über den externen Server authentifiziert. Beispiele für externe Server sind LDAP-Server und Server für die Webzugriffskontrolle.

Abhängig von der Konfiguration haben Sie möglicherweise nur interne Benutzer, nur externe Benutzer oder eine Kombination aus beiden Benutzertypen haben. Wenn Sie Unica mit Windows™ Active Directory integrieren und LDAP aktivieren, sind nur externe Benutzer möglich.

Weitere Informationen zur Integration von Unica mit einem LDAP- oder Windows™ Active Directory-Server finden Sie in den entsprechenden Abschnitten dieses Handbuchs.

Verwalten von externen Benutzern

Die Attribute externer Benutzerkonten werden normalerweise über das externe System verwaltet. Innerhalb von Unica können Sie die folgenden Aspekte eines externen Benutzerkontos steuern: Datenquellen, Benachrichtigungseinstellungen und Ländereinstellungen für Unica-Anwendungen sowie Mitgliedschaften in internen Gruppen (jedoch nicht in externen Gruppen).

Bestimmen von internen und externen Benutzern in der Unica-Benutzeroberfläche

Im Unica-Abschnitt „Benutzer“ haben interne und externe Benutzer unterschiedliche Symbole.

- Interne Benutzer - 
- Externe Benutzer - 

Eigenschaften interner Benutzerkonten

Administratoren können die Eigenschaften von Benutzerkonten verwalten, die mit der Unica Platform-Benutzeroberfläche erstellt wurden.

Ein Benutzer hat ein Kennwort vergessen

In Unica Platform werden Kennwörter von internen Benutzern in Hash-Form gespeichert und können nicht mehr in Klartext wiederhergestellt werden. Sie müssen Benutzern mit einem internen Konto, die ihr Kennwort vergessen haben, ein neues Kennwort zuordnen.

Zurücksetzen eines Kennworts

Benutzer mit einem internen Konto können ihr Kennwort selbst ändern, indem sie das ursprüngliche Kennwort angeben und das neue Kennwort eingeben und bestätigen. Der

Unica-Administrator kann nach Bedarf ebenfalls das Kennwort eines beliebigen Benutzers zurücksetzen.

Ablaufdaten für Kennwörter

Auf der Seite „Konfiguration“ können Sie Ablaufintervalle für die Kennwörter aller Benutzer festlegen. Zudem können Sie Ablaufdaten für einzelne Benutzer festlegen, wenn das systemweite Ablaufdatum nie abläuft.

Systemstatus von Benutzerkonten

Der Systemstatus eines Benutzers ist entweder „aktiv“ oder „inaktiviert“. Ein Benutzer mit einem inaktivierten Konto kann sich nicht an Unica-Anwendungen anmelden. Wenn ein inaktiviertes Benutzerkonto zuvor aktiv war und mindestens einer Gruppe angehört hat, können Sie dieses Benutzerkonto erneut aktivieren. Wenn Sie ein inaktiviertes Benutzerkonto wieder aktivieren, bleibt die Gruppenzugehörigkeit erhalten.

Alternative Anmeldung

Für jedes Benutzerkonto kann eine alternative Anmeldung angegeben werden. Eine alternative Anmeldung ist in der Regel erforderlich, wenn der Unica Campaign-Listener auf einem UNIX™-System als Root ausgeführt wird.

Datenquellen

Ein Benutzer benötigt die entsprechenden Berechtigungsnachweise, um auf die Datenquellen zuzugreifen, die von einigen Unica-Anwendungen genutzt werden. Diese Berechtigungsnachweise können als Datenquellen in den Eigenschaften des Benutzerkontos eingegeben werden.

Wenn ein Benutzer in einer Unica-Anwendung wie Unica Campaign arbeitet und dazu aufgefordert wird, Datenquelleninformationen einzugeben, speichert die Unica-Anwendung diese Informationen im Unica Platform-Datenspeicher. Diese Datenquellen erscheinen in der Liste der Datenquellen eines Benutzers in Unica Platform, auch wenn sie nicht mit der Unica-Benutzeroberfläche erstellt wurden.

Hinzufügen von internen Benutzerkonten

Verwenden Sie diese Prozedur, um interne Benutzerkonten hinzuzufügen.

1. Klicken Sie auf **Einstellungen > Benutzer**.
2. Klicken Sie auf **Neuer Benutzer**.
3. Füllen Sie das Formular aus und klicken Sie auf **Änderungen speichern**.

   Verwenden Sie Sonderzeichen in Anmeldenamen mit Vorsicht. Zulässige Sonderzeichen werden im Verweis der Seite „Neuer Benutzer“ aufgeführt.
4. Klicken Sie auf **OK**.

   Der Name des neuen Benutzers wird in der Liste angezeigt.

Löschen von internen Benutzerkonten

Verwenden Sie diese Prozedur, um interne Benutzerkonten zu löschen.

Wichtig: Werden Unica Campaign-Berechtigungen so eingerichtet, dass der Besitz oder Zugriff auf ein Unica Campaign-Objekt auf einen einzelnen Benutzer beschränkt ist, so kann nach dem Löschen dieses Benutzerkontos nicht mehr auf das Objekt zugegriffen werden. Stattdessen sollten Sie solche Konten inaktivieren anstatt sie zu löschen.

1. Klicken Sie auf **Einstellungen > Benutzer**.
2. Klicken Sie auf den Benutzernamen des Kontos, das Sie löschen möchten.
3. Klicken Sie auf **OK**.

Ändern des Ablaufdatums für das Kennwort eines internen Benutzers

Verwenden Sie diese Prozedur, um das Datum des Kennwortablaufs für interne Benutzer zu ändern.

Einschränkung: Wenn die systemweite Eigenschaft für den Kennwortablauf **Allgemeines | Kennworteinstellungen | Gültigkeit (in Tagen)** auf den Wert „0“ gesetzt ist, kann das Kennwortablaufdatum eines internen Benutzers nicht geändert werden.

1. Klicken Sie auf **Einstellungen > Benutzer**.
2. Klicken Sie auf den Benutzernamen.
3. Klicken Sie am unteren Rand der Seite auf den Link **Eigenschaften bearbeiten**.
4. Ändern Sie das Datum im Feld **Kennwortablauf**.
5. Klicken Sie auf **OK**.

Zurücksetzen von internen Benutzerkennwörtern

Verwenden Sie diese Prozedur, um interne Benutzerkennwörter zurückzusetzen.

1. Klicken Sie auf **Einstellungen > Benutzer**.

   Im linken Teilfenster wird die Liste **Benutzer** angezeigt.
2. Klicken Sie auf den Benutzernamen, den Sie ändern möchten.
3. Klicken Sie am unteren Rand der Seite auf den Link **Kennwort zurücksetzen**.
4. Geben Sie das neue Kennwort in das Feld **Kennwort** ein.
5. Geben Sie das gleiche Kennwort in das Feld **Bestätigen** ein.
6. Klicken Sie auf **Änderungen speichern**, um die Änderungen zu speichern.
7. Klicken Sie auf **OK**.

Anmerkung: Wenn Benutzerkennwörter zurückgesetzt werden, werden Benutzer aufgefordert, ihr Kennwort bei der nächsten Anmeldung in einer Unica-Anwendung zu ändern.

Ändern der Eigenschaften von internen Benutzerkonten

Verwenden Sie diese Prozedur, um die Eigenschaften interner Benutzerkonten zu ändern.

1. Klicken Sie auf **Einstellungen > Benutzer**.
2. Klicken Sie auf den Namen des Kontos, das Sie ändern möchten.
3. Klicken Sie am unteren Rand der Seite auf den Link **Eigenschaften bearbeiten**.
4. Bearbeiten Sie die Felder je nach Bedarf.
5. Klicken Sie auf **Änderungen speichern**, um die Änderungen zu speichern.
6. Klicken Sie auf **OK**.

Ändern des Systemstatus interner Benutzer

Verwenden Sie diese Prozedur, um den Systemstatus interner Benutzer zu ändern.

1. Klicken Sie auf **Einstellungen > Benutzer**.
2. Klicken Sie auf den Namen des Kontos, das Sie ändern möchten.
3. Klicken Sie am unteren Rand der Seite auf den Link **Eigenschaften bearbeiten**.
4. Wählen Sie in der Dropdown-Liste **Status** den Status aus. Die Optionen **AKTIV** und **DEAKTIVIERT** sind verfügbar.

   Anmerkung: Wenn Sie die Option **DEAKTIVIERT** auswählen, kann der Benutzer sich nicht mehr an Unica-Anwendungen anmelden. Benutzer mit Administratorzugriff auf Unica Platform können ihr eigenes Konto nicht deaktivieren.

5. Klicken Sie auf **Änderungen speichern**, um die Änderungen zu speichern.
6. Klicken Sie auf **OK**.

Hinzufügen von Datenquellen interner Benutzer

Verwenden Sie diese Prozedur zum Hinzufügen von Datenquellen interner Benutzer.

1. Klicken Sie auf **Einstellungen > Benutzer**.
2. Klicken Sie auf den Namen des Kontos, das Sie ändern möchten.
3. Klicken Sie unten auf der Seite auf den Link **Datenquellen bearbeiten**.
4. Klicken Sie auf **Neue hinzufügen**.

5. Füllen Sie das Formular aus und klicken Sie auf **Änderungen speichern**, um Ihre Änderungen zu speichern.
6. Klicken Sie auf **OK**.

Ändern von Datenquellen interner Benutzer

Verwenden Sie diese Prozedur, um Kennwörter oder Anmeldenamen für Datenquellen zu ändern.

1. Klicken Sie auf **Einstellungen > Benutzer**.
2. Klicken Sie auf den Namen des Kontos, das Sie ändern möchten.
3. Klicken Sie unten auf der Seite auf den Link **Datenquellen bearbeiten**.
4. Klicken Sie für den **Datenquellennamen**, den Sie ändern möchten, auf Datenquellenname.
5. Bearbeiten Sie die Felder.

   Falls Sie kein neues Kennwort angeben wird das alte Kennwort verwendet.
6. Füllen Sie das Formular aus und klicken Sie auf **Änderungen speichern**, um Ihre Änderungen zu speichern.
7. Klicken Sie auf **OK**.

Löschen von Datenquellen interner Benutzer

Verwenden Sie diese Prozedur, um Datenquellen interner Benutzer zu löschen.

1. Klicken Sie auf **Einstellungen > Benutzer**.
2. Klicken Sie auf den Namen des Kontos, das Sie ändern möchten.
3. Klicken Sie unten auf der Seite auf den Link **Datenquellen bearbeiten**.
4. Klicken Sie auf den Namen der Datenquelle, den Sie ändern möchten.
5. Klicken Sie auf **Löschen**.
6. Klicken Sie auf **OK**.

Seiten für Benutzermanagement

Sehen Sie sich diese Tabelle an, wenn Sie Hilfe beim Ausfüllen der Felder auf der Seite für Benutzer benötigen.

Seite „Neuer Benutzer“

Tabelle 3. Felder der Seite „Neuer Benutzer“

Feld	Beschreibung
Vorname	Der Vorname des Benutzers.
Nachname	Der Nachname des Benutzers.
Anmeldung	Der Anmeldename des Benutzers. Dies ist das einzige erforderliche Feld. Nur die folgenden Sonderzeichen sind in Anmeldenamen zulässig. • Groß- und Kleinbuchstaben (A bis Z, a bis z) • Zahlen (0 bis 9) • Kommerzielles A-Zeichen (@) • Bindestrich (-) • Unterstrich (_) • Punkt (.) • Doppelbyte-Zeichen (z.B. chinesische Zeichen) Verwenden Sie keine anderen Sonderzeichen (einschließlich Leerzeichen) in Anmeldenamen.
Passwort	Ein Kennwort für den Benutzer. Befolgen Sie bei der Erstellung eines Kennworts diese Regeln.

Tabelle 3. Felder der Seite „Neuer Benutzer“ (Fortsetzung)

Feld	Beschreibung
	• Bei Kennwörtern ist die Groß- und Kleinschreibung zu beachten. So ist beispielsweise `kennwort` nicht das Gleiche wie `Kennwort`. • Verwenden Sie eine beliebige Kombination aus Zeichen bei der Erstellung oder Änderung von Kennwörtern in Unica. Weitere Bedingungen für die Erstellung von Kennwörtern finden Sie auf der Seite „Konfiguration“. Um die Bedingungen für Ihre Installation von Unica anzuzeigen, klicken Sie auf den Link **Kennwortregeln** neben dem Feld **Kennwort**.
Kennwort bestätigen	Das gleiche Kennwort, das Sie auch im Feld **Kennwort** eingegeben haben.
Titel	Der Titel des Benutzers.
Department	Die Abteilung des Benutzers.
Unternehmen	Das Unternehmen des Benutzers.
Land	Das Land des Benutzers.
Adresse	Die Adresse des Benutzers.
Telefon (geschäftlich)	Die geschäftliche Telefonnummer des Benutzers.
Mobiltelefon	Die Mobiltelefonnummer des Benutzers.
Telefon (privat)	Die private Telefonnummer des Benutzers.
E-Mail-Adresse	Die E-Mail-Adresse des Benutzers. Der Inhalt dieses Feldes muss den in RFC 821 definierten Richtlinien bezüglich E-Mail-Adressen entsprechen. Weitere Informationen finden Sie unter RFC 821.

Tabelle 3. Felder der Seite „Neuer Benutzer“ (Fortsetzung)

Feld	Beschreibung
Alternative Anmeldung	Der UNIX™-Anmeldename des Benutzers, falls vorhanden. Eine alternative Anmeldung ist in der Regel erforderlich, wenn der Unica Campaign-Listener auf einem UNIX™-System als Root ausgeführt wird.
Status	Wählen Sie in der Dropdown-Liste AKTIV oder INAKTIVIERT aus. AKTIV ist standardmäßig ausgewählt. Inaktivierte Benutzer können sich an keiner Unica-Anwendung anmelden.

Seite „Eigenschaften bearbeiten“

Mit Ausnahme der in der folgenden Tabelle enthaltenen Felder sind die Felder identisch mit denen auf der Seite „Neuer Benutzer“.

Tabelle 4. Felder auf der Seite „Eigenschaften bearbeiten“

Feld	Beschreibung
Passwort	Dieses Feld ist auf der Seite „Eigenschaften bearbeiten“ nicht verfügbar.
Anmeldung	Dieses Feld ist auf der Seite „Eigenschaften bearbeiten“ nicht verfügbar.
Kennwortablauf	Das Datum im Format der Ländereinstellung (für Deutsch beispielsweise `TT.MM.JJJJ`). Sie können das Ablaufdatum eines Benutzers nicht ändern, wenn das systemweite Ablaufdatum nie abläuft.
IBM® Digital Analytics-Benutzername	Wenn die Integration mit IBM Digital Analytics aktiviert ist und Sie Benutzer manuell erstellen möchten, geben Sie den Digital Analytics-Benutzernamen des Benutzers hier im Rahmen des Konfigurationsprozesses ein.

Seite „Kennwort zurücksetzen“

Tabelle 5. Felder auf der Seite „Kennwort zurücksetzen“

Feld	Beschreibung
Passwort	Das neue Kennwort.
Bestätigen	Das gleiche Kennwort, das Sie auch im Feld **Kennwort** eingegeben haben.

Seiten „Neue Datenquelle" und „Datenquelleneigenschaften bearbeiten“

Tabelle 6. Felder auf der Seite „Neue Datenquelle“

Feld	Beschreibung
Datenquelle	Der Name einer Datenquelle, auf die der Benutzer aus einer Unica-Anwendung heraus zugreifen können soll. Bei Unica-Namen wird die Groß- und Kleinschreibung beim Anzeigen beibehalten. Beim Vergleichen und Erstellen wird jedoch nicht zwischen Groß- und Kleinschreibung unterschieden. Es ist beispielsweise nicht möglich, sowohl eine Datenquelle mit dem Namen `customer` als auch eine Datenquelle mit dem Namen `Customer` zu erstellen.
Datenquellenanmeldung	Der Anmeldename für diese Datenquelle.
Datenquellenkennwort	Das Kennwort für diese Datenquelle. Ist für das Datenquellenkonto kein Kennwort erforderlich, können Sie dieses Feld leer lassen.
Kennwort bestätigen	Erneut das Kennwort für diese Datenquelle (falls das Feld **Datenquellenkennwort** leer gelassen wurde, kann dieses Feld auch leer bleiben).

Ländereinstellung

Sie können die Ländereinstellung für interne und externe Benutzer festlegen. Diese Einstellung wirkt sich auf die Anzeige von Sprache, Uhrzeit, Zahlen und Datumsangaben in Unica-Anwendungen aus.

Ländereinstellungen können in Unica Platform auf zwei Arten festgelegt werden.

Global

Die Konfigurationseigenschaft `Platform | Bereichseinstellung` auf der Seite **Einstellungen > Konfiguration** legt die Ländereinstellung global fest.

Pro Benutzer

Ein Attribut auf der Seite **Einstellungen > Benutzer** legt die Ländereinstellung für einzelne Benutzer fest. Diese Einstellung überschreibt die globale Einstellung.

Die Verfügbarkeit der Ländereinstellungen, die pro Benutzer oder global festgelegt werden können, kann je nach Unica-Anwendung variieren, und nicht alle Unica-Anwendungen unterstützen diese Ländereinstellung in Unica Platform. Informationen zum Bestimmen der Verfügbarkeit und Unterstützung der Eigenschaft `Bereichseinstellung` finden Sie in der jeweiligen Produktdokumentation.

Anmerkung: Die Verfügbarkeit der Ländereinstellungen, die pro Benutzer oder global festgelegt werden können, kann je nach Unica-Anwendung variieren. Nicht alle Unica-Anwendungen unterstützen diese Ländereinstellung. Informationen zum Bestimmen der Verfügbarkeit und Unterstützung für Ländereinstellungen in Unica finden Sie in der entsprechenden Produktdokumentation.

Festlegen der Benutzervorgabe für die Ländereinstellung

Verwenden Sie diese Prozedur, um die Ländereinstellung für einen Benutzer festzulegen.

1. Klicken Sie auf **Einstellungen > Benutzer**.
2. Klicken Sie auf den Benutzernamen, für den Sie Ländereinstellungen festlegen möchten.
3. Klicken Sie am unteren Rand der Seite auf den Link **Bearbeitungseinstellungen**.
4. Klicken Sie im linken Teilfenster auf **Unica Platform**.
5. Wählen Sie in der Dropdown-Liste **Bereich** eine Option aus.
6. Klicken Sie auf **Änderungen speichern**.

Synchronisation externer Benutzer

Wenn Unica für die Integration mit einem Windows™ Active Directory- oder LDAP-Server konfiguriert wurde, werden Benutzer und Gruppen automatisch in vordefinierten Intervallen synchronisiert.

Die automatische Synchronisation verfügt nur über eine eingeschränkte Funktionalität.

- Benutzer, die vom LDAP-Server gelöscht wurden, werden während der automatischen Synchronisation nicht gelöscht.

Sie können eine vollständige Synchronisation aller Benutzer und Gruppen mit der Synchronisationsfunktion im Benutzerbereich von Unica erzwingen.

Erzwingen der Synchronisation externer Benutzer

Verwenden Sie diese Prozedur, um die Synchronisation von Benutzern zu erzwingen, wenn Unica mit einem LDAP-Server oder einem System zur Webzugriffskontrolle integriert ist.

1. Melden Sie sich bei Unica an und klicken Sie auf **Einstellungen > Benutzer**.
2. Klicken Sie auf **Synchronisieren**.

   Benutzer und Gruppen werden synchronisiert.

Sicherheitsmanagement

Unica Platform unterstützt Rollen und Berechtigungen für die Steuerung des Benutzerzugriffs auf Objekte und Funktionen in Unica-Anwendungen.

In den meisten Fällen verwenden nur Unica Platform selbst und Unica Campaign die Seite „Benutzerrollen und Berechtigungen“ zur detaillierten Verwaltung des Benutzerzugriffs auf Anwendungen.

Die anderen Unica-Produkte verwenden einige Basisrollen für den Anwendungszugriff, die auf der Seite „Benutzerrollen und Berechtigungen“ festgelegt werden, und haben entweder keine detaillierten Sicherheitseinstellungen oder die Sicherheitseinstellungen werden nicht über die Seite „Benutzerrollen und Berechtigungen“ verwaltet.

In Unica Plan ist das Einrichten der Basisrollen auf der Seite „Benutzerrollen und Berechtigungen“ beispielsweise nur der Ausgangspunkt zur Entwicklung eines angepassten Sicherheitsschemas. Unica Plan hat ein detailliertes Sicherheitsschema, das Sie über eine Benutzerschnittstelle auf den Unica Plan-Seiten verwalten können.

In diesem Handbuch wird erklärt, wie die Funktionen auf der Seite "Benutzerrollen und Berechtigungen" verwendet werden, und es werden die Basissicherheitsrollen und -berechtigungen auf dieser Seite für die verschiedenen Produkte gezeigt. Bei anderen Produkten als Unica Platform finden Sie Informationen zum Sicherheitsmanagement, die nicht in diesem Handbuch zu finden sind, in der Dokumentation für das betreffende Produkt.

Berechtigungen und Aufgaben des Sicherheitsadministrators in Unica Platform

Nur Benutzer mit der Rolle „AdminRole“ oder „PlatformAdminRole“ in Unica Platform haben Zugriff auf Funktionen zur Sicherheitsverwaltung für weitere Benutzerkonten außer ihrem eigenen Konto.

In einer Umgebung mit mehreren Partitionen können nur Benutzer mit der Rolle „PlatformAdminRole“ Benutzer in anderen Partitionen verwalten. Benutzer mit der Rolle „AdminRole“ können nur Benutzer in ihrer eigenen Partition verwalten.

Der Sicherheitsadministrator kann auf den Seiten „Benutzergruppen“ und „Benutzerrollen und Berechtigungen“ die folgenden Aufgaben ausführen.

- Erstellen interner Gruppen und Verwalten ihrer Zugehörigkeit und Partitionszuordnung
- Erstellen von Rollen für Unica Platform und Unica Campaign, sofern erforderlich, und Zuweisen von Berechtigungen zu diesen Rollen
- Verwalten des Benutzerzugriffs auf Unica-Anwendungen durch Zuweisen von Rollen an einzelne Benutzer und/oder interne und externe Gruppen

Lesen Sie diese Übersicht, um sich mit den folgenden Punkten vertraut zu machen.

- Unterschied zwischen internen und externen Gruppen
- Vorgehensweise zum Erstellen interner Gruppen und Zuweisen von Rollen und Berechtigungen
- Eigenschaften interner Gruppen
- Die vorkonfigurierten Benutzerkonten, -gruppen und -rollen in Unica Platform

Sonderzeichen in Rollen- und Richtliniennamen

Bei der Erstellung von Rollen- oder Richtliniennamen sind nur folgende Zeichen erlaubt.

- Groß- und Kleinbuchstaben (`A bis Z`)
- Zahlen (`0 bis 9`)
- Einfaches Anführungszeichen (`'`)
- Bindestrich (`-`)
- Unterstrich (`_ `)
- Kommerzielles A-Zeichen (`@`)
- Schrägstrich (`/`)
- Runde Klammer
- Doppelpunkt (`:`)
- Semikolon (`;`)
- Leerzeichen (außer als erstes Zeichen)
- Doppelbyte-Zeichen (z.B. chinesische Zeichen)

Rollen und Berechtigungen in Unica Platform und Unica Campaign

Rollen in Unica Platform und Unica Campaign sind eine konfigurierbare Sammlung von Berechtigungen. Sie können für jede Rolle in Unica Platform und Unica Campaign Berechtigungen festlegen, mit denen der Zugriff auf die Anwendung gesteuert wird.

Sie können die Standardrollen verwenden oder neue Rollen erstellen. Die verfügbaren Berechtigungen werden vom System definiert; Sie können keine neue Berechtigung erstellen.

Informationen über Rollenzuordnungen

Normalerweise werden Benutzer mit den Berechtigungen ausgestattet, die den Funktionen entsprechen, die dieser in der Organisation ausführt, wenn er Unica verwendet. Sie können Rollen an Gruppen oder an einzelne Benutzer zuordnen. Der Vorteil der Rollenzuordnung nach Gruppe besteht darin, dass Sie eine Kombination aus Rollen der Gruppe zuordnen können. Wenn Sie an dieser Kombination zu einem späteren Zeitpunkt etwas ändern möchten, können Sie dies in einem Mal tun und müssen diesen Vorgang nicht mehrmals für verschiedene Benutzer ausführen. Wenn Sie Rollen nach Gruppe zuordnen, können Sie Benutzer den Gruppen hinzufügen oder sie daraus entfernen, um den Benutzerzugriff zu steuern.

Auswertung von Rollen

Wenn ein Benutzer über mehrere Rollen verfügt, wertet das System die Berechtigungen aus all diesen Rollen zusammen aus. Die Möglichkeit eines Benutzers, eine Funktion für ein bestimmtes Objekt auszuführen, wird dann entsprechend der aggregierten Berechtigungen aus allen Rollen gewährt oder verweigert. Im Fall von Unica Campaign wird die Möglichkeit, eine Funktion für ein bestimmtes Objekt auszuführen, auf der Grundlage der Sicherheitsrichtlinie des Objekts gewährt oder verweigert.

Übersicht über Verwaltung des Benutzerzugriffs auf Anwendungen in Unica Platform

Mit den Funktionen zur Sicherheitsverwaltung von Unica Platform wird der Benutzerzugriff auf Anwendungen in mehreren Schritten verwaltet. Die folgende Vorgehensweise bietet einen Überblick über das grundlegende Verfahren, das an anderer Stelle in diesem Handbuch detailliert beschrieben wird.

1. Planen Sie die Rollen, mit denen Sie den Benutzerzugriff auf Unica-Produkte steuern wollen. Konfigurieren Sie Rollen und zugehörige Berechtigungen je nach Bedarf.
2. Planen Sie, welche Gruppen erforderlich sind, um Ihre Sicherheitsanforderungen zu erfüllen. Je nach Systemkonfiguration ist es möglich, nur interne Gruppen, nur externe Gruppen oder eine Kombination aus beiden Gruppen zu erstellen.
3. Erstellen Sie die erforderlichen internen und externen Gruppen.
4. Weisen Sie den einzelnen Rollen Gruppen zu.
5. Wenn es nur interne Benutzerkonten gibt, erstellen Sie die erforderlichen internen Benutzerkonten.
6. Weisen Sie auf der Basis des für Benutzer vorgesehenen Anwendungszugriffs den einzelnen Gruppen Benutzer oder den einzelnen Benutzern Rollen zu.

Arten von Grupen: intern und extern

Wenn Unica mit einen externen Server integriert ist (beispielsweise mit einem unterstützten LDAP-Server oder einem System zur Webzugriffskontrolle), werden zwei Arten von Gruppen (interne und externe Gruppen) unterstützt: intern und extern

- **Interne Gruppen** – Gruppen, die über die Sicherheitsbenutzeroberfläche in Unica erstellt wurden. Diese Benutzer werden über Unica authentifiziert.
- **Externe Gruppen** – Unica-Gruppen, die Gruppen im externen System zugeordnet sind. Beispiele für externe Server sind LDAP-Server und Server für die Webzugriffskontrolle.

Achtung: Eine in diesem Handbuch als externe Gruppe bezeichnete Gruppe ist eine Gruppe, die in Unica erstellt, aber einem externen System zugeordnet wurde.

Abhängig von der Konfiguration können Sie nur interne Gruppen, nur externe Gruppen oder eine Kombination aus beiden Gruppen haben.

Weitere Informationen zur Integration von Unica mit einem LDAP- oder Windows™ Active Directory-Server finden Sie in den entsprechenden Abschnitten dieses Handbuchs.

Verwalten von externen Gruppen

Die Zugehörigkeit zu externen Gruppen wird über das externe System verwaltet.

Sie können externen Unica-Gruppen Rollen auf die gleiche Weise zuordnen wie internen Gruppen.

Verwalten interner Gruppen und Untergruppen

Sie können unendlich viele interne Gruppen definieren. Jeder interne oder externe Benutzer kann Mitglied mehrerer interner Gruppen und Untergruppen sein.

Eine Untergruppe übernimmt die Benutzermitglieder nicht, die der übergeordneten Gruppe zugewiesen sind, aber sie übernimmt die Rollen, die den übergeordneten Gruppen zugewiesen sind. Eine Gruppe und die zugehörigen Untergruppen gehören immer zu derselben Partition.

Nur interne Gruppen können einer Partition zugeordnet werden und nur der Benutzer platform_admin oder eine Person mit einem Konto mit der Rolle PlatformAdminRole kann Gruppen in allen Partitionen einer Umgebung mit mehreren Partitionen erstellen.

Partitions- und Sicherheitsmanagement

Partitionen in Unica Campaign und den damit zusammenhängenden Produkten stellen eine Möglichkeit dar, Daten in Verbindung mit unterschiedlichen Benutzergruppen zu sichern. Bei der Partitionierung wird die Partition eines Benutzers so angezeigt, als ob es sich dabei um eine separat ausgeführte Unica Campaign-Instanz handelt, ohne Anzeichen dafür, dass andere Partitionen auf demselben System ausgeführt werden. In diesem Abschnitt wird auf die besonderen Überlegungen bezüglich des Sicherheitsmanagements in einer Umgebung mit mehreren Partitionen eingegangen.

Benutzerzugehörigkeit in einer Partition

Benutzer werden auf Grundlage Ihrer Gruppenzugehörigkeit einer Partition zugewiesen. Die Gruppe wird einer Partition zugewiesen. Danach werden die Benutzer einer Gruppe zugeordnet, damit sie auf eine Partition zugreifen können.

Eine Gruppe oder Untergruppe kann nur einer einzigen Partition zugewiesen werden. Übergeordnete Gruppen übernehmen die Partitionszugehörigkeit nicht von ihren Untergruppen. Nur der Benutzer „platform_admin“ oder ein anderes Konto mit der Rolle „PlatformAdminRole“ kann eine Gruppe einer Partition zuordnen.

Ein Benutzer sollte jeweils nur einer Partition angehören.

Informationen über Rollen und Partitionen

Eine Rolle ist immer in den Kontext einer Partition eingebettet. In einer Umgebung mit nur einer Partition werden alle Rollen automatisch in der Standardpartition (partition1) erstellt. In einer Umgebung mit mehreren Partitionen wird eine Rolle in der Partition des Benutzers erstellt, der diese erstellt hat. Dies gilt jedoch nicht für den Benutzer „platform_admin“ und alle anderen Konten mit der Rolle „PlatformAdminRole“. Mit diesen Konten können Rollen in allen Partitionen erstellt werden.

Weitere Informationen zu Partitionen

In diesem Abschnitt finden Sie Anweisungen zum Zuweisen einer Gruppe zu einer Partition und zum Zuweisen von Benutzern zu Gruppen. Eine vollständige Beschreibung der Konfiguration von Partitionen finden Sie in der Dokumentation zur Unica Campaign-Installation.

Vorkonfigurierte Benutzer und Rollen

Wenn Unica zum ersten Mal installiert wird, sind drei Benutzer vorkonfiguriert und erhalten systemdefinierte Rollen in Unica Platform und Unica Campaign (siehe Beschreibung in diesem Abschnitt).

Diese internen Benutzerkonten verfügen über das Standardkennwort „password“.

Benutzerkonto „platform_admin“

Das Benutzerkonto „platform_admin“ ermöglicht einem Unica-Administrator, die Konfiguration, Benutzer und Gruppen eines Produkts in allen Partitionen einer Umgebung mit mehreren Partitionen zu verwalten und alle Unica Platform-Funktionen (mit Ausnahme der Berichterstellung, die über eigene Rollen verfügt) zu verwenden, ohne zuerst nach Partition filtern zu müssen. Standardmäßig verfügt dieses Konto in Unica Platform über die folgenden Rollen.

- In Unica Platform in der Standardpartition partition1
  - AdminRole
  - UserRole
  - PlatformAdminRole

  Mit diesen Rollen kann der Benutzer „platform_admin“ alle Verwaltungsaufgaben in Unica Platform ausführen, jedoch nicht die für Berichtsfunktionen. Wenn zusätzliche Partitionen erstellt werden, kann der Benutzer „platform_admin“ auf Benutzer, Gruppen, Rollen und Konfigurationen in den zusätzlichen Partitionen zugreifen und diese verwalten.

  Die Rolle „PlatformAdminRole“ ist insofern einzigartig, als kein Benutzer die Berechtigungen dieser Rolle ändern kann. Nur ein Benutzer mit dieser Rolle kann einem anderen Benutzer die Rolle „PlatformAdminRole“ zuordnen.
- In Unica Campaign in der Standardpartition partition1
  - Globale Richtlinienrolle „Admin“

  Mit dieser Rolle kann der Benutzer „platform_admin“ alle Aufgaben in Unica Campaign durchführen.

Standardmäßig verfügt dieser Benutzer über keinerlei Zugriffsberechtigungen auf Unica-Produkte über Unica Platform und Unica Campaign hinaus.

Benutzerkonto „asm_admin“

Das Benutzerkonto „asm_admin“ ermöglicht einem Unica-Administrator die Verwaltung von Benutzern und Gruppen in einer Umgebung mit einer einzelnen Partition sowie die Nutzung

aller Unica Platform-Funktionen (mit Ausnahme der Berichterstellung, die über eigene Rollen verfügt). Dieses Konto verfügt über die folgenden Rollen.

- In Unica Platform in der Standardpartition partition1
  - AdminRole
  - UserRole

  Mit Ausnahme der unten aufgeführten Aufgaben kann der Benutzer „asm_admin“ mit diesen Rollen alle Verwaltungsaufgaben in Unica Platform in der Partition ausführen, zu der asm_admin gehört. Dies ist standardmäßig die Partition „partition1“.

  Diese Rollen ermöglichen es dem Benutzer, die Seite „Konfiguration“ zu verwalten. Diese Seite wird bei keinem Benutzer nach Partition gefiltert. Aus diesem Grund sollten Sie die Berechtigung für die Seite „Konfiguration verwalten“ aus der Rolle „AdminRole“ in Unica Platform entfernen und Konfigurationsaufgaben dem Benutzer „platform_admin“ vorbehalten.

  Folgende Ausnahmen sind möglich:

  - Damit auf die Berichtsfunktionen zugegriffen werden kann, muss die Rolle „ReportsSystem“ gewährt werden.
  - Dieser Benutzer kann die Rolle „PlatformAdminRole“ keinem anderen Benutzer und keiner anderen Gruppe zuordnen.

Konto „demo“

Das Konto „demo“ verfügt über die folgenden Rollen.

- In Unica Platform in der Standardpartition partition1
  - UserRole

  Diese Rolle ermöglicht es dem Benutzer „demo“, seine Kontoattribute auf der Seite „Benutzer“ zu ändern. Die Rollen oder Partitionen für sein Konto oder der Zugriff auf andere Funktionen in Unica Platform können jedoch nicht geändert werden. Standardmäßig verfügt dieser Benutzer über keinerlei Zugriffsberechtigungen auf die Unica-Produkte.
- In Unica Campaign in der Standardpartition partition1

◦ Globale Richtlinienrolle „Review“

Mit dieser Rolle kann der Demo-Benutzer Lesezeichen erstellen und Kampagnen, Sitzungen, Angebote, Segmente und Berichtsfunktionen in Unica Campaign anzeigen.

Partitionsübergreifende Administratorberechtigungen

In einer Umgebung mit mehreren Partitionen ist mindestens ein Benutzerkonto mit der Rolle „PlatformAdminRole“ in Unica Platform erforderlich, damit Sie die Sicherheit für Unica-Benutzer über alle Partitionen hinweg verwalten können.

Das Konto „platform_admin“ ist mit der Rolle „PlatformAdminRole“ vorkonfiguriert. Das Konto „platform_admin“ ist ein Superuserkonto, das nicht über die Benutzerfunktionen in Unica gelöscht oder inaktiviert werden kann. Dieses Konto unterliegt jedoch denselben Kennwortbeschränkungen wie andere Benutzer auch. Beispielsweise kann jemand, der versucht, sich als platform_admin anzumelden, N Mal hintereinander ein falsches Kennwort eingeben. Je nach den in Kraft befindlichen Kennwortregeln kann das Konto platform_admin im System inaktiviert werden. Zur Wiederherstellung dieses Kontos müssen Sie eine der folgenden Aktionen ausführen:

- Wenn es einen anderen Benutzer mit der Rolle „PlatformAdminRole“ in Unica Platform gibt, melden Sie sich mit den Informationen dieses Benutzers an und setzen das Kennwort des Benutzers „platform_admin“ zurück bzw. erstellen Sie ein anderes Konto mit der Rolle „PlatformAdminRole“ in Unica Platform.
- Wenn es nur einen einzigen Benutzer mit der Rolle „PlatformAdminRole“ in Unica Platform gibt (beispielsweise platform_admin) und dieser Benutzer inaktiviert ist, können Sie ein neues Konto „platform_admin“ erstellen, indem Sie das von Unica Platform bereitgestellte Dienstprogramm `restoreAccess` verwenden.

Um zu vermeiden, dass der Zugriff PlatformAdminRole mit dem Dienstprogramm `restoreAccess` wiederhergestellt werden muss, empfiehlt es sich, mehr als ein Konto mit den Berechtigungen der Rolle „PlatformAdminRole“ zu erstellen.

Hinzufügen einer internen Gruppe

Verwenden Sie diese Prozedur, um eine interne Gruppe hinzuzufügen.

1. Klicken Sie auf **Einstellungen > Benutzergruppen**.
2. Klicken Sie über der Liste **Gruppenhierarchie** auf **Neue Gruppe**.
3. Füllen Sie die Felder **Gruppenname** und **Beschreibung** aus.

   Wichtig: Geben Sie Gruppen nicht die Namen von systemdefinierten Rollen. Nennen Sie eine Gruppe beispielsweise nicht „Admin“, da dies ein in Unica Campaign verwendeter Rollenname ist. Wird dieser Aspekt nicht beachtet, können Probleme bei Upgrades auftreten.

4. Klicken Sie auf **Änderungen speichern**.

   Der Name der neuen Gruppe wird in der Liste **Gruppenhierarchie** angezeigt.

Hinzufügen einer Untergruppe

Verwenden Sie diese Prozedur, um eine interne Untergruppe hinzuzufügen.

1. Klicken Sie auf **Einstellungen > Benutzergruppen**.
2. Klicken Sie auf den Namen der Gruppe, der Sie eine Untergruppe hinzufügen möchten.
3. Klicken Sie auf **Neue Untergruppe**.
4. Füllen Sie die Felder **Gruppenname** und **Beschreibung** aus.

   Wichtig: Geben Sie Untergruppen nicht die Namen von systemdefinierten Rollen. Nennen Sie eine Untergruppe beispielsweise nicht „Admin“, da dies ein in Unica Campaign verwendeter Rollenname ist. Wird dieser Aspekt nicht beachtet, können Probleme bei Upgrades auftreten.

5. Klicken Sie auf **Änderungen speichern**.

Die neue Untergruppe wird der entsprechenden Gruppe in der Liste **Gruppenhierarchie** hinzugefügt.

Tipp: Falls das Symbol für den Ordner der übergeordneten Gruppe geschlossen ist, klicken Sie auf das Pluszeichen (+), um die Liste einzublenden.

Löschen einer Gruppe oder Untergruppe

Bedenken Sie, dass Mitglieder von Gruppen oder untergeordneten Gruppen ihre diesen Gruppen zugewiesenen Rollen verlieren, wenn Sie die Gruppen löschen. Auch übergeordnete Gruppen der gelöschten Gruppe verlieren die entsprechenden Rollenzuordnungen, sofern die Rollen nicht auch direkt diesen übergeordneten Gruppen zugewiesen sind.

1. Klicken Sie auf **Einstellungen > Benutzergruppen**.
2. Klicken Sie auf den Namen der Gruppe oder untergeordneten Gruppe, die Sie löschen möchten.

   Anmerkung: Wollen Sie bei geschlossenem Ordnersymbol für die übergeordnete Gruppe eine Untergruppe auswählen, klicken Sie auf das Pluszeichen (+), um die Liste einzublenden.

3. Klicken Sie am oberen Rand des rechten Teilfensters auf die Schaltfläche **Gruppe löschen**.
4. Klicken Sie auf **OK**.

Ändern der Beschreibung einer Gruppe oder Untergruppe

Verwenden Sie diese Prozedur, um die Beschreibung einer Gruppe oder Untergruppe zu ändern.

1. Klicken Sie auf **Einstellungen > Benutzergruppen**.
2. Klicken Sie auf den Namen der Gruppe oder untergeordneten Gruppe, dessen Beschreibung Sie ändern möchten.

   Anmerkung: Wollen Sie bei geschlossenem Ordnersymbol für die übergeordnete Gruppe eine Untergruppe auswählen, klicken Sie auf das Pluszeichen (+), um die Liste einzublenden.

3. Klicken Sie auf **Eigenschaften bearbeiten**.
4. Bearbeiten Sie die Beschreibung wie gewünscht.
5. Klicken Sie auf **Änderungen speichern**, um die Änderungen zu speichern.
6. Klicken Sie auf **OK**.

Zuweisen einer Gruppe zu einer Partition

Dieses Verfahren ist nur bei der Konfiguration mehrerer Partitionen für Unica Campaign erforderlich. Nur ein Konto mit der Rolle PlatformAdminRole (beispielsweise der Benutzer „platform_admin“) kann diese Aufgabe ausführen.

1. Bestimmen Sie, welche Gruppen Sie jeder einzelnen Partition zuordnen möchten. Falls erforderlich, erstellen Sie die Gruppen.
2. Klicken Sie auf **Einstellungen > Benutzergruppen**.
3. Klicken Sie auf den Namen der Gruppe oder untergeordneten Gruppe, die Sie einer Partition zuordnen möchten.
4. Klicken Sie auf **Eigenschaften bearbeiten**.
5. Wählen Sie in der Dropdown-Liste **Partitions-ID** die gewünschte Partition aus.

   Dieses Feld ist nur bei der Konfiguration mehrerer Partitionen verfügbar.
6. Klicken Sie auf **Änderungen speichern**, um die Änderungen zu speichern.
7. Klicken Sie auf **OK**.

Hinzufügen eines Benutzers zu einer Gruppe oder Untergruppe

Verwenden Sie diese Prozedur, um einer Gruppe oder Untergruppe einen Benutzer hinzuzufügen.

1. Klicken Sie auf **Einstellungen > Benutzer**.

   Anmerkung: Die gleiche Aufgabe können Sie auf der Seite **Benutzergruppen ausführen**, indem Sie auf den Gruppennamen und anschließend auf die Option **Benutzer bearbeiten** klicken.

2. Klicken Sie auf den Benutzernamen, den Sie ändern möchten.
3. Klicken Sie am unteren Rand der Seite auf den Link **Gruppen bearbeiten**.
4. Klicken Sie im Feld **Verfügbare Gruppen** auf einen Gruppennamen.
5. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Gruppenname erscheint im Feld **Gruppen**.
6. Klicken Sie auf **Änderungen speichern**, um die Änderungen zu speichern.
7. Klicken Sie auf **OK**.

   Die Benutzerkontodetails werden einschließlich der zugeordneten Gruppe oder Untergruppe angezeigt.

Entfernen eines Benutzers aus einer Gruppe oder Untergruppe

Verwenden Sie diese Prozedur, um einen Benutzer aus einer Gruppe oder Untergruppe zu entfernen.

Wichtig: Durch das Entfernen eines Benutzers aus einer Gruppe oder Untergruppe werden auch die Rollen des Benutzers, die der Gruppe oder Untergruppe zugewiesen sind, entfernt.

1. Klicken Sie auf **Einstellungen > Benutzer**.
2. Klicken Sie auf den Benutzernamen, den Sie ändern möchten.
3. Klicken Sie am unteren Rand der Seite auf den Link **Gruppen bearbeiten**.

4. Klicken Sie im Feld **Gruppen** auf einen Gruppennamen.
5. Klicken Sie auf die Schaltfläche **Entfernen**.

   Der Gruppenname wird ins Feld **Verfügbare Gruppen** verschoben.
6. Klicken Sie auf **Änderungen speichern**, um die Änderungen zu speichern.
7. Klicken Sie auf **OK**.
8. Klicken Sie am unteren Rand der Seite auf den Link **Eigenschaften bearbeiten**.
9. Ändern Sie den Namen oder die Beschreibung wie gewünscht.
10. Klicken Sie auf **Änderungen speichern**, um die Änderungen zu speichern.
11. Klicken Sie auf **OK**.

Seiten für Benutzergruppenmanagement

Diese Felder werden zum Konfigurieren von Benutzergruppen verwendet.

Felder der Seiten „Neue Gruppe“, „Neue Untergruppe“ und „Eigenschaften bearbeiten“

Tabelle 7. Felder der Seiten „Neue Gruppe“, „Neue Untergruppe“ und „Eigenschaften bearbeiten“

Feld	Beschreibung
Gruppenname	Der Gruppenname. Sie dürfen maximal 64 Zeichen verwenden. Folgende Zeichen sind bei der Erstellung des Gruppennamens erlaubt. • Groß- und Kleinbuchstaben (`A bis Z`) • Zahlen (`0 bis 9`) • Einfaches Anführungszeichen (`'`) • Bindestrich (`-`) • Unterstrich (`_ `) • Kommerzielles A-Zeichen (`@`) • Schrägstrich (`/`) • Runde Klammer

Tabelle 7. Felder der Seiten „Neue Gruppe“, „Neue Untergruppe“ und „Eigenschaften bearbeiten“ (Fortsetzung)

Feld	Beschreibung
	• Doppelpunkt (:) • Semikolon (;) • Leerzeichen (außer als erstes Zeichen) • Doppelbyte-Zeichen (beispielsweise alphanumerische chinesische Zeichen) Geben Sie Gruppen oder Untergruppen nicht die Namen von systemdefinierten Rollen. Nennen Sie eine Gruppe beispielsweise nicht „Admin“, da dies ein in Unica Campaign verwendeter Rollenname ist. Wird dieser Aspekt nicht beachtet, können Probleme bei Upgrades auftreten. Unica -Namen sollten zu Anzeigezwecken groß geschrieben werden. Beim Vergleichen und Erstellen wird jedoch nicht zwischen Groß- und Kleinschreibung unterschieden (so können beispielsweise „Admin“ und „admin“ nicht als separate Gruppennamen verwendet werden). Wenn Sie eine Untergruppe erstellen, sollten Sie der Gruppe einen Namen geben, der im Bezug zu der übergeordneten Gruppe steht.
Beschreibung	Die Beschreibung der Gruppe. Sie dürfen maximal 256 Zeichen verwenden. Es ist von Vorteil, wenn Sie in der Beschreibung die Rollen angeben, die Sie der Gruppe oder untergeordneten Gruppe zuordnen möchten. So können Sie auf der Detailseite der Gruppe auf einen Blick die Rollen und die Benutzer sehen.
Partitions-ID	Nur bei der Konfiguration mehrerer Partitionen verfügbar.

Tabelle 7. Felder der Seiten „Neue Gruppe“, „Neue Untergruppe“ und „Eigenschaften bearbeiten“ (Fortsetzung)

Feld	Beschreibung
	Wenn Sie eine Partition einer Gruppe zuordnen, werden die Mitglieder der Gruppe Mitglieder dieser Partition. Ein Benutzer kann Mitglied bei nur einer Partition sein.

Felder der Seiten „Benutzer bearbeiten“ und „Rollen bearbeiten“

Tabelle 8. Felder der Seiten „Benutzer bearbeiten“ und „Rollen bearbeiten“

Feld	Beschreibung
Verfügbare Gruppen oder verfügbare Rollen	Eine Liste mit Gruppen und untergeordneten Gruppen oder Rollen, denen der Benutzer nicht zugeordnet ist.
Gruppen oder Rollen	Eine Liste mit Gruppen und untergeordneten Gruppen oder Rollen, denen der Benutzer zugeordnet ist.

Erstellen einer Rolle

Neue Rollen sollten nur für Produkt erstellt werden, die über detaillierte Berechtigungen verfügen. Die Funktion zur Berichterstellung und einige Unica-Produkte verfügen nur über grundlegende Berechtigungen, sodass es nicht erforderlich ist, zusätzliche Rollen für diese Produkte zu erstellen.

1. Klicken Sie auf **Einstellungen > Benutzerrollen Berechtigungen**.
2. Klicken Sie auf das Pluszeichen neben dem Produktnamen in der linken Liste und klicken Sie anschließend auf den Namen der Partition, in der Sie die Rolle erstellen möchten.
3. Für Unica Campaign gilt: Falls Sie eine neue Rolle unter der globalen Richtlinie erstellen möchten, klicken Sie auf „Globale Richtlinie“.
4. Klicken Sie auf **Rollen hinzufügen und Berechtigungen zuweisen**.

5. Klicken Sie auf **Rolle hinzufügen**.
6. Geben Sie einen Namen und eine Beschreibung für die Rolle ein.
7. Klicken Sie auf **Änderungen speichern**, um die Rolle zu speichern. Klicken Sie auf **Berechtigungen speichern und bearbeiten**, um zur Seite „Berechtigungen“ zu wechseln und Berechtigungen für die Rollen in der Liste hinzuzufügen oder zu ändern.

Ändern von Rollenberechtigungen

Verwenden Sie diese Prozedur, um Rollenberechtigungen zu ändern.

1. Klicken Sie auf **Einstellungen > Benutzerrollen Berechtigungen**.
2. Klicken Sie in der linken Liste auf das Pluszeichen neben einem Produkt und klicken Sie anschließend auf den Namen der Partition, in der Sie eine Rolle ändern möchten.
3. Für Unica Campaign gilt: Falls Sie eine neue Rolle unter der globalen Richtlinie oder einer benutzererstellten Richtlinie erstellen möchten, klicken Sie auf den Richtliniennamen.
4. Klicken Sie auf **Rollen hinzufügen und Berechtigungen zuweisen**.
5. Klicken Sie auf **Berechtigungen speichern und bearbeiten**
6. Klicken Sie auf das Plus-Symbol neben einer Gruppe, um alle verfügbaren Berechtigungen und den Status dieser Berechtigungen innerhalb jeder einzelnen Rolle anzuzeigen.
7. Klicken Sie in der Rollenspalte, in der Sie die Berechtigungen ändern möchten, auf das Feld in den Berechtigungszeilen, um den Status auf „Gewährt“, „Nicht gewährt“ oder „Abgelehnt“ zu setzen.
8. Klicken Sie auf **Änderungen speichern**, um Ihre Änderungen zu speichern.

   Klicken Sie auf **Änderungen zurücksetzen**, um die Änderungen seit Ihrer letzten Speicherung rückgängig zu machen und auf der Seite Berechtigungen zu bleiben, oder klicken Sie auf **Abbrechen**, um Ihre Änderungen seit Ihrer letzten Speicherung zu verwerfen und zur Partitions- oder Richtlinienseite zu wechseln.

Entfernen einer Rolle aus dem System

Verwenden Sie diese Prozedur, um eine Rolle aus Unica zu entfernen.

Wichtig: Wenn Sie eine Rolle entfernen, wird diese aus allen Benutzern und Gruppen entfernt, denen sie zugeordnet war.

1. Klicken Sie auf **Einstellungen > Benutzerrollen Berechtigungen**.
2. Klicken Sie in der linken Liste auf das Pluszeichen neben einem Produkt und klicken Sie anschließend auf den Namen der Partition, in der Sie eine Rolle erstellen möchten.
3. Für Unica Campaign gilt: Falls Sie eine neue Rolle unter der globalen Richtlinie erstellen möchten, klicken Sie auf „Globale Richtlinie“.
4. Klicken Sie auf **Rollen hinzufügen und Berechtigungen zuweisen**.
5. Klicken Sie für die zu entfernende Rolle auf den Link **Entfernen**.
6. Klicken Sie auf **Änderungen speichern**.

Zuordnen einer Rolle zu einer Gruppe oder Entfernen einer Rolle aus einer Gruppe

Wenn Sie einer Gruppe eine Rolle hinzufügen bzw. eine Rolle aus einer Gruppe entfernen, übernehmen oder verlieren die Mitglieder dieser Gruppe diese Rolle.

1. Klicken Sie auf **Einstellungen > Benutzergruppen**.
2. Klicken Sie auf den Namen der Gruppe, mit der Sie arbeiten möchten.
3. Klicken Sie auf **Rollen zuweisen**.

   Rollen, die der Gruppe nicht zugewiesen sind, werden auf der linken Seite der Anzeige im Feld **Verfügbare Rollen** angezeigt. Rollen, die der Gruppe derzeit zugeordnet sind, werden auf der rechten Seite im Feld **Rollen** angezeigt.
4. Klicken Sie im Feld Verfügbare Rollen auf einen Rollennamen, um ihn auszuwählen.
5. Klicken Sie auf **Hinzufügen** oder **Entfernen**, um den Rollennamen von einem Feld in das andere Feld zu verschieben.
6. Klicken Sie auf **Änderungen speichern**, um die Änderungen zu speichern.
7. Klicken Sie auf **OK**.

Zuweisen einer Rolle zu einem Benutzer und Entfernen einer Rolle

Mithilfe des Fensters **Rollen bearbeiten** weisen Sie eine Rolle einem Benutzer zu oder entfernen Sie eine Rolle eines Benutzers.

Gehen Sie folgt vor, um einem Benutzer eine Rolle zuzuweisen oder um eine Rolle zu entfernen:

1. Klicken Sie auf **Einstellungen > Benutzer**.
2. Klicken Sie auf den Namen des Benutzerkontos, mit dem Sie arbeiten möchten.
3. Klicken Sie auf **Rollen bearbeiten**.

   Rollen, die nicht dem Benutzer zugeordnet sind, werden auf der linken Seite des Bildschirms im Feld **Verfügbare Rollen** angezeigt. Rollen, die dem Benutzer momentan zugewiesen sind, werden auf der rechten Seite im Feld **Ausgewählte Rollen** angezeigt.
4. Wählen Sie eine Rolle im Feld **Verfügbare Rollen** aus. Führen Sie eine der folgenden Aufgaben aus:
   - Wählen Sie im Feld **Verfügbare Rollen** eine Rolle aus und klicken Sie auf **Hinzufügen**, um einem Benutzer eine Rolle zuzuweisen.
   - Wählen Sie im Feld **Ausgewählte Rollen** eine Rolle aus und klicken Sie auf **Entfernen**, um eine Rolle eines Benutzers zu entfernen.
5. Klicken Sie auf **Änderungen speichern** und klicken Sie dann auf **OK**.

Definitionen von Berechtigungsstatus

Für jede Rolle können Sie festlegen, welche Berechtigungen gewährt, nicht gewährt oder verweigert werden. Diese Berechtigungen legen Sie auf der Seite **Einstellungen > Benutzerrollen und Berechtigungen** fest.

Die Status haben die folgende Bedeutung.

- **Gewährt** - gekennzeichnet durch ein Häkchen  . Berechtigungen werden explizit gewährt, um diese bestimmte Funktion auszuführen, solange keine der anderen Rollen des Benutzers die Berechtigung verweigert.
- **Verweigert** - gekennzeichnet durch ein "X"  . Berechtigungen zum Ausführen dieser Funktion werden explizit verweigert, unabhängig von den anderen Rollen des Benutzers, die die Berechtigung gewähren.
- **Nicht gewährt** - gekennzeichnet durch einen Kreis  . Berechtigungen werden weder explizit gewährt noch verweigert, um eine bestimmte Funktion auszuführen. Wenn diese Berechtigung nicht explizit durch eine der Benutzerrollen gewährt wird, ist der Benutzer nicht berechtigt, diese Funktion durchzuführen.

Berechtigungen für Produkte, die nur Basisrollen verwenden

Die folgende Tabelle definiert die Funktionen der Rollen für die Unica Produkte, die nur Basisrollen verwenden. Weitere Informationen finden Sie in der Produktdokumentation.

Tabelle 9. Berechtigungen für Produkte, die nur Basisrollen verwenden

Anwendungen	Rollen
Leads	Leads-Rollen sind für die zukünftige Verwendung reserviert.
Berichte	• ReportsSystem – gewährt die Berechtigung `report_system`, die den Zugriff auf die Optionen **SQL-Berichtsgenerator** und **Synchronisation der Berichtsordnerberechtigungen** im Menü **Einstellungen** ermöglicht. • ReportsUser – gewährt die Berechtigung `report_user`, die vom -Authentifizierungsprovider genutzt wird, der nur auf dem IBM® Cognos® 11 BI-System installiert ist. Weitere Informationen zu den Authentifizierungsoptionen für die IBM® Cognos® 11 BI-Integration und die Art und Weise, wie der -Authentifizierungsprovider die Berichtsberechtigungen verwendet, finden Sie im Installations- und Konfigurationshandbuch zu Cognos-Berichten.

Tabelle 9. Berechtigungen für Produkte, die nur Basisrollen verwenden (Fortsetzung)

Anwendungen	Rollen
Unica Deliver	• Deliver_Admin – Bietet uneingeschränkten Zugriff auf alle Funktionen. • Deliver_User - Für zukünftige Verwendung reserviert. Der Zugriff wird weiterhin über die Sicherheitsrichtlinien in Unica Campaign definiert. Ausführliche Informationen hierzu finden Sie im Unica Deliver Startup- und Administratorhandbuch.
Unica Interact	• InteractAdminRole – Bietet uneingeschränkten Zugriff auf alle Funktionen.
Unica Collaborate	• collab_admin – Bietet uneingeschränkten Zugriff auf alle Funktionen. • corporate - Berechtigung zur Verwendung von Unica Campaign und Unica Collaborate, um wiederverwendbare Listen und On-Demand-Kampagnenvorlagen zu entwickeln. Berechtigung zur Erstellung und Ausführung von Unternehmenskampagnen. • field - Berechtigung zur Teilnahme an Unternehmenskampagnen und zur Erstellung und Ausführung von Listen und On-Demand-Kampagnen in Unica Collaborate.
Unica Plan	• PlanUserRole - Benutzer mit der Rolle „PlanUserRole“ verfügen standardmäßig über nur sehr wenige Berechtigungen in Unica Plan. Sie können keine Pläne, Programme oder Projekte erstellen und haben eingeschränkte Sicherheitsberechtigungen auf die Administrationseinstellungen. • PlanAdminRole - Benutzer mit der Rolle „PlanAdminRole“ verfügen standardmäßig über die meisten Berechtigungen in Unica Plan. Hierzu gehört der Zugriff auf alle Verwaltungs- und Konfigurationseinstellungen und somit über umfangreiche Zugriffsberechtigungen.

Tabelle 9. Berechtigungen für Produkte, die nur Basisrollen verwenden (Fortsetzung)

Anwendungen	Rollen
	Der Zugriff wird weiterhin über die Sicherheitsrichtlinien in Unica Plan definiert.
Unica Journey	• JourneyAdmin: Benutzer haben Zugriff auf alle Verwaltungs- und Konfigurationseinstellungen, was einen breiten Zugriffsbereich ermöglicht. • JourneyUser: Benutzer haben beschränkten Zugriff auf Verwaltungs- und Konfigurationseinstellungen. Sie können die Einstellungen nur anzeigen, aber keine groben Operationen für Sie ausführen.
Unica Centralized Offer Management	OfferAdmin: Benutzer haben Zugriff auf alle Verwaltungs- und Konfigurationseinstellungen, was einen breiten Zugriffsbereich ermöglicht. OfferUser: Benutzer haben beschränkten Zugriff auf Verwaltungs- und Konfigurationseinstellungen.
IBM SPSS Modeler Advantage Enterprise Marketing Management Edition	• SPSSUser - Benutzer mit der Rolle „SPSSUser“ haben folgende Berechtigungen: ◦ Ausführen von Berichten ◦ Anzeigen von Elementen in ihren Content-Repositories. ◦ Durchführen von Scorings • SPSSAdmin - Benutzer mit der Rolle „SPSSAdmin“ verfügen über alle Berechtigungen, die in IBM SPSS Modeler Advantage Enterprise Marketing Management Edition aktiviert sind. Hierzu gehört der Zugriff auf alle Verwaltungs- und Konfigurationseinstellungen.

Berechtigungen für Unica Platform

In der folgenden Tabelle werden die Berechtigungen beschrieben, die Sie Rollen in Unica Platform zuordnen können.

Tabelle 10. Berechtigungen für die Unica Platform

Berechtigung	Beschreibung
Seite „Benutzeradministration“	Berechtigt den Benutzer die Durchführung aller Benutzerverwaltungsaufgaben auf der Seite Benutzer für Benutzerkonten in seiner eigenen Partition: Hinzufügen und Löschen von internen Benutzerkonten und Ändern von Attributen, Datenquellen und Rollenzuweisungen
Seite „Benutzerzugriff“	Berechtigt den Benutzer, die Seite „Benutzer“ anzuzeigen.
Seite 'Benutzergruppen verwalten'	Berechtigt einen Benutzer dazu, auf der Seite „Benutzergruppen“ alle Aktionen auszuführen. Ausgenommen hiervon ist das Zuweisen einer Partition zu einer Gruppe; hierzu ist nur der Benutzer „platform_admin“ berechtigt. Diese Berechtigung ermöglicht es dem Benutzer, Gruppen zu erstellen, zu modifizieren und zu löschen, Gruppenzugehörigkeiten zu verwalten und Gruppen Rollen zuzuordnen.
Seite „Benutzerrollen verwalten“	Berechtigt den Benutzer, alle Aktionen auf der Seite Benutzerrollen und -berechtigungen durchzuführen: Erstellen, ändern und löschen Sie Rollen in Unica Platform und Unica Campaign und weisen Sie für alle aufgelisteten Unica-Produkte Benutzer zu Rollen zu.
Seite 'Konfiguration verwalten'	Berechtigt den Benutzer, alle Aktionen auf der Seite "Konfiguration" durchzuführen: Berechtigt den Benutzer, alle Aktionen auf der Seite "Konfiguration" durchzuführen: Modifizieren von Eigenschaftswerten, Erstellen neuer Kategorien von Vorlagen und Lö-

Tabelle 10. Berechtigungen für die Unica Platform (Fortsetzung)

Berechtigung	Beschreibung
	schen von Kategorien, die über den Link **Kategorie löschen** verfügen.
Seite 'Datenfilter verwalten'	Berechtigt den Benutzer, alle Aktionen auf der Seite Datenfilter durchzuführen: Datenfilterzuweisungen vornehmen und entfernen.
Seite „Geplante Aufgaben verwalten“	Berechtigt einen Benutzer dazu, alle Aktionen auf der Seite „Zeitplanmanagement“ durchzuführen: Zeitplandefinitionen anzeigen und ändern sowie Ausführungen anzeigen.
Dashboards verwalten	Berechtigt einen Benutzer dazu, alle Aktionen auf den Seiten „Dashboards“ durchzuführen: Erstellen, Anzeigen, Ändern und Löschen von Dashboards, Zuweisen von Dashboardadministratoren und Verwalten des Dashboardzugriffs.

Berechtigungen für Opportunity Detect

In der folgenden Tabelle werden die Berechtigungen beschrieben, die Sie Rollen in Opportunity Detect zuweisen können.

Alle Berechtigungen mit dem Status **Nicht gewährt** gelten als **Verweigert**.

Tabelle 11. Berechtigungen in Opportunity Detect

Berechtigung	Beschreibung
Nur Ansicht	Zugriff auf die gesamte Benutzeroberfläche im schreibgeschützten Modus.
Trigger entwerfen	• Kann Arbeitsbereiche erstellen und Triggersysteme entwerfen. • Kann alle triggerbezogenen Ressourcen erstellen, ändern und löschen.

Tabelle 11. Berechtigungen in Opportunity Detect (Fortsetzung)

Berechtigung	Beschreibung
	• Kann auf die Seiten mit Arbeitsbereichen, Komponenten, Zielgruppenebenen, Datenquellen und Listen der benannten Werte zugreifen. • Kann nicht auf die Seite mit den Servergruppen oder auf die Registerkarte zur Implementierung eines Arbeitsbereichs zugreifen. • Kann einen Stapelverarbeitungslauf nicht auslösen. • Kann keine Objekte verwalten, die der Web-Service erstellt, wenn Opportunity Detect mit Unica Interact integriert ist.
Ausführung zu Testzwecken	• Bereitstellen von Implementierungskonfigurationen und Ausführen von Stapelimplementierungskonfigurationen auf Servergruppen, die nicht für den Produktionsbetrieb vorgesehen sind. • Zugriff auf die Seiten für Servergruppen und die Registerkarte zur Implementierung eines Arbeitsbereichs, aber keine Angabe einer Servergruppe für den Produktionsbetrieb. • Keine Bereitstellung oder Ausführung von Implementierungskonfigurationen, die eine Produktionsservergruppe verwenden.
Ausführung zu Produktionszwecken	• Bereitstellen von Implementierungskonfigurationen und Ausführen von Stapelimplementierungskonfigurationen auf beliebigen Servergruppen. • Durchführen aller Aufgaben auf der Seite für Servergruppen und auf den Registerkarten für die Implementierung und Stapelverarbeitungsläufe einschließlich der Angabe einer Servergruppe für den Produktionsbetrieb.
Echtzeit verwalten	Verwalten von Objekten, die der Web-Service erstellt, wenn Opportunity Detect mit Unica Interact integriert ist, um den Echtzeitmodus zu aktivieren.

Tabelle 11. Berechtigungen in Opportunity Detect (Fortsetzung)

Berechtigung	Beschreibung
	Lässt Folgendes zu: • Löschen von Arbeitsbereichen und Komponenten, die vom Web-Service erstellt wurden. • Starten und Stoppen von Echtzeit-Implementierungskonfigurationen und Aktualisieren von deren Protokollebene. Benutzer, die nur über diese Berechtigung verfügen, können keine Verarbeitungsläufe für Echtzeit-Implementierungskonfigurationen starten. Die folgenden Aufgaben können von niemandem ausgeführt werden, auch nicht, wenn er über diese Berechtigung verfügt: • Löschen und Aktualisieren von Zielgruppenebenen, Datenquellen, Listen mit benannten Werten, Servergruppen oder Implementierungskonfigurationen, die vom Web-Service erstellt wurden. • Erstellen und Bereitstellen von Implementierungskonfigurationen, die vom Web-Service erstellt wurden.

Konfigurationsmanagement

Bei der Erstinstallation von Unica werden auf der Seite „Konfiguration“ nur die Eigenschaften, mit denen Unica Platform konfiguriert wird, und einige globale Konfigurationseinstellungen angezeigt. Wenn Sie zusätzliche Unica-Anwendungen installieren, werden die Eigenschaften zur Konfiguration dieser Anwendungen in Unica Platform registriert. Diese Eigenschaften werden dann auf der Seite „Konfiguration“ angezeigt. Dort können Sie die zugehörigen Werte festlegen oder bearbeiten.

Einige Anwendungen verfügen möglicherweise über zusätzliche Konfigurationseigenschaften, die nicht im zentralen Repository gespeichert sind.

Ausführliche Informationen zu allen Konfigurationsoptionen für die Anwendung finden Sie in der Anwendungsdokumentation.

Eigenschaftskategorien

Nach der Unica Platform-Erstinstallation sind die Kategorien **Berichte**, **Allgemeines** und **Unica Platform** verfügbar. Die folgenden Kategorien enthalten Eigenschaften, die für alle in einer Suite installierten Unica-Anwendungen gelten.

- Die Standardeinstellung für die Ländereinstellung
- Die Kategorie **Sicherheit** sowie Unterkategorien mit Eigenschaften, in denen Anmeldemodi und modusspezifische Einstellungen angegeben werden
- Kennworteinstellungen
- Eigenschaften, mit denen Datenfilter konfiguriert werden
- Eigenschaften, mit denen Zeitpläne konfiguriert werden
- Eigenschaften, mit denen die Berichtsfunktion konfiguriert wird
- Eigenschaften, mit denen konfiguriert wird, wie Alerts behandelt werden.

Je nach installierten Unica-Anwendungen sind in zusätzlichen Kategorien anwendungsspezifische Kategorien und Unterkategorien enthalten. Nach der Installation von Unica Campaign enthält die Kategorie **Campaign** beispielsweise Eigenschaften und Unterkategorien, die sich auf Unica Campaign beziehen.

Kategorietypen

Eine Kategorie kann einem von drei möglichen Typen angehören, die durch unterschiedliche Symbole gekennzeichnet werden.

Tabelle 12. Symbole für Kategorietypen

Kategorietyp	Symbol
Kategorien, deren Eigenschaften konfiguriert werden können	

Tabelle 12. Symbole für Kategorietypen (Fortsetzung)

Kategorietyp	Symbol
Kategorien, deren Eigenschaften nicht konfiguriert werden können	
Vorlagenkategorien, mit denen eine Kategorie erstellt werden kann Die Namen von Vorlagenkategorien sind auch kursiv geschrieben und stehen in Klammern.	

Vorlagen zum Duplizieren von Kategorien

Die Eigenschaften einer Unica-Anwendung werden bei der Installation der Anwendung in Unica Platform registriert. Wenn Benutzer für eine Anwendung duplizierte Kategorien zu Konfigurationszwecken erstellen müssen, wird eine Kategorienvorlage bereitgestellt.

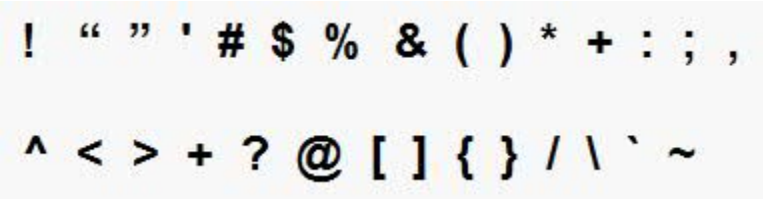
Duplizieren Sie die Vorlage, um eine Kategorie zu erstellen. Sie können beispielsweise eine neue Unica Campaign-Partition oder -Datenquelle erstellen, indem Sie die entsprechende Vorlage duplizieren.

Außerdem können Sie jede Kategorie, die aus einer Vorlage erstellt wurde, auch wieder löschen.

Einschränkungen bei der Benennung von Kategorien

Bei der Benennung einer aus einer Vorlage erstellten Kategorie gelten folgende Einschränkungen.

- Der Name muss innerhalb der Kategorien derselben Ebene in der Struktur (d. h. bei Kategorien innerhalb derselben übergeordneten Kategorie) eindeutig sein.
- Die nachfolgend aufgeführten Zeichen sind in Kategorienamen nicht zulässig.



Zudem darf der Name nicht mit einem Punkt beginnen.

Eigenschaftsbeschreibungen

Sie können folgendermaßen auf Eigenschaftsbeschreibungen zugreifen:

- Klicken Sie auf **Hilfe > Hilfe zu dieser Seite**, um die Onlinehilfe zu starten. Rufen Sie ein Thema auf, in dem alle Eigenschaften für die von Ihnen angezeigte Seite beschrieben werden.
- Klicken Sie auf **Hilfe > Produktdokumentation**, um eine Seite zu öffnen, von der aus Sie auf alle Produktdokumentationen im Online- oder PDF-Format zugreifen können. Sämtliche Eigenschaftsbeschreibungen sind im Anhang des Unica PlatformAdministratorhandbuchs verfügbar.

Aktualisierungsfunktion

Die Schaltfläche „Aktualisieren“ oben in der Navigationsstruktur „Konfiguration“ ermöglicht die folgenden Funktionen.

- Aktualisierung des Inhalts der Struktur. Dies ist nützlich, wenn Sie die neuesten Informationen zu den Konfigurationseinstellungen abrufen möchten. Diese Einstellungen wurden möglicherweise aktualisiert, nachdem Sie die Struktur angezeigt haben (beispielsweise, wenn die Registrierung einer Anwendung vorgenommen oder aufgehoben wurde oder wenn eine andere Person Einstellungen aktualisiert hat).

- Wiederherstellen des Zustands der Navigationsstruktur, in dem sie sich bei Ihrer letzten Auswahl eines Knotens befand. Die Struktur wird dazu entsprechend reduziert oder erweitert.

Wichtig: Wenn Sie sich im Bearbeitungsmodus befinden und dann auf **Aktualisieren** klicken, kehrt die Seite zum schreibgeschützten Modus zurück. Alle nicht gespeicherten Änderungen gehen verloren.

Standardbenutzervorgabe für die Ländereinstellung

Unica Platform enthält ein Standardattribut für die Ländereinstellung, das für alle Unica-Anwendungen gilt, die dieses Attribut implementieren.

Diese Standardeinstellung können Sie festlegen, indem Sie in der Kategorie **Platform** den Wert der Eigenschaft **Bereichseinstellung** angeben.

Weitere Informationen zu dieser Eigenschaft finden Sie in der Onlinehilfe im Bereich „Konfiguration“ oder im Unica PlatformAdministratorhandbuch. Informationen darüber, ob eine Unica-Anwendung dieses Attribut implementiert, finden Sie in der Dokumentation zu dieser Anwendung.

Sie können diese Standardwerte zudem für einzelne Benutzer überschreiben, indem Sie den Wert dieser Eigenschaft im Benutzerkonto ändern.

Navigieren zu einer Kategorie

Verwenden Sie diese Prozedur, um auf der Seite „Konfiguration“ zu einer Kategorie zu navigieren.

1. Melden Sie sich bei Unica an.
2. Klicken Sie auf **Einstellungen > Konfiguration** in der Symbolleiste.

   Auf der Seite „Konfiguration“ wird die Baumstruktur der Konfigurationskategorien angezeigt.
3. Klicken Sie auf das Pluszeichen neben einer Kategorie.

Die Kategorie wird geöffnet, und die Unterkategorien werden angezeigt. Falls die Seite Eigenschaften enthält, werden diese zusammen mit ihren aktuellen Werten angezeigt.

Die internen Namen für die Kategorien werden unter der Seitenüberschrift angezeigt. Sie verwenden diese internen Namen, wenn Sie Kategorien und deren Eigenschaften mit dem Dienstprogramm `configTool` manuell importieren oder exportieren.

4. Erweitern Sie die Kategorien und Unterkategorien, bis die Eigenschaft, die Sie bearbeiten möchten, angezeigt wird.

Bearbeiten von Eigenschaftswerten

Verwenden Sie diese Prozedur, um auf der Seite „Konfiguration“ einen Eigenschaftswert zu ändern.

1. Navigieren Sie zur Kategorie, die die Eigenschaft enthält, die Sie festlegen wollen.

   Auf der Seite „Einstellungen“ der Kategorie wird eine Liste der Eigenschaften in der Kategorie mit ihren aktuellen Werten angezeigt.
2. Klicken Sie auf **Einstellungen bearbeiten**.

   Auf der Seite „Einstellungen bearbeiten“ der Kategorie werden die Eigenschaftswerte in bearbeitbaren Feldern angezeigt.
3. Geben Sie Werte ein bzw. bearbeiten Sie diese wie gewünscht.

   In UNIX™ ist bei allen Datei- und Verzeichnisnamen die Groß- und Kleinschreibung zu beachten. Eingegebene Datei- und Ordnernamen müssen bezüglich der Groß- und Kleinschreibung mit dem Datei- oder Ordnernamen auf der UNIX™-Maschine übereinstimmen.
4. Klicken Sie auf **Änderungen speichern**, um die Änderungen zu speichern. Klicken Sie auf **Abbrechen**, um die Seite ohne Speichern zu schließen.

Erstellen einer Kategorie aus einer Vorlage

Verwenden Sie diese Prozedur, um auf der Seite „Konfiguration“ eine Kategorie aus einer Vorlage zu erstellen.

1. Navigieren Sie auf der Seite „Konfiguration“ zu der Vorlagenkategorie, die Sie duplizieren möchten.

   Im Gegensatz zu anderen Kategorien sind Vorlagenkategorien kursiv geschrieben und stehen in Klammern.
2. Klicken Sie auf die Vorlagenkategorie.
3. Geben Sie einen Namen in das Feld **Neuer Kategoriename** ein (erforderlich).
4. Sie können die Eigenschaften innerhalb der neuen Kategorie sofort oder später bearbeiten.
5. Klicken Sie auf **Änderungen speichern**, um die neue Konfiguration zu speichern.

Die neue Kategorie wird in der Navigationsstruktur angezeigt.

Löschen einer Kategorie

Verwenden Sie diese Prozedur, um auf der Seite „Konfiguration“ eine Kategorie zu löschen.

Auf der Seite „Konfiguration“ können einige Kategorien gelöscht werden, andere jedoch nicht. Jede Kategorie, die Sie aus einer Vorlage erstellt haben, können Sie auch wieder löschen. Wenn ein Unica-Produkt registriert wurde, können möglicherweise auch einige der darin enthaltenen Kategorien gelöscht werden.

1. Navigieren Sie auf der Seite „Konfiguration“ zu der Kategorie, die Sie löschen möchten, und wählen Sie die Kategorie aus, um die Seite „Einstellungen“ der Kategorie zu öffnen.

   Kann die geöffnete Kategorie gelöscht werden, erscheint ein Link **Kategorie löschen**.
2. Klicken Sie auf den Link **Kategorie löschen**.

   Es erscheint ein Fenster mit der Frage: Möchten Sie "category name" wirklich löschen?
3. Klicken Sie auf **OK**.

Die Kategorie wird nicht mehr in der Navigationsstruktur angezeigt.

Dashboard-Management

Dashboards sind konfigurierbare Seiten mit nützlichen Informationen für Benutzergruppen, die über unterschiedliche Rollen in Ihrem Unternehmen verfügen. Die Komponenten, aus denen Dashboards bestehen, werden als Portlets bezeichnet. Dashboards können vordefinierte Portlets oder von Ihnen erstellte Portlets enthalten.

Sie können Dashboards selbst erstellen und konfigurieren oder die vorgefertigten Dashboards verwenden. Vorgefertigte Dashboards enthalten vordefinierte Portlets in Kombinationen, die für Benutzer mit einer Vielzahl von Rollen innerhalb Ihres Unternehmens nützlich sind.

Sie können auch eigene benutzerdefinierte Portlets über die Unica-Produktseiten, über Seiten Ihres Unternehmens-Intranets oder über Internetseiten erstellen.

Planung von Dashboards

Beraten Sie sich mit dem Marketing Management-Team über folgende Punkte, wenn Sie die Verwendung der Dashboardfunktion in Ihrem Unternehmen planen.

- Welche Dashboards werden von den Benutzern benötigt?
- Welche Benutzer benötigen Zugriff auf welche Dashboards?
- Welche Portlets sollten zu den Dashboards hinzugefügt werden?
- Wer übernimmt die Rolle des Dashboardadministrators für die einzelnen Dashboards, nachdem diese bereitgestellt wurden? Der Dashboardadministrator verwaltet den Benutzerzugriff auf das Dashboard und passt den individuellen Inhalt und das Layout des Dashboards ggf. an.

Dashboardzielgruppen

Sie können steuern, wer Ihre Dashboards anzeigen kann, indem Sie den Dashboards Gruppen oder einzelne Benutzern zuordnen. Mitglieder einer Gruppe können auf Dashboards zugreifen, die dieser Gruppe zugeordnet sind. Benutzer, die nicht Mitglieder dieser Gruppe sind, können diese Dashboards nicht anzeigen.

Sie können zudem globale Dashboards erstellen, die von allen Unica-Benutzern einer Partition unabhängig von der Gruppenzugehörigkeit oder Einzelzuordnungen verwendet werden können.

Wenn Sie ein globales Dashboard erstellen, sollten Sie Portlets hinzufügen, die für eine möglichst große Anzahl von Benutzern von Interesse sind. Ist beispielsweise Unica Campaign installiert, sollten Sie das Portlet „Eigene benutzerdefinierte Lesezeichen“ (ein vordefiniertes Unica-Portlet) aufnehmen.

Erforderliche Benutzerberechtigungen zum Anzeigen von Dashboards

Dashboards ermöglichen es Unica-Benutzern, Seiten aus mehreren Produkten (z.B.Unica Plan und Unica Campaign) auf einer einzigen Seite anzuzeigen, unabhängig von den konfigurierten Berechtigungen dieser Benutzer in den jeweiligen Produkten.

Bei einigen Dashboard-Portlets können Benutzer Aufgaben in einem Unica-Produkt auszuführen, indem sie auf einen Link in einem Portlet klicken, um eine Seite zu öffnen, mit der sie arbeiten können. Wenn der Benutzer nicht über die erforderlichen Berechtigungen für die Aufgabe verfügt, wird die Seite nicht angezeigt.

Einige Inhalte in Portlets werden abhängig vom jeweiligen Benutzer gefiltert. Wenn ein Benutzer z. B. nie direkt mit Kampagnen arbeitet, werden im Portlet „Eigene aktuelle Kampagnen“ möglicherweise keine Links angezeigt.

Vordefinierte Portlets

Unica stellt zwei Typen von vordefinierten Dashboard-Portlets bereit, die Sie aktivieren und einem der von Ihnen erstellten Dashboards hinzufügen können.

Vordefinierte Unica-Portlets verwenden Unica Platform-Mechanismen für die einmalige Anmeldung (Single Sign-on) zum Zugriff auf den Unica-Inhalt. Benutzer werden nicht zur Angabe ihrer Berechtigungsnachweise aufgefordert, wenn sie ein Dashboard anzeigen, das diese Portlets enthält.

- Liste: Eine Liste benutzerspezifischer Unica-Elemente. Beispiele für Listenportlets sind „Eigene aktuelle Kampagnen“ (Unica Campaign), „Eigene Alerts“ (Unica Plan und der Bericht „Übersicht nach Kontinenten“ (Digital Analytics for On Premises).
- IBM® Cognos® oder Unica Insights-Berichte: Eine speziell formatierte Version von Unica-Berichten.

Sie können auch eigene angepasste Dashboard-Portlets erstellen.

Verfügbarkeit von vordefinierten Portlets

Unica stellt für viele Produkte vordefinierte Portlets bereit. Die Verfügbarkeit der vordefinierten Portlets ist abhängig von den installierten Unica-Produkten. Die Berichts-Portlets sind zudem nur verfügbar, wenn die Berichtsfunktion mit Unica Insights oder IBM Cognos implementiert ist.

Sie müssen die vordefinierten Portlets in Unica Platformaktivieren, bevor Sie sie in einem Dashboard verwenden können. Unica-Portlets werden in Unica Platform aufgelistet, unabhängig davon ,ob das Produkt, zu dem sie gehören, installiert ist oder nicht. Es hat sich bewährt, nur die Portlets zu aktivieren, die zu installierten Produkten gehören. Nur die aktivierten Portlets werden in der Liste mit den Portlets, die einem Dashboard hinzugefügt werden können, aufgeführt.

Unica Plan Berichtsportlets

In der folgenden Tabelle werden die Unica Plan-Dashboard-Portlets beschrieben, die nach der Installation von Unica Insights oder des Cognos Unica Plan Reports-Package für Cognos verfügbar sind.

Tabelle 13. Unica Plan Standardberichtsportlets

Bericht	Beschreibung
Budget nach Projekttyp	Ein Beispielbericht mit einem 3-D-Kreisdiagramm, das das Budget pro Projekttyp für das laufende Kalenderjahr zeigt. Für diesen Bericht ist das Finanzmanagementmodul erforderlich.

Tabelle 13. Unica Plan Standardberichtsportlets (Fortsetzung)

Bericht	Beschreibung
Beendete Projekte nach Quartal	Ein Beispielbericht mit einem 3-D-Balkendiagramm, das die Anzahl der in diesem Quartal vorzeitig, termingerecht oder verspätet abgeschlossenen Projekte zeigt.
Prognose nach Projekttyp	Ein Beispielbericht mit einem 3-D-Kreisdiagramm, das die prognostizierten Ausgaben pro Projekttyp für das laufende Kalenderjahr zeigt.
Manager-Genehmigungsübersicht	Ein Beispielbericht mit Daten zu aktiven und abgeschlossenen Genehmigungen für alle Projekte im System mit dem Status „Wird ausgeführt“.
Manager-Aufgabe-Übersicht	Ein Beispielbericht mit Daten zu aktiven und abgeschlossenen Aufgaben für alle Projekte mit dem Status „Wird ausgeführt“.
Finanzposition für Marketing	Ein Beispielbericht, der eine Zeitachse mit den budgetierten, prognostizierten, festgeschriebenen und Ist-Beträgen für alle Pläne mit beliebigem Status im laufenden Kalenderjahr zeigt. Für diesen Bericht ist das Finanzmanagementmodul erforderlich.
Eigene Aufgabe-Übersicht	Ein Beispielbericht, der Daten zu allen aktiven und abgeschlossenen Aufgaben für den Benutzer, der den Bericht anzeigt, in allen Projekten mit dem Status „Wird ausgeführt“ zeigt.
Eigene Genehmigungsübersicht	Ein Beispielbericht zeigt Daten über aktive und abgeschlossene Genehmigungen für den Benutzer, der diesen Bericht in allen Projekten mit dem Status „In Bearbeitung“ anzeigt.
Projekte nach Projekttyp	Ein Beispielbericht mit einem 3-D-Kreisdiagramm, das alle Projekte im System mit dem Status „Wird ausgeführt“ nach Vorlagentyp anzeigt.

Tabelle 13. Unica Plan Standardberichtsportlets (Fortsetzung)

Bericht	Beschreibung
Projekte nach Status	Ein Beispielbericht mit einem 3-D-Balkendiagramm, das alle Projekte im System nach Status anzeigt: „Entwurf“, „Wird ausgeführt“, „Zurückgestellt“, „Abgebrochen“ und „Abgeschlossen“.
Angeforderte und beendete Projekte	Ein Beispielbericht mit einem Zeitachsendiagramm, das die Anzahl der Projektanforderungen und die Anzahl der abgeschlossenen Projekte pro Monat zeigt. Dieser Bericht berücksichtigt nur Projektanforderungen mit dem folgenden Status: „Übergeben“, „Akzeptiert“ und „Zurückgegeben“.
Ausgaben nach Projekttyp	Ein Beispielbericht mit einem 3-D-Kreisdiagramm, das den tatsächlich pro Projekttyp ausgegebenen Betrag im laufenden Kalenderjahr zeigt. Für diesen Bericht ist das Finanzmanagementmodul erforderlich.

Unica Plan-Listenportlets

Wenn das Unica Plan-Berichtspaket nicht installiert ist, haben Sie weiterhin Zugriff auf die in Ihrem Dashboard verfügbaren Unica Plan-Listenportlets.

Ihr Systemadministrator wählt die Portlets aus, die Mitglieder Ihres Unternehmens dem Dashboard hinzufügen können. Zum Verwalten Ihrer Dashboards und Hinzufügen von Portlets zu Dashboards wählen Sie **Dashboard > Dashboard erstellen** aus.

Tabelle 14. Unica Plan-Standardlistenportlets

Bericht	Beschreibung
Genehmigungen mit Handlungsbedarf	Liste mit Genehmigungen, für die eine Aktion Ihrerseits erforderlich ist.

Tabelle 14. Unica Plan-Standardlistenportlets (Fortsetzung)

Bericht	Beschreibung
Meine Tasks verwalten	Liste Ihrer anstehenden und aktiven Tasks und Genehmigungen mit dem Status „Nicht gestartet“ und „In Bearbeitung“. Eine Option, um den Status jedes Elements zu ändern, wird angezeigt. • Bei Tasks können Sie den Status in „Abschließen“ oder „Überspringen“ ändern. • Bei Genehmigungen mit dem Status „Nicht gestartet“ können Sie den Status in „Übergeben“ oder „Abbrechen“ ändern. • Bei Genehmigungen mit dem Status „In Bearbeitung“, deren Eigentümer Sie sind, können Sie den Status in „Stoppen“, „Abschließen“ oder „Abbrechen“ ändern. • Bei Genehmigungen mit dem Status „In Bearbeitung“, die Ihnen zur Genehmigung zugewiesen sind, können Sie den Status in „Genehmigen“ oder „Ablehnen“ ändern.
Eigene aktive Projekte	Listet Ihre aktiven Projekte auf.
Eigene Benachrichtigungen	Listet Ihre Unica Plan-Alerts auf.
Status eigener Projekte	Listet den Namen, den Status, den Prozentsatz abgeschlossener Tasks und die Anzahl der Task, die Ihnen zugewiesen sind, für jedes Projekt auf, dessen Eigentümer Sie sind oder für das Sie als Prüfer oder Mitglied angegeben sind. Der Prozentsatz abgeschlossener Tasks wird folgendermaßen berechnet: `(Number of Finished Tasks + Number of Skipped Tasks)/ Total Number of Workflow Tasks`

Tabelle 14. Unica Plan-Standardlistenportlets (Fortsetzung)

Bericht	Beschreibung
	• Um den aktuellen Status eines Projekts neu zu berechnen, klicken Sie auf . Die Neuberechnung des Status erfolgt nur für die Anzeige in diesem Portlet. Sie erfolgt an keiner anderen Stelle in Unica Plan. **Anmerkung:** Projektstatusberechnungen können nur in 5-Minuten-Intervallen erfolgen. • Wenn Sie mehr als 100 Projekte besitzen, klicken Sie auf **Alle anzeigen**, um die Liste in einem neuen Dialogfeld zu öffnen. • Zum Exportieren der aufgelisteten Projektdaten in eine CSV-Datei klicken Sie auf **Exportieren**. • Übersichtsdaten zu einem Projekt können Sie auf der Registerkarte **Übersicht** anzeigen. Zum Anzeigen weiterer Metriken für den Projektstatus klicken Sie auf den Indikator für den Prozentsatz abgeschlossener Task. Zum Anzeigen der Liste **Eigene Tasks** klicken Sie auf die Zahl in der Spalte „Tasks“.
Eigene Anforderungen	Listet Anforderungen auf, deren Eigentümer Sie sind.
Meine Aufgaben	Listet Tasks auf, deren Eigentümer Sie sind.
Projekte über dem Budget	Listet alle Projekte im Kalenderjahr auf, die das Budget überschritten haben. **Anmerkung:** Für diesen Bericht ist das Finanzmanagementmodul erforderlich.

Berichtsportlets für Unica Campaign

Die Unica Insights- oder IBM®Cognos®-Berichtsportlets werden als Teil des Unica Campaign-Berichtspakets bereitgestellt. Mit Berichtsportlets können Sie Antwortraten und die Kampagneneffektivität analysieren.

Nach der Aktivierung können Sie jedem von Ihnen selbst erstellten Dashboard vordefinierte Dashboard-Portlets hinzufügen. Zum Verwalten Ihrer Dashboards und Hinzufügen von Portlets zu Dashboards klicken Sie auf **Dashboard > Dashboard erstellen**.

Tabelle 15. IBM® Cognos®Berichtsportlets für Unica Campaign

Bericht	Beschreibung
Unica Campaign -Renditevergleich	Ein Bericht, in dem auf übergeordneter Ebene die Rendite von erstellten oder aktualisierten Kampagnen des Benutzers verglichen wird, der den Bericht anzeigt.
Unica Campaign -Antwortratenvergleich	Ein Bericht, in dem die Antwortraten von einer oder mehreren Kampagnen verglichen werden, die von dem Benutzer erstellt oder aktualisiert wurden, der den Bericht anzeigt.
Unica Campaign -Ertragsvergleich nach Angebot	Ein Bericht, in dem der bis dato erzielte Ertrag pro Kampagne mit Angeboten verglichen wird, die von dem Benutzer erstellt oder aktualisiert wurden, der den Bericht anzeigt.
Angebotsantworten in den letzten 7 Tagen	Ein Bericht, in dem die Anzahl der Antworten verglichen wird, die in den letzten 7 Tagen eingegangen sind. Grundlage bilden die einzelnen Angebote, die von dem Benutzer erstellt oder aktualisiert wurden, der den Bericht anzeigt.
Rücklaufquote Angebotsantworten	Ein Bericht, in dem die Antwortrate nach Angebot verglichen wird. Grundlage bildet das Angebot, das von dem Benutzer erstellt oder aktualisiert wurde, der den Bericht anzeigt.
Aufschlüsselung der Angebotsantworten	Ein Bericht, in dem die aktiven Angebote nach Status aufgeschlüsselt angezeigt werden. Grundlage bilden die Angebote, die

Tabelle 15. IBM® Cognos®Berichtsportlets für Unica Campaign (Fortsetzung)

Bericht	Beschreibung
	von dem Benutzer erstellt oder aktualisiert wurden, der den Bericht anzeigt.

Unica Campaign-Listenportlets

Die Unica Campaign-Standardlistenportlets stehen auch zur Verwendung in Dashboards zur Verfügung, wenn das Berichtspaket für Unica Campaign nicht installiert ist.

Tabelle 16. Unica Campaign-Listenportlets

Bericht	Beschreibung
Eigene benutzerdefinierte Lesezeichen	Eine Liste mit Links zu Webseiten oder Dateien, die von dem Benutzer erstellt wurden, der den Bericht anzeigt.
Eigene aktuelle Kampagnen	Eine Liste der Kampagnen, die kürzlich von dem Benutzer erstellt wurden, der den Bericht anzeigt.
Eigene aktuelle Sitzungen	Eine Liste der Sitzungen, die kürzlich von dem Benutzer erstellt wurden, der den Bericht anzeigt.
Unica Campaign - Monitorportlet	Eine Liste der kürzlich oder zurzeit ausgeführten Kampagnen, die durch den Benutzer erstellt wurden, der den Bericht anzeigt.

Unica Deliver Berichtsportlets

Die folgenden Dashboard-Portlets sind mit Unica Insights oder mit dem Unica Deliver-Berichtspaket erhältlich.

Bericht	Beschreibung
Kürzlich erfolgte E-Mail-Bounce-Antworten	Dieser Dashboardbericht stellt Daten für verschiedene Typen von E-Mail-Zurückweisungen in Form eines Balkendiagramms dar. Das Diagramm stellt die aktuellen Zurückwei-

Bericht	Beschreibung
	sungsantworten für die letzten fünf Mailings dar, die vor dem aktuellen Tag gesendet wurden.
Kürzlich erfolgte E-Mail-Kampagnen gesendet	Dieser Dashboardbericht stellt eine Zusammenfassung Ihrer letzten Mailing-Aktivitäten bereit. Er listet die Gesamtsummen für Nachrichtenübertragungen, Antworten der Empfänger und E-Mail-Zurückweisungen für die letzten fünf Mailings dar, die vor dem aktuellen Tag gesendet wurden.

Unica Interact Berichtsportlet

Leistung Interaktionspunkt – Zeigt die Anzahl der pro Interaktionspunkt angenommenen Angebote innerhalb von sieben Tagen.

Dieser Dashboardbericht ist so definiert, dass er auf den interaktiven Kanal mit der ID 1 verweist. Wenn Sie zusätzliche Versionen dieses Berichts erstellen möchten (für Berichte zu zusätzlichen interaktiven Kanälen) oder die ID des interaktiven Kanals, auf die dieser Bericht verweist, geändert werden soll, lesen Sie die Informationen unter Konfigurieren des Dashboard-Portlets "Interaktionspunkterfolg" (auf Seite 67).

Konfigurieren des Dashboard-Portlets "Interaktionspunkterfolg"

Unica Interact hat einen Cognos® Dashboard-Bericht: Übersicht der Interaktionspunkte. Da Dashboardberichte Benutzer nicht zur Eingabe von Abfrageparametern auffordern, handelt es sich bei der Kanal-ID des interaktiven Kanals im Bericht "Leistung Interaktionspunkt" um einen statischen Wert. Die Kanal-ID für diesen Bericht ist standardmäßig auf 1 gesetzt. Wenn die Kanal-ID für Ihre Implementierung nicht korrekt ist, können Sie den Bericht anpassen und die Kanal-ID im Filterausdruck des Berichts ändern.

Zum Anpassen der Cognos®-Berichte benötigen Sie Kenntnisse in der Erstellung von Cognos®-Berichten. Ausführliche Informationen zum Erstellen und Bearbeiten von Cognos®BI-Berichten finden Sie in der Cognos® BI-Dokumentation und hier insbesondere im Cognos®BI Report Studio - Benutzerhandbuch für professionelles Authoring für die von Ihnen verwendete Version von Cognos®.

Informationen zu den Abfragen und Datenelementen im Bericht "Interaktionspunkterfolg" finden Sie in der Referenzliteratur, die zum Lieferumfang des Unica Interact-Berichtspakets gehört.

Wenn Sie ein Diagramm für mehrere interaktive Kanäle im Dashboard anzeigen wollen, dann müssen Sie eine Kopie des Dashboards "Interaktionspunkterfolg" erstellen und die Kanal-ID ändern. Erstellen Sie dann ein neues Dashboard-Portlet für den neuen Bericht und fügen Sie es Ihren Dashboards hinzu.

Unica Collaborate-Listenportlets

In diesem Abschnitt werden die Unica Collaborate-Standardportlets beschrieben, die zur Verwendung in Dashboards zur Verfügung stehen.

Tabelle 17. Unica Collaborate-Listenportlets

Bericht	Beschreibung
Listenverwaltung	Eine Liste der aktiven Listen für den Benutzer, der den Bericht anzeigt.
Kampagnenverwaltung	Eine Liste aktiver Unternehmenskampagnen und On-Demand-Kampagnen für den Benutzer, der den Bericht anzeigt.
Abonnementmanagement	Eine Liste der Abonnements von Unternehmenskampagnen des aktuellen Benutzers.
Kalender	Im Kalender wird der Zeitplan für aktive Unternehmenskampagnen und On-Demand-Kampagnen angezeigt.

Unica Optimize-Listenportlets

Hier werden die Unica Optimize-Standardportlets beschrieben, die zur Verwendung in Dashboards zur Verfügung stehen.

Die folgenden Portlets sind ausschließlich für die Verwendung im Unica-Dashboard verfügbar.

Tabelle 18. Unica Optimize-Listenportlets

Eine zweispaltige Tabelle, welche die Listenportlets in Unica Optimize beschreibt.

Bericht	Beschreibung
Eigene aktuelle Unica Optimize Sitzungen	Eine Liste der letzten zehn Unica Optimize-Sitzungen, die von dem Benutzer, der den Bericht anzeigt, innerhalb der letzten 30 Tage ausgeführt wurden.
Eigene kürzlich erfolgreiche Unica Optimize-Ausführungsinstanzen	Eine Liste der letzten zehn Unica Optimize-Sitzungen, die von dem Benutzer, der den Bericht anzeigt, ausgeführt und innerhalb der letzten 30 Tage erfolgreich abgeschlossen wurden.
Eigene kürzlich fehlgeschlagene Unica Optimize-Ausführungsinstanzen	Eine Liste der letzten zehn Unica Optimize-Sitzungen, die von dem Benutzer, der den Bericht anzeigt, ausgeführt wurden und innerhalb der letzten 30 Tage nicht erfolgreich abgeschlossen wurden.

Vorgefertigte Dashboards

Unica stellt vorgefertigte Dashboards bereit, die geeignete Portlets für verschiedene Benutzergruppen enthalten.

Verfügbarkeit vorgefertigter Dashboards

Vorgefertigte Dashboards sind verfügbar, sobald Sie Unica Platform installiert haben. Um diese Dashboards jedoch vollständig zu implementieren, müssen Sie auch alle Produkte installieren, die zur Unterstützung der enthaltenen Portlets erforderlich sind, und die Portlets müssen aktiviert werden.

Damit ein vorgefertigtes Dashboard verfügbar ist, muss mindestens eines der die vorgefertigten Dashboards unterstützenden Produkte installiert sein. Wenn ein vorgefertigtes Dashboard beispielsweise Portlets enthält, die aus Unica Campaign und Unica Deliver stammen, ist das Dashboard nur verfügbar, wenn eines dieser Produkte

installiert ist. Ist keines der beiden Produkte installiert, wird das Dashboard nicht in der Benutzeroberfläche angezeigt. Wenn eines der Produkte fehlt, werden die von diesem Produkt abhängigen Portlets mit einer Nachricht angezeigt, in der darauf hingewiesen wird, dass sie nicht verfügbar sind.

Liste vorgefertigter Dashboards

In der folgenden Tabelle sind die vorgefertigten Dashboards beschrieben: Es werden der Zweck, die Portlets, aus denen vorgefertigte Dashboards bestehen können, und die erforderlichen Produkte beschrieben.

Tabelle 19. Liste vorgefertigter Dashboards

Vorgefertigtes Dashboard	Zweck	Portlets	Erforderliche Produkte
Kampagnenverwaltung	Dieses Dashboard zeigt die Finanzergebnisse von Kampagnen an.	• Finanzübersicht nach Angebot • Kampagnenerfolgsvergleich	• Unica Campaign • Unica Insights oder Unica Campaign Berichtspaket
Projekt- und Datenverkehrsmanagement	Dieses Dashboard stellt Statusaktualisierungen für Projekte bereit.	• Eigene Aufgaben • Eigene Benachrichtigungen • Eigene aktive Projekte • Eigene Task-Übersicht • Angeforderte und beendete Projekte	• Unica Plan • Unica Insights oder Unica Plan Berichtspaket

Tabelle 19. Liste vorgefertigter Dashboards (Fortsetzung)

Vorgefertigtes Dashboard	Zweck	Portlets	Erforderliche Produkte
		• Genehmigungen mit Handlungsbedarf • Eigene Genehmigungsübersicht • Projekte nach Status	
Projektmitglied	Dieses Dashboard zeigt Aufgaben, für die eine Aktion erforderlich ist, und ermöglicht Benutzern, abgeschlossene Aufgaben zu schließen.	• Eigene Aufgaben • Eigene aktive Projekte • Eigene Benachrichtigungen • Eigene Anfragen	Unica Plan
Projektanfragen und -genehmigungen	Dieses Dashboard zeigt Aufgaben an, für die eine Aktion erforderlich ist, und stellt Statusaktualisierungen für Projekte bereit. Zudem bietet es eine gute Übersicht über die Finanzposition für das Marketing und über die Ausgaben.	• Genehmigungen mit Handlungsbedarf • Eigene Benachrichtigungen • Finanzposition für Marketing • Projekte nach Projekttyp • Budget nach Projekttyp	• Unica Plan mit dem Finanzmanagementmodul • Unica Insights oder Unica Plan Berichtspaket

Tabelle 19. Liste vorgefertigter Dashboards (Fortsetzung)

Vorgefertigtes Dashboard	Zweck	Portlets	Erforderliche Produkte
		• Ausgaben nach Projekttyp • Beendete Projekte nach Quartal	
Projekt-Finanzdaten	Dieses Dashboard bietet eine gute Übersicht über die Finanzposition für das Marketing sowie über die Ausgaben.	• Genehmigungen mit Handlungsbedarf • Finanzposition für Marketing • Benachrichtigung • Projekte nach Typ • Beendete Projekte nach Quartal	• Unica Plan mit dem Finanzmanagementmodul • Unica Insights oder Unica Plan Berichtspaket

IBM® Cognos® Bericht Leistungsaspekte

Es ist empfehlenswert, Berichte zu Dashboards hinzuzufügen, da durch das visuelle Element große Datenmengen einfach überblickt werden können. Da Berichte jedoch zusätzliche Verarbeitungsressourcen belegen, kann die Leistung abnehmen, wenn viele Benutzer regelmäßig auf Dashboards mit vielen Berichten zugreifen.

Unternehmen gehen je nach Anforderungen unterschiedlich mit Daten um. Dieser Abschnitt enthält einige allgemeine Richtlinien, die dabei helfen sollen, die Leistung von Dashboards zu verbessern, die IBM® Cognos®-Berichte enthalten. Alle Richtlinien beziehen sich auf IBM® Cognos®-Berichtsportlets, da diese die meisten Ressourcen benötigen.

Planung läuft in IBM® Cognos®

IBM® Cognos® Berichte können in regelmäßigen Zeitabständen ausgeführt werden. Wenn ein Bericht geplant wird, wird er nicht jedes Mal ausgeführt, wenn ein Benutzer auf ein Dashboard mit diesem Bericht zugreift. Das Ergebnis ist eine verbesserte Leistung der Dashboards mit dem Bericht.

Nur Unica Berichte ohne Benutzer-ID-Parameter können in Cognos® geplant werden. Berichte ohne ID-Parameter sehen für alle Benutzer gleich aus, weil die Daten nicht anhand der Benutzer-ID gefiltert werden. Folgende Portlets können nicht geplant werden.

- Alle vordefinierten Unica Campaign Portlets
- Die vordefinierten Unica Plan Portlets „Eigene Aufgabenübersicht“ und „Eigene Genehmigungsübersicht“

Die Planung von Berichten wird in IBM® Cognos® ausgeführt. Weitere Informationen zu allgemeinen Planungsaufgaben finden Sie in der Cognos®-Dokumentation. Die besonderen Planungsanforderungen an Dashboard-Portlets finden Sie unter Planen eines Dashboardberichts (auf Seite 74).

Datenaspekte

Es empfiehlt sich, Ausführungen auf Grundlage der Daten im Bericht zu planen. Beispielsweise kann der Dashboardbericht „Angebotsantworten in den letzten 7 Tagen“ jede Nacht ausgeführt werden, sodass er relevante Informationen zu den sieben Tagen vor dem aktuellen Tag enthält. Der Dashboardbericht „Finanzposition für Marketing“ muss dagegen nur einmal pro Woche ausgeführt werden, da die Finanzindikatoren nach Quartal verglichen werden.

Benutzererwartungen

Als zusätzliche Überlegung sollte in die Planung mit einfließen, wie häufig die vorgesehenen Benutzer des Berichts eine Aktualisierung der Daten benötigen. Sie sollten die Benutzer diesbezüglich befragen, wenn die Zeitpläne erstellt werden.

Richtlinien

Es folgen einige allgemeine Richtlinien, die Sie bei der Planung von IBM® Cognos®-Dashboardberichten unterstützen.

- Berichte mit Rollup-Informationen sollten generell so geplant werden, dass sie jede Nacht ausgeführt werden.
- Berichte mit umfangreichen Berechnungen sollten in einen Zeitplan aufgenommen werden.

Planen eines Dashboardberichts

Um einen Dashboardbericht zu planen (vordefiniertes Portlet oder vom Benutzer erstelltes Portlet), müssen Sie zunächst eine Ansicht erstellen und planen und anschließend das Portlet konfigurieren (siehe Beschreibung).

Anmerkung: Sie können nur Berichte planen, die nicht nach Benutzern gefiltert sind.

1. Kopieren Sie den Bericht in Cognos® und speichern Sie ihn unter einem neuen Namen.
2. Öffnen Sie den kopierten Bericht in Cognos® und speichern Sie ihn als Ansicht mit dem gleichen Namen wie der Originalbericht. Speichern Sie ihn im Ordner `Unica Dashboard/ Product` , wobei `Product` der entsprechende Produktordner ist.
3. Planen Sie die Ansicht in Cognos®.
4. Fügen Sie (falls noch nicht erfolgt) in Unica den Bericht dem Dashboard hinzu.
5. Nur wenn der Bericht eines der vordefinierten Portlets ist, gehen Sie in Unica wie folgt vor.
    - Klicken Sie auf der Seite „Dashboardadministration“ auf das Symbol **Portlet bearbeiten** neben dem betreffenden Portlet.
    - Wählen Sie neben der Frage **Wurde dieser Bericht geplant?** die Option **Ja** aus.
    - Klicken Sie auf **Speichern**.

Dashboardkonfiguration

Die Themen in diesem Abschnitt beschreiben, wie Sie Dashboards konfigurieren.

Erforderliche Berechtigungen zum Verwalten von Dashboards

Nur Benutzer mit der Berechtigung „Dashboards verwalten“ in einer Partition können alle Dashboards in dieser Partition verwalten. Standardmäßig wird diese Berechtigung Benutzern mit der Unica Platform-Rolle „AdminRole“ erteilt.

Bei der Erstinstallation von Unica Platform wird einem vordefinierten Benutzer (asm_admin) diese Rolle für die Standardpartition (partition1) zugeteilt. Die erforderlichen Berechtigungsnachweise für Dashboardadministratoren erhalten Sie von Ihrem Administrator.

Ein Benutzer mit der Unica Platform-Rolle „AdminRole“ kann jedem anderen Unica-Benutzer die Berechtigung zum Verwalten einzelner Dashboards in der Partition erteilen, zu der dieser Benutzer gehört. Dashboards werden im Unica Platform-Dashboardverwaltungsbereich verwaltet.

Dashboard-Layout

Wenn Sie einem neuen Dashboard zum ersten Mal ein Portlet hinzufügen, wird ein Fenster geöffnet, in dem Sie aufgefordert werden, ein Layout auszuwählen und zu speichern. Sie können das Layout später ändern, indem Sie die Registerkarte für das Dashboard und dann ein anderes Layout auswählen.

Folgende Optionen stehen zur Verfügung:

- 3 Spalten, gleiche Breite
- 2 Spalten, gleiche Breite
- 2 Spalten, 2/3-1/3-Breite
- 1 Spalte, volle Breite
- Benutzerdefiniert

Dashboards und Partitionen

Wenn Sie Dashboards in einer Umgebung mit mehreren Partitionen verwalten, sollten Sie diesen Abschnitt lesen, um zu verstehen, wie mehrere Partitionen Dashboards beeinflussen.

In einer Umgebung mit mehreren Partitionen kann ein Benutzer nur die Dashboards anzeigen oder verwalten, die der Partition zugeordnet sind, zu der der Benutzer gehört.

Wenn ein Dashboardadministrator ein Dashboard erstellt, gelten die folgenden partitionsbezogenen Regeln.

- Jedes Dashboard, das erstellt wird, ist nur für die Benutzer verfügbar, die zu derselben Partition gehören, zu der auch der Benutzer, der das Dashboard erstellt hat, gehört.
- Nur die vordefinierten Portlets, die in der Partition aktiviert sind, zu der der Administrator gehört, sind zum Einschließen in das Dashboard verfügbar.
- Nur die Gruppen und Benutzer, die derselben Partition wie der Administrator zugeordnet sind, sind für eine Zuweisung zum Dashboard verfügbar.

Übersicht über das Arbeiten mit Dashboards in einer Umgebung mit mehreren Partitionen

Sind mehrere Partitionen konfiguriert, führen Sie die folgenden Anleitungen zum Konfigurieren von Dashboards aus.

1. Bevor Sie mit Dashboards arbeiten, ordnen Sie jeder Partition mindestens eine Gruppe zu und ordnen Sie anschließend jeder Gruppe die entsprechenden Benutzer zu.

   Nur der Benutzer "platform_admin" oder ein anderer Benutzer mit den Berechtigungen von „PlatformAdminRole“ kann diese Aufgabe ausführen.
2. Stellen Sie für jede Partition sicher, dass mindestens ein Benutzer über die Berechtigung „Dashboards verwalten“ verfügt und notieren Sie sich diese Benutzernamen.

   Die Unica Platform-Rolle „AdminRole“ verfügt standardmäßig über diese Berechtigung, aber Sie möchten möglicherweise eine Rolle mit stärker eingeschränktem Zugriff für Dashboardadministratoren erstellen. Diese Dashboardadministratoren können alle Dashboards auf ihrer Partition verwalten.
3. Gehen Sie für jede Partition, die in Ihrem System konfiguriert ist, wie im Folgenden beschrieben vor.
   a. Verwenden Sie ein Konto, das zur Partition gehört und alle Dashboards auf einer Partition verwalten kann, für die Anmeldung an Unica.

      Verwenden Sie dafür die Liste der Benutzer, die Sie im vorherigen Schritt erstellt haben.

b. Aktivieren Sie auf der Seite **Einstellungen > Dashboard-Portlets** die vordefinierten Portlets gemäß Ihren Anforderungen.
c. Erstellen Sie auf der Seite „Dashboardadministration“ die erforderlichen Dashboards und fügen Sie die Portlets hinzu.
d. Ordnen Sie jedem nicht globalen Dashboard Benutzer hinzu, die das Dashboard anzeigen können.

   Sie können dem Dashboard einzelne Benutzer oder Gruppen hinzufügen.
e. Fügen Sie jedem Dashboard mindestens einen Benutzer als Dashboardadministrator hinzu.

Aktivieren oder Inaktivieren vordefinierter Portlets

Führen Sie diese Aufgabe aus, bevor Sie mit dem Erstellen von Dashboards beginnen. Sie sollten nur Portlets aktivieren, die zu installierten Unica-Produkten gehören.

1. Melden Sie sich bei Unica an und wählen Sie **Einstellungen > Dashboard-Portlets** aus.
2. Klicken Sie auf die Kontrollkästchen neben den Namen der Portlets, um die Portlets zu aktivieren oder zu inaktivieren.

   Ein Kontrollkästchen mit Häkchen kennzeichnet aktivierte Portlets. Wird das Häkchen entfernt, wird ein Portlet inaktiviert.

   Die von Ihnen ausgewählten Portlets sind aktiviert und für die Einbindung in die Dashboards verfügbar.

Erstellen eines nicht vorgefertigten Dashboards

Verwenden Sie diese Prozedur, um ein Dashboard zu erstellen, das nicht vorgefertigt ist.

1. Wählen Sie in Unica die Option **Dashboard** aus, um die Seite „Dashboardadministration“ zu öffnen.

   Alle Dashboards, die Ihrer Partition zugeordnet sind, werden angezeigt.
2. Klicken Sie auf **Dashboard erstellen**, um die Seite „Dashboard erstellen“ zu öffnen.
3. Geben Sie einen eindeutigen Titel (erforderlich) und eine Beschreibung (optional) ein.
4. Wählen Sie grundlegende Berechtigungen aus.

- Wenn Sie den Zugriff auf Benutzer beschränken möchten, die zu einer dem Dashboard zugeordneten Gruppe gehören, dann wählen Sie **Benutzer- oder gruppenspezifisches Dashboard** aus.
- Wenn alle Benutzer in der Partition in der Lage sein sollen, das Dashboard anzuzeigen, wählen Sie **Globales Dashboard für jeden** aus.

5. Wählen Sie unter **Typ** die Option **Dashboard erstellen** aus.
6. Klicken Sie auf **Speichern**.

   Ihr neues Dashboard wird als Registerkarte auf der Seite "Dashboardadministration" angezeigt und auf der Registerkarte „Administration“ aufgelistet.

Sie können jetzt Portlets hinzufügen.

Erstellen eines vorgefertigten Dashboards

Verwenden Sie diese Prozedur, um ein vorgefertigtes Dashboard zu erstellen.

1. Stellen Sie sicher, dass die Portlets, aus denen das zu erstellende, vorgefertigte Dashboard besteht, aktiviert sind.
2. Wählen Sie in Unica die Option **Dashboard** aus, um die Seite „Dashboardadministration“ zu öffnen.
3. Klicken Sie auf **Dashboard erstellen**.
4. Wählen Sie unter **Typ** die Option **Vorgefertigte Dashboards verwenden** aus.

   Die verfügbaren vorgefertigten Dashboards werden aufgelistet.
5. Wählen Sie das gewünschte vorgefertigte Dashboard aus und klicken Sie auf **Weiter**.

   Eine Liste der Portlets, die im vorgefertigten Dashboard enthalten sind, wird angezeigt. Die Liste weist darauf hin, wenn ein Portlet nicht verfügbar ist, entweder weil das erforderliche Produkt nicht installiert oder das Portlet nicht aktiviert ist.
6. Klicken Sie auf **Speichern**, um die Erstellung des Dashboards abzuschließen.

   Ihr neues Dashboard wird als Registerkarte auf der Seite "Dashboardadministration" angezeigt und auf der Registerkarte „Administration“ aufgelistet. Sie können die enthaltenen Portlets jetzt gegebenenfalls ändern.

Hinzufügen eines vordefinierten Portlets zu einem Dashboard

Verwenden Sie diese Prozedur, um einem Dashboard ein vordefiniertes Portlet hinzuzufügen.

1. Wählen Sie in Unica die Option **Dashboard** und dann die Registerkarte des Dashboards aus, mit dem Sie arbeiten möchten.
2. Klicken Sie auf **Portlets verwalten**, um eine Liste der aktivierten Portlets anzuzeigen.

   Sie können die Seite „Portlets verwalten“ auch über die Registerkarte „Administration“ aufrufen, indem Sie im Dashboard auf das Symbol „Portlets verwalten“ klicken.
3. Wählen Sie das Kontrollkästchen neben Portlets aus, um die Portlets für das Hinzufügen zum Dashboard auszuwählen.

   Sie können die folgenden Funktionen für die Auswahl von Portlets verwenden.

   - Filtern Sie die Liste der Portlets nach dem Namen oder nach dem Produkt, das die Quelle des Portlets ist.
   - Zeigen Sie alle Portlets gleichzeitig an oder blättern Sie durch die Liste.
   - Klicken Sie auf Spaltenüberschriften, um die Liste nach Quelle oder Portletname in auf- oder absteigender Reihenfolge alphabetisch zu sortieren.
4. Klicken Sie auf **Aktualisieren**.

   Die ausgewählten Portlets werden dem Dashboard hinzugefügt.

Entfernen eines Portlets aus einem Dashboard

Verwenden Sie diese Prozedur, um ein Portlet aus einem Dashboard zu entfernen.

1. Wählen Sie in Unica die Option **Dashboard** aus.

   Die Seite „Dashboardadministration“ wird geöffnet. Alle Ihrer Partition zugeordneten Dashboards werden zusammen mit einer Liste der jeweiligen Portlets angezeigt.
2. Klicken Sie in dem Dashboard, aus dem Sie ein Portlet entfernen möchten, neben dem Portlet, das Sie entfernen möchten, auf das Symbol **Löschen**.
3. Klicken Sie auf **Ja, löschen** bei der Eingabeaufforderung.

   Das Portlet wird aus dem Dashboard entfernt.

Ändern des Namens oder der Eigenschaften eines Portlets

Verwenden Sie diese Prozedur, um den Namen oder die Eigenschaften eines Portlets zu ändern.

1. Wählen Sie in Unica die Option **Dashboard** aus

   Die Seite „Dashboardadministration“ wird geöffnet. Alle Ihrer Partition zugeordneten Dashboards werden zusammen mit einer Liste der jeweiligen Portlets angezeigt.
2. Klicken Sie in dem Dashboard, mit dem Sie arbeiten möchten, neben dem Portlet, dessen Namen Sie ändern möchten, auf das Symbol **Portlet bearbeiten**.

   Das Fenster „Portlet bearbeiten“ wird geöffnet.
3. Bearbeiten Sie den Namen, die Beschreibung, die URL oder ausgeblendete Variablen des Portlets.
4. Klicken Sie auf **Speichern**.

Ändern des Namens oder der Eigenschaften eines Dashboards

Verwenden Sie diese Prozedur, um den Namen oder die Eigenschaften eines Dashboards zu ändern.

1. Wählen Sie in Unica die Option **Dashboard** aus

   Die Seite „Dashboardadministration“ wird geöffnet. Alle Dashboards, die Ihrer Partition zugeordnet sind, werden angezeigt.
2. Klicken Sie unten in dem Dashboard, mit dem Sie arbeiten möchten, auf das Symbol **Einstellungen verwalten**.

   Die Registerkarte „Einstellungen“ wird geöffnet.
3. Klicken Sie auf das Symbol **Dashboard bearbeiten**.

   Das Fenster „Dashboard bearbeiten“ wird geöffnet.
4. Bearbeiten Sie den Titel, die Beschreibung oder den Typ des Dashboards, aktivieren oder inaktivieren Sie das Dashboard oder ändern Sie die Einstellung, die festlegt, ob Benutzer das Layout ändern können.
5. Klicken Sie auf **Speichern**.

Löschen eines Dashboards

Verwenden Sie diese Prozedur, um ein Dashboard zu löschen.

1. Wählen Sie in Unica die Option **Dashboard** aus

   Die Seite „Dashboardadministration“ wird geöffnet. Alle Dashboards, die Ihrer Partition zugeordnet sind, werden angezeigt.
2. Klicken Sie unten in dem Dashboard, mit dem Sie arbeiten möchten, auf das Symbol **Dashboard löschen**.
3. Klicken Sie auf **Ja, löschen**, wenn Sie dazu aufgefordert werden.

   Das Dashboard wird gelöscht.

Zuordnen oder Ändern eines Dashboardadministrators

Verwenden Sie diese Prozedur, um einen Dashboardadministrator zuzuordnen oder zu ändern.

1. Wählen Sie in Unica die Option **Dashboard** aus

   Die Seite „Dashboardadministration“ wird geöffnet. Alle Ihrer Partition zugeordneten Dashboards werden zusammen mit einer Liste der jeweiligen Portlets angezeigt.
2. Klicken Sie unten in dem Dashboard, mit dem Sie arbeiten möchten, auf das Symbol **Berechtigungen verwalten**.
   Die Registerkarte „Berechtigungen verwalten“ wird geöffnet.
3. Klicken Sie auf das Symbol **Dashboardbenutzer verwalten**.
   Die Seite „Dashboardadministratoren verwalten“ wird geöffnet. Alle Ihrer Partition zugeordneten Dashboards werden zusammen mit einer Liste der jeweiligen Portlets angezeigt.
4. Aktivieren oder inaktivieren Sie die Namen.

   Benutzer, deren Namen ausgewählt sind, besitzen Administratorberechtigungen für das Dashboard.

   Sie können wie folgt vorgehen, um Benutzer zu suchen.

- Filtern Sie die Liste, indem Sie einen Benutzernamen ganz oder teilweise in das Feld **Suchen** eingeben.
- Zeigen Sie alle Benutzer oder nur nicht zugeordnete Benutzer oder nur zugeordnete Benutzer an.
- Sortieren Sie die Liste, indem Sie auf Spaltenüberschriften klicken.
- Zeigen Sie alle Benutzer gleichzeitig (auf der Grundlage der Filterkriterien) an oder blättern Sie die Liste durch.

5. Klicken Sie auf **Aktualisieren**.

Seite „Portlets verwalten“

In dieser Tabelle finden Sie die Hilfe zum Ausfüllen der Felder auf der Seite „Portlets verwalten“.

Tabelle 20. Felder auf der Seite „Portlets verwalten“

Feld	Beschreibung
Filter	Geben Sie einen Produkt- oder Portletnamen ganz oder teilweise ein, um die Porletliste auf der Basis des Produkts zu filtern, das den Bericht oder den Portletnamen bereitstellt.
Benutzerdefiniertes Portlet erstellen	Klicken Sie hier, um eine Seite zu öffnen, in der Sie ein Portlet erstellen können, das eine URL verwendet, die Sie erhalten haben.
Quick Link-Portlet erstellen	Klicken Sie hier, um ein Fenster zu öffnen, in dem Sie ein Quick Link-Portlet erstellen können.

Quick Link-Portlets

Quick Links sind vordefinierte Links zu Unica-Produkten. Einige Quick Links ermöglichen es Benutzern, grundlegende Aktionen im Unica-Produkt innerhalb des Dashboards auszuführen, ohne zum Produkt navigieren zu müssen. Sie können Portlets konfigurieren, die eine Reihe von Quick Links enthalten, die Sie ausgewählt haben.

Quick Links für Unica-Produkte werden installiert, wenn das Produkt installiert wird. Beginnend mit dem Release 9.0.0 stellt nur Unica Plan Quick Links zur Verfügung. Für Quick Links gelten die gleichen Sicherheitsaspekte wie für vordefinierte Portlets.

Um ein Quick Link-Portlet zu einem Ihrer Dashboards hinzuzufügen, klicken Sie auf **Portlets verwalten > Quick Link-Portlet erstellen** und wählen die Quick Links aus, die Sie einbinden möchten.

In der folgenden Tabelle werden die Quick Links beschrieben, die verfügbar sind, wenn Unica Plan installiert ist.

Tabelle 21. Liste der Quick Link-Portlets

Quick Link	Funktion
Neue Projektanfrage erstellen	Öffnet ein Popup-Fenster, in dem Sie eine Projektvorlage zum Erstellen einer Projektanfrage auswählen können. Sie können auch auf **Weiter** klicken, um den Assistenten für Projektanfragen in der Anwendung zu öffnen.
Neues Projekt erstellen	Öffnet ein Popup-Fenster, in dem Sie eine Projektvorlage zum Erstellen eines Projekts auswählen können. Sie können auch auf **Weiter** klicken, um den Projektassistenten in der Anwendung zu öffnen.
Rechnung hinzufügen	Öffnet den Assistenten „Rechnung hinzufügen“ in der Anwendung.
Projekte	Öffnet die Seite „Projektliste“ in der Anwendung.
Berichte	Öffnet die Seite **Analyse > Operationsanalyse**.
Ressourcenbibliothek	Öffnet die Seite „Assetbibliothek“ in der Anwendung.
Genehmigungen	Öffnet die Seite „Genehmigungsliste“ in der Anwendung.

Erstellen eines Quick Link-Portlets

Verwenden Sie diese Prozedur, um ein Quick Link-Portlet zu erstellen.

1. Klicken Sie in dem Dashboard, dem Sie ein Quick Link-Portlet hinzufügen möchten, auf **Portlets verwalten**.

   Die Seite „Portlet verwalten“ wird geöffnet, auf der die vordefinierten Portlets aufgelistet werden.
2. Klicken Sie auf **Quick Link-Portlet erstellen**.
3. Geben Sie einen Portletnamen und eine Beschreibung ein. Wählen Sie die Quick Links aus, die das Portlet enthalten soll.
4. Klicken Sie auf **Speichern**, um die Portleterstellung abzuschließen und das Portlet zum Dashboard hinzuzufügen.

Benutzerdefinierte Portlets

Die Themen in diesem Abschnitt beschreiben, wie Sie benutzerdefinierte Portlets erstellen und verwenden.

Benutzerdefinierte Portlettypen und Verfügbarkeit

Sie können Portlets aus den folgenden Unica-Seitentypen erstellen.

- Alle Cognos®-Berichte, einschließlich Unica Interact-Bericht „Leistung Interaktionspunkt“, die so angepasst wurden, dass sie auf zusätzliche interaktive Kanäle verweisen. Sie können alle vorhandenen Dashboardberichte wie in diesem Handbuch beschrieben anpassen. Sie können auch Berichte anpassen, die keine Dashboardberichte sind. Details zum Anpassen eines Berichts, der kein Dashboardbericht ist, finden Sie im *UnicaInstallations- und Konfigurationshandbuch für Berichte*.
- Quick Link-Portlets, die Sie mithilfe vordefinierter Links zu Unica-Produkten erstellen können.
- Alle Digital Analytics for On Premises- oder Digital Analytics for On Premises-On-Demand-Berichte oder -Dashboards, die automatisch aktualisiert werden.
- Alle IBM Digital Analytics-Berichte.

Zusätzlich können Sie ein Portlet aus einer Seite im Internet oder im Intranet des Unternehmens erstellen.

Von Ihnen erstellte Portlets können in jedem Dashboard verwendet werden. Ihre benutzerdefinierten Portlets werden im Fenster „Portlets verwalten“ aufgelistet. Hier können Sie die Portlets einem Dashboard hinzufügen.

Authentifizierungsaspekte bei benutzerdefinierten Portlets

Wenn Sie vorhaben, Portlets zu erstellen, sollten Sie die folgenden Authentifizierungsaspekte berücksichtigen.

- Handelt es sich bei dem Portlet um einen Digital Analytics for On Premises-Bericht einer Installation, die Unica Platform zur Authentifizierung oder aber keine Authentifizierung verwendet, oder um den Dashboardbericht eines beliebigen anderen Unica-Produkts, das Unica Platform zur Authentifizierung verwendet, werden Benutzer nicht zur Angabe von Berechtigungsnachweisen aufgefordert, wenn sie das Portlet anzeigen.
- Handelt es sich bei dem Portlet um den Digital Analytics for On Premises-Bericht einer Installation, die nicht Unica Platform für die Authentifizierung verwendet, muss der Benutzer seine Anmeldeberechtigungsnachweise ein Mal pro Browsersitzung eingeben.
- Wenn das Portlet ein NetInsight OnDemand-Bericht oder eine Internet- oder Intranetseite ist, für die eine Authentifizierung benötigt wird, zeigt das Portlet dasselbe Verhalten wie ein Browser. Der Benutzer muss Anmeldeberechtigungsnachweise in den Inhalt der Seite eingeben, wenn er die Seite erstmals während einer Browsersitzung anzeigt. Danach sorgen Cookies dafür, dass der Benutzer weiterhin angemeldet bleibt.
- Handelt es sich bei dem Portlet um einen IBM Digital Analytics-Bericht, können Benutzer nur die Berichte anzeigen, für die sie in Digital Analytics über Berechtigungen verfügen. Wenn eine einmalige Anmeldung (Single Sign-on) mit Digital Analytics aktiviert ist, können Benutzer Digital Analytics-Berichte in Unica Platform-Dashboards anzeigen, ohne ihre Berechtigungsnachweise eingeben zu müssen. Andernfalls müssen Benutzer ihre Digital Analytics-Berechtigungsnachweise eingeben, um Digital Analytics-Berichte in Unica Platform-Dashboards anzeigen zu können.

Übersicht über den Portleterstellungsprozess

Dieser Abschnitt bietet einen Überblick über die Schritte zur Erstellung eines Portlets, die an anderer Stelle in diesem Handbuch detailliert beschrieben sind.

Benötigen Sie weitere Informationen zur Ausführung dieses Verfahrens, sehen Sie sich die zugehörigen Referenzen an.

1. Besorgen Sie sich die URL der Seite, die Sie als Portlet verwenden möchten, und bereiten Sie sie vor.

   Sie müssen hierzu die URL anfordern und sie entsprechend ändern.

   Sie können Portlets aus den folgenden Quellen erstellen.

   - Digital Analytics for On Premises Bericht
   - IBM Cognos® Bericht
   - Digital Analytics Bericht
   - NetInsight OnDemand Bericht und Seiten im Internet oder im Intranet
2. Fügen Sie die URL zur `Platform_Admin_URL.properties` Datei hinzu.

   Die `Platform_Admin_URL.properties`Datei befindet sich im `conf`-Verzeichnis unter Ihrer Unica Platform-Installation.
3. Stoppen Sie die Unica Platform Webanwendung und starten Sie sie erneut.
4. Fügen Sie das Portlet einem Dashboard hinzu.

Vorbereiten der URL von einem Digital Analytics for On Premises-Bericht

Verwenden Sie diese Prozedur für Berichte in einer Digital Analytics for On Premises-Installation.

1. Zeigen Sie den Bericht in Digital Analytics for On Premises an, den Sie exportieren möchten.

   Wenn Sie ein Digital Analytics for On Premises-Dashboard verwenden, wird nur der Bericht oben links im Dashboard exportiert.

2. Klicken Sie auf das Symbol **Exportieren**  , das sich in der Symbolleiste rechts oben im Bericht befindet.

   Das Fenster „Exportoptionen“ wird geöffnet.
3. Füllen Sie die Felder wie folgt aus.
   - Wählen Sie **Portlet-URL** in der Dropdown-Liste **Exporttyp** aus.
   - Wählen Sie `Web-Browser` in der Dropdown-Liste **Berichtsformat** aus.
   - Geben Sie die Anzahl der in den Bericht aufzunehmenden Werte an.
   - Geben Sie die Breite der Berichtsgrafik in Pixel ein. Die Größe von Berichten über Pfade wird unabhängig von dem für die Breite angegebenen Wert automatisch angepasst. Berichte über gestapelte Balken überschreiten die angegebene Breite automatisch um 30%.
   - Wählen Sie die Option zum Ausblenden des Berichtskopfs aus, da Sie den Titel des Portlets bearbeiten können.
4. Klicken Sie auf **Exportieren**.

   Die Berichts-URL wird im Dialogfenster angezeigt.
5. Kopieren Sie die URL und fügen Sie sie in einen Texteditor ein.
6. Fügen Sie am Anfang der Berichts-URL Folgendes hinzu:

   `Your_HCL_Unica_URL``/suiteSignOn?target=`

   wobei *`Your_HCL_Unica_URL`* die Anmeldungs-URL für Ihre Installation von Unica ist.

   Angenommen, Sie verfügen über die folgenden Informationen:

   - Ihre Berichts-URL ist `MyReportURL`
   - Die Anmeldungs-URL für Ihre Installation von Unica ist `http://myHost.myDomain:7001/unica`

   Ihre endgültige URL wäre dann `http://myHost.myDomain:7001/unica/suiteSignOn?target=MyReportURL`

Vorbereiten der URL von einem IBM® Cognos®-Dashboardbericht

Die URL eines IBM® Cognos®-Dashboard-Portlets hat das folgende Format.

Informationen zum Erstellen von Dashboardberichten mit IBM® Cognos® finden Sie im UnicaInstallations- und Konfigurationshandbuch für Berichte.

`http(s)://HOST.DOMAIN:port/unica/reports/jsp/dashboard_portlet.jsp?product=Product& report=ReportName`

Dabei gilt Folgendes:

- *Product*ist der Name des Unterordners der Unica-Anwendung im Ordner **Unica Dashboards** auf dem IBM® Cognos®-System. Dies ist: `Campaign`, `Interact` oder `Plan` bei Unica Plan. (Plan ist der frühere Name der Unica Plan-Anwendung).
- *ReportName* ist der Name des Dashboardberichts. Beispiel: Kampagnenerfolgsvergleich

Beispiel:

```
http://serverX.example.com:7001/unica/reports/jsp/dashboard_portlet.jsp?product=Campaign&report=Campaign Performance Comparison
```

Falls Sie den Bericht geplant haben, fügen Sie folgende Zeichenfolge an das Ende der URL an:

```
&isView=true
```

Vorbereiten der URL von einem Digital Analytics-Bericht

Verwenden Sie diese Prozedur für Digital Analytics-Berichte.

Wenn Sie möchten, dass Benutzer Digital Analytics Berichte in Dashboards anzeigen können, ohne sich an Digital Analytics anzumelden, müssen Sie die einmalige Anmeldung (Single Sign-on) zwischen Unica und Digital Analytics aktivieren.

1. Melden Sie sich an Digital Analytics an und navigieren Sie zu dem Bericht, den Sie als Portlet hinzufügen möchten.
2. Kopieren Sie die im Browser angezeigte URL.

Der Link wird in Ihre Zwischenablage kopiert und kann in das Feld IBM® Digital Analytics im Fenster „Benutzerdefiniertes Portlet erstellen“ in Unica Platform eingefügt werden.

Sie können die URL in einen Texteditor einfügen, um sicherzustellen, dass sie nicht überschrieben wird, falls Sie zunächst etwas anderes kopieren wollen, bevor Sie die URL zum Erstellen eines Portlets verwenden.

Vorbereiten der URL von einer Intranet- oder Internetseite

Legen Sie für Portlets, die aus Intranet- oder Internetseiten erstellt wurden (einschließlich Digital Analytics for On Premises-Seiten), in Ihrem Browser die gewünschte Seite fest und kopieren Sie die URL aus dem Adressfeld Ihres Browsers.

Verwenden Sie die kopierte URL, wenn Sie Ihr benutzerdefiniertes Portlet erstellen.

Hinzufügen eines benutzerdefinierten Portlets zu einem Dashboard

Wenden Sie diese Vorgehensweise an, um ein benutzerdefiniertes Portlet zu einem Dashboard hinzuzufügen.

Vor der Ausführung dieser Prozedur sollten Sie die folgenden Schritte ausgeführt haben:

- Vorbereiten einer URL, wie an anderer Stelle in diesem Abschnitt beschrieben.
- URL wurde zur `Platform_Admin_URL.properties`-Datei hinzugefügt, sie befindet sich im `conf`-Verzeichnis unter Ihrer Unica Platform-Installation.
- Stoppen und erneutes Starten der Unica Platform-Webanwendung.

1. Wählen Sie in Unica die Option **Dashboard** und dann die Registerkarte des Dashboards aus, mit dem Sie arbeiten möchten.
2. Klicken Sie auf **Portlets verwalten**.

   Das Fenster **Portlets verwalten** wird geöffnet.
3. Klicken Sie auf **Benutzerdefiniertes Portlet** erstellen.

   Das Fenster **Benutzerdefiniertes Portlet erstellen** wird geöffnet.

4. Führen Sie je nach Typ des hinzuzufügenden Portlets eine der folgenden Schrittfolgen aus.

   Wenn Sie ein Portlet erstellen, das kein Digital Analytics Berichtsportlet ist, gehen Sie wie folgt vor.

   - Wählen Sie unter **Typ** die Option **Benutzerdefiniert** aus.
   - Füllen Sie die Felder **Name** und **Beschreibung** aus.
   - Fügen Sie den Inhalt der Zwischenablage (sie enthält die zuvor abgefragte URL) in das Feld **URL** ein.

   Wenn Sie ein Digital Analytics-Berichtsportlet erstellen, gehen Sie wie folgt vor.

   - Wählen Sie unter **Typ** die Option **IBM Digital Analytics** aus.
   - Füllen Sie die Felder **Name** und **Beschreibung** aus.
   - Fügen Sie den Inhalt der Zwischenablage (sie enthält die zuvor abgefragte URL) in das Feld URL von **IBM Digital Analytics** ein.
5. Klicken Sie auf **Speichern**.

   Das Fenster wird geschlossen und die Registerkarte „Administration“ wird wieder angezeigt. Das neue Portlet befindet sich in der linken oberen Ecke, wo es möglicherweise ein zuvor hinzugefügtes Portlet verdeckt. Klicken Sie auf die Portletüberschrift und ziehen Sie das Portlet an eine geeignete Position im Dashboard.

Dynamische Tokens

Bei der Definition von benutzerdefinierten Dashboard-Portlets können vordefinierte Tokens verwendet werden, die durch die Werte ersetzt werden, die in Unica Platform für den beim Aufrufen des Portlets aktiven Benutzer gespeichert sind.

Dieses Feature ist nicht für benutzerdefinierte Portlets von Digital Analytics verfügbar.

Es werden folgende Tokens unterstützt.

- `<user_name>`
- `<user_first_name>`

- `<user_last_name>`
- `<user_email>`

Die URL wird mit ausgeblendeten Variablen aufgerufen, die als Anforderungsparameter übergeben werden.

Die Werte müssen in den Benutzerangaben in Unica Platform enthalten sein. Außerdem müssen Sie die Namen der von der Zielwebsite verwendeten Variablen kennen.

Um diese Tokens zu verwenden, geben Sie die Wertepaare in das Feld **Ausgeblendete Variablen** auf der Seite „Benutzerdefiniertes Portlet erstellen“ ein. Wenn Sie mehrere Tokens verwenden, trennen Sie sie jeweils mit einem Semikolon.

Nehmen Sie z. B. an, Sie möchten den Vor- und Nachnamen eines Benutzers in einer Portlet-URL senden. In dem Fall erwartet die empfangende Website, dass `fname` und `lname` den Vor- und Nachnamen des Benutzers enthalten. Dafür füllen Sie die Felder **URL** und **Ausgeblendete Variablen** folgendermaßen aus.

- **URL** - `www.example.com`
- **Ausgeblendete Variablen** - `fname=<user_first_name>;lname=<user_last_name>`

Seite „Benutzerdefiniertes Portlet erstellen“

In dieser Tabelle finden Sie Hilfe zum Ausfüllen der Felder auf der Seite „Benutzerdefiniertes Portlet“.

Tabelle 22. Felder auf der Seite „Benutzerdefiniertes Portlet erstellen“

Feld	Beschreibung
Type	Wählen Sie den Portlettyp aus: ein Portlet, das nicht aus Digital Analytics stammt, oder ein Portlet aus Digital Analytics.
Name	Geben Sie einen geeigneten Namen für das Portlet ein.
Beschreibung	Geben Sie eine Beschreibung ein, an der andere Administratoren ablesen können, warum das Portlet Teil dieses Dashboards ist.

Tabelle 22. Felder auf der Seite „Benutzerdefiniertes Portlet erstellen“ (Fortsetzung)

Feld	Beschreibung
URL oder Digital Analytics-URL	Fügen Sie Ihre vorbereitete URL ein.
Ausgeblendete Variablen	Nur verfügbar, wenn das Portlet nicht aus Digital Analytics stammt. Wenn für Ihr Portlet eine Anmeldung der Benutzer erforderlich ist, können Sie Name/Wert-Paare eingeben, um diese Berechtigungsnachweise sicher an die Site zu senden. Sie müssen den erwarteten Variablennamen von der Webseite abrufen.

Verwalten der Dashboardzugehörigkeit

Die Themen in diesem Abschnitt beschreiben, wie die Zugehörigkeit zu Dashboards verwaltet wird.

Der Dashboard Administrator

Wenn Ihnen die Rolle eines Dashboardadministrators übertragen wurde, sind Sie für das Verwalten der Zugehörigkeit, des Layouts und des Inhalts dieses Dashboards verantwortlich. In diesem Abschnitt wird beschrieben, wie die Zugehörigkeit zu einem Dashboard verwaltet wird.

Gewähren oder Entziehen von Dashboardzugehörigkeiten

Verwenden Sie diese Prozedur, um Dashboardzugehörigkeiten zu gewähren oder zu entziehen.

1. Wählen Sie in Unica die Option **Dashboard** und dann die Registerkarte des Dashboards aus, mit dem Sie arbeiten möchten.
2. Klicken Sie unten in dem Dashboard, mit dem Sie arbeiten möchten, auf das Symbol **Berechtigungen verwalten**.

   Die Registerkarte „Berechtigungen verwalten“ wird geöffnet.
3. Klicken Sie auf das Symbol **Dashboardbenutzer verwalten**.

Die Seite „Dashboardbenutzer verwalten“ wird geöffnet.

4. Wählen Sie das Kontrollkästchen aus oder ab, um die Zugriffsberechtigung für das Dashboard zu erteilen oder zu entfernen.

   Benutzer, deren Namen ausgewählt sind, können das betreffende Dashboard anzeigen.

   Sie können wie folgt vorgehen, um Benutzer zu suchen.

   - Filtern Sie die Liste, indem Sie einen Benutzernamen ganz oder teilweise in das Feld **Suchen** eingeben.
   - Zeigen Sie alle Benutzer oder nur nicht zugeordnete Benutzer oder nur zugeordnete Benutzer an.
   - Sortieren Sie die Liste, indem Sie auf Spaltenüberschriften klicken.
   - Zeigen Sie alle Benutzer gleichzeitig (auf der Grundlage der Filterkriterien) an oder blättern Sie die Liste durch.
5. Klicken Sie auf **Aktualisieren**.

Unica-Scheduler

Mit dem Unica-Scheduler können Sie einen Prozess konfigurieren, der in bestimmten Intervallen ausgeführt werden soll.

Planbare Elemente

Sie können die folgenden Elemente planen.

- Unica Campaign Ablaufdiagrammausführungen

  Anmerkung: Der Unica-Scheduler ist vollständig unabhängig vom Prozess 'Zeitplan' in Unica Campaign.

- Unica Optimize Optimierungssitzung und Ablaufdiagrammausführungen nach der Optimierung
- Unica Deliver Mailings
- Unica Plan Masseninaktivierungen

- Aufrufe an externe APIs
- Unica Warnung und Benachrichtigungen
- Externe Batch- oder Shell-Scripts

Zeitpläne und Ausführungen

Der Scheduler arbeitet mit zwei grundlegenden Konzepten: Zeitpläne und Ausführungen.

- Ein Zeitplan ist eine Aufgabe, die ein Mal oder wiederholt ausgeführt werden soll. Bei der Definition eines Zeitplans geben Sie das Unica-Objekt, das Start- und Enddatum und wahlweise die Häufigkeit der Aufgabenausführung (sog. Wiederholungsstruktur) an.
- Eine Ausführung ist die Ausführungsinstanz eines Zeitplans.

Zeitplantypen

Es gibt drei Arten von Zeitplänen.

- Auf der Basis der Zeit. Ausführungen erfolgen zu bestimmten Zeiten.
- Auf der Basis von Triggern. Ausführungen erfolgen, wenn ein Zeitplan einen angegebenen Trigger empfängt (beispielsweise wenn ein anderer Zeitplan einen Trigger bei erfolgreicher oder fehlerhafter Ausführung sendet oder wenn das Zeitplandienstprogramm einen Trigger sendet).
- Auf der Basis mehrerer Ausführungen. Ausführungen sind abhängig von anderen Zeitplänen und treten nur auf, wenn mehrere andere Zeitpläne ihre Ausführungen angeschlossen haben.

Zeitplanbenachrichtigungen

Sie können Benachrichtigungen konfigurieren, die für von Ihnen erstellte Zeitpläne an Sie gesendet werden. Administratoren können Benachrichtigungen konfigurieren, die für von beliebigen Benutzern erstellte Zeitpläne an Benutzergruppen gesendet werden.

Scheduler-Trigger, die bei Erfolg oder Fehler von Ausführungen gesendet werden

Beim Erstellen oder Bearbeiten eines Zeitplans können Sie einen Trigger konfigurieren, den der Zeitplan bei Erfolg oder Fehler einer Ausführung sendet. Sie können zudem Zeitpläne konfigurieren, die diese Trigger überwachen.

Trigger funktionieren produktübergreifend. Ein Unica Campaign-Ablaufdiagramm kann beispielsweise einen Trigger senden, der ein Unica Deliver-Mailing startet.

Ein Trigger ist eine Textzeichenfolge, die der Unica-Scheduler senden kann, wenn eine Ausführung erfolgreich war oder fehlgeschlagen ist. Jeder Zeitplan kann einen Trigger bei erfolgreichem Abschluss einer Ausführung und einen Trigger beim Fehlschlagen einer Ausführung senden. Zudem kann jeder Zeitplan einen Trigger für eine erfolgreiche Ausführung und einen Trigger für eine fehlgeschlagene Ausführung überwachen.

Alle Zeitpläne, die einen Trigger überwachen, erhalten alle gesendeten Trigger. Ein Zeitplan leitet jedoch eine Ausführung nur ein, wenn er den Trigger erhält, den er überwacht. Auf diese Weise können unzählige Abhängigkeiten zwischen Zeitplänen erstellt werden.

Nach dem Erstellen eines Triggers wird er in einer Dropdown-Liste mit Triggern in der Scheduler-Benutzeroberfläche angezeigt. Auf diese Weise kann er leicht wiederverwendet werden.

Beispiel für Trigger

Sie können eine Gruppe von Unica Campaign-Ablaufdiagrammen planen, die gleichzeitig ausgeführt werden sollen, indem Sie sie so konfigurieren, dass sie denselben Trigger überwachen, der über das Dienstprogramm scheduler_console_client (auf Seite 369) von einem anderen Zeitplan oder einer externen Anwendung gesendet werden kann. Außerdem können Sie mit Triggern eine Gruppe von Ablaufdiagrammen in einer Reihe nacheinander ausführen.

Im folgenden Beispiel wird demonstriert, wie eine Reihe von Ablaufdiagrammen festgelegt wird, die in einer bestimmten Reihenfolge ausgeführt werden sollen.

- Ablaufdiagramm 1 wird mit dem Trigger „Ablaufdiagramm 1 Ausführung abgeschlossen“ geplant, der nach erfolgreich abgeschlossener Ausführung gesendet wird.
- Ablaufdiagramm 2 wird folgendermaßen geplant:
    - Wird gestartet, wenn der Trigger „Ablaufdiagramm 1 Ausführung abgeschlossen“ empfangen wird.
    - Sendet den Trigger „Ablaufdiagramm 2 Ausführung abgeschlossen“ nach erfolgreich abgeschlossener Ausführung.
- Ablaufdiagramm 3 wird so geplant, dass es nach Empfang des Triggers „Ablaufdiagramm 2 Ausführung abgeschlossen“ gestartet wird.

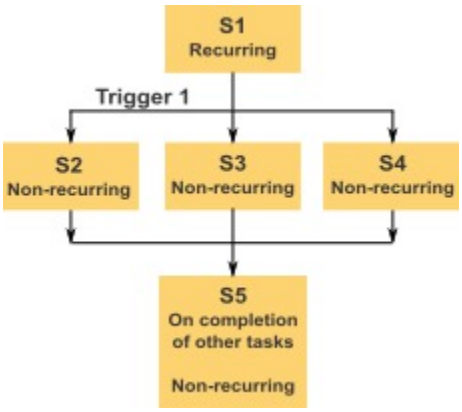
Start-Trigger

Ein Zeitplan, der mit einem Start-Trigger eingerichtet wird, wartet schon direkt nach der Erstellung auf einen Trigger, unabhängig von seinem eigenen Startdatum. Der Trigger überschreibt das Startdatum jedoch nicht. Wenn ein Zeitplan beispielsweise den 12. Dezember 2016 als Startdatum hat und den Start-Trigger am 5. Dezember 2016 empfängt, wird die Ausführung dennoch erst am 12. Dezember 2016 gestartet.

Vom Abschluss mehrerer Ausführungen abhängige Zeitpläne

Sie können einen Zeitplan so konfigurieren, dass er nur ausgeführt wird, wenn mehrere andere Zeitpläne ihre Ausführung abgeschlossen haben. Verwenden Sie hierzu die Option **Bei Abschluss anderer Aufgaben** in der Dropdown-Liste **Startzeitpunkt**.

Beispiel: Es ist ein Zeitplan (S1) vorhanden, der mit einer Wiederholungsstruktur konfiguriert ist. S1 verfügt über einen Trigger, der jedes Mal gesendet wird, wenn eine S1-Ausführung erfolgreich abgeschlossen wird. Drei weitere Zeitpläne, S2, S3 und S4, sind so konfiguriert, dass sie gestartet werden, wenn sie den abgehenden Trigger von S1 empfangen. Sie können einen weiteren Zeitplan (S5) konfigurieren, der ausgeführt wird, wenn S2, S3 und S4 erfolgreich abgeschlossen werden. S5 wird nur dann ausgeführt, wenn alle drei Zeitpläne, von denen er abhängt, abgeschlossen werden. In dem folgenden Diagramm wird dieses Beispiel veranschaulicht.



Um ein Szenario wie das im Beispiel beschriebene einzurichten, müssen Sie S5 mit der Option **Bei Abschluss anderer Aufgaben** in der Dropdown-Liste **Startzeitpunkt** konfigurieren.

Wenn Sie eine Ausführung so konfigurieren, dass sie auf diese Art von anderen Ausführungen abhängig ist, sollten Sie folgende Hinweise beachten.

- Die Zeitpläne, von denen der Zeitplan, den Sie konfigurieren, abhängt, dürfen sich nicht wiederholen. In dem oben beschriebenen Beispiel dürfen S2, S3 und S4 sich nicht wiederholen. Da S1 sich jedoch wiederholt, wiederholen sich S2, S3 und S4 als Folge der S1-Ausführungen auch.
- Der Zeitplan, der von anderen Zeitplänen abhängt, darf sich ebenfalls nicht wiederholen. In dem Beispiel darf sich S5 nicht wiederholen. Auch hier gilt: da sich S1 wiederholt, wiederholt sich S5 als Folge davon auch.
- Der Zeitplan, der von anderen Zeitplänen abhängt, kann nicht als eines der Kriterien in der Option **Bei Abschluss anderer Aufgaben** für einen anderen Zeitplan verwendet werden. Im Beispiel kann S5 nicht als Kriterium in der Option **Bei Abschluss anderer Aufgaben** für einen anderen Zeitplan verwendet werden.
- Wenn Sie einen Zeitplan löschen möchten, der mit der Option **Bei Abschluss anderer Aufgaben** konfiguriert wurde, müssen Sie zuerst die Konfiguration ändern, um die Option **Bei Abschluss anderer Aufgaben** zu entfernen. Anschließend können Sie den Zeitplan löschen.

Planen der von externem Script gesendeten Trigger

Der Unica Scheduler kann auf Trigger reagieren, die von einer externen Anwendung gesendet werden. Das Dienstprogramm `scheduler_console_client` ermöglicht diese Funktion. Dieses Dienstprogramm gibt Trigger aus, die einen oder mehrere Zeitpläne starten können, die diesen Trigger überwachen sollen.

Da `scheduler_console_client` eine Stapelscript-Anwendung ist, kann sie von externen Anwendungen aufgerufen werden, eventuell mithilfe eines weiteren Stapelscripts.

Wenn Sie beispielsweise einen Zeitplan einrichten, der den Trigger „T1“ überwacht, können Sie das Dienstprogramm `scheduler_console_client` mit dem folgenden ausführen, um den T1-Trigger zu senden: `scheduler_console_client.bat -v -t T1`

Das Dienstprogramm kann die folgenden Informationen bereitstellen.

- Eine Liste der Zeitpläne, die konfiguriert sind, um einen bestimmten Trigger zu überwachen.
- Informationen darüber, ob es den Trigger erfolgreich gesendet hat. Das Dienstprogramm kann nicht berichten, ob der Zeitplan, der den Trigger überwacht, erfolgreich ausgeführt wurde. Diese Informationen sind auf den Seiten für das Scheduler-Management verfügbar.

Sie können mit diesem Dienstprogramm keinen Zeitplan konfigurieren, der einen Trigger überwacht oder einen Trigger ändert, den ein Zeitplan überwacht. Sie müssen diese Aktionen in der Scheduler-Benutzeroberfläche ausführen.

Beispielscript

Nachfolgend wird ein Beispiel für ein Script gezeigt, das das Dienstprogramm `scheduler_console_client` veranlasst, die Zeichenfolge „example_trigger“ abzusetzen. Dieser Trigger würde eine Ausführung eines Zeitplans auslösen, der für die Überwachung von „example_trigger“ zuständig ist.

Ein solches Script kann von einer externen Anwendung aufgerufen werden, wenn diese Anwendung ein Ereignis generiert.

In dem Beispielscript wird vorausgesetzt, dass sich das Script in demselben Verzeichnis wie das Dienstprogramm befindet.

```
@rem**************************************************
@rem This script is used to call the Platform
@rem scheduler_console_client.
@rem**************************************************

echo Now starting scheduler trigger.
set JAVA_HOME=c:\jdk15_12
call scheduler_console_client.bat -v -t example_trigger

@rem**************************************************
```

Anmerkungen zur Sicherheit

Die Zeitplanung innerhalb der Unternehmensanwendungen gilt als Administratoraktivität. Voraussetzung ist, dass der Benutzer, der eine Ausführungsberechtigung für das Dienstprogramm `scheduler_console_client` im Hostbetriebssystem hat, ebenfalls berechtigt ist, Trigger abzusetzen.

Um zu verhindern, dass Benutzer mit diesem Dienstprogramm einen Trigger absetzen, sollten Sie diesem Benutzer die Ausführungsberechtigung für das Dienstprogramm `scheduler_console_client` entziehen.

Scheduler-Wiederholungsstruktur

Sie können einen Zeitplan einrichten, um wiederholte Ausführungen zu planen, indem Sie eine Wiederholungsstruktur konfigurieren. Alle Wiederholungsstrukturen, die Sie einrichten, beginnen nach der angegebenen Startzeit.

Sie verfügen über mehrere Optionen für Wiederholungsstrukturen.

- Vordefiniert – Eine Gruppe allgemeiner Wiederholungsstrukturen, aus denen Sie eine Auswahl treffen können
- Cron-Ausdruck – Eine Zeichenfolge, die aus sechs oder sieben durch Leerzeichen getrennte Felder besteht und eine Gruppe von Uhrzeiten darstellt
- Einfache benutzerdefinierte Wiederholungsstruktur – Eine Benutzeroberfläche zum Erstellen von Wiederholungsstrukturen, die der Benutzeroberfläche vieler allgemeiner Besprechungsscheduler ähnelt

Alle Scheduler-Wiederholungsstrukturen basieren auf Cron-Ausdrücken. Der Scheduler stellt vordefinierte Muster in der Benutzeroberfläche bereit, damit diese Cron-Ausdrücke einfacher erstellt werden können. Wenn Sie eigene benutzerdefinierte Cron-Ausdrücke schreiben, empfiehlt es sich, eine aussagekräftige Beschreibung der Wiederholungsstruktur bereitzustellen. Dadurch können Personen, die beim Lesen dieser Ausdrücke nicht geübt sind, das Muster besser verstehen.

Wichtig: Alle Wiederholungsstrukturen werden am Ende des nächsten längeren Zeitintervalls zurückgesetzt. Wenn Sie z. B. ein benutzerdefiniertes wöchentliches Muster festlegen, das alle drei Wochen ausgeführt werden soll, wird es jeweils in der dritten Woche jedes Monats ausgeführt, weil das Muster am Ende jedes Monats zurückgesetzt wird. Dies ist ein Merkmal sämtlicher Cron-Ausdrücke. Wenn Sie einen Zeitplan festlegen möchten, der in Woche 3, 6, 9, 12 usw. ausgeführt wird, müssen Sie einen separaten Zeitplan für jedes gewünschte Ausführungsdatum erstellen.

Zeitzonenunterstützung

Sie können Ausführungen so planen, dass sie im Kontext einer der Weltzeitzonen ausgeführt werden.

Wenn Sie einen Zeitplan erstellen, ist der Standardwert immer die Zeitzone des Servers, auf dem Unica Platform installiert ist. Sie können jedoch eine beliebige andere Zeitzone auswählen, die in der Dropdown-Liste **Zeitzone auswählen** aufgeführt ist. Diese Optionen werden als GMT-Zeiten dargestellt, gefolgt von dem allgemein verwendeten Begriff für

die betreffende Zeitzone. Beispiele: (GMT-08:00) Pitcairninsel oder (GMT-08:00) Pacific Standard Time (USA Kanada).

Die ausgewählte Zeitzone wird auf alle Aspekte des Zeitplans einschließlich der folgenden angewendet.

- Auf den Registerkarten „Zeitpläne“ und „Ausführungen“ angezeigte Informationen
- Wiederholungsstrukturen und Trigger

Schedulerrichtwerte

Über Richtwerte wird die Leistung verwaltet, wenn eine große Anzahl an Prozessen voraussichtlich hohe Anforderungen an das System stellt. Richtwerte basieren auf Planergruppen, die Sie auf der Seite **Einstellungen > Konfiguration** konfigurieren. Sie weisen einer Gruppe einen Richtwert zu und verknüpfen dann Zeitpläne mit dieser Gruppe.

Der Richtwert ist die höchste Anzahl von dieser Gruppe zugeordneten Ausführungen, die gleichzeitig ausgeführt werden können. Wenn die Ressourcenbelegung auf dem Server reduziert werden soll, können Sie den Richtwert auf einen niedrigeren Wert festlegen. Nur Zeitpläne, die im Unica Scheduler erstellt wurden, können begrenzt werden.

Keine Richtwert in der Standardgruppe

Alle Zeitpläne müssen einer Richtgruppe angehören. Sollen keine Richtwerte für einen Zeitplan aktiviert werden, nehmen Sie ihn in die Standardplanergruppe auf (dies ist die im Feld **Planergruppe** bei der Erstellung eines Zeitplans ausgewählte Standardoption). Diese Gruppe weist einen hohen Richtwert auf, was bedeutet, dass praktisch keine Regulierung erfolgt.

Richtwertausnahmen

Wenn Sie ein Ablaufdiagramm in Unica Campaign oder mit dem Dienstprogramm Unica Campaign `unica_svradm` ausführen, werden diese Ausführungen beim Richtwert nicht berücksichtigt, und die Ausführung beginnt sofort.

Beispiele für Richtwerte

- Wenn die Systemressourcen knapp sind, können Sie über Richtwerte die Auslastung eines Servers verwalten. Wenn beispielsweise eine große Anzahl komplexer Unica Campaign-Ablaufdiagramme ausgeführt werden muss, können Sie diese einer Richtgruppe zuordnen, die die Anzahl der gleichzeitig ausführbaren Ablaufdiagramme begrenzt. Mithilfe dieser Richtwerte können Sie die Arbeitslast auf dem Unica Campaign-Server oder der Marketing-Datenbank verwalten.
- Mit Richtwerten können Sie die Prioritäten für Zeitpläne festlegen. Wenn Sie Zeitpläne mit hoher Priorität einer Gruppe mit hohem Richtwert zuordnen, stellen Sie damit sicher, dass Ausführungen dieser Zeitpläne mit den verfügbaren Systemressourcen so effizient wie möglich ausgeführt werden. Zeitpläne mit niedrigerer Priorität sollten Gruppen mit niedrigeren Richtwerten zugewiesen werden.
- Wenn Sie mit einem Ablaufdiagramm arbeiten, das mit einer Wiederholungsstruktur geplant wurde, können Sie mithilfe von Richtwerten sicherstellen, dass Ausführungen nacheinander und ohne Überschneidung durchgeführt werden. Angenommen, Sie haben ein geplantes Ablaufdiagramm mit einer Wiederholungsstruktur, die 10 Stunden lang einmal pro Stunde ausgeführt werden soll. Wenn die Ausführung des Ablaufdiagramms länger als eine Stunde dauert, wird möglicherweise die nächste Ausführung begonnen, bevor die vorhergehende Ausführung abgeschlossen ist. Dies würde zu einem Fehler führen, weil das derzeit immer noch ausgeführte Ablaufdiagramm gesperrt wäre. Damit dies nicht geschieht, können Sie eine Richtgruppe mit der Schwelle `1` erstellen und den Ablaufdiagrammzeitplan dieser Gruppe zuordnen.

Konfigurieren der Richtwerte für Unica-Scheduler

Sie müssen eine Richtgruppe für jeden geplanten Objekttyp festlegen.

1. Navigieren Sie auf der Seite „Konfiguration“ über `Platform > Scheduler Terminplanregistrierungen > [Produkt] > [Objekt] > Richtgruppe zu einer der Richtgruppenvorlagen`.
2. Erstellen Sie eine Kategorie aus der Richtgruppenvorlage.

Der Wert, den Sie für `Richtwert festlegen`, ist die höchste Anzahl von dieser Gruppe zugeordneten Ausführungen, die gleichzeitig ausgeführt werden können. Auszuführende Zeitpläne, die den Richtwert überschreiten, werden in der Reihenfolge in die Warteschlange gestellt, in der die Ausführungsbenachrichtigungen im Zeitplan eingehen.

Die konfigurierten Planergruppen erscheinen in der Dropdown-Liste **Planergruppe** in der Benutzeroberfläche des Zeitplaners zum Erstellen und Bearbeiten von Zeitplänen.

Sie müssen eine Richtgruppe für jeden Objekttyp erstellen, dessen Ausführungen Sie auf diese Weise steuern möchten. Richtgruppen für Ablaufdiagramme sind beispielsweise nur zur Planung von Ablaufdiagrammen verfügbar. Mailing-Richtgruppen sind nur zur Planung von Mailings verfügbar.

3. Weisen Sie der Gruppe je nach Bedarf einen oder mehrere Zeitpläne zu.

Whitelist-Voraussetzung für externe Aufgaben (nur mit FixPack 10.0.0.1)

Nur wenn Sie Unica Platform FixPack 10.0.0.1 angewendet haben, gilt für alle externen Aufgaben, die Sie zum Planen von API-Aufrufen oder -Scripts erstellt haben, eine Whitelist-Voraussetzung.

Bevor Sie eine externe Aufgabe planen können, müssen Sie die API oder das Script zu einer Whitelist hinzufügen, die sich im Verzeichnis `conf` unter Ihrer Unica Platform-Installation befindet.

Hinzufügen eines Scripts zur Whitelist

Nur wenn Sie Unica Platform FixPack 10.0.0.1 angewendet haben, müssen Sie diese Prozedur ausführen, bevor Sie externe Aufgaben zum Planen eines Scripts erstellen.

Das Script muss sich auf dem Webanwendungsserver befinden, auf dem Unica Platform bereitgestellt wurde.

1. Öffnen Sie die Whitelist-Datei für Scripts in einem Texteditor.

   Die Whitelist-Datei für Skripte ist `Platform_Admin_Scheduler_Scripts.properties`. Die Datei befindet sich im `conf`-Verzeichnis unter Ihrer Unica Platform-Installation.
2. Geben Sie den vollständigen Pfad des Stapel- oder Shell-Scripts ein, das Sie planen möchten, und beziehen Sie die Anzahl der in dem Script verwendeten Parameter mit ein, das Sie gerade planen.

   Angenommen beispielsweise, Sie möchten ein Script mit dem Namen `RunETLJobs.bat` planen und dafür sind die folgenden drei Parameter erforderlich: username, password, db_table.

   Sie würden folgenden Eintrag in die Whitelist-Datei machen. Der Eintrag umfasst den absoluten Pfad des Scripts gefolgt von einem Leerzeichen und der Anzahl der verwendeten Parameter. Die Anzahl der Parameter muss genau mit der im geplanten Script verwendeten Anzahl der Parameter übereinstimmen.

   ```
   C:\Scripts\RunETLJobs.bat 3
   ```

   Wenn Sie den Zeitplan erstellen, geben Sie im Feld **Ausführungsparameter** die Parameternamen, wie im folgenden Beispiel dargestellt, zwischen doppelten Nummernzeichen (##) gefolgt von einem Leerzeichen ein.

   ```
   C:\Scripts\RunETLJobs.bat ##username## ##password##
   ##db_table##
   ```
3. Speichern und schließen Sie die Whitelist-Datei.

   Jetzt können Sie das Script auf der Registerkarte „Zeitpläne“ auf der Seite **Einstellungen > Zeitplanmanagement** planen.

Hinzufügen einer API zur Whitelist

Nur wenn Sie Unica Platform FixPack 10.0.0.1 angewendet haben, müssen Sie diese Prozedur ausführen, bevor Sie eine externe Aufgabe zum Planen eines API-Aufrufs erstellen.

1. Öffnen und bearbeiten Sie die Whitelist-Datei für APIs in einem Texteditor.

   Die Whitelist-Datei für APIs ist `Platform_Admin_Scheduler_API.properties`. Die Datei befindet sich im `conf`-Verzeichnis unter Ihrer Unica Platform-Installation.
2. Geben Sie die URI der API ein, die Sie planen möchten, und beziehen Sie, wenn Abfrageparameter verwendet werden, die entsprechenden Parameternamen ohne die Angabe von Werten mit ein.

   Angenommen beispielsweise, Sie möchten folgenden API-Aufruf unter Verwendung aller angezeigten Abfrageparameter planen.

   ```
   http://www.example.com/tickets?
   fields=id&state=open&sort=updated_at
   ```

   Sie würden folgenden Eintrag in die Whitelist-Datei machen und dabei alle Parameter auflisten.

   ```
   http://www.example.com/tickets?fields&state&sort
   ```

   Mit diesem Whitelist-Eintrag können Sie API-Aufrufe planen, die einige der oder alle aufgelisteten Parameter verwenden. Beispiel:

   - `http://www.example.com/tickets`
   - `http://www.example.com/tickets?fields=id`
   - `http://www.example.com/tickets?fields=id&state=open`
   - `http://www.example.com/tickets?fields=id&state=open&sort=updated_at`
   - `http://www.example.com/tickets?fields=id&sort=updated_at`
   - `http://www.example.com/tickets?fields=id&state=open`

   API-Aufrufe, in denen nicht aufgelistete Abfrageparameter verwendet werden, können nicht geplant werden. Die Zeitplanvalidierung schlägt fehl, wenn Parameter verwendet werden, die nicht in der Whitelist enthalten sind.
3. Speichern und schließen Sie die Whitelist-Datei.

   Jetzt können Sie den API-Aufruf auf der Registerkarte „Zeitpläne“ auf der Seite **Einstellungen > Zeitplanmanagement** planen.

Bewährte Verfahren zur Konfiguration von Zeitplänen

Hier werden bewährte Verfahren zur Planung und Konfiguration geplanter Ausführungen von Unica-Objekten aufgeführt.

Beachten Sie diese Richtlinien, um eine optimale Leistung und einfache Durchführbarkeit zu erreichen.

- Weil geplante Ausführungen auf dem System ausgeführt werden, auf dem das Clientprodukt installiert ist, berücksichtigen Sie die Skalierungsmöglichkeiten des Clientsystems. Versetzen Sie Ausführungen oder verwenden Sie Richtwerte zur Optimierung des Systems.
- Planen Sie, wenn möglich, schwere Jobs bei niedrigen Systemlastzeiten.
- Vermeiden Sie überlappende Ausführungen, da in diesem Fall Fehler auftreten können.
    - Gehen Sie vorsichtig vor, wenn dasselbe Objekt in mehreren Zeitplänen verwendet wird. Wenn Sie beispielsweise das Ablaufdiagramm F1 in drei Zeitplänen verwenden, können diese Zeitplandefinitionen möglicherweise dazu führen, dass eine Ausführung gestartet wird, bevor die vorherige Ausführung abgeschlossen ist, was zu Fehlern führen kann.
    - Wenn eine Ablaufdiagrammausführung manuell oder durch ein externes Script initiiert wurde, schlägt ein nachfolgender Versuch einer beliebigen Methode der Ablaufdiagrammausführung aufgrund einer Sperre fehl, wenn die vorherige Ausführung noch nicht abgeschlossen wurde.
- Der Scheduler erstellt eine große Menge an Daten. Wenn Sie bei dem Scheduler Leistungsprobleme beobachten, sollten Sie nicht mehr benötigte Zeitplandefinitionen entfernen.

Wichtig: Beim Entfernen einer Zeitplandefinition wird auch der zugehörige Ausführungsverlauf aus der Datenbank entfernt.

Um Assistent „Zeitplan erstellen“

In diesem Abschnitt werden die Seiten zur Erstellung eines Zeitplans detailliert beschrieben.

Die folgende Tabelle enthält eine Beschreibung der Felder, die Sie verwenden, wenn Sie Ausführungen von Unica Campaign-Ablaufdiagrammen, Unica Deliver-Mailings, Unica Optimize-Sitzungen, externen Scripts und API-Aufrufen planen.

Tabelle 23. Felder im Assistenten „Zeitplan erstellen“

Feld	Beschreibung
Aufgabentyp auswählen	Der Typ des zu planenden Objekts. Es stehen folgende Optionen zur Verfügung: • **Externe Aufgabe - Skript** Ermöglicht Ihnen die Planung des Aufrufs von in Stapel- oder Shell-Scripts definierten Aufgaben, die sich außerhalb von Unica befinden. Das Script muss nur dann in einer Whitelist-Datei aufgeführt werden, die sich im Verzeichnis `conf` unter Ihrer Unica Platform-Installation befindet, wenn Sie Unica Platform FixPack 10.0.0.1 angewendet haben. Zudem muss sich das Script auf dem Webanwendungsserver befinden, auf dem Unica Platform bereitgestellt wurde. • **Externe Aufgabe - API** Ermöglicht Ihnen die Planung des Aufrufs von APIs, die sich außerhalb von Unica befinden. Die API muss nur dann in einer Whitelist-Datei aufgeführt werden, die sich im Verzeichnis `conf` unter Ihrer Unica Platform-Installation befindet, wenn Sie Unica Platform FixPack 10.0.0.1 angewendet haben. • **Unica Campaign Ablaufdiagramm** Ermöglicht Ihnen die Planung des Aufrufs von Unica Campaign-Ablaufdiagrammen. Nach Auswahl dieser Option wird die Unica Campaign-Listenseite aufgerufen, auf der Sie eine Kampagne auswählen, optional Überschreibungsparameter für Ab-

Tabelle 23. Felder im Assistenten „Zeitplan erstellen“ (Fortsetzung)

Feld	Beschreibung
	laufdiagramme festlegen und die Ausführung eines Ablaufdiagramms planen können. • **Unica Optimize Sitzung** Ermöglicht Ihnen die Planung des Aufrufs von Unica Optimize-Sitzungen. Nach Auswahl dieser Option wird die Unica Optimize-Sitzungslistenseite aufgerufen, auf der Sie eine Sitzung auswählen und die Ausführung der Sitzung planen können. • **Unica Deliver Senden** Ermöglicht Ihnen die Planung des Aufrufs von Unica Deliver-Mailings. Nach Auswahl dieser Option wird die Unica Deliver-Seite für die Mailing-Liste aufgerufen, in der Sie das Mailing auswählen und planen können. • **Unica Plan-Masseninaktivierung** Ermöglicht Ihnen die Planung der Masseninaktivierung von Projekten in Unica Plan. Nach Auswahl dieser Option wird die Unica Plan-Seite „Administrationseinstellungen“ aufgerufen, auf der Sie auf **Deaktivierungsverwaltung** klicken und die Massendeaktivierung planen können. • **Benachrichtigung** Ermöglicht Ihnen die Planung von Alerts für Benutzer von Unica. Nach Auswahl dieser Option wird ein Fenster geöffnet, in dem Sie den Nachrichtentitel, den Nachrichtentext und den Schweregrad angeben können. Nachdem Sie auf **Diesen Alert planen** geklickt haben, können Sie einen Zeitplan für den Alert erstellen. Benutzer können Ihre Benachrichtigungsabonnements auf Basis des Schweregrads verwalten. • **Benachrichtigung**

Tabelle 23. Felder im Assistenten „Zeitplan erstellen“ (Fortsetzung)

Feld	Beschreibung
	Ermöglicht Ihnen die Planung von Benachrichtigungen für Benutzer von Unica. Nach Auswahl dieser Option wird ein Fenster geöffnet, in dem Sie den Nachrichtentitel, den Nachrichtentext und den Schweregrad angeben können. Nachdem Sie auf **Diese Benachrichtigung planen** geklickt haben, können Sie einen Zeitplan für die Benachrichtigung erstellen. Benutzer können Ihre Benachrichtigungsabonnements auf Basis des Schweregrads verwalten.
Zeitplanname	Geben Sie einen Namen für den Zeitplan ein.
Planergruppe	Wenn Sie Richtgruppen erstellt haben, können Sie diesen Zeitplan einer Gruppe zuordnen, um die Anzahl der Ausführungen dieses Zeitplans zu begrenzen, die zur gleichen Zeit ausgeführt werden können. Auf der Seite „Konfiguration“ konfigurierte Richtgruppen werden als Optionen in diesem Feld angezeigt
Beschreibung	Geben Sie eine Beschreibung für den Zeitplan ein.
Parameter ausführen	Wird verwendet, wenn Sie APIs und Scripts planen. Nur wenn Sie Unica Platform FixPack 10.0.0.1 angewendet haben, gilt für alle externen Aufgaben, die Sie zum Planen von API-Aufrufen oder -Scripts erstellt haben, eine Whitelist-Voraussetzung. Bevor Sie eine externe Aufgabe planen können, müssen Sie die API oder das Script zu einer Whitelist hinzufügen, die sich im Verzeichnis `conf` unter Ihrer Unica Platform-Installation befindet. • Geben Sie für API-Zeitpläne die URI und beliebige Parameter in dem in den Beispielen dargestellten Format ein. API ohne Parameter: `http://example.com`

Tabelle 23. Felder im Assistenten „Zeitplan erstellen“ (Fortsetzung)

Feld	Beschreibung

	API mit Parameter: `http://www.example.com/tickets?fields=id&state=open&sort=updated_at`
	
	Momentan werden im URI keine Unica Platform-Tokens unterstützt.
	• Geben Sie für Scriptzeitpläne den vollständigen Pfad zu dem Script auf dem Unica Platform-Server und beliebige Parameter in dem in den Beispielen dargestellten Format ein. Geben Sie die Parameternamen zwischen doppelten Nummernzeichen (##) gefolgt von einem Leerzeichen ein.
	◦ Windows™ Beispiele
	
	Script mit Parametern: `C:\Scripts\ExecuteDatabaseJob.bat`
	
	Script mit Parametern:
	
	`C:\Scripts\RunETLJobs.bat ##username## ##password## ##db_table##`
	◦ UNIX™ Beispiele
	
	Script mit Parametern: `/opt/ExecuteDatabaseJob.sh`
	
	Script mit Parametern:
	
	`/opt/RunETLJobs.sh ##username## ##password## ##db_table##`
	
	Die Ausführung dieser Aufgaben erfolgt asynchron. Von Unica Platform wird der Erfolg oder das Fehlschlagen der Script- oder API-Aufgaben nicht protokolliert. Der Status gibt lediglich an, ob diese Aufgaben erfolgreich gestartet wurden.

Tabelle 23. Felder im Assistenten „Zeitplan erstellen“ (Fortsetzung)

Feld	Beschreibung
Bei erfolgreichem Abschluss einen Trigger senden	Bei einem erfolgreichen Abschluss können Ausführungen dieses Zeitplans einen Trigger senden. Geben Sie hierzu den Trigger-Text hier ein. Andere Zeitpläne können eingerichtet werden, um diesen Trigger zu erkennen.
Bei einem Fehler einen Trigger senden	Bei fehlgeschlagenen Ausführungen können Ausführungen dieses Zeitplans einen Trigger senden. Geben Sie hierzu den Trigger-Text hier ein. Andere Zeitpläne können eingerichtet werden, um diesen Trigger zu erkennen.
Suchtags/Schlüsselwörter	Geben Sie alle Tags ein, die Sie dem Zeitplan zur Verwendung in Suchoperationen zuordnen wollen. Trennen Sie mehrere Einträge durch Kommas.
Zeitplanstatus	Gibt an, ob der Zeitplan aktiviert oder inaktiviert ist. Das Inaktivieren eines Zeitplans gilt nur für zukünftige Ausführungen dieses Zeitplans oder für Ausführungen, die in eine Warteschlange eingestellt wurden. Momentan durchgeführte Ausführungen sind nicht betroffen. Der Standardstatus lautet **Aktiviert**.
Zeitzone auswählen	Wenn Sie eine andere als die Standardoption des Servers auswählen, dann werden in den Spalten **Start**, **Ende** und **Zuletzt aktualisiert** auf der Seite „Zeitplanmanagement“ sowohl die Standardzeit des Servers als auch die Uhrzeit in der ausgewählten Zone angezeigt.
Startzeitpunkt	Wählen Sie eine der folgenden Optionen aus, um festzulegen, wann der Zeitplan zum ersten Mal ausgeführt werden soll. Die angegebene Startzeit gilt nur für die erste Ausführung. Sie legt fest, wann ein Zeitplan erstmals ausgeführt werden soll. Wenn eine der folgenden Bedingungen vorliegt, müsste die tatsächliche erste Ausführung nach dem Startdatum erfolgen.

Tabelle 23. Felder im Assistenten „Zeitplan erstellen“ (Fortsetzung)

Feld	Beschreibung
	• Der Zeitplan ist so konfiguriert, dass auf einen Auslöser gewartet wird. • Der Zeitplan ist Mitglied einer Richtgruppe. • Der Zeitplan verwendet ein Wiederholungsmuster. • **Jetzt** • **An einem Datum und zu einer Zeit** - Wählen Sie einen Zeitpunkt (Datum und Uhrzeit) aus. • **Bei einem Trigger** – Wählen Sie einen existierenden Trigger aus oder geben Sie einen neuen Trigger ein. Wenn Sie einen neuen Trigger eingeben, müssen Sie einen Zeitplan konfigurieren, um diese Zeichenfolge bei erfolgreicher oder fehlgeschlagener Ausführung zu senden. • **Bei einem Trigger nach einem Datum** - Wählen Sie einen vorhandenen Trigger aus oder geben Sie einen neuen Trigger ein und wählen Sie Datum und Uhrzeit aus. Wenn Sie einen neuen Trigger eingeben, müssen Sie einen Zeitplan konfigurieren, um diese Zeichenfolge bei erfolgreicher oder fehlgeschlagener Ausführung zu senden. • **Bei Abschluss sonstiger Aufgaben** - Wählen Sie ein Element aus einer Liste vorhandener Zeitpläne aus. Der Zeitplan wird nur ausgeführt, wenn die Ausführung der anderen ausgewählten Zeitpläne abgeschlossen ist.
Anzahl der Ausführungen	Wählen Sie eine der folgenden Optionen aus, um die Anzahl der Ausführungen festzulegen.

Tabelle 23. Felder im Assistenten „Zeitplan erstellen“ (Fortsetzung)

Feld	Beschreibung
	• **Nur einmal ausführen** - Der Zeitplan wird einmal ausgeführt. Die Ausführung erfolgt dann an dem von Ihnen angegebenen Startdatum zu der festgelegten Uhrzeit. • **Nach n Läufen stoppen** - Die Ausführungen werden nach einer bestimmten Anzahl von Ausführungen (unabhängig davon, ob die Ausführungen erfolgreich waren oder fehlgeschlagen sind) oder nach dem Erreichen des Enddatums gestoppt (je nachdem, welches Ereignis eher eintritt). • **An einem Datum und zu einer Zeit stoppen** – Ausführungen werden so lange gestartet, bis der festgelegte Endzeitpunkt erreicht ist. Falls eine Ausführung aufgrund von Richtwerten verspätet ausgeführt wird, kann die Ausführung auch noch nach dem festgelegten Zeitpunkt erfolgen. • **Bei Abschluss sonstiger Aufgaben** - Der Zeitplan wird nur dann ausgeführt, wenn alle anderen für diese Option ausgewählten Aufgaben erfolgreich abgeschlossen wurden. Wenn Sie auf die Schaltfläche **Wiederholungen definieren** klicken, dann können Sie eine der folgenden Optionen auswählen. • **Vordefinierte Wiederholungsstruktur verwenden** - Wählen Sie eine Struktur in der Liste aus. Unica Platform bietet eine Reihe vordefinierter Wiederholungsstrukturen. Sie können jedoch auch Ihre eigene Struktur durch Hinzufügen von Eigenschaften auf der Seite „Konfiguration“ erstellen. • **Einfache benutzerdefinierte Wiederholungsstruktur verwenden** - Wählen Sie ein Intervall aus. • **Cron-Wiederholungsausdruck verwenden** - Geben Sie einen gültigen Cron-Ausdruck ein.

Ausführen von Ausschlüssen

10.0.0.2 Ab dem Release von 10.0 Fixpack 2 können Sie Ausschlussregeln erstellen, die dazu dienen, die Zeitplanerausführung für bestimmte Tage oder Zeiten auszusetzen. Dabei können Sie mehrere Regeln für verschiedene Zeitpläne hinzufügen.

Sie haben die Möglichkeit, Ausschlussregeln für bestimmte Zeitpläne zu erstellen oder eine einzelne Regel auf mehrere Zeitpläne anzuwenden. Außerdem können Sie die Regeln aktivieren bzw. inaktivieren oder die Ausschlussregeln löschen, wenn sie nicht mehr benötigt werden.

Die Funktion zum Ausführen von Ausschlüssen steht zur Verfügung, wenn Sie ein Upgrade auf das Release von 10.0 Fixpack 2 durchführen.

Für diese Funktion wurden zwei neue Systemtabellen eingeführt. Weitere Details zu den Systemtabellen finden Sie im Handbuch Unica Platform-Systemtabellen.

Anzeigen von Ausschlussregeln

Die bereits für Zeitpläne definierten Ausschlussregeln können über die Registerkarte „Ausschlussregeln ausführen“ auf der Seite „Zeitplanmanagement“ angezeigt werden.

Welche Informationen im Feld **Vorherige 1 Ausführung und 2 nächste Ausführungen** angezeigt werden, hängt von der Schedulerdefinition ab. Diese wird aktuell nicht auf die Ausschlussregeln hin geprüft.

Führen Sie zum Anzeigen von Ausschlussregeln die folgenden Schritte aus:

1. Melden Sie sich an Unica Platform als Administrator an.
2. Klicken Sie auf **Einstellungen > Zeitplanmanagement**.
3. Klicken Sie auf **Ausschlüsse ausführen**.

Sie können die Ausschlussregeln anzeigen und die verschiedenen Aufgaben für die Regeln angeben. Außerdem können Sie den Status der Regeln, die verschiedenen Zeitpläne, auf die sie angewendet werden, den Ausschlusszeitraum und den Ausschlusstyp für die Regeln anzeigen.

Darüber hinaus können Sie mithilfe einer Platzhaltersuche im Textfeld **Filter** nach Ausschlussregeln suchen.

Hinzufügen von Ausschlussregeln

Ausschlussregeln können für Zeitpläne und Ausführungen hinzugefügt werden. Sie können absolute oder relative Regeln hinzufügen und die Zeitpläne auswählen, für die die Regeln zur Anwendung kommen sollen.

Absolute Ausschlussregeln werden für eine angegebene Zeitdauer festgelegt. Die relativen Ausschlussregeln werden nur einmal festgelegt und waren auf ein einziges Jahr beschränkt. Ab der Version 11.0 sollten neben dem jährlichen relativen Datum auch die wöchentliche und monatliche Datumszeit konfigurierbar sein. Ausschlussregeln können aktiviert oder inaktiviert sowie auf mehrere Zeitpläne angewendet werden.

Wenn Sie eine Ausschlussregel hinzufügen möchten, führen Sie die folgenden Schritte aus:

1. Melden Sie sich an Unica Platform als Administrator an.
2. Klicken Sie auf **Einstellungen > Zeitplanmanagement**.
3. Klicken Sie auf der Registerkarte **Ausschlüsse ausführen** auf **Ausschlussregeln hinzufügen**.
4. Geben Sie auf der Registerkarte **Regeldefinition** unter **Regelname** den Regelnamen an.
5. **Optional:** Geben Sie die **Beschreibung** an.
6. Wählen Sie als **Regelstatus** die Option **Aktiviert** oder **Deaktiviert** aus.

   Standardmäßig ist **Aktiviert** ausgewählt.
7. Wählen Sie den **Ausschlusstyp** aus.

   Führen Sie bei Auswahl von Absolut die folgenden Schritte aus:
   a. Wählen Sie die **Zeitzone** aus.

      Standardmäßig ist die Standardzeitzone des Servers ausgewählt.
   b. Wählen Sie das **Startdatum und die Startzeit** aus.
   c. Wählen Sie das **Enddatum und die Endzeit** aus.

   Führen Sie bei Auswahl von **Relativ** die folgenden Schritte aus:

a. Wählen Sie die Zeitzone aus. Standardmäßig ist die Zeitzone des Servers ausgewählt.
b. Wählen Sie, wann Sie beginnen möchten. 1. Jetzt 2. An einem Datum und zu einer Zeit - Wählen Sie einen Zeitpunkt (Datum und Uhrzeit) aus.
c. Konfigurieren der Wiederholungsstrukturen zur Einrichtung eines relativen Ausführungsausschlusses. Alle Wiederholungsstrukturen, die Sie einrichten, beginnen nach der angegebenen Start- und Endzeit Die Optionen für die Wiederholungsstruktur sind 1. Für wöchentliche Benutzer sollte es möglich sein, einen oder mehrere Wochentage auszuwählen, die mit einem Startdatum und einer Endzeit verbunden sind. 2.bei monatlichen Benutzern sollte die Möglichkeit bestehen, einen Tag im Monat auszuwählen, der mit einer Start- und Endzeit verbunden ist. 3.für jährliche Benutzer sollte die Möglichkeit bestehen, einen Tag im Jahr zu wählen, der mit einer Start- und Endzeit verbunden ist.
d. Wählen Sie Stopp nach n Ereignissen - Stopp der relativen Ausführungsausschluss-Regel nach der angegebenen Anzahl von Ausführungen (unabhängig davon, ob die relative Ausführungsausschluss-Regel erfolgreich ist oder nicht)
e. An einem Datum und zu einer Zeit stoppen auswählen - Relative Ausführungsausschlussregeln wird initiiert, Ausführungen werden so häufig wie definiert gestartet, bis der festgelegte Endzeitpunkt (Datum und Uhrzeit) erreicht ist.

Anmerkung: Ausgewählt werden kann ein Datum des aktuellen Jahres. Wenn Sie ein relatives Datum auswählen, werden alle Zeitpläne für den gesamten Tag übersprungen.

8. Wählen Sie auf der Registerkarte **Auswählbare Zeitpläne** den Zeitplan aus, für den Sie die Ausschlussregel anwenden möchten, indem Sie die folgenden Schritte ausführen:

a. Suchen Sie nach den verfügbaren Zeitplänen, indem Sie in das Textfeld **Filter** eine Platzhaltersuche eingeben.

b. Wählen Sie aus **Verfügbare Zeitpläne** die Zeitpläne aus.

c. Klicken Sie auf  .

Die geplanten Zeitpläne werden in die Tabelle **Ausgewählte Zeitpläne** verschoben.

d. Klicken Sie auf **Speichern**.

9. Klicken Sie auf **Speichern**.

Löschen von Ausschlussregeln

Sie können die in Ihrem System vorhandenen Ausschlussregeln nur löschen, wenn die Regeln keinen Zeitplänen oder Ausführungen zugeordnet sind.

Wenn Sie eine Ausschlussregel löschen möchten, führen Sie die folgenden Schritte aus:

1. Wählen Sie auf der Registerkarte **Ausschlüsse ausführen** die Regel aus, die Sie löschen möchten.

   Anmerkung: Stellen Sie sicher, dass die Ausschlussregel, die Sie löschen möchten, keinem Zeitplan bzw. keiner Ausführung zugeordnet ist.

2. Klicken Sie auf **Löschen**.
3. Bestätigen Sie den Löschvorgang.

Aktivieren und Inaktivieren von Ausschlussregeln

Ausschlussregeln aktivieren und inaktivieren können Sie während Sie die Regeln erstellen, aber auch nach deren Erstellung. Standardmäßig ist eine neue Regel, die erstellt wird, immer „Aktiviert“.

Wenn Ausschlussregeln, die auf Zeitpläne angewendet werden, inaktiviert sind, werden alle Zeitplanausführungen weiterhin wie zuvor ausgeführt. Wenn Ausschlussregeln aktiviert sind, werden die Regeln auf die Zeitpläne angewendet und die Zeitpläne werden gemäß den angewendeten Ausschlusskriterien ausgeführt.

Wenn Sie eine Ausschlussregel aktivieren oder inaktivieren möchten, führen Sie die folgenden Schritte aus:

1. Wählen Sie auf der Registerkarte **Ausschlüsse ausführen** eine inaktivierte Regel aus.
2. Klicken Sie auf **Aktivieren**.

   Der Status der Regel ändert sich in „Aktiviert“.
3. Zum Inaktivieren einer Regel wählen Sie eine aktivierte Regel aus.
4. Klicken Sie auf **Deaktivieren**.

   Der Status der Regel ändert sich in „Inaktiviert“.

Importieren von Ausschlussregeln

Sie können Ausschlussregeln importieren und diese auf Zeitpläne oder Ausführungen im System anwenden. Zum Importieren der Regeln kann eine XML-Datei verwendet werden.

Für den Import der Ausschlussregeln muss die XML-Datei in dem entsprechenden Format vorliegen. Das Format der XML-Datei können Sie anzeigen, indem Sie in der Benutzerschnittstelle auf **Ausschlussregeln importieren** klicken.

Ein Muster einer Ausschlussregeldatei wird im Rahmen der Installation im Verzeichnis `<platform_home>\conf\` unter dem Dateinamen `Exclusion_Rule.xml` bereitgestellt.

Führen Sie zum Importieren von Ausschlussregeln die folgenden Schritte aus:

1. Klicken Sie auf der Registerkarte **Ausschlüsse ausführen** auf **Ausschlussregeln importieren**.
2. Erstellen Sie die XML-Datei zum Importieren der Regeln in dem bereitgestellten Format.
3. Klicken Sie auf **Durchsuchen**, um die Datei auszuwählen.
4. Klicken Sie auf **Speichern**.

Erläuterung der XML-Datei für den Import von Ausschlussregeln

Die XML-Datei, mit der Ausschlussregeln importiert werden können, enthält bestimmte Tags, die die Ausschlussregeln definieren.

Tags in der XML-Datei

In der folgenden Tabelle sind die Tags in der XML-Datei aufgelistet, mit deren Hilfe Ausschlussregeln importiert werden können.

Tabelle 24. Tags in der XML-Datei

Tag	Beschreibung
ruleName	Name der Ausschlussregel.
ruleDescription	Beschreibung der Ausschlussregel.
ruleStartDate	Datum, an dem die Ausschlussregel beginnt. Das Datum muss im Format MM/TT/JJJJ vorliegen.
ruleStartTime	Uhrzeit, zu der die Ausschlussregel beginnt. Die Uhrzeit muss im Format HH:MM:SS vorliegen.
ruleEndDate	Datum, an dem die Ausschlussregel endet. Das Datum muss im Format MM/TT/JJJJ vorliegen.
ruleEndTime	Uhrzeit, zu der die Ausschlussregel endet. Die Uhrzeit muss im Format HH:MM:SS vorliegen.
SchedulerID	IDs des Schedulers, auf den die Ausschlussregel anzuwenden ist. Es können mehrere Scheduler-Aufgaben-IDs angegeben werden. Die IDs der Scheduler-Aufgaben sind in der Datenbank in der Tabelle `USCH_TASK` abgelegt.
ruleStatus	Status der Ausschlussregel. Der Wert kann `Enabled` oder `Disabled` sein.

Mithilfe der Tags lassen sich auch mehrere Ausschlussregeln definieren. Verwenden Sie die Regeltags mehrmals und ändern Sie sie wie erforderlich ab, um mehrere Regeln zu definieren.

Muster-XML-Datei für den Import von Ausschlussregeln

Benutzern wird eine Muster-XML-Datei für den Import von Ausschlussregeln zur Verfügung gestellt. Damit haben sie die Möglichkeit, durch Wiederverwendung der darin enthaltenen Tags und Ändern der Werte eine neue, Ihren Anforderungen entsprechende XML-Datei zu erstellen.

Die folgenden XML-Tags können verwendet werden, um eine XML-Datei für den Import von Ausschlussregeln zu erstellen.

```
<rules>
 <rule>
  <ruleName>Rule1</ruleName><!-- specify rule name -->
  <ruleDescription>Rule for skipping 1/13 to 1/19.</ruleDescription><!--
 specify rule description -->
  <ruleStartDate>1/13/2017</ruleStartDate><!-- specify exclusion start
 date. This should be of format MM/DD/YYYY -->
  <ruleStartTime>8:00:00</ruleStartTime><!-- specify exclusion start time.
 This should be of format HH:MM:SS-->
  <ruleEndDate>1/19/2017</ruleEndDate><!-- specify exclusion end date. This
 should be of format MM/DD/YYYY -->
  <ruleEndTime>18:15:00</ruleEndTime><!-- specify exclusion end time. This
 should be of format HH:MM:SS -->
  <SchedulerIDs>
   <SchedulerID>10</SchedulerID> <!-- specify scheduler task Ids, on which
 this rule should get applied. This needs to be obtained from database. -->
   <SchedulerID>15</SchedulerID>
  </SchedulerIDs>
  <ruleStatus>Enabled</ruleStatus> <!-- specify exclusion rule status.
 valid values Enabled/Disabled -->
 </rule>
</rules>
<rules>
 <rule>
```

```
 <ruleName>Rule2</ruleName><!-- specify rule name -->
 <ruleDescription>Rule for skipping 2/6 to 2/10</ruleDescription><!--
specify rule description -->
 <ruleStartDate>2/6/2017</ruleStartDate><!-- specify exclusion start date.
This should be of format MM/DD/YYYY -->
 <ruleStartTime>00:00:00</ruleStartTime><!-- specify exclusion start time.
This should be of format HH:MM:SS-->
 <ruleEndDate>2/10/2017</ruleEndDate><!-- specify exclusion end date. This
should be of format MM/DD/YYYY -->
 <ruleEndTime>23:59:59</ruleEndTime><!-- specify exclusion end time. This
should be of format HH:MM:SS -->
 <SchedulerIDs>
  <SchedulerID>45</SchedulerID> <!-- specify scheduler task Ids, on which
this rule should get applied. This needs to be obtained from database. -->
  <SchedulerID>88</SchedulerID>
 </SchedulerIDs>
 <ruleStatus>Disabled</ruleStatus> <!-- specify exclusion rule status.
valid values Enabled/Disabled -->
 </rule>
</rules>
```

Aspekte bei der Verwendung des Schedulers mit Unica Campaign

Bei der Verwendung des Unica-Schedulers mit Unica Campaign sind bestimmte Konfigurationsaufgaben erforderlich.

- Manuelle Starts von Ablaufdiagrammausführungen oder Ablaufdiagrammbefehle in Befehlszeilen haben keine Auswirkungen auf den Scheduler und umgekehrt. Es gibt jedoch eine Ausnahme. Wenn eine mit einer beliebigen Methode initiierte Ablaufdiagrammausführung nicht abgeschlossen wurde, schlägt der nächste Versuch der Ablaufdiagrammausführung aufgrund einer Sperre fehl.

- Scheduler-Trigger interagieren nicht mit Unica Campaign-Ablaufdiagramm-Triggern. Trigger, die vom Zeitplanprozess oder dem Unica Campaign-Trigger-Dienstprogramm `unica_actrg` gesendet wurden, können nicht die Ausführung von Zeitplänen im Unica-Scheduler bewirken und umgekehrt.

Unterschied zwischen der Vorgehensweise bei Unica Campaign-Ablaufplänen und dem Unica-Scheduler

Ab Release 8.0 von Unica Platform soll der Unica-Scheduler den Unica Campaign-Zeitplanprozess für die Planung von Ausführungen vollständiger Ablaufdiagramme ersetzen. Der Unica-Scheduler ist effizienter, da er keine Serversystemressourcen verbraucht, wenn das Ablaufdiagramm nicht gerade ausgeführt wird.

Der Unica-Scheduler startet ein Ablaufdiagramm, auch wenn noch kein Ablaufdiagramm ausgeführt wurde, während der Unica Campaign-Zeitplanprozess in einem Ablaufdiagramm nur funktioniert, wenn die Ablaufdiagrammausführung bereits gestartet wurde.

Der Unica Campaign-Zeitplanprozess ist für die vollständige Kompatibilität mit früheren Versionen und für andere Zwecke vorbehalten, die nicht mit dem Unica-Scheduler behandelt werden. Sie könnten den Unica Campaign-Zeitplanprozess verwenden, um Unica Campaign-Trigger zu versenden oder die Ausführung von abhängigen Prozessen zu verzögern.

Verwenden Sie den Unica-Scheduler nicht, um ein Ablaufdiagramm zu planen, das den Unica Campaign-Zeitplanprozess als Prozess der höchsten Ebene zum Starten der Durchführung von Ablaufdiagrammen verwendet. Normalerweise ist nur eine der beiden Optionen erforderlich. Erscheint jedoch der Zeitplanprozess in einem Ablaufdiagramm, das vom Unica-Scheduler gestartet wurde, funktioniert er wie konfiguriert; vom Unica-Scheduler und dem Zeitplanprozess benötigte Bedingungen müssen erfüllt sein, bevor nachfolgende Prozesse ausgeführt werden können.

Anders als der Unica-Scheduler kann der Unica Campaign-Zeitplanprozess externe Trigger senden, um Befehlszeilenscripts aufzurufen. Der Unica-Scheduler kann nur an die eigenen Pläne Trigger senden.

Berechtigungen für das Planen von Ablaufdiagrammen

Zum Planen von Unica Campaign-Ablaufdiagrammen mit dem Unica Scheduler sind die folgenden Berechtigungen erforderlich.

Tabelle 25. Berechtigungen für das Planen

Berechtigung	Beschreibung
Ablaufdiagramm zur Stapelverarbeitung planen	Lässt das Planen von Ablaufdiagrammen mit den Standardausführungsparametern zu
Überschreiben von Ablaufdiagramm zur Stapelverarbeitung planen	Lässt das Überschreiben der Standardausführungsparametern zum Planen von Ablaufdiagrammen zu
Ablaufdiagramm zur Stapelverarbeitung ausführen	Lässt das Ausführen von Ablaufdiagrammen zu (erforderlich, damit geplante Ablaufdiagramme erfolgreich ausgeführt werden können)

Anmerkung: Wenn ein geplantes Ablaufdiagramm ausgeführt wird, erfolgt die Ausführung über den Unica Platform-Benutzer, der die geplante Aufgabe erstellt hat. Wenn dieses Benutzerkonto inaktiviert oder gelöscht wird, können alle zuvor von diesem Benutzer geplanten Ablaufdiagramme nicht ausgeführt werden. Wenn Sie dieses Benutzerkonto inaktivieren, jedoch die Ausführung der zuvor geplanten Ablaufdiagramme zulassen möchten, belassen Sie den Status des Benutzerkontos bei „aktiv“ und gewähren Sie dafür nur die Berechtigung „Run Batch Flowcharts“.

Ablaufdiagrammplan mit Standardparametern erstellen

Führen Sie die folgenden Schritte aus, um ein Ablaufdiagramm mit Standardparametern zu planen.

1. Klicken Sie im Modus **Ansicht** auf der Registerkarte **Ablaufdiagramm** auf das Symbol **Zeitpläne** und wählen Sie **Element planen** aus. Dadurch wird das Fenster „Ablaufdiagrammparameter überschreiben“ geöffnet. Alle Parameter in diesem Bildschirm sind optional.
2. Klicken Sie auf die Schaltfläche **Ausführung planen** im unteren Teilfenster. Dadurch wird ein Fenster geöffnet, in dem Sie ein Ablaufdiagramm mit Standardparametern planen können.
3. Füllen Sie die Felder im Feld **Zeitplan Ablaufdiagramm** aus. Wenn Sie das Ablaufdiagramm mehrmals ausführen möchten, klicken Sie auf **Wiederholungen definieren**, um eine Wiederholungsstruktur zu konfigurieren.
4. Klicken Sie auf **Nach diesem Zeitplan ausführen**.

Informationen zum Überschreiben der Standardparameter für Zeitpläne zur Unica Campaign-Ablaufdiagrammausführung

Sie können die Standardparameter außer Kraft setzen, wenn Sie eine Ablaufdiagrammausführung planen.

Wenn Sie eine Ablaufdiagrammausführung in Unica Campaign planen, verwendet der Scheduler die Standardausführungsparameter, die für das Ablaufdiagramm definiert wurden. Diese Parameter umfassen folgende Komponenten:

- Der Tabellenkatalog mit den Tabellenzuordnungen, die das Ablaufdiagramm verwendet
- Alle Benutzervariablenwerte, die im Ablaufdiagramm definiert wurden
- Berechtigungsnachweise für alle Datenquellen, auf die das Ablaufdiagramm zugreift. Der Standard ist der Benutzer, der das Ablaufdiagramm plant.

Diese Standardwerte können in Unica Campaign überschrieben werden, um sie für verschiedene Datenquellen auszuführen oder unterschiedliche Ergebnisse zu erzielen, ähnlich den Funktionen, die vom Dienstprogramm `unica_svradm` bereitgestellt werden. Sie können z.B. mehrere Ausführungen für ein einzelnes Ablaufdiagramm planen, um unterschiedliche Kombinationen von Werten für Benutzervariablen zu testen. Sie können einen alternativen Tabellenkatalog angeben, um von Ihrer Produktionsdatenbank zu einer

Beispieldatenbank für diese Testausführungen zu wechseln. Wenn Ihre Organisation unterschiedliche Datenbankanmeldungen für Test- und Produktionsausführungen erfordert, können Sie entsprechende Berechtigungsnachweise angeben.

Ausführungsparameter zum Planen von Unica Campaign-Ablaufdiagrammen

Wenn Sie ein Unica Campaign-Ablaufdiagramm planen, kann das Ablaufdiagramm eine Zeichenfolge mit Ausführungsparametern an den Unica Scheduler weitergeben. Diese Zeichenfolge wird danach an Unica Campaign zurückgegeben, wenn eine Ausführung gestartet wird.

In Unica Campaign werden alle Werte, die im Dialogfenster **Ablaufdiagrammparameter überschreiben** festgelegt wurden, als eine einzelne Zeichenfolge an den Scheduler übermittelt. Diese Zeichenfolge wird im Feld **Ausführungsparameter** angezeigt.

Ablaufdiagrammplan erstellen

Mit dieser Prozedur können Sie ein Ablaufdiagramm planen.

1. Klicken Sie im Modus **Ansicht** auf einer Ablaufdiagramm-Registerkarte auf das Symbol **Zeitpläne** und wählen Sie **Planen** aus.

   Das Dialogfenster "Ablaufdiagrammparameter überschreiben für..." wird geöffnet.
2. Wenn Sie die standardmäßigen Ablaufdiagrammparameter überschreiben wollen, dann füllen Sie die Felder im Dialogfenster aus, um Ihre eigenen Ablaufdiagrammparameter anzugeben. Dies ist ein optionaler Schritt.

   Sie können mehrere Benutzervariablen und Datenquellen hinzufügen, indem Sie auf die Links **Benutzervariable hinzufügen** und **Datenquelle hinzufügen** klicken.

   Das System führt keine Syntaxüberprüfung für die Parameter durch, die Sie in diese Felder eingeben. Überprüfen Sie also sorgfältig, ob Sie die korrekten Werte eingegeben haben, bevor Sie fortfahren.

   Wenn Sie die standardmäßigen Ablaufdiagrammparameter nicht überschreiben wollen, dann fahren Sie mit dem nächsten Schritt fort.

3. Klicken Sie auf **Ausführung planen**, um den Dialog „Zeitplan erstellen“ zu öffnen.

   Sie können definieren, wann der Zeitplan ausgeführt werden soll. Optional können Sie auch die Einstellungen für Wiederholungen, Trigger (Auslöser) und die Richtwerte festlegen.
4. Klicken Sie auf **Nach diesem Zeitplan ausführen**.

Wichtig: Wenn Sie ein Ablaufdiagramm planen, basiert die geplante Aufgabe auf dem Ablaufdiagrammnamen. Wird der Ablaufdiagrammname nach dem Erstellen einer geplanten Aufgabe geändert, schlägt die geplante Aufgabe fehl.

Seite „Ablaufdiagrammparameter überschreiben“

In der folgenden Tabelle werden die Felder des Dialogs „Ablaufdiagrammparameter überschreiben“ beschrieben. Alle bearbeitbaren Felder dieses Dialogfensters sind optional. Das System führt keine Syntaxüberprüfung für die Parameter durch, die Sie in diese Felder eingeben. Überprüfen Sie also sorgfältig, ob Sie die korrekten Werte eingegeben haben, bevor Sie fortfahren.

Die von Ihnen in diesem Dialog eingegebenen Werte werden auf der nächsten Seite des Assistenten im Feld **Parameter ausführen** angezeigt.

Tabelle 26. Felder auf der Seite „Ablaufdiagrammparameter überschreiben“

Feld	Beschreibung
Ablaufdiagramm-ID	Eindeutige ID für das Ablaufdiagramm. Dieses Feld ist schreibgeschützt und wird automatisch ausgefüllt.
Campaign - Ablaufdiagrammname	Der Name der Kampagne, Kampagnencode und Ablaufdiagrammname. Dieses Feld ist schreibgeschützt und wird automatisch ausgefüllt.
Name der Katalogdatei	Geben Sie eine gespeicherte Tabellenkatalogdatei an, die Sie für diese Ausführung verwenden wollen.

Tabelle 26. Felder auf der Seite „Ablaufdiagrammparameter überschreiben“ (Fortsetzung)

Feld	Beschreibung
Name der Benutzervariable	Geben Sie den Namen einer beliebigen Benutzervariablen ein, die im Ablaufdiagramm definiert wurde.
Wert	Geben Sie einen Wert für die Benutzervariable ein.
Datenquellenname	Geben Sie den Namen einer beliebigen Datenquelle ein, auf die das Ablaufdiagramm zugreift.
Anmeldung	Verwenden Sie dieses Feld zum Überschreiben des standardmäßigen Anmeldenamens für die angegebene Datenquelle. Standardmäßig wird der Anmeldename des Benutzers verwendet, der den Zeitplan erstellt.
Passwort	Verwenden Sie dieses Feld zum Überschreiben des standardmäßigen Kennworts für die angegebene Datenquelle. Standardmäßig wird das Kennwort des Benutzers verwendet, der den Zeitplan erstellt.

Zeitplanbenachrichtigungen

Sie können für jeden Zeitplan Benachrichtigungen konfigurieren, wenn Sie über den Status geplanter Ausführungen informiert werden wollen. Zudem können Benutzer mit Administratorberechtigungen in Unica Platform Gruppen einrichten, an die Benachrichtigungen gesendet werden sollen.

Einzelne Zeitplanbenachrichtigungen

Sie können Benachrichtigungen für Zeitpläne erst erstellen, nachdem Sie den Zeitplan erstellt und gespeichert haben, nicht jedoch während des Erstellungsprozesses. Sie können konfigurieren, durch welche Statusarten eine Benachrichtigung ausgelöst wird und ob die Benachrichtigungen für die einzelnen Zeitpläne an Ihr E-Mail-Konto gesendet oder im Posteingang für Benachrichtigungen angezeigt werden sollen oder ob beide Möglichkeiten aktiviert werden sollen.

Zeitplanbenachrichtigungen für Gruppen

Wenn auch andere Benutzer als der Ersteller des Zeitplans Zeitplanbenachrichtigungen erhalten sollen, können Sie gruppenbasierte Benachrichtigungen aktivieren. Zum Konfigurieren von Gruppenbenachrichtigungen benötigen Sie Administratorberechtigungen in Unica Platform.

Die Konfigurationseigenschaft **Gruppenname, der Jobbenachrichtigungen erhält** ist für jeden Objekttyp, der geplant werden kann, in der Kategorie **Platform | Scheduler | Terminplanregistrierungen | [Produkt] | [Objekttyp]** auf der Seite **Einstellungen > Konfiguration** enthalten. Alle Mitglieder der in dieser Konfigurationseigenschaft angegebenen Gruppe erhalten Benachrichtigungen für alle Zeitpläne für diesen Objekttyp (beispielsweise Kampagnenablaufdiagramme).

Gruppenmitglieder erhalten für geplante Ausführungen konfigurierte Benachrichtigungen, die sich im Status **Lange Dauer** oder **Nicht gestartet/In Warteschlange** befinden. Sie erhalten keine Benachrichtigungen für Ausführungen mit dem Status **Bei Fehlschlagen**, **Bei Erfolg** oder **Unbekanntes/Sonstiges Problem**.

Durch Hinzufügen oder Entfernen von Benutzern in einer Gruppe können Sie steuern, wer diese Benachrichtigung erhält.

Konfigurieren von Benachrichtigungen für erstellte Zeitpläne

Mit dieser Prozedur können Sie Benachrichtigungen für alle von Ihnen erstellen Zeitpläne konfigurieren. Sie können Benachrichtigungen für Zeitpläne erst erstellen, wenn der Zeitplan erstellt und gespeichert wurde, aber nicht während des Erstellungsprozesses.

1. Wählen Sie **Einstellungen > Zeitplanmanagement** aus und klicken Sie auf den Namen des Zeitplans, für den Sie Benachrichtigungen konfigurieren möchten.
2. Klicken Sie auf **Jobbenachrichtigungen** bearbeiten, um das Fenster „Eigene Jobbenachrichtigungen“ zu öffnen, und klicken Sie dann auf **Neu**.
3. Füllen Sie die Felder aus und klicken Sie auf **Speichern**.

Löschen oder Ändern von Benachrichtigungen für erstellte Zeitpläne

Sie können selbst erstellte Benachrichtigungen löschen oder ändern.

1. Wählen Sie **Einstellungen > Meine Jobbenachrichtigungen** aus, um das Fenster „Meine Jobbenachrichtigungen“ zu öffnen.
2. Wählen Sie zum Löschen von Benachrichtigungen die Benachrichtigung aus, die Sie löschen möchten, und klicken Sie auf **Löschen**.
3. Klicken Sie zum Ändern von Benachrichtigungen auf den Namen der Benachrichtigung, die Sie ändern möchten, um das Fenster „Jobbenachrichtigung bearbeiten“ zu öffnen. Nehmen Sie in dem Fenster die gewünschten Änderungen vor und speichern Sie die Änderungen.

Konfigurieren von Zeitplanbenachrichtigungen für eine Benutzergruppe

Mit dieser Prozedur können Sie Benachrichtigungen für alle Zeitpläne konfigurieren, die an angegebene Benutzergruppen gesendet werden. Für diese Prozedur benötigen Sie Administratorberechtigungen in Unica Platform.

1. Rufen Sie auf der Seite **Einstellungen > Konfiguration** die Kategorie **Unica Platform | Zeitplaner | Terminplanregistrierungen** auf.
2. Legen Sie für jeden Objekttyp, für den Sie gruppenbasierte Benachrichtigungen aktivieren möchten, als Wert der Eigenschaft **Name der die Jobbenachrichtigungen erhaltenden Gruppe** den Namen der Gruppe fest, die Benachrichtigungen für diesen Objekttyp empfangen soll.

   Sie können vorhandene Gruppen verwenden oder Gruppen für diese Benachrichtigungen erstellen.

   Möglicherweise wollen Sie eine Gruppe für jeden Objekttyp einrichten, für den Sie gruppenbasierte Benachrichtigungen aktivieren wollen.
3. Weisen Sie auf der Seite „Benutzergruppen“ den Gruppen, die Sie im vorherigen Schritt angegeben haben, die erforderlichen Benutzer zu.

Seite „Eigene Jobbenachrichtigungen“

Sie können Zeitplanbenachrichtigungen auf der Seite „Eigene Jobbenachrichtigungen“ konfigurieren.

Tabelle 27. Felder der Seite „Eigene Jobbenachrichtigungen“

Feld	Definitionen
Benachrichtigungstitel	Geben Sie einen Namen für die Benachrichtigung ein.
Condition	Wählen Sie die Statusbedingung aus, durch die eine Benachrichtigung ausgelöst wird. Sie können für jeden Status, für den eine Benachrichtigung ausgelöst werden soll, eine andere Benachrichtigung erstellen.
Die Benachrichtigung senden an	Wählen Sie aus, wie die Benachrichtigung empfangen werden soll. Die Benachrichtigung kann an das E-Mail-Konto gesendet werden, das dem Unica-Benutzerkonto zugeordnet ist, sie kann in den Benachrichtigungen in der Benutzeroberfläche angezeigt oder auf beide Arten ausgegeben werden.
Benachrichtigungsstatus	Wählen Sie aus, ob diese Benachrichtigung aktiv oder inaktiv ist. Wenn Sie den inaktiven Modus auswählen, werden keine Benachrichtigungen gesendet.

Zeitplanmanagement

Sie können alle Zeitpläne über die Seite **Einstellungen > Zeitplanmanagement** verwalten. Sie müssen über die Berechtigung für die Seite „Geplante Aufgaben verwalten“ in Unica Platform verfügen, um Zeitpläne verwalten zu können.

Im Folgenden werden die Registerkarten von der Seite „Geplante Aufgaben“ aufgeführt.

- Zeitpläne - Auf dieser Registerkarte können Sie Zeitpläne erstellen und Zeitplandefinitionen anzeigen oder löschen. Sie können auf den Zeitplannamen klicken, um eine Definition zu bearbeiten und dabei z.B. Benachrichtigungen hinzuzufügen und den Zeitplan zu aktivieren oder zu inaktivieren.
- Ausführungen - Auf dieser Registerkarte können Sie in der Warteschlange befindliche und abgeschlossene Ausführungen aller Zeitpläne anzeigen, eine in der Warteschlange befindliche Ausführung abbrechen oder eine Ausführung löschen. Sie können auf den Zeitplannamen klicken, um eine Definition zu bearbeiten und dabei z.B. Benachrichtigungen hinzuzufügen und den Zeitplan zu aktivieren oder zu inaktivieren.

Zeitpläne und Partitionen

In einer Umgebung mit mehreren Partitionen werden nur die Zeitpläne angezeigt, die in der Partition erstellt werden, der Sie angehören. Nur wenn Sie über die Rolle „PlatformAdminRole“ verfügen, können Sie alle geplanten Ausführungen in allen Partitionen anzeigen.

Unbekannter Status

Wenn eine große Anzahl an Ausführungen mit unbekanntem Status angezeigt wird, können Sie die Abfragehäufigkeit des Schedulers anpassen, indem Sie einen Wert für die Eigenschaft **Platform | Scheduler | Maximale Anzahl von Abfragen des unbekannten Status** auf der Seite **Einstellungen > Konfiguration** festlegen. Diese Eigenschaft gibt an, wie oft der Scheduler den Status einer Ausführung überprüft, bevor der Status „Unbekannt“ gemeldet wird.

Der Status „Unbekannt“ gibt an, dass Unica Platform nicht feststellen kann, ob der Job ausgeführt wird, abgeschlossen wurde oder fehlgeschlagen ist.

Wenn in Ihrem Unternehmen eine große Anzahl von Jobs geplant ist, kann das Erhöhen der Abfragefrequenz negative Auswirkungen auf die Leistung haben.

Zeitplanlistenfilter

Auf den Registerkarten „Ausführungen“ und „Zeitpläne“ können Sie die Zeitplanliste filtern.

Sie können Text in das Feld oben rechts in der Liste eingeben, um einen Schnellfilter zu aktivieren, der Ihren Suchbegriff mit den Werten vergleicht, die in allen Spalten der Liste vorkommen. Wenn Ihr Suchbegriff in einer der Spalten enthalten ist, dann wird der Zeitplan oder die Ausführung in die Suchergebnisse aufgenommen.

Zum Aufrufen der erweiterten Suche können Sie auf **Zeitplanlistenfilter bearbeiten** klicken, um ein Fenster zu öffnen, in dem Sie die Kriterien für die Auswertung auf Basis der Attribute der aufgelisteten Zeitpläne oder Ausführungen festlegen können.

Inaktivieren und Aktivieren mehrerer Zeitpläne (nur mit FixPack 10.0.0.1)

Wenn Sie Unica Platform FixPack 10.0.0.1 angewendet haben, können Sie auf der Registerkarte „Zeitpläne“ mehrere Zeitpläne auswählen und diese durch Klicken auf die Schaltfläche **Deaktivieren** oder **Aktivieren** oben in der Liste deaktivieren oder aktivieren.

Sie können diese Funktion zur Masseninaktivierung und -aktivierung zusammen mit dem Filter zum Abrufen einer Liste der Zeitpläne, die Sie inaktivieren oder aktivieren möchten, verwenden. Wenn Sie beispielsweise beim Erstellen von Zeitplänen Suchtags hinzugefügt haben, können Sie die Liste so filtern, dass nur Zeitpläne mit einem bestimmten Tag angezeigt werden. Anschließend können Sie alle diese Zeitpläne auswählen und mit einem einzigen Klick inaktivieren oder aktivieren.

Wenn Sie eine geplante Aufgabe inaktivieren, werden nicht alle, von einem Auslöser der inaktivierten Aufgabe abhängigen Zeitpläne inaktiviert. Sie werden allerdings nicht ausgeführt, da sie den Auslöser nicht empfangen.

Seiten zum Zeitplanmanagement

Sie können auf die Seiten zum Zeitplanmanagement durch Auswählen von **Einstellungen > Zeitplanmanagement** oder durch Auswählen von **Zeitplan anzeigen** im Menü **Ausführen** eines Ablaufdiagramms zugreifen.

Registerkarte „Zeitpläne“

Tabelle 28. Felder und Links auf der Registerkarte „Zeitpläne“

Feld oder Link	Beschreibung
 Inaktivieren	Inaktivieren Sie mindestens einen ausgewählten Zeitplan. Nur verfügbar, wenn Sie Unica Platform FixPack 10.0.0.1 angewendet haben.
 Aktivieren	Aktivieren Sie mindestens einen ausgewählten Zeitplan. Nur verfügbar, wenn Sie Unica Platform FixPack 10.0.0.1 angewendet haben.
Zeitplan erstellen	Klicken Sie auf dieses Element, um einen Assistenten zu öffnen, in dem Sie einen Zeitplan einrichten können.
Zeitplanlistenfilter bearbeiten	Klicken Sie auf dieses Element, um einen erweiterten Filter für die Liste zu erstellen.
Löschen	Löschen einzelner oder mehrerer ausgewählter Zeitpläne. Sie können Zeitpläne auswählen, indem Sie in der Spalte links neben dem Zeitplan klicken. Um alle Zeitpläne auszuwählen, müssen Sie oben in der Spalte auf der linken Seite klicken.
Aktualisieren	Klicken Sie auf dieses Element, um die Liste zu aktualisieren.
Filter	Klicken Sie auf dieses Element, um einen einfachen Filter für die Liste zu erstellen.
Zeitplanname	Der Zeitplan, von dem die Ausführung eine Instanz darstellt.
Zeitplanstatus	Gibt an, ob der Zeitplan aktiviert oder inaktiviert ist.
Geplantes Element	Der Name des auszuführenden Objekts.
Elementtyp	Der Typ des auszuführenden Objekts.

Tabelle 28. Felder und Links auf der Registerkarte „Zeitpläne“ (Fortsetzung)

Feld oder Link	Beschreibung
Erstellt durch	Der Benutzername des Kontos, mit dem der Zeitplan erstellt wurde.
Starttrigger	Wenn der Zeitplan von einem Trigger (Auslöser) abhängig ist, der Trigger, der die Ausführung des Zeitplans auslöst.
Start	Datum und Uhrzeit der geplanten ersten Ausführung dieser Aufgabe.
Wiederholungsstruktur	Eine Beschreibung der Wiederholungsstruktur.
Ende	Datum und Uhrzeit der geplanten letzten Ausführung dieser Aufgabe. **Anmerkung:** Gilt nur für wiederholt auftretende geplante Aufgaben.
Vorherige 1 Ausführung und 2 nächste Ausführungen	Datum und Uhrzeit der vorherigen Ausführung und der nächsten beiden geplanten Ausführungen. **Anmerkung:** Gilt nur für wiederholt auftretende geplante Aufgaben. Die Informationen für die vorherige Ausführung und die nächsten beiden geplanten Ausführungen werden gemäß der Schedulerdefinition angezeigt. Diese wird aktuell nicht auf die Ausschlussregeln hin geprüft.
Abhängigkeiten	Wenn das geplante Objekt von anderen Objekten abhängig ist, werden diese hier aufgeführt.

Tabelle 28. Felder und Links auf der Registerkarte „Zeitpläne“ (Fortsetzung)

Feld oder Link	Beschreibung
Trigger bei Erfolg	Die Zeichenfolge, die gesendet wird, wenn das Produkt den erfolgreichen Abschluss einer Ausführung dieses Zeitplans meldet. Dieses Feld ist leer, sofern kein Trigger bei Erfolg festgelegt wurde.
Trigger bei Fehler	Die Zeichenfolge, die gesendet wird, wenn das Produkt einen fehlgeschlagenen Abschluss einer Ausführung dieses Zeitplans meldet. Dieses Feld ist leer, sofern kein Trigger bei „Fehler“ festgelegt wurde.

Registerkarte „Ausführungen“

Tabelle 29. Felder und Links der Registerkarte „Ausführungen“

Feld oder Link	Beschreibung
Zeitplanlistenfilter bearbeiten	Klicken Sie auf dieses Element, um einen erweiterten Filter für die Liste zu erstellen.
Löschen	Löschen einzelner oder mehrerer ausgewählter Zeitpläne. Sie können Zeitpläne auswählen, indem Sie in der Spalte links neben dem Zeitplan klicken. Um alle Zeitpläne auszuwählen, müssen Sie oben in der Spalte auf der linken Seite klicken.
Als abgebrochen markieren	Abbrechen einzelner oder mehrerer ausgewählter Zeitpläne.
Aktualisieren	Klicken Sie auf dieses Element, um die Liste zu aktualisieren.
Filter	Klicken Sie auf dieses Element, um einen einfachen Filter für die Liste zu erstellen.
Ausführungs-ID	Die Identifikationsnummer, die der Ausführung in den Unica Platform-Systemtabellen zugewiesen wurde.
Zeitplanname	Der vom Ersteller festgelegte Name des Zeitplans.

Tabelle 29. Felder und Links der Registerkarte „Ausführungen“ (Fortsetzung)

Feld oder Link	Beschreibung
Geplantes Element	Der Name des auszuführenden Objekts.
Elementtyp	Der Typ des auszuführenden Objekts.
Start	Datum und Uhrzeit, zu der die Ausführung gestartet wurde.
Letzte Aktualisierung	Zeitpunkt (Datum und Uhrzeit), zu dem die Informationen für diese Ausführung aktualisiert wurden.
Ausführungsstatus	Status der Ausführung gemäß der Definition im Scheduler: • **Geplant** - Die Ausführung wurde noch nicht gestartet. • **In Warteschlange** - Der Zeitplaner (Scheduler) hat die Ausführung gestartet, aufgrund von Richtwertbedingungen konnte das Unica-Produkt die geplante Ausführung jedoch noch nicht beginnen. • **Beendet** - Die Ausführung wurde beendet und hat den Status „Erfolgreich“ oder „Fehlgeschlagen“ zurückgegeben. • **Abgebrochen** - Ein Benutzer hat eine Ausführung durch Klicken auf **Als abgebrochen** markieren auf der Seite „Geplante Ausführungen“ abgebrochen. Befand sich die Ausführung in der Warteschlange, als der Benutzer sie als abgebrochen markiert hat, wird sie nicht ausgeführt. Wurde die Ausführung bereits gestartet, wird sie von dieser Aktion nicht gestoppt, sondern als abgebrochen markiert, und werden alle für diese Ausführung konfigurierten Trigger nicht gesendet. Darüber hinaus werden Ausführungen, die von der abgebrochenen Ausführung abhängen, nicht ausgeführt. • **Unbekannt** - Gibt an, dass Unica Platform nicht feststellen kann, ob der Job momentan noch ausgeführt wird, abgeschlossen wurde oder fehlgeschlagen ist.

Tabelle 29. Felder und Links der Registerkarte „Ausführungen“ (Fortsetzung)

Feld oder Link	Beschreibung
Ausführungsstatus	Status der Ausführung des Objekts, der von dem Produkt definiert wurde, das die Ausführung durchführt. Der Status in diesem Feld wird aktualisiert, wenn die Ausführung den Status „Abgebrochen“ meldet und nach dem Neustart einen anderen Status an den Scheduler sendet.
Details	Informationen zur Ausführung – durch das Produkt bereitgestellt. Bei einer Ablaufdiagrammausführung beinhaltet dies beispielsweise den Ablaufdiagrammnamen und die Ablaufdiagramm-ID, den Fehler bei einer fehlgeschlagenen Ausführung und die abgelaufene Zeit bei einer erfolgreichen Ausführung.

Zeitplanlistenfilter bearbeiten - Zeitpläne

Tabelle 30. Zeitplanlistenfilter auf Registerkarte „Zeitpläne“ bearbeiten

Spalte	Beschreibung
Nach Suchtags/Schlüselwörtern filtern	Wählen Sie dieses Kontrollkästchen aus, wenn Suchtags oder Schlüsselwörter in den Filter aufgenommen werden sollen. Die Zeichenfolge, die Sie hier eingeben, wird mit den Zeichenfolgen abgeglichen, die in den Feldern **Suchtags/Schlüsselwörter** eingegeben werden, wenn Zeitpläne erstellt werden.
Suchtags/Schlüsselwörter	Geben Sie die Suchtags oder Schlüsselwörter ein, die im Filter verwendet werden sollen.
Nach anderen Kriterien filtern	Wählen Sie dieses Kontrollkästchen aus, wenn zusätzliche Kriterien in Ihren Filter aufgenommen werden sollen.
Ausführungsmetadaten	Wählen Sie eine der folgenden Optionen aus, die in Ihre Regel aufgenommen werden soll. Gültige Optionen sind:

Tabelle 30. Zeitplanlistenfilter auf Registerkarte „Zeitpläne“ bearbeiten (Fortsetzung)

Spalte	Beschreibung
	• **Zeitplanname** • **Zeitplanstatus** • **Elementtyp** • **Erstellt durch** • **Geplantes Element**
Condition	Wählen Sie eine der folgenden Optionen aus, um festzustellen, wie Ihre Regel ausgewertet wird. • **Übereinstimmungen** • **Beginnt mit** • **Endet mit** • **Enthält**
Wert	Geben Sie den Wert ein, der auf die Regel angewendet werden soll, oder wählen Sie einen Wert aus. Die Optionen können abhängig von den für die Regel ausgewählten Metadaten variieren. • **Zeitplanname** Geben Sie die gewünschten Zeichen ein. • **Zeitplanstatus** Die Optionen für die Werte lauten **Aktiviert** und **Deaktiviert**. • **Elementtyp** Die Optionen für die Werte sind die verschiedenen Zeitplantypen. • **Erstellt durch** Geben Sie die gewünschten Zeichen ein. Ihr Wert wird mit den Anmeldenamen der Benutzer verglichen.

Tabelle 30. Zeitplanlistenfilter auf Registerkarte „Zeitpläne“ bearbeiten (Fortsetzung)

Spalte	Beschreibung
	• **Geplantes Element** Geben Sie die gewünschten Zeichen ein. Die hier von Ihnen eingegebene Zeichenfolge wird mit dem Text in der Spalte **Geplantes Element** verglichen.
And / Or	Wählen Sie einen dieser Operatoren für jede Regel aus, die Sie erstellen.

Zeitplanlistenfilter bearbeiten - Ausführungen

Tabelle 31. Zeitplanlistenfilter auf Registerkarte „Ausführungen“ bearbeiten

Spalte	Beschreibung
Filtern basierend auf Zeit	Wählen Sie dieses Kontrollkästchen aus, wenn Sie Ausführungen anzeigen wollen, die in einem bestimmten Zeitintervall aufgetreten sind.
Zeitzone	Wenn Sie eine andere Option als die Standardoption des Servers auswählen, dann verwendet die Suche die ausgewählte Zeitzone zur Berechnung der Zeitpläne, die sich innerhalb des angegebenen Datumsbereichs befinden.
Liste wird ausgeführt für letzte n Instanzen	Bei wiederholt ausgeführten Ausführungen müssen Sie angeben, wie viele vorherige Ausführungen in der Liste angezeigt werden sollen.
Liste wird ausgeführt von	Geben Sie ein Zeitintervall für die in der Liste aufgeführten Ausführungen an.
Nach anderen Kriterien filtern	Wählen Sie dieses Kontrollkästchen aus, wenn zusätzliche Kriterien in Ihren Filter aufgenommen werden sollen.
Ausführungsmetadaten	Wählen Sie eine der folgenden Optionen aus, die in Ihren Filter aufgenommen werden soll.

Tabelle 31. Zeitplanlistenfilter auf Registerkarte „Ausführungen“ bearbeiten (Fortsetzung)

Spalte	Beschreibung
	Gültige Optionen sind: • **Zeitplanname** • **Ausführungsstatus** • **Ausführungsstatus** • **Geplantes Element**
Condition	Wählen Sie eine der folgenden Optionen aus, um festzustellen, wie Ihre Kriterien ausgewertet werden. • **Übereinstimmungen** • **Beginnt mit** • **Endet mit** • **Enthält**
Wert	Geben Sie den Wert ein, der auf den Filter angewendet werden soll, oder wählen Sie einen Wert aus. Die Optionen können abhängig von den für die Regel ausgewählten Metadaten variieren. • **Zeitplanname** Geben Sie die gewünschten Zeichen ein. • **Ausführungsstatus** Wertoptionen sind: ◦ **Queued** ◦ **Running** ◦ **Completed** ◦ **Unbekannt** ◦ **Abgebrochen** • **Ausführungsstatus**

Tabelle 31. Zeitplanlistenfilter auf Registerkarte „Ausführungen“ bearbeiten (Fortsetzung)

Spalte	Beschreibung
	Die Optionen der Werte sind **Erfolgreich**, **Wird ausgeführt**, **Abgebrochen**, **Fehlgeschlagen** und **Unbekannt**. • **Geplantes Element** Geben Sie die gewünschten Zeichen ein. Die hier von Ihnen eingegebene Zeichenfolge wird mit dem Text in der Spalte **Geplantes Element** verglichen.
And / Or	Wählen Sie einen dieser Operatoren für jede Regel aus, die Sie erstellen.

Auf SAML 2.0 basierende föderierte Authentifizierung

Unica Platform implementiert einen auf SAML 2.0 basierenden Identitätsprovider (IdP), der eine Single Sign-on-Föderation zwischen Unica-Produkten oder zwischen Unica-Produkten und Anwendungen anderer Anbieter aktiviert.

Eine Föderation ist eine Gruppe von IdPs und Anwendungen, die in einer vertrauenswürdigen Umgebung zusammenarbeiten und Services für einander mit SAML 2.0 (Security Assertion Markup Language) basierend auf Standards bereitstellen.

Anwendungen, die Mitglieder einer Föderation sind, werden als Service Provider (SPs) bezeichnet. Der IdP-Server und die SPs können vor Ort oder in einer Cloud gehostet werden.

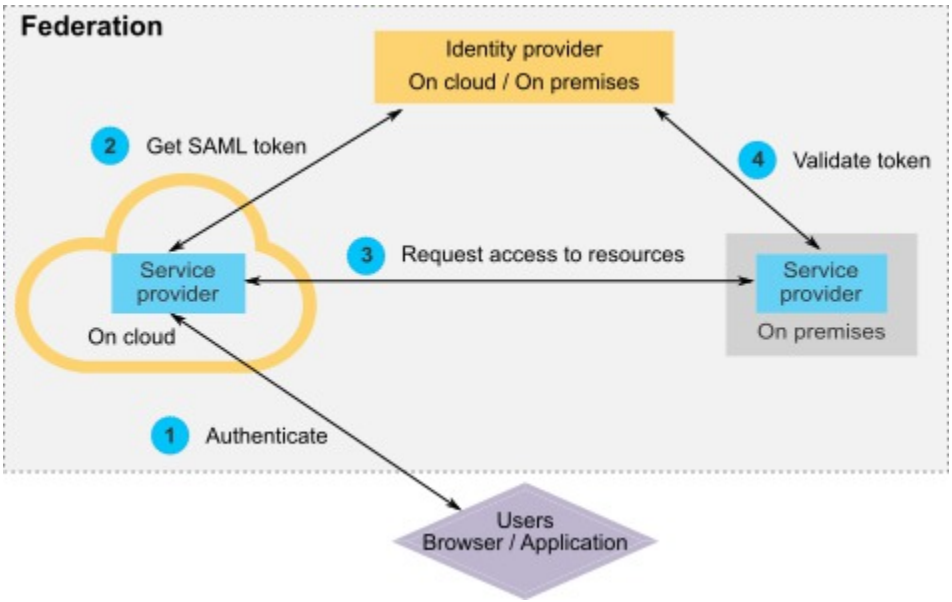
Eine SAML 2.0-Föderation unterstützt verschiedene Authentifizierungsmechanismen für Single Sign-on. Ein Benutzer kann beispielsweise in einem SP authentifiziert werden, der den Authentifizierungsmechanismus dieser Anwendung verwendet (z. B. intern, OAuth, OpenId, SAML, Kerberos). Anschließend kann der Benutzer auf andere SPs mit föderiertem Single Sign-on zugreifen, wenn die Anwendungen Teil derselben Föderation sind und der Benutzer entsprechend zugeordnet ist.

Der IdP-Server erzeugt, validiert oder löscht Token basierend auf Benutzerzuordnungen. Datenzugriffsobjekte werden für die unterstützen Datenbanktypen implementiert und in den IdP-Server eingeschlossen.

Ein Administrator ordnet Benutzer-IDs zwischen SPs zu, um Single Sign-on-Zugriff für zugeordnete Benutzer bereitzustellen. Beispiel: Angenommen, SP_A und SP_B sind Mitglieder derselben Föderation. Benutzer1 ist ein Konto in SP_A und Benutzer2 ist ein Konto in SP_B. Das Konto von Benutzer1 wird in der Föderation dem Konto von Benutzer2 zugeordnet. Wenn sich ein Benutzer mit den Berechtigungsnachweisen von Benutzer1 bei SP_A anmeldet, verfügt dieser Benutzer über Single Sign-on-Zugriff auf SP_B. Und wenn sich ein Benutzer bei SP_B mit den Berechtigungsnachweisen von Benutzer2 anmeldet, verfügt dieser Benutzer über Single Sign-on-Zugriff auf SP_A.

Diagramm

Im folgenden Diagramm ist diese Föderation dargestellt.



Komponenten der HCL Implementierung

Die Implementierung des auf SAML 2.0 basierenden föderierten Single Sign-on umfasst die folgenden Komponenten.

Diese Komponenten befinden sich im Verzeichnis `tools/lib` unter Ihrer Unica Platform-Installation.

- Ein auf SAML 2.0 basierender IdP-Server, der als WAR-Datei bereitgestellt wird: `idp-server.war`
- Eine Clientfassade: `idp-client.jar`

  Die IdP-Clientfassade ist eine Java™-Implementierung mit einer API, die mit Sicherheitstoken arbeitet. Sie wird als JAR-Datei bereitgestellt. Die Javadoc™ Dokumentation für die API ist in Unica Platform Javadoc™ enthalten.

  Die IdP-Clientfassade aktiviert Java™-SPs für die schnelle Integration mit dem IdP-Server und um Teil der Föderation zu werden.

Unterstützte Anwendungsfälle

Durch die aktuelle Implementierung können SPs mit Sicherheitstoken arbeiten, um die Single-Sign-on-Authentifizierung zwischen den SPs zu erreichen.

Generieren eines neuen SAML-Token

Die Implementierung kann ein neues SAML-Token für einen Benutzer generieren, der eine Single Sign-on-Authentifizierungsanforderung initiiert. Dieser Benutzer muss dem IdP-Server zugeordnet werden. Der IdP-Server erzeugt basierend auf den Berechtigungsnachweisen der vertrauenswürdigen Partei und der Benutzerzuordnung ein neues Sicherheitstoken und setzt es mit einer SAML 2.0-Zusicherung ab.

Beispiel: Wenn Benutzer1 von SP_A zu Benutzer2 mit SP_B auf dem IdP-Server zugeordnet ist und Benutzer1 versucht, auf SP_B-Ressourcen zuzugreifen, generiert der IdP-Server ein Sicherheitstoken für Benutzer1 als vertrauenswürdige Partei.

Validieren eines vorhandenen SAML-Token

Die Implementierung kann ein vorhandenes SAML-Token validieren, das durch einen SP dargestellt wird und das die Zugriffsanforderung von einem Benutzer von einem anderen SP empfängt. Der SP validiert zunächst das Sicherheitstoken und die Clientzuordnung mit dem IdP-Server, um den zugeordneten Benutzer in der eigenen Domäne zu identifizieren.

Beispiel: Wenn SP_A versucht, im Namen von Benutzer1 auf SP_B-Ressourcen zuzugreifen, und das IdP-Sicherheitstoken darstellt, übergibt SP_B dieses Token an den IdP-Server. Wenn das Token gültig und Benutzer1 zu einem SP_B-Benutzer zugeordnet ist, löst der IdP-Server den SP_B-Benutzer in der SP_B-Domäne auf und gibt die Zusicherung zurück.

Löschen eines vorhandenen SAML-Token

Die Implementierung kann ein vorhandenes SAML-Token für einen SP-Benutzer löschen, wenn sich ein Benutzer beim System abmeldet oder das Zeitlimit der Sitzung aufgrund von Inaktivität überschritten wird. Der IdP-Server löscht das Token basierend auf den Berechtigungsnachweisen der vertrauenswürdigen Partei und der Benutzerzuordnung und setzt die Zeitmarke für den letzten Zugriff zurück, wenn die Abmeldeanforderung empfangen wird. Die Zuordnung des Benutzers wird dadurch NICHT gelöscht.

Einschränkungen

Die aktuelle Implementierung unterstützt die folgenden Anwendungsfälle nicht.

- Erzeugen einer neuen Benutzerzuordnung zwischen SP-Benutzern über eine Benutzerschnittstelle oder API
- Aktualisieren einer vorhandenen Benutzerzuordnung zwischen SP-Benutzern über eine Benutzerschnittstelle oder API
- Löschen einer vorhandenen Benutzerzuordnung zwischen SP-Benutzern über eine Benutzerschnittstelle oder API

Föderierte Authentifizierung und Partitionen

Wenn Ihre Unica-Umgebung über mehrere Partitionen verfügt, können Sie separate, auf SAML 2.0 basierende föderierte Authentifizierungen pro Partition einrichten. Um dies zu implementieren, müssen Sie auf der Seite **Einstellungen > Konfiguration** neue Eigenschaften in der Kategorie **Unica Platform | Sicherheit | Föderierte Authentifizierung | Partitionen | Partition[n]** für jede Partition erzeugen.

Implementieren der föderierten Authentifizierung

Führen Sie die Prozedur in diesem Abschnitt aus, um die auf SAML 2.0 basierende föderierte Authentifizierung mit ExperienceOne Produkten zu implementieren.

Erstellen des Daten-Repositorys

Erstellen Sie die beiden Datenbanktabellen `TP_MASTER` und `TP_MAPPING` für Benutzerzuordnungen. Für die Erstellung der Tabellen kann jedes beliebige Schema verwendet werden.

Im folgenden Beispiel werden SQL-Scripts im Verzeichnis `scripts` in der Datei `idp-server.war` bereitgestellt.

- `DatabaseScript_DB2.sql`
- `DatabaseScript_Oracle.sql`
- `DatabaseScript_SQL.sql`

In der folgenden Tabelle werden die Felder in den Datenbanktabellen erläutert, die von den Scripts erzeugt werden.

Tabelle 32. Felder in der `TP_MASTER`-Tabelle

Feld	Beschreibung
`TP_ID`	Primärschlüssel. Die eindeutige ID für einen registrierten Service-Provider.
`TP_NAME`	Der Name des Service-Providers.
`TP_INFO`	Eine Beschreibung des Service Anbieter.
`KEY_ALIAS`	Eindeutiger Schlüssel. Der Aliasname des Service Provider-Keystores. Erzwingt einen eindeutigen Aliasnamen. Sie können die Bedingung UNIQUE löschen, wenn Sie denselben Keystore-Alias für mehrere Service-Provider verwenden möchten.

Tabelle 33. Felder in der `TP_MAPPING`-Tabelle

Feld	Beschreibung
`TP_CLIENT_ID`	Fremdschlüssel. Die `TP_ID` des anfordernden Service-Providers.

Tabelle 33. Felder in der `TP_MAPPING`-Tabelle (Fortsetzung)

Feld	Beschreibung
	Teil eines zusammengesetzten Primärschlüssels, der vier Spalten umfasst, um sicherzustellen, dass diese Tabelle keine duplizierten Zuordnungen enthält.
`TP_FOR_USER_ID`	Die ID des Benutzers, der die Anforderung vom anfordernden Service-Provider absetzt. Teil eines zusammengesetzten Primärschlüssels, der vier Spalten umfasst, um sicherzustellen, dass diese Tabelle keine duplizierten Zuordnungen enthält. Muss mindestens 4 Zeichen umfassen und bis zu 24 Zeichen lang sein und darf nur alphanumerische Zeichen, Bindestriche und Unterstriche enthalten: `[a-zA-Z0-9_-]`
`TP_SP_ID`	Fremdschlüssel. Die `TP_ID` des bedienenden Service-Providers. Teil eines zusammengesetzten Primärschlüssels, der vier Spalten umfasst, um sicherzustellen, dass diese Tabelle keine duplizierten Zuordnungen enthält. Muss mindestens 4 Zeichen umfassen und bis zu 24 Zeichen lang sein und darf nur alphanumerische Zeichen, Bindestriche und Unterstriche enthalten: `[a-zA-Z0-9_-]`
`TP_MAPPED_USER_ID`	Die ID des Benutzers im bedienenden Service-Provider. Teil eines zusammengesetzten Primärschlüssels, der vier Spalten umfasst, um sicherzustellen, dass diese Tabelle keine duplizierten Zuordnungen enthält.
`SAML_TOKEN`	Eindeutiger Schlüssel. ID des SAML-Tokens. Erzwingt die Generierung eines eindeutigen Tokens. Sie können die Bedingung UNIQUE löschen, wenn Sie dasselbe Token für mehrere Service-Provider verwenden möchten.

Tabelle 33. Felder in der `TP_MAPPING`-Tabelle (Fortsetzung)

Feld	Beschreibung
`LAST_REQUEST`	Zeitmarke der letzten erfolgreichen Anforderung.

Konfigurieren der IdP-Datenquelle im Webanwendungsserver

Tomcat, WebSphere® und WebLogic sind unterstützte Webanwendungsserver für den IdP-Server. Nachdem der IdP-Server auf dem Webanwendungsserver bereitgestellt wurde, konfigurieren Sie eine JNDI-Datenquelle, um den IdP-Server mit dem Daten-Repository zu verbinden.

Details zum Konfigurieren einer JNDI-Datenquelle können Sie der Dokumentation Ihres Webanwendungsservers entnehmen.

Die folgende Konfiguration ist beispielsweise erforderlich, um die Datenquelle für eine Oracle-Datenbank in einem Tomcat-Server zu erzeugen. Definieren Sie in der Datei `conf/context.xml` unter Ihrer Tomcat-Installation eine neue Ressource.

```
<Resource name="idp_datasource"
auth="Container"
type="javax.sql.DataSource"
maxActive="100" maxIdle="30" maxWait="10000"
username="your_username" password="your_password"
driverClassName="com.microsoft.sqlserver.jdbc.SQLServerDriver"
url="jdbc:sqlserver://localhost:1433;DatabaseName=IdPServer"/>
```

Registrieren Sie diese Ressource in der Datei `conf/web.xml` unter Ihrer Tomcat-Installation.

```
<resource-ref>
<description>SQL Server Datasource example</description>
<res-ref-name>idp_datasource</res-ref-name>
<res-type>javax.sql.DataSource</res-type>
<res-auth>Container</res-auth>
</resource-ref>
```

Einrichten der Klassenpfade für IBM® IdP-Clientfassade

Wenn Sie die IBM® IdP-Clientfassade verwenden möchten, müssen Sie JAR-Dateien im Klassenpfad Ihres IdP-Servers und der SPs hinzufügen.

1. Rufen Sie die erforderlichen JAR-Dateien wie im Folgenden beschrieben ab und platzieren Sie diese JAR-Dateien auf dem IdP-Server und den Servern, die Ihre SPs hosten.
    - Suchen Sie die Datei `unica.war` im Unica Platform-Installationsverzeichnis. Extrahieren Sie die Datei `unica.war`, navigieren Sie zum Verzeichnis `WEB-INF\lib` und kopieren Sie die folgenden JAR-Dateien.
        - `bcprov-jdk15.jar`
        - `esapi-2.0.1.jar`
        - `jersey-core-1.17.jar`
        - `jersey-server-1.17.jar`
        - `jersey-servlet-1.17.jar`
        - `joda-time-2.2.jar`
        - `opensaml-2.6.1.jar`
        - `openws-1.5.1.jar`
        - `xmlsec-1.5.6.jar`
        - `xmltooling-1.4.1.jar`
    - `asm-3.1.jar`

      Führen Sie den Download über die folgende Adresse durch: http://mvnrepository.com/artifact/asm/asm/3.1.
    - `jcl-over-slf4j-1.7.5.jar`

      Führen Sie den Download über die folgende Adresse durch: http://mvnrepository.com/artifact/org.slf4j/jcl-over-slf4j/1.7.5.
    - `slf4j-api-1.7.5.jar`

      Führen Sie den Download über die folgende Adresse durch: http://mvnrepository.com/artifact/org.slf4j/slf4j-api/1.7.5.
2. Fügen Sie die im vorherigen Schritt abgerufenen JAR-Dateien im Klassenpfad Ihres IdP-Servers und im Klassenpfad der einzelnen SPs hinzu.

3. Fügen Sie für jeden SP, den Sie in die Föderation einschließen möchten, außerdem die folgende JAR-Datei für die Clientfassade zum Klassenpfad hinzu: : `idp-client.jar` Diese JAR-Datei wird zusammen mit Ihrer Unica Platform-Installation bereitgestellt.

Bereitstellen des IdP-Servers

Die Datei `IdP-Server.war` kann zusammen mit der Unica Platform-WAR-Datei auf demselben Server oder separat bereitgestellt werden. Es besteht keine direkte Abhängigkeit zwischen diesen beiden WAR-Dateien.

Konfigurieren des IdP-Servers

Der IdP-Server speichert den Keystore in seiner Konfiguration, um das SAML-Token von SPs zu bestätigen. Die Konfigurationen werden in der Datei `IdPServerConfig.properties` im Ordner `conf` des Webanwendungsservers gespeichert, auf dem der IdP-Server bereitgestellt ist.

Die in diesem Abschnitt gezeigten Abfragen sind generisch. Wenn Sie die Abfrage für Ihren Datenbanktyp ändern müssen, verwenden Sie einen der folgenden Suffixe im Schlüssel und geben Ihre neue Abfrage als Wert ein.

- `Sql`
- `Oracle`
- `db2`

Um beispielsweise die Abfrage in der Eigenschaft `com.ibm.ocm.idp.server.query.token.create` für DB2® zu ändern, bearbeiten Sie die Eigenschaft wie folgt.

```
com.ibm.ocm.idp.server.query.token.create.db2 = new query
```

Anmerkung: Die Reihenfolge und Anzahl an Spalten in der geänderten Abfrage müssen der ursprünglichen Abfrage entsprechen.

Referenz: Datei IdPServerConfig.properties

In diesem Abschnitt sind die Standardwerte der Eigenschaften in der Konfigurationsdatei und alle unterstützten Werte für die Eigenschaften aufgeführt.

`com.ibm.ocm.idp.server.keystore.path`

Der absolute Pfad der Keystore-Datei auf der Hostmaschine des Webanwendungsservers.

Standardwert: path/idp.jks

`com.ibm.ocm.idp.server.keystore.passkey`

Hauptschlüssel des Keystore.

Standardwert: `idp001`

`com.ibm.ocm.idp.server.keystore.alias`

Alias des Keystore.

Standardwert: `idp`

`com.ibm.ocm.idp.server.certificate.issuer`

URL des Zertifikatsausstellers.

Standardwert: `http://localhost:8080/idp/`

`com.ibm.ocm.idp.server.token.validity`

Token-Gültigkeitszeitraum in Sekunden.

Standardwert: `3600`

`com.ibm.ocm.idp.server.enable`

Protokollfunktion für IdP-Server.

Standardwert: True

`com.ibm.ocm.idp.server.dao.class`

Implementierung eines datenbankspezifischen Datenzugriffsobjekts.

Folgende DAOs werden unterstützt:

`com.ibm.ocm.idp.server.dao.IdPServerSQLDAO`

`com.ibm.ocm.idp.server.dao.IdPServerOracleDAO`

`com.ibm.ocm.idp.server.dao.IdPServerDB2DAO`

Standardwert: `com.ibm.ocm.idp.server.dao.IdPServerSQLDAO`

`com.ibm.ocm.idp.server.datasource.name`

Name der JNDI-Datenquelle, der im Anwendungsserver definiert ist.

Standardwert: `idp_datasource`

`com.ibm.ocm.idp.server.query.token.create`

Abfrage zum Erzeugen von Token.

Standardwert:

```
UPDATE TP_MAPPING
SET SAML_TOKEN = ?, LAST_REQUEST = ?
WHERE TP_CLIENT_ID = ?
AND TP_FOR_USER_ID = ?
AND TP_SP_ID = ?
```

`com.ibm.ocm.idp.server.query.token.get`

Abfrage zum Abrufen von Token.

Standardwert:

```
SELECT SAML_TOKEN,
LAST_REQUEST FROM TP_MAPPING
WHERE TP_CLIENT_ID = ?
AND TP_FOR_USER_ID = ?
AND TP_SP_ID = ?
```

`com.ibm.ocm.idp.server.query.mapping.validate`

Abfrage zum Validieren einer Benutzerzuordnung.

Standardwert:

```
SELECT TP_MAPPED_USER_ID FROM TP_MAPPING
WHERE TP_CLIENT_ID = ?
AND TP_FOR_USER_ID = ?
AND TP_SP_ID = ?
```

`com.ibm.ocm.idp.server.query.token.delete`

Abfrage zum Löschen von Token.

Standardwert:

```
UPDATE TP_MAPPING SET SAML_TOKEN = null,
LAST_REQUEST = null
WHERE TP_CLIENT_ID = ?
AND TP_FOR_USER_ID = ?
AND TP_SP_ID = ?
```

`com.ibm.ocm.idp.server.query.client.get`

Abfrage zum Abrufen von Kundendetails.

Standardwert:

```
SELECT TP_ID, TP_NAME, TP_INFO, KEY_ALIAS
FROM TP_MASTER
WHERE TP_ID = ?
```

Abrufen von Keystores und Importieren dieser Keystores auf den IdP-Server

Um die Zusicherung vertrauenswürdiger Parteien aufzubauen, sind einzelne Keystores für jede integrierende Anwendung und den IdP-Server erforderlich.

Rufen Sie Keystores für den IdP-Server und für alle SPs ab, die Sie in die Föderation einschließen möchten. Sie können die Keystores mit dem Java™-Keytool-Dienstprogramm generieren, oder Sie können sie von einer Zertifizierungsstelle abrufen.

Wenn Sie Keystores mit dem Keytool-Dienstprogramm generieren, ist im Folgenden ein typischer Workflow für diese Aufgabe mit Beispielbefehlen dargestellt. In diesen Beispielen lautet der Java™ 6-Keytool-Pfad `C:\Program Files (x86)\Java\jre7\bin\keytool`.

- Der IdP-Administrator generiert einen Keystore für den IdP-Server und exportiert das Zertifikat.

```
# Generate IdP JKS from keytool
c:\temp> "keytool_path\keytool" -genkey -keyalg RSA -alias idp
-keystore idp.jks -storepass idp001 -validity 360 -keysize 2048
# Export IdP certificate from JKS
c:\temp> "keytool_path\keytool" -export -alias idp -file idp.cer
-keystore idp.jks
```

- Ein SP-Administrator generiert einen Keystore und exportiert ihn.

```
# Generate Service Provider JKS from keytool
c:\temp> "keytool_path\keytool" -genkey -keyalg RSA -alias SP_1
-keystore SP_1.jks -storepass SP001 -validity 360 -keysize 2048
# Export Service Provider certificate from JKS
c:\temp> "keytool_path\keytool" -export -alias SP_1 -file SP_1.cer
-keystore SP_1.jks
```

  Der SP-Administrator sendet das Zertifikat anschließend an den IdP-Administrator.

- Der IdP-Administrator importiert das SP-Zertifikat auf den IdP-Server.

```
# Import Service Provider certificate into IdP JKS
c:\temp> "keytool_path\keytool" -import -alias SP_1
-trustcacerts -file SP_1.cer -keystore idp.jks
```

Einstellen von Konfigurationseigenschaften auf der Seite „Konfiguration“

Legen Sie Konfigurationseigenschaften auf der Seite **Einstellungen > Konfiguration** fest, um die föderierte Authentifizierung in Unica zu konfigurieren.

Legen Sie Konfigurationseigenschaften unter den folgenden Kategorien fest.

- **Unica Platform | Sicherheit | Föderierte Authentifizierung**
- **Unica Platform | Sicherheit | Föderierte Authentifizierung | Partitionen | Partition[n]**

In der Kontexthilfe der Eigenschaft oder unter den zugehörigen Themenlinks in diesem Abschnitt finden Sie Anweisungen zum Einrichten der Werte.

Onboarding-Service-Providers und -Benutzer

Der IdP-Serveradministrator muss rechtzeitig Einträge in der Tabelle `TP_MASTER` vornehmen, um SPs und Benutzer einzuschließen.

Nachfolgend ist ein SQL-Beispiel für das Einschließen eines SP dargestellt.

```
INSERT INTO TP_MASTER
 (TP_ID, TP_NAME, TP_INFO, KEY_ALIAS)
 VALUES
 ('SP_Id', 'SP display name', 'SP description', 'keystore alias name')
```

Nachdem die vertrauenswürdigen Parteien beim IdP-Server registriert wurden, kann der IdP-Serveradministrator Benutzer für das föderierte Single Sign-on zuordnen.

Die Benutzerzuordnungen müssen zwischen SPs streng im Verhältnis 1:1 erfolgen. Beispiel: Benutzer1 von SP_A darf NUR zu einem Benutzer in SP_B zugeordnet werden. Benutzer1 von SP_A kann jedoch einem anderen Benutzer in SP_C in derselben Föderation zugeordnet werden.

Im Folgenden ist eine Beispielabfrage für das Hinzufügen von Benutzern in der Tabelle `TP_MAPPING` dargestellt.

```
INSERT INTO TP_MAPPING
(TP_CLIENT_ID, TP_FOR_USER_ID, TP_SP_ID, TP_MAPPED_USER_ID, SAML_TOKEN)
VALUES
(’SP1_Id’, ’SP1_user_Id’, ’SP2_Id’, ’SP2_user_id’,'dummy1')
```

Anmerkung: Die Einträge für `TP_SP_ID` und `TP_FOR_USER_ID` müssen zwischen vier und maximal 24 Zeichen umfassen und dürfen nur alphanumerische Zeichen, Bindestriche und Unterstreichungszeichen enthalten: `[a-zA-Z0-9_-]`. Fügen Sie eindeutige Dummy-Einträge für die Spalte `SAML_TOKEN` ein, da diese Spalte keine Nullwerte und keine doppelten Werte zulässt.

Verwenden der IdP-Clientfassade zum Generieren von Tokens und Übergeben der Tokens an Service-Provider

Wenn ein Benutzer authentifiziert wurde und auf die Services eines anderen SP zugreifen möchte, rufen Sie den folgenden Code auf SP-Seite auf.

Der Code generiert das folgende Token.

```
// One time properties to initialize the IdP client.
Properties properties = new Properties();
properties.put(IdPClient.IDP_SERVER_URL, "URL");
properties.put(IdPClient.IDP_CLIENT_CERTIFICATE_ISSUER, "URL");
properties.put(IdPClient.IDP_CLIENT_KEYSTORE_PATH, "JKS file path");
properties.put(IdPClient.IDP_CLIENT_KEYSTORE_PASSKEY, "JKS passkey");
properties.put(IdPClient.IDP_CLIENT_KEYSTORE_ALIAS, "Certificate alias");
// Get the IdP client factory singleton instance
//with the specified parameters.
IdPClientFactory clientFactory = IdPClientFactory.getInstance(properties);
// Get the partition specific client facade to do the assertion.
IdPClientFacade clientFacade = clientFactory.getIdPClientFacade(partition);
// Establish SSO Login with the IdP server
IdPClientToken token = clientFacade.doIdPLogin(clientId, forUserId, spId);
```

Nachdem das Token abgerufen wurde, kann es an die Ziel-SPs übergeben werden, um basierend auf den dem Benutzer zugeordneten Rollen und Berechtigungen auf deren Ressourcen zuzugreifen.

```
// Security token is validated at Service Provider side.
IdPClientAssertion assertion = spFacade.assertIdPToken(clientId, forUserId,
 spId,
token.getTokenId());
// Retrieve the principal from the assertion, if there is no exception.
String principal = assertion.getMappedUser();
```

Die Clientfassade beachtet Multi-Tenant-Objekte und kann für die separate Konfiguration jeder Partition verwendet werden. Um dieses Feature zu verwenden, hängen Sie die Client-ID an jeden Eigenschaftsnamen an. Beispiel:

```
properties.put(IdPClient.IDP_CLIENT_KEYSTORE_PATH +
".partition1", "JKS file path");
properties.put(IdPClient.IDP_CLIENT_KEYSTORE_PASSKEY +
".partition1", "JKS passkey");
properties.put(IdPClient.IDP_CLIENT_KEYSTORE_ALIAS +
".partition1", "Certificate alias");
```

Referenz: RESTful-Services

Verwenden Sie diese Informationen, um Probleme bei der Verwendung der Clientfassade zu beheben oder um ihre eigene SAML 2.0-Implementierung mit dem IdP-Server zu entwickeln, die durch IBM bereitgestellt wird.

Die REST-APIs werden mit der Nutzlast von XML-Daten implementiert. Die SAML-Zusicherung wird direkt an die POST-Methoden mit digitalen Signaturen übergeben.

Nur die POST-Methode wird für alle Verben unterstützt, um einen einheitlichen Methodenzugriff sicherzustellen und Sicherheitszusicherungen zu erzwingen, die auf den XML-Nutzdaten basieren. Andere Methoden wie GET, PUT und DELETE geben eine Fehlermeldung zurück. Die folgende Tabelle stellt die Verben dar, die die unterstützten Anwendungsfälle implementieren.

Tabelle 34. Unterstützte Verben

Ressource	Veröffentlichen
`<idp>/saml/token/clientId/forUserId/spId/create`	Neues SAML-Token generieren.
`<idp>/saml/token/clientId/forUserId/spId/validate`	Vorhandenes SAML-Token validieren.
`<idp>/saml/token/clientId/forUserId/spId/delete`	Vorhandenes SAML-Token löschen.

Zugehörige Konzepte

Dieser Abschnitt enthält allgemeine Informationen zu den Technologien, die für die ExperienceOne-Implementierung von SAML 2.0 verwendet wurden, die auf föderiertem Single Sign-on basiert.

Security Assertion Markup Language 2.0 (SAML 2.0)

SAML 2.0 ist eine Version des SAML-Standards für den Austausch von Authentifizierungs- und Autorisierungsdaten zwischen Sicherheitsdomänen. SAML 2.0 ist ein XML-basiertes Protokoll, das Sicherheitstoken mit Zusicherungen verwendet, um Informationen zu einem Prinzipal (in der Regel ein Endbenutzer) zwischen einer SAML-Autorität, also einem Identitätsprovider, und einem SAML-Consumer, also einem SP, zu übergeben. SAML 2.0 ermöglicht webbasierte Authentifizierungs- und Autorisierungsszenarios einschließlich domänenübergreifendem Single Sign-on (SSO), um den Verwaltungsaufwand für die Verteilung von mehreren Authentifizierungstoken zum Benutzer zu reduzieren. Weitere Informationen finden Sie unter http://en.wikipedia.org/wiki/SAML_2.0.

Identitäts-Provider (IdP)

Der IdP, der auch als Identity Assertion Provider bezeichnet wird, gibt Identifizierungsinformationen für alle SPs aus, die interagieren oder Services innerhalb des Systems bereitstellen. Diese werden über ein Authentifizierungsmodul archiviert, das ein Sicherheitstoken als Alternative für die explizite Authentifizierung eines Benutzers

innerhalb einer Sicherheitsrealm verifiziert. In einer Perimeterauthentifizierung muss ein Benutzer nur einmal authentifiziert (Single Sign-on) und zusammen mit einem Sicherheitstoken übergeben werden, das durch einen Identity Assertion Provider für jedes System verarbeitet wird, auf das es zugreifen muss. Weitere Informationen finden Sie unter http://en.wikipedia.org/wiki/Identity_provider.

Public-Key-Verschlüsselung

Ein Verschlüsselungsalgorithmus, der auch als asymmetrische Verschlüsselung bezeichnet wird, der zwei separate Schlüssel erfordert, von denen einer geheim (oder privat) und der andere öffentlich ist. Die beiden Teile dieses Schlüsselpaares sind zwar unterschiedlich, mathematisch aber miteinander verbunden. Der Public Key wird verwendet, um einfachen Text zu verschlüsseln oder um eine digitale Signatur zu verifizieren. Mit dem Private Key wird demgegenüber verschlüsselter Text entschlüsselt oder eine digitale Signatur erzeugt. Weitere Informationen finden Sie unter http://en.wikipedia.org/wiki/Public-key_cryptography.

Einmalige Anmeldung (Single Sign-on) zwischen Unica und IBM Digital Analytics aktivieren

Wenn Ihre Organisation IBM Digital Analytics verwendet, können Sie eine einmalige Anmeldung (Single Sign-on; SSO) zwischen Digital Analytics und Unica aktivieren.

Die einmalige Anmeldung ermöglicht den Benutzern die Navigation zu Digital Analytics-Berichten aus der Unica-Benutzeroberfläche heraus, ohne dass sie aufgefordert werden, sich anzumelden.

Wenn auf Digital Analytics-Berichte in Unica-Dashboards verwiesen wird, ermöglicht die einmalige Anmeldung den Benutzern, diese Berichte anzuzeigen (falls sie in Digital Analytics Zugriff auf diese Berichte haben).

Zwei Optionen zum Aktivieren der einmaligen Anmeldung (Single Sign-on; SSO) zwischen Unica und IBM Digital Analytics

Sie können zum Aktivieren der einmaligen Anmeldung zwischen zwei Optionen wählen.

- Sie können Digital Analytics so konfigurieren, dass automatisch ein Digital Analytics-Benutzerkonto erstellt wird, wenn ein Unica-Benutzer zum ersten Mal zu Digital Analytics wechselt.

  Diese Option bietet sich an, wenn alle Unica-Benutzer eine einmalige Anmeldung für Digital Analytics verwenden sollen.
- Sie können Unica-Benutzerkonten für eine einmalige Anmeldung konfigurieren, indem Sie die bereits vorhandenen Digital Analytics-Anmeldenamen jedes Benutzers zur Detailseite des jeweiligen Benutzers in Unica hinzufügen.

  Wenn Sie diese Option auswählen, müssen alle Benutzer, für die der Zugriff auf Digital Analytics erforderlich ist, über ein Digital Analytics-Konto verfügen.

  Diese Option bietet sich an, wenn nur ein Subset der Unica-Benutzer über eine einmalige Anmeldung für Digital Analytics verfügen soll.

Berechtigungen in Digital Analytics für Benutzer mit einmaliger Anmeldung (Single-Sign-on-Benutzer)

Wenn die Option zum automatischen Erstellen von Konten in Digital Analytics **nicht** ausgewählt ist, verfügen Benutzer mit einmaliger Anmeldung in Digital Analytics über die Berechtigungen, die sie bei einer direkten Anmeldung an Digital Analytics hätten.

Wenn die Option zum automatischen Erstellen von Konten in Digital Analytics ausgewählt ist, verfügen Benutzer mit einmaliger Anmeldung in Digital Analytics über die folgenden Berechtigungen.

- Die Benutzer verfügen standardmäßig über die Berechtigungen, die der Digital Analytics-Gruppe erteilt wurden, die der Administrator für alle automatisch erstellten Benutzer konfiguriert hat.

  Die Administratoren können die Berechtigungen ändern, die dieser Gruppe zugeordnet sind.
- Außerdem kann der Administrator das automatische Erstellen von Konten für Benutzer, die bereits über ein Digital Analytics Konto verfügen, außer Kraft setzen.

Wenn die automatische Erstellung für einen Benutzer außer Kraft gesetzt wird, verfügt dieser Benutzer über die Berechtigungen, die er hätte, wenn er sich direkt an Digital Analytics anmelden würde.

Koordination der Serveruhr

Die Systemzeit auf dem Server, auf dem Unica Platform implementiert ist, muss mit der Systemzeit auf dem Digital Analytics-Server übereinstimmen. Bei einer einmaligen Anmeldung sind auf dem Digital Analytics-Server bis zu 15 Minuten Unterschied (900 Sekunden) zwischen den beiden Serversystemzeiten zulässig.

Sie sollten generell die Systemzeiten miteinander synchronisieren. Um eine ordnungsgemäße Synchronisation sicherzustellen, sollten Sie das NTP (Network Time Protocol) verwenden.

Wenn Sie Ihre Serversystemzeit nicht synchronisieren können und möglicherweise 15 Minuten (oder mehr) Unterschied zwischen den Systemzeiten entstehen können, können Sie die Konfigurationseinstellung **Zeitabweichungsanpassung (Sekunden)** in der Coremetrics®Kategorie "Coremetrics" in Unica Platform so festlegen, dass die angegebene Zahl den Unterschied zwischen den beiden Systemzeiten widerspiegelt.

Konfigurieren der einmaligen Anmeldung (Single Sign-on; SSO) zwischen Unica und Digital Analytics mit automatischer Benutzerkontenerstellung

Verwenden Sie diese Prozedur, um die einmalige Anmeldung (Single Sign-on; SSO) zwischen Unica und Digital Analytics mit automatischer Benutzerkontenerstellung zu konfigurieren.

1. Bestimmen Sie die Digital Analytics-Client-ID, die Sie für die einmalige Anmeldung zwischen Unica und Digital Analytics verwenden möchten.

   Notieren Sie sich die Client-ID, da Sie sie später benötigen.
2. Melden Sie sich an Digital Analytics als Benutzer mit Administratorberechtigung und mit Zugriff auf die Client-ID, die Sie im vorherigen Schritt ausgewählt haben, an, klicken Sie auf den Link „Administrator“ und navigieren Sie zur Seite „Globale Benutzerauthentifizierung“.

- Geben Sie im Feld **Geheimer Schlüssel für gemeinsame Nutzung für Enterprise Marketing Management** eine Zeichenfolge ein, die den Regeln entspricht, die neben dem Feld in den zugehörigen Anweisungen erläutert werden.

  Notieren Sie sich diese Zeichenfolge, da Sie sie später benötigen.
- Klicken Sie unter „Automatische Erstellung von Benutzerkonten“ auf **Aktiviert**.
- Wählen Sie eine Benutzergruppe aus, zu der alle automatisch erstellten Benutzer gehören sollen.

  Diese Gruppe sollte mindestens über die folgenden Web Analytics-Berechtigungen verfügen:

  - Dashboards > Standarddashboards anzeigen
  - Berichte > Sitemetriken
  - Berichte > Insights

3. Melden Sie sich bei Unica als Benutzer mit Administratorberechtigung an und navigieren Sie zur Seite **Einstellungen > Benutzer**.
4. Wählen Sie einen Benutzer aus oder erstellen Sie einen und konfigurieren Sie wie folgt eine Datenquelle für diesen Benutzer.
   - **Datenquelle** - Geben Sie einen Namen ein.
   - **Anmeldung für Datenquelle** - Geben Sie die Client-ID ein, die Sie in Schritt 1 notiert haben.
   - **Datenquellenkennwort** - Geben Sie den geheimen Schlüssel für gemeinsame Nutzung ein, den Sie in Schritt 2 notiert haben.

   Wenn Sie mehrere Partitionen verwenden, müssen Sie diese Aufgabe auf jeder Partition, auf der Benutzer die einmalige Anmeldung verwenden sollen, durchführen.

   Alternativ dazu können Sie das Benutzerkonto „platform_admin“ für diesen Schritt verwenden. Da dieser Benutzer Mitglied aller Partitionen ist, ist die Datenquelle auf allen Partitionen verfügbar.
5. Navigieren Sie in Unica Platform zur Seite **Einstellungen > Benutzergruppen** und gehen Sie wie folgt vor.

- Erstellen Sie eine neue Gruppe und fügen Sie die Rolle „CMUser“ zu dieser Gruppe hinzu.
- Fügen Sie alle Benutzer, die über eine einmalige Anmeldung verfügen sollen, als Mitglied zu dieser Gruppe hinzu.

Wenn Sie mehrere Partitionen verwenden, müssen Sie diese Aufgabe auf jeder Partition, auf der Benutzer die einmalige Anmeldung verwenden sollen, durchführen.

6. Navigieren Sie in Unica Platform zur Seite **Einstellungen > Konfiguration** und legen Sie die Konfigurationseigenschaften wie folgt fest.

Tabelle 35. Konfigurationseigenschaften zur Aktivierung der einmaligen Anmeldung mit Digital Analytics

Eigenschaft	Wert
Digital Analytics | Enable IBM Digital Analytics	True
Digital Analytics | Integration | Partitionen | Partition[n] | Platform user for IBM Digital Analytics account	Geben Sie den Anmeldenamen für das Unica Platform-Benutzerkonto ein, das Sie in Schritt 4 verwendet haben.
Digital Analytics | Integration | Partitionen | Partition[n] | Datasource for IBM Digital Analytics account	Geben Sie den Namen der Datenquelle ein, die Sie in Schritt 4 erstellt haben.

Wenn Sie mehrere Partitionen besitzen, müssen Sie **Digital Analytics \| Integration \| Partitionen \| partitionTemplate** verwenden, um für jede Partition mit Benutzern, die über eine einmalige Anmeldung verfügen sollen, eine Gruppe von Konfigurationseigenschaften zu erstellen.

Der Name der mit der Vorlage erstellten Kategorie muss genau dem Namen der betreffenden Unica Campaign-Partition entsprechen.

7. Gehen Sie für jeden Benutzer, für den Sie das automatische Erstellen eines Kontos außer Kraft setzen möchten, wie im Folgenden beschrieben vor.

- Navigieren Sie in Unica Platform zur Seite **Einstellungen > Benutzer**.
- Geben Sie den -Digital AnalyticsAnmeldenamen des Benutzers im Feld **Digital Analytics-Benutzername** auf der Detailseite für den Benutzer ein.

Dies ist nur bei Benutzern möglich, die bereits über ein Digital Analytics-Konto verfügen.

Anmerkung: Wenn kein Konto mit diesem Anmeldenamen in Digital Analytics vorhanden ist, wird ein Konto für diesen Benutzer mit dem Namen erstellt, den Sie hier eingeben, und nicht mit dem Unica Platform-Anmeldenamen des Benutzers.

8. Konfigurieren Sie den Webanwendungsserver für die einmalige Anmeldung (Single Sign-on) mit Digital Analytics.

Konfigurieren der einmaligen Anmeldung zwischen Unica und Digital Analytics mit manueller Benutzerkontenerstellung

Verwenden Sie diese Prozedur, um die einmalige Anmeldung (Single Sign-on) zwischen Unica und Digital Analytics mit manueller Benutzerkontenerstellung zu konfigurieren.

1. Bestimmen Sie die Digital Analytics-Client-ID, die Sie für die einmalige Anmeldung zwischen Unica und Digital Analytics verwenden möchten.

   Notieren Sie sich die Client-ID, da Sie sie später benötigen.
2. Melden Sie sich an Digital Analytics als Benutzer mit Administratorberechtigung und mit Zugriff auf die Client-ID, die Sie im vorherigen Schritt ausgewählt haben, an, klicken Sie auf den Link „Administrator“ und navigieren Sie zur Seite „Globale Benutzerauthentifizierung“.
   - Geben Sie im Feld **Geheimer Schlüssel für gemeinsame Nutzung für Enterprise Marketing Management** eine Zeichenfolge ein, die den Regeln entspricht, die neben dem Feld in den zugehörigen Anweisungen erläutert werden.

     Notieren Sie sich diese Zeichenfolge, da Sie sie später benötigen.
   - Klicken Sie unter „Automatische Erstellung von Benutzerkonten“ auf **Deaktiviert**.

3. Melden Sie sich bei Unica als Benutzer mit Administratorberechtigung an und navigieren Sie zur Seite **Einstellungen > Benutzer**.
4. Wählen Sie einen Benutzer aus oder erstellen Sie einen und konfigurieren Sie wie folgt eine Datenquelle für diesen Benutzer.
    - **Datenquelle** - Geben Sie einen Namen ein.
    - **Anmeldung für Datenquelle** - Geben Sie die Client-ID ein, die Sie in Schritt 1 notiert haben.
    - **Datenquellenkennwort** - Geben Sie den geheimen Schlüssel für gemeinsame Nutzung ein, den Sie in Schritt 2 notiert haben.

    Wenn Sie mehrere Partitionen verwenden, müssen Sie diese Aufgabe auf jeder Partition, auf der Benutzer die einmalige Anmeldung verwenden sollen, durchführen.

    Alternativ dazu können Sie das Benutzerkonto „platform_admin“ für diesen Schritt verwenden. Da dieser Benutzer Mitglied aller Partitionen ist, ist die Datenquelle auf allen Partitionen verfügbar.
5. Navigieren Sie in Unica Platform zur Seite **Einstellungen > Benutzergruppen** und gehen Sie wie folgt vor.
    - Erstellen Sie eine neue Gruppe und fügen Sie die Rolle „DMUser“ zu dieser Gruppe hinzu.
    - Fügen Sie alle Benutzer, die über eine einmalige Anmeldung verfügen sollen, als Mitglied zu dieser Gruppe hinzu.

    Wenn Sie mehrere Partitionen verwenden, müssen Sie diese Aufgabe auf jeder Partition, auf der Benutzer die einmalige Anmeldung verwenden sollen, durchführen.
6. Navigieren Sie in Unica Platform zur Seite **Einstellungen > Konfiguration** und legen Sie die Konfigurationseigenschaften wie folgt fest.

Tabelle 36. Konfigurationseigenschaften zur Aktivierung der einmaligen Anmeldung mit Digital Analytics

Eigenschaft	Wert
Digital Analytics | Enable IBM Digital Analytics	True

Eigenschaft	Wert
Digital Analytics | Integration | Partitionen | Partition[n] | Platform user for IBM Digital Analytics account	Geben Sie den Anmeldenamen für das Unica Platform-Benutzerkonto ein, das Sie in Schritt 4 verwendet haben.
Digital Analytics | Integration | Partitionen | Partition[n] | Datasource for IBM Digital Analytics account	Geben Sie den Namen der Datenquelle ein, die Sie in Schritt 4 erstellt haben.

Wenn Sie mehrere Partitionen besitzen, müssen Sie **Digital Analytics | Integration | Partitionen | partitionTemplate** verwenden, um für jede Partition mit Benutzern, die über eine einmalige Anmeldung verfügen sollen, eine Gruppe von Konfigurationseigenschaften zu erstellen.

Der Name der mit der Vorlage erstellten Kategorie muss genau dem Namen der betreffenden Unica Campaign-Partition entsprechen.

7. Navigieren Sie in Unica Platform zur Seite **Einstellungen > Benutzer**.
8. Geben Sie für jeden Benutzer, für den Sie die einmalige Anmeldung aktivieren möchten, den Digital Analytics-Anmeldenamen dieses Benutzers im Feld **IBM Digital Analytics-Benutzername** auf der Seite „Eigenschaften bearbeiten“ für den Benutzer ein.

   Anmerkung: Wenn ein Benutzer über genau dieselben Anmeldenamen in Unica und in Digital Analytics verfügt, müssen Sie diesen Schritt nicht ausführen.

9. Konfigurieren Sie den Webanwendungsserver für die einmalige Anmeldung mit Digital Analytics.

Konfigurieren von WebLogic für einmalige Anmeldung zwischen Digital Analytics und Unica

Führen Sie diese Prozedur in der WebLogic-Domäne aus, auf der Unica Platform implementiert ist, um sicherzustellen, dass Benutzer Digital Analytics-Berichte in Dashboards anzeigen können, ohne sich anmelden zu müssen.

1. Öffnen Sie das Script `setDomainEnv`, das sich im Verzeichnis `bin` des Verzeichnisses der WebLogic-Domäne befindet.
2. Fügen Sie `-Dweblogic.security.SSL.ignoreHostnameVerification=true` zu `JAVA_OPTIONS` hinzu.

Konfigurieren von WebSphere® für einmalige Anmeldung zwischen Digital Analytics und Unica

Führen Sie diese Prozedur in der WebSphere®-Zelle und dem Knoten aus, auf der/dem Unica Platform implementiert ist, um sicherzustellen, dass Benutzer Digital Analytics-Berichte in Dashboards anzeigen können, ohne sich anmelden zu müssen.

1. Melden Sie sich an der WebSphere®-Administrationskonsole an.
2. Erweitern Sie **Sicherheit** und klicken Sie auf **Verwaltung von SSL-Zertifikaten und Schlüsseln**.
3. Klicken Sie unter **Konfigurationseinstellungen** auf **Sicherheitskonfigurationen für Endpunkt verwalten**.
4. Navigieren Sie zur Ausgangskonfiguration für die Zelle und den Knoten, auf der/dem Unica Platform implementiert ist.
5. Klicken Sie unter **Zugehörige Elemente** auf **Keystores und Zertifikate** und klicken Sie auf den Keystore **NodeDefaultTrustStore**.
6. Klicken Sie unter **Weitere Eigenschaften** auf **Unterzeichnerzertifikate** und **Vom Port abrufen**.

   Füllen Sie die Felder wie folgt aus.

   - **Hostname**: `welcome.coremetrics.com`
   - **Port**: `443`
   - **Alias**: `coremetrics_cert`

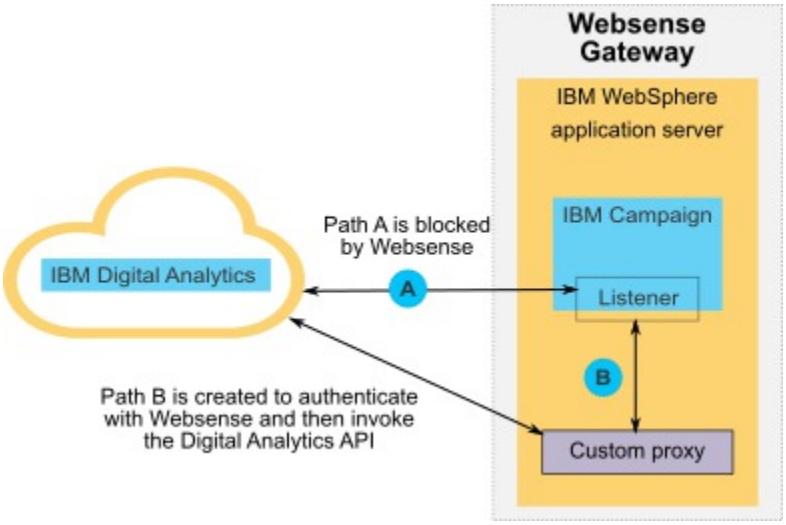
Digital Analytics-Integration mit Websense mithilfe eines angepassten Proxys

Unica Platform bietet einen benutzerdefinierten Proxy, um die Integration von Unica Campaign, das on-Premise gehostet wird, und Digital Analytics in der Cloud zu ermöglichen, wenn Websense eine erforderliche Komponente der Umgebung ist.

Der angepasste Proxy wird nur für WebSphere Application Server unterstützt.

Nach dem Installieren des benutzerdefinierten Proxy können Sie Single Sign-on und die Integration von Digital Analytics und Unica Campaign konfigurieren.

Der benutzerdefinierte Proxy ist eine Java-Servlet-Implementierung, die als Forward Proxy fungiert. Dieser wird zwischen dem Unica Campaign Listener und Digital Analytics eingefügt. Der angepasste Proxy fungiert als Endpunkt für den Unica Campaign Listener und wird zum Aufrufen von Digital Analytics APIs verwendet. Intern authentifiziert sich der angepasste Proxy selbst beim Websense-Inhaltsgateway und ruft dann über eine sichere Verbindung die APIs außerhalb des Netzes auf.



Bereitstellen des angepassten Proxys unter WebSphere

Führen Sie diese Prozedur aus, um den angepassten Proxy zu installieren. Dieser benutzerdefinierte Proxy wird nur zusammen mit dem WebSphere-Anwendungsserver unterstützt.

Beachten Sie, dass Sie die ProxyServer-Anwendung in demselben WebSphere-Profil bereitstellen können, in dem Sie auch Unica Campaign bereitgestellt haben, oder aber ein anderes WebSphere-Profil verwenden können.

1. Kopieren Sie die Datei `ProxyServer.war` an eine Position, auf die über den WebSphere-Server zugegriffen werden kann.

   Die Datei `ProxyServer.war` befindet sich im Verzeichnis `tools\lib` im Unica Platform-Installationsverzeichnis.
2. Stellen Sie die Datei `ProxyServer.war` wie folgt bereit.
   - Wählen Sie den Pfad **Detailliert - Alle Installationsoptionen und Parameter** anzeigen für die Installation aus.
   - Sie können einen beliebigen Anwendungsnamen angeben.
   - Sie müssen **JavaServer Pages-Dateien vorkompilieren** nicht auswählen.
   - Füllen Sie die Felder der Seite zum Initialisieren von Parametern für Servlets wie folgt aus.
     - **proxy_host** - Host-URL oder IP-Adresse des Websense-Servers
     - **proxy_port** - Portnummer des Websense-Servers
     - **proxy_username** - Benutzername für Websense-Authentifizierung
     - **Proxy_password** - Kennwort für Websense-Authentifizierung
     - **target_url** - Endpunkt-URL für Digital Analytics, die in Unica Campaign bereits konfiguriert ist
   - Legen Sie auf der Seite „Kontextstammverzeichnisse für Webmodule zuordnen“ für das Kontextstammverzeichnis den Wert `proxy` fest.
   - Greifen Sie nach Abschluss der Bereitstellung auf die ProxyServer-Anwendung in einem Browser unter `http://WebSphere_host:Port/proxy` zu.

     Sie sollten eine Nachricht erhalten: IBM OCM Secure Proxy Server V.x

Importieren des Digital Analytics-Zertifikats für WebSphere ohne abgehenden Zugriff

Wenden Sie diese Vorgehensweise an, wenn WebSphere nicht über abgehenden Zugriff auf den Digital Analytics-Server verfügt.

1. Rufen Sie das digitale Zertifikat von der Digital Analytics-Site ab.

   Rufen Sie zum Abrufen des Zertifikats die Digital Analytics-URL auf und klicken Sie dann auf das Sperrsymbol im Adressfeld Ihres Browsers. Ihr Browser öffnet ein Fenster, in dem Sie das Zertifikat herunterladen können.

2. Importieren Sie das Zertifikat in die WebSphere-JVM. Verwenden Sie hierzu das Java-Programm „keytool“.

   Beispiel (es wurden Zeilenumbrüche hinzugefügt):

   ```
   /keytool -import -file DA_Certificate.cer
   -alias da_alias
   -keystore WebSphere_JRE_home/lib/security/cacerts
   ```

   Geben Sie das Kennwort an. Das Standardkennwort von „keytool“ lautet „changeit“.
3. Fügen Sie in der WebSphere-Administrationskonsole die folgenden benutzerdefinierten Eigenschaften hinzu.
   - javax.net.ssl.trustStore: *WebSphere_JRE_home*/lib/security/cacerts
   - javax.net.ssl.trustStorePassword: *your_password*
   - javax.net.ssl.trustStoreType: jks

Importieren des Digital Analytics-Zertifikats für WebSphere mit abgehendem Zugriff

Wenden Sie diese Vorgehensweise an, wenn WebSphere über abgehenden Zugriff auf den Digital Analytics-Server verfügt.

1. Erweitern Sie in der WebSphere-Administrationskonsole die Ansicht von **Sicherheit** und klicken Sie dann auf Verwaltung von **SSL-Zertifikaten und Schlüsseln**.
2. Klicken Sie unter **Konfigurationseinstellungen** auf **Sicherheitskonfigurationen für Endpunkt verwalten**.
3. Wählen Sie die entsprechende abgehende Konfiguration aus, um zum Verwaltungsbereich **(cell):..Node0xCell:(node):..Node0x** zu navigieren.
4. Klicken Sie unter **Zugehörige Elemente** auf **Keystores und Zertifikate** und klicken Sie dann auf den Keystore **NodeDefaultTrustStore** (oder den Keystore, den Sie in WebSphere Application Server verwendet haben).
5. Klicken Sie unter **Weitere Eigenschaften** auf **Unterzeichnerzertifikate** und **Vom Port abrufen**.

a. Geben Sie im Feld **Host** den Namen des Digital Analytics-Servers ein.

   Beispiel: `export.coremetrics.com`.

b. Geben Sie im Feld **Port** den Wert `443` ein.

c. Geben Sie im Feld **Alias** einen Aliasnamen ein.

6. Klicken Sie auf **Unterzeichnerdaten abrufen** und überprüfen Sie, ob die Zertifikatsinformationen sich auf ein Zertifikat beziehen, dem Sie vertrauen können
7. Wenden Sie die Konfiguration an und speichern Sie sie.

Nächste Schritte

Nach der Installation des angepassten Proxy-Servers und dem Import des Digital Analytics Zertifikats müssen Sie in den nächsten Schritten die einmalige Anmeldung (SSO = Single Sign-on) aktivieren und die Integration zwischen Digital Analytics und Unica Campaign konfigurieren.

Gehen Sie wie folgt vor, um die Einrichtung Ihrer Umgebung abzuschließen.

- Richten Sie Single Sign-on ein und befolgen Sie dazu die Anleitungen im *Unica PlatformAdministratorhandbuch im Kapitel zur Verwendung von Single Sign-on zwischen Unica und Digital Analytics.*
- Richten Sie die Integration ein und befolgen Sie dazu die Anleitungen im *Unica CampaignAdministratorhandbuch* im Kapitel zur Unica Campaign-Integration mit anderen -Produkten.

Wichtig: Die Integrationsprozedur umfasst das Einrichten der Konfigurationseigenschaft `ServiceURL` unter **Campaign | Partitionen | Partition[n] | Coremetrics**. Wenn Sie den angepassten Proxy verwenden, dann müssen Sie diese Eigenschaft auf den Wert `http://WebSphere_host:Port/proxy` setzen und dann für die Unica Platform-Webanwendung einen Neustart durchführen.

Integration zwischen Unica und Windows™indows Active Directory

Unica Platform kann für die Integration mit Windows™ Active Directory-Server oder einem anderen LDAP-Server (LDAP = Lightweight Directory Access Protocol) konfiguriert werden. Durch Integration von Unica in einen Verzeichnisserver können Sie Benutzer und Gruppen an einem zentralen Ort verwalten. Die Integration ermöglicht ein flexibles Modell für die Erweiterung der Autorisierungsrichtlinien des Unternehmens in Unica Anwendungen. Durch die Integration werden Unterstützungskosten reduziert, und es wird weniger Zeit für die Implementierung einer Produktionsanwendung benötigt.

Eine Liste der unterstützten Verzeichnisserver finden Sie im Dokument Empfohlene Softwareumgebungen und Mindestsystemvoraussetzungen.

Funktionen bei der Integration in Active Directory

Durch die Integration von Unica Platform mit Windows™ Active Directory werden die in diesem Abschnitt beschriebenen Funktionen bereitgestellt.

Authentifizierung bei der Integration in Active Directory

Unica-Anwendungen senden eine Abfrage an Unica Platform, um Informationen zur Benutzerautorisierung abzurufen.

- Frühere Versionen von Unica Platform enthielten Unterstützung für die integrierte Microsoft Windows-Anmeldung auf NTLMv1-Basis. Mit Einführung von Microsoft Windows 2008 Server und Microsoft Windows 7 wurde der standardmäßige Mindeststandard geändert und es ist nun die Verwendung des NTLMv2-Protokolls erforderlich. NTLMv2 wird nativ nicht von Unica Platform unterstützt.

  Allerdings können Sie die NTLMv2-Authentifizierung so konfigurieren, dass Benutzer für alle Unica-Anwendungen authentifiziert werden, wenn Sie sich im Unternehmensnetz anmelden, und dass hierfür kein Kennwort erforderlich ist, um sich bei den Unica-Anwendungen anzumelden. Die Benutzerauthentifizierung erfolgt auf Grundlage der Windows™-Anmeldung. Die Anmeldeanzeigen der Anwendung werden umgangen.

Zur Konfiguration der NTLMv2-Authentifizierung müssen Sie die Schritte ausführen, die in diesem Abschnitt beschrieben sind:

- Wenn die NTLMv2-Authentifizierung nicht aktiviert wurde, dann müssen sich Benutzer weiterhin über die Unica-Anmeldeanzeige anmelden und dazu ihre Windows™-Berechtigungsnachweise verwenden.

Verwalten interner und externer Benutzer

Wenn die NTLMv2-Authentifizierung aktiviert ist, werden alle Benutzer auf dem Active Directory-Server erstellt und verwaltet. (Sie haben nicht die Möglichkeit, Benutzer in Unica Platform zu erstellen. Diese Benutzer werden in diesem Handbuch als „interne Benutzer“ bezeichnet.) Wenn Sie interne Benutzer erstellen müssen, darf die NTLMv2-Authentifizierung nicht aktiviert werden.

Wenn die Integration konfiguriert wurde, können Sie die importierten Benutzerkonten in Unica Platform nicht hinzufügen, ändern oder löschen. Sie müssen diese Managementaufgaben auf der LDAP-Seite ausführen. Ihre Änderungen werden bei der Synchronisation importiert. Wenn Sie importierte Benutzerkonten in Unica Platform ändern, können Benutzer auf Probleme bei der Authentifizierung stoßen.

Benutzerkonten, die Sie auf der LDAP-Seite löschen, werden auf Unica Platform nicht gelöscht. Sie müssen diese Konten in Unica Platform manuell deaktivieren. Es ist sicherer, diese gelöschten Benutzerkonten zu inaktivieren, anstatt sie zu löschen, da Benutzer Eigentumszugriffsrechte auf Ordner in Unica Campaign haben. Wenn Sie ein Benutzerkonto löschen, das Eigentümer eines Ordners ist, sind die Objekte in dem betreffenden Ordner nicht mehr verfügbar.

Synchronisieren

Wenn Unica für die Integration in einen Active Directory-Server konfiguriert wurde, werden Benutzer und Gruppen automatisch in zuvor festgelegten Intervallen synchronisiert.

Die automatische Synchronisation verfügt nur über eine eingeschränkte Funktionalität.

- Benutzer, die vom LDAP-Server gelöscht wurden, werden während der automatischen Synchronisation nicht gelöscht.

Sie können eine vollständige Synchronisation aller Benutzer und Gruppen mit der Synchronisationsfunktion im Benutzerbereich von Unica erzwingen. Alternativ hierzu können Sie sich auch an die Services wenden, um das Definieren einer verdeckten Konfigurationseigenschaft anzufordern, durch die bei der automatischen Synchronisation eine vollständige Synchronisation durchgeführt wird.

Importieren von Benutzern auf der Basis von Gruppen oder Attributen

Sie können einen von zwei Filtertypen wählen, um die Benutzerkonten auszuwählen, die vom LDAP-Server in Unica Platform importiert werden.

Sie müssen zwischen gruppenbasiertem und attributbasiertem Import wählen. Mehrere Methoden gleichzeitig werden nicht unterstützt.

Gruppenbasierter Import

Unica Platform importiert Gruppen und die zugehörigen Benutzer aus der Datenbank des Verzeichnisservers über eine regelmäßige Synchronisationsaufgabe, die automatisch Informationen vom Verzeichnisserver abruft. Wenn Unica Platform Benutzer und Gruppen aus der Serverdatenbank importiert, werden die Gruppenzugehörigkeiten nicht geändert. Um diese Änderungen zu erfassen, müssen Sie eine manuelle Synchronisation durchführen.

Sie können Unica-Berechtigungen zuordnen, indem Sie eine Active Directory-Gruppe einer Unica-Gruppe zuordnen. Aufgrund dieser Zuweisung können neue Benutzer, die der Active Directory-Gruppe zugeordnet wurden, die Berechtigungen übernehmen, die für die entsprechende Unica-Gruppe festgelegt wurden.

Eine Untergruppe in Unica Platform übernimmt die Active Directory-Zuordnungen oder Benutzerzugehörigkeiten ihrer übergeordneten Gruppen nicht.

Weitere Informationen zum Konfigurieren des gruppenbasierten Imports finden Sie weiter unten in diesem Kapitel.

Attributbasierter Import

Wenn Sie keine Gruppen in Ihrem Active Directory-Server erstellen möchten, die sich auf bestimmte Unica-Produkte beziehen, haben Sie die Möglichkeit, die importierten Benutzer durch die Angabe von Attributen zu steuern. Dazu müssen Sie folgende Schritte während des Konfigurationsprozesses ausführen.

1. Bestimmen Sie die Zeichenfolge, die in Ihrem Active Directory-Server für das Attribut verwendet wird, nach dem Sie filtern möchten.
2. Setzen Sie die Eigenschaft **Unica Platform | Sicherheit | LDAP-Synchronisation | LDAP-Attributname für Benutzerreferenz** auf `DN`.

   Damit wird Unica Platform mitgeteilt, dass die Synchronisation nicht auf einer Gruppe mit Mitgliedsreferenzen basiert, sondern auf einer Organisationseinheit oder Organisation.
3. Wenn Sie die Eigenschaft **Übersicht LDAP-Referenzen** konfigurieren, setzen Sie den Abschnitt "Filter" des Werts auf das Attribut, nach dem Sie suchen möchten. Verwenden Sie für den Filter die Zeichenfolge, die Sie in Schritt 1 festgelegt haben.

Wenn Sie die attributbasierte Synchronisation verwenden, ist die periodische Synchronisation immer eine vollständige Synchronisation und keine partielle Synchronisation, die für die gruppenbasierte Synchronisation ausgeführt wird. Für die attributbasierte Synchronisation sollten Sie die Eigenschaft **LDAP-Synchronisationsintervall** auf einen hohen Wert setzen oder auf `0`, um die automatische Synchronisation zu inaktivieren und sich auf die vollständige Synchronisation zu verlassen, wenn Benutzer zum Verzeichnis hinzugefügt werden.

Folgen Sie zum Konfigurieren der Integration den Anweisungen weiter unten in diesem Kapitel. Ziehen Sie dabei für die Schritte zum Festlegen der Konfigurationseigenschaften die voranstehenden Anweisungen heran.

Informationen zu Active Directory und Partitionen

In Umgebungen mit mehreren Partitionen wird die Partitionszugehörigkeit eines Benutzers von der Gruppe bestimmt, zu der der Benutzer gehört, wenn die Gruppe einer Partition zugeordnet wird. Ein Benutzer kann nur zu einer Partition gehören. Wenn daher ein Benutzer Mitglied mehrerer Active Directory-Gruppen ist und diese Gruppen Unica-Gruppen zugeordnet sind, die ihrerseits verschiedenen Partitionen zugewiesen sind, muss das System eine einzelne Partition für diesen Benutzer wählen.

Diese Situation sollte nach Möglichkeit vermieden werden. Tritt sie aber dennoch ein, gilt die Partition der Unica-Gruppe, die zuletzt einer Active Directory-Gruppe zugeordnet war, als diejenige, der der Benutzer angehört. Informationen dazu, welche LDAP-Gruppe

zuletzt zugeordnet war, finden Sie in den Active Directory-Gruppenzuordnungen, die im Konfigurationsbereich angezeigt werden. Diese werden in chronologischer Reihenfolge mit den letzten Zuweisungen an letzter Stelle angezeigt.

Sonderzeichen in Anmeldenamen

Nur die folgenden Sonderzeichen sind in Anmeldenamen zulässig: Punkt (.), Unterstreichungszeichen (_) und Bindestrich (-). Wenn andere Sonderzeichen (einschließlich Leerzeichen) im Anmeldenamen eines Benutzers enthalten sind, den Sie von Ihrem Active Directory-Server in die Unica Platform importieren wollen, müssen Sie den Anmeldenamen so ändern, dass der Benutzer bei der Anmeldung oder bei der Ausführung administrativer Aufgaben keine Probleme bekommt (sofern der Benutzer Administratorberechtigung besitzt).

Voraussetzungen für die Integration in Active Directory

Um die Integrationsfunktionen von Windows™ Active Directory nutzen zu können, müssen Unica-Anwendungen in einem unterstützten Betriebssystem installiert werden.

Zusätzlich zur Implementierung der NTLMv2-Authentifizierung müssen Benutzer, die auf Unica-Anwendungen zugreifen, folgende Bedingungen erfüllen:

- Es wird ein System verwendet, auf dem ein unterstütztes Windows™-Betriebssystem ausgeführt wird.
- Die Anmeldung muss als ein Mitglied der Windows™ Active Directory-Domäne erfolgen, über die Unica die Authentifizierung durchführt.
- Es wird ein unterstützter Browser verwendet.

Roadmap für den Konfigurationsprozess: Integration in Active Directory

Verwenden Sie diese Roadmap für den Konfigurationsprozess, um die Aufgaben zu suchen, die zur Integration von Unica mit Windows™ Active Directory erforderlich sind. Die Spalte „Abschnitt“ stellt Links zu den Themen bereit, in denen die Aufgaben ausführlich beschrieben werden.

Tabelle 37. Roadmap für den Konfigurationsprozess: Integration in Active Directory

Topic	Informationen
Erhalt erforderlicher Informationen *(auf Seite 177)*	Einholen von Informationen über Ihren Windows™ Active Directory-Server, der für die Integration mit Unica benötigt wird.
Gruppenzugehörigkeit, Zuordnung und Anwendungszugriff *(auf Seite 180)*	Bei einer gruppenbasierten Synchronisation das Identifizieren oder Erstellen der Gruppen in Unica Platform, denen Sie Ihre Active Directory-Gruppen zuordnen werden.
Speichern von Berechtigungsnachweisen für Verzeichnisserver in Unica Platform *(auf Seite 180)*	Wenn Ihr Verzeichnisserver anonyme Zugriffe nicht erlaubt (die gängigste Art der Konfiguration), konfigurieren Sie ein Unica-Benutzerkonto und legen Sie dafür einen Benutzernamen mit Administratorberechtigung für den Verzeichnisserver und ein entsprechendes Kennwort fest.
• Festlegen der Verbindungseigenschaften für LDAP-Anmeldung in Unica *(auf Seite 182)* • Festlegen der LDAP-Synchronisationseigenschaften *(auf Seite 183)* • Festlegen von Eigenschaften zur Zuordnung von Benutzerattributen *(auf Seite 184)* • Zuordnung von LDAP-Gruppen zu Unica-Gruppen *(auf Seite 185)*	Konfigurieren von Unica Platform für die Integration, indem Sie die Werte auf der Seite „Konfiguration“ festlegen.
Testen der Synchronisation *(auf Seite 186)*	Überprüfen, dass Benutzer wie erwartet importiert werden, und bei einer gruppenbasierten Synchronisation sicherstellen, dass

Tabelle 37. Roadmap für den Konfigurationsprozess: Integration in Active Directory (Fortsetzung)

Topic	Informationen
	Benutzer und Gruppen ordnungsgemäß synchronisieren.
Einrichten eines Active Directory-Benutzers mit PlatformAdminRole-Berechtigungen *(auf Seite 187)*	Einrichten des Administratorzugriffs auf Unica Platform. Erforderlich, wenn die NTLMv2-Authentifizierung aktiviert ist.
Festlegen des Sicherheitsmodus zum Aktivieren der NTLMv2-Authentifizierung *(auf Seite 187)*	Festlegen der Sicherheitsmodus-Werte auf der Seite „Konfiguration“.
Konfiguration für Internet Explorer *(auf Seite)*	Festlegen einer benutzerdefinierten Sicherheitsebene in jeder Instanz des Internet Explorers, die für den Zugriff auf Unica verwendet wird. Dies ist für die NTLMv2-Authentifizierung erforderlich, um zu verhindern, dass für Benutzer die Unica-Anmeldeanzeige angezeigt wird.
Erneutes Starten des Webanwendungsservers *(auf Seite 188)*	Dieser Schritt ist erforderlich, um zu gewährleisten, dass sämtliche Ihrer Änderungen angewandt werden.
Testen der Anmeldung als Active Directory-Benutzer *(auf Seite 188)*	Prüfen Sie, dass Sie sich in Unica als Active Directory-Benutzer anmelden können.

Erhalt erforderlicher Informationen

Rufen Sie die erforderlichen Informationen über den Verzeichnisserver ab, den Sie für die Integration verwenden möchten. Sie verwenden diese Informationen beim Konfigurationsprozess, um Berechtigungsnachweise für Verzeichnisserver zu speichern und Werte von Konfigurationseigenschaften festzulegen.

Beziehen Sie die folgenden Informationen.

- Besorgen Sie sich den Namen und den Port des Server-Hosts.
- Bestimmen Sie einen Benutzer, der über Suchberechtigungen für den Verzeichnisserver verfügt, und tragen Sie die folgenden Informationen über den Benutzer zusammen.
    - Anmeldename.
    - Passwort
    - Definierter Name (DN)
- Besorgen Sie sich die folgenden Informationen für den Verzeichnisserver.
    - Vollständig qualifizierter Hostname oder IP-Adresse
    - Der Port, auf dem der Server empfangsbereit ist.
- Bestimmen Sie die Zeichenfolge, die Ihr Verzeichnisserver für das Benutzerattribut im Gruppenobjekt benutzt. Üblicherweise wird der Wert `uniquemember` in LDAP-Servern und `member` in Windows™ Active Directory-Servern verwendet. Sie sollten dies auf Ihrem Verzeichnisserver überprüfen.
- Fordern Sie die folgenden erforderlichen Benutzerattribute an.
    - Bestimmen Sie die Zeichenfolge, die Ihr Verzeichnisserver für das Benutzeranmeldungsattribut benutzt. Diese Zeichenfolge ist immer erforderlich. Üblicherweise ist der Wert `uid` in LDAP-Servern und `sAMAccountName` in Windows™ Active Directory-Servern. Überprüfen Sie diese Zeichenfolge auf Ihrem Verzeichnisserver.
    - Nur wenn Unica Campaign in einer UNIX™-Umgebung installiert ist, ermitteln Sie die Zeichenfolge, die von Ihrem Verzeichnisserver für das alternative Anmeldeattribut verwendet wird.
- Wenn Sie die attributbasierte Synchronisation verwenden, rufen Sie die Zeichenfolgen für die Attribute (mindestens eins) ab, die Sie für diesen Zweck verwenden möchten.
- Falls Sie mit Unica Platform zusätzliche (optionale), auf Ihrem Verzeichnisserver gespeicherte Benutzerattribute importieren möchten, bestimmen Sie die Zeichenfolgen, die Ihr Verzeichnisserver für Folgendes verwendet.
    - Vorname
    - Nachname
    - Position des Benutzers

- Department
- Unternehmen
- Land
- E-Mail-Adresse des Benutzers
- Adresse 1
- Telefon (geschäftlich)
- Mobiltelefon
- Telefon (privat)

Informationen über definierte Namen

Damit die Verzeichnisserver-Integration in Unica aktiviert werden kann, muss der definierte Name (DN) für einen Benutzer und für Gruppen bestimmt werden. Der definierte Name eines Objekts auf dem Verzeichnisserver ist der vollständige Pfad durch Baumstruktur des Verzeichnisservers zu diesem Objekt.

DNs bestehen aus den folgenden Komponenten:

- Organisationseinheit (OE). Dieses Attribut wird verwendet, um einen Namespace auf der Grundlage der Organisationsstruktur anzugeben. Eine OE wird normalerweise einem vom Benutzer erstellten Container oder Ordner auf dem Verzeichnisserver zugeordnet.
- Allgemeiner Name (Common Name, CN). Dieses Attribut stellt das Objekt selbst innerhalb des Verzeichnisservers dar.
- Domänenkomponente (Domain Component, DC). Ein definierter Name, der Domänenkomponentenattribute verwendet, verfügt für jede Domänenebene unter dem Stammverzeichnis über eine Domänenkomponente. Dies bedeutet, dass ein Domänenkomponentenattribut für jedes Element vorhanden ist, das im Domänennamen durch einen Punkt abgetrennt wird.

Der definierte Name eines Objekts kann über die Administrationskonsole des Verzeichnisservers bestimmt werden.

Gruppenzugehörigkeit, Zuordnung und Anwendungszugriff

Hier werden die Richtlinien beschrieben, die bei der Zuordnung der Verzeichnisservergruppen zu Unica Platform-Gruppen beachtet werden müssen.

- Identifizieren oder Erstellen Sie die Verzeichnisservergruppen, dessen Mitglieder Sie in Unica Platform importieren möchten. Wenn diese Gruppen zu Unica Platform-Gruppen zugeordnet sind, werden Mitglieder dieser Gruppen automatisch als Unica-Benutzer erstellt.

  Mitglieder der Untergruppen Ihres Verzeichnisservers werden nicht automatisch importiert. Um Benutzer aus Untergruppen zu importieren, müssen Sie die untergeordneten Gruppen zu Unica Platform-Gruppen oder -Untergruppen zuordnen.

  Sie dürfen ausschließlich statische Verzeichnisservergruppen zuordnen; dynamische oder virtuelle Gruppen werden nicht unterstützt.
- Identifizieren oder Erstellen Sie die Gruppen in der Unica Platform, denen Sie Verzeichnisservergruppen zuordnen werden.
- Ordnen Sie den zuzuordnenden Gruppen einen entsprechenden Anwendungszugriff zu.

Speichern von Berechtigungsnachweisen für Verzeichnisserver in Unica Platform

Wenn Ihr Verzeichnisserver anonyme Zugriffe nicht erlaubt, müssen Sie ein Unica-Benutzerkonto konfigurieren, das den Benutzernamen und das Kennwort eines Verzeichnisserverbenutzers enthält (siehe Beschreibung in der folgenden Prozedur).

1. Melden Sie sich an Unica als ein Benutzer mit Admin-Zugriff an.
2. Wählen Sie ein Unica-Benutzerkonto aus oder erstellen Sie es, damit dieses Konto über alle Verzeichnisserverberechtigungsnachweise eines LDAP-Benutzers mit Leseberechtigung für alle Benutzer- und Gruppeninformationen auf dem LDAP-Server verfügt. Befolgen Sie diese Richtlinien.
   - In einem nachfolgenden Schritt setzen Sie den Wert der Konfigurationseigenschaft `Unica Platform-Benutzer für LDAP-Berechtigungsnachweis` auf den Benutzernamen für dieses Unica-

Benutzerkonto. Der Standardwert dieser Eigenschaft ist `asm_admin`, ein Benutzer, der in jeder neuen Unica Platform-Installation verwendet wird. Sie können das Konto `asm_admin` verwenden, um die Verzeichnisserver-Berechtigungsnachweise dort zu speichern.

- Der Name dieses Unica-Benutzerkontos darf nicht mit dem Benutzernamen eines Verzeichnisserver-Benutzers übereinstimmen.

3. Fügen Sie eine Datenquelle für dieses Unica-Benutzerkonto hinzu, um die Berechtigungsnachweise zu speichern, die Unica Platform für die Verbindung zum LDAP-Server verwendet. Befolgen Sie diese Richtlinien.

Tabelle 38. Datenquellenfelder zum Speichern von Berechtigungsnachweisen

Feld	Richtlinie
Datenquellenname	Sie können einen beliebigen Namen eingeben. Beachten Sie jedoch, dass in einem späteren Schritt der Wert der Konfigurationseigenschaft `Datenquelle für LDAP-Berechtigungsnachweise` mit diesem Datenquellennamen übereinstimmen muss. Damit Übereinstimmung mit dem Standardwert für diese Eigenschaft besteht und sie den Wert nicht festlegen müssen, geben Sie `LDAPServer` als Datenquellenname ein.
Datenquellenanmeldung	Geben Sie den definierten Namen (DN) des Benutzers mit Verwaltungsaufgaben und mit Leseberechtigung für alle Benutzer- und Gruppeninformationen an, der mit Unica synchronisiert wird. Der neue definierte Name ähnelt dem folgenden: `uidcn=user1,ou=someGroup,dc=systemName,dc=com` Alternativ können Sie den Rootbenutzernamen verwenden, der Zugriff auf alle Gruppen auf dem LDAP-Server hat. Der Standardrootbenutzer und die Angabe dieses Benutzers für die unterstützten Verzeichnisserver werden nachfolgend gezeigt.

Feld	Richtlinie

	• Der Rootbenutzer für den Active Directory Server ist Administrator. Sie können diesen Benutzer wie folgt angeben.
	`domain\ldap_admin_username`
	• Der Rootbenutzer für Oracle Directory Server ist Directory Manager. Sie können diesen Benutzer wie folgt angeben.
	`cn=Directory Manager`
	• Der Rootbenutzer für IBM Security Directory Server ist root. Sie können diesen Benutzer wie folgt angeben.
	`cn=root`

Datenquellenkennwort	Geben Sie das Kennwort des Benutzers mit Verwaltungsaufgaben an, dessen Anmeldename Sie in das Feld **Datenquelle für Anmeldung** eingegeben haben.

Festlegen der Verbindungseigenschaften für LDAP-Anmeldung in Unica

In den Eigenschaften für das LDAP-Anmeldeverfahren werden Verbindungsdetails angegeben, die das System verwendet, um die Verbindung zum Verzeichnisserver herzustellen.

1. Klicken Sie auf **Einstellungen > Konfiguration** und navigieren Sie zu der Kategorie **Unica Platform | Sicherheit | Details zum Anmeldeverfahren | LDAP**.
2. Legen Sie Werte der folgenden Konfigurationseigenschaften fest.

   Informationen zum Festlegen der einzelnen Eigenschaften finden Sie in den zugehörigen Referenzinformationen.

   - `Hostname des LDAP-Servers`
   - `LDAP-Server-Port`
   - `Benutzersuchfilter`

- In Unica Platform gespeicherte Berechtigungsnachweise verwenden
- Unica Platform-Benutzer für LDAP-Berechtigungsnachweise
- Datenquelle für LDAP-Berechtigungsnachweis
- Basis-DN
- SSL für LDAP-Verbindung verlangen

Festlegen der LDAP-Synchronisationseigenschaften

Mit den Eigenschaften für die LDAP-Synchronisation werden Details angegeben, die das System verwendet, um sich am Verzeichnisserver anzumelden und Benutzer für den Import zu identifizieren. Einige dieser Eigenschaften steuern auch die Häufigkeit und andere Details des automatischen Synchronisationsprozesses.

1. Klicken Sie auf **Einstellungen > Konfiguration** und navigieren Sie zur Kategorie **Platform | Sicherheit | LDAP-Synchronisation**.
2. Legen Sie im Abschnitt **LDAP-Eigenschaften** die Werte der folgenden Konfigurationseigenschaften fest.

   In der Kontexthilfe der Eigenschaft oder unter dem zugehörigen Themenlink in diesem Abschnitt finden Sie Anweisungen zum Einrichten der Werte.

   - LDAP-Synchronisation aktiviert
   - LDAP-Synchronisationsintervall
   - LDAP-Synchronisation verzögert
   - LDAP-Synchronisationszeitlimitüberschreitung
   - LDAP-Synchronisationsumfang
   - LDAP-Provider-URL
   - SSL für LDAP-Verbindung erforderlich (optional)
   - Unica-Gruppentrennzeichen für LDAP-Konfiguration
   - LDAP-Trennzeichen für Referenzkonfiguration
   - Unica Platform-Benutzer für LDAP-Berechtigungsnachweise
   - Datenquelle für LDAP-Berechtigungsnachweis
   - LDAP-Attributname für Benutzerreferenz
   - Regelmäßige LDAP-Basis-DN-Suche inaktiviert

- `Benutzeranmeldung`
- Verschiedene Benutzerattribute wie Abteilung, Land, und Berufsbezeichnung des Benutzers (optional)

Festlegen von Eigenschaften zur Zuordnung von Benutzerattributen

Diese Eigenschaften geben die Benutzerattribute an, die das System aus dem Verzeichnisserver importiert.

1. Klicken Sie auf **Einstellungen > Konfiguration** und navigieren Sie zur Kategorie **Platform | Sicherheit | LDAP-Synchronisation**.
2. Legen Sie im Abschnitt **Benutzerattribute zuordnen** die Werte für die Zuweisung der aufgelisteten Unica-Benutzerattribute zu den Benutzerattributen auf Ihrem Verzeichnisserver fest.

   Wenn Sie die gruppenbasierte Synchronisation verwenden, ist die einzige Eigenschaft, die Sie zuordnen müssen, `Benutzeranmeldung`. Üblicherweise ist der Wert `uid` in LDAP-Servern und `sAMAccountName` in Windows™ Active Directory-Servern. Verwenden Sie den überprüften Wert (siehe Beschreibung in „Erhalt erforderlicher Informationen").

   Wenn Sie die attributbasierte Synchronisation verwenden, ordnen Sie die Attribute zu, nach denen Sie suchen möchten.

   Beachten Sie Folgendes:

   - Die hier zugeordneten Eigenschaften werden für die importierten Benutzer bei jeder Unica Platform-Synchronisation mit Ihrem Verzeichnisserver ersetzt.
   - Unica Platform erfordert, dass E-Mail-Adressen der in RFC 821 angegebenen Definition entsprechen. definierten Richtlinien entsprechen. Sollten die E-Mail-Adressen auf Ihrem Verzeichnisserver diesem Standard nicht entsprechen, ordnen Sie diese nicht als zu importierende Attribute zu.
   - Falls Ihre Verzeichnisserverdatenbank zulässt, dass ein Attribut mehr Zeichen enthält als in den Unica Platform-Systemtabellen zugelassen werden (siehe nachfolgende Tabelle), wird der Attributtyp entsprechend gekürzt.

Tabelle 39. Anzahl zulässiger Zeichen für Benutzerattribute

Attribut	Zulässige Länge
Benutzeranmeldung (erforderlich)	256
Vorname	128
Nachname	128
Position des Benutzers	128
Department	128
Unternehmen	128
Land	128
E-Mail-Adresse des Benutzers	128
Adresse 1	128
Telefon (geschäftlich)	20
Mobiltelefon	20
Telefon (privat)	20
Alternative Anmeldung (erforderlich unter UNIX™)	256

Zuordnung von LDAP-Gruppen zu Unica-Gruppen

Benutzer, die den Verzeichnisservergruppen angehören, die Sie hier zuordnen, werden importiert und zu Mitgliedern der hier angegebenen Unica Platform-Gruppen.

Wichtig: Ordnen Sie keine Gruppen zu, die den Benutzer `asm_admin` als Mitglied haben.

1. Klicken Sie auf **Einstellungen > Konfiguration** und navigieren Sie zur Kategorie **Unica | Unica Platform | Sicherheit | LDAP-Synchronisation | LDAP-Referenz auf Unica Platform-Gruppenübersicht**.
2. Erstellen Sie für jede Verzeichnisservergruppe, die Sie einer Unica Platform-Gruppe zuordnen möchten, eine Kategorie **LDAP-Referenz auf Unica Platform-Gruppe**, indem Sie die Vorlage *(LDAP reference to Unica Platform group map)* auswählen. Legen Sie die folgenden Eigenschaften fest.
   - `Neuer Kategoriename`
   - `Übersicht LDAP-Referenzen`
   - `Unica Platform-Gruppe`

   Folgende Werte ordnen beispielsweise die LDAP-Gruppe `MarketingPlatformUsers` den Gruppen Unica Platform `marketingopsUsers` und `campaignUsers` zu (`FILTER` wird nicht verwendet).

   - `LDAP-Referenzen`: `cn=MarketingPlatformUsers,cn=Users, dc=myCompany,dc=com`
   - `Unica Platform-Gruppe`: `marketingopsUsers;campaignUsers`

Testen der Synchronisation

Überprüfen Sie, ob Benutzer und Gruppen ordnungsgemäß zwischen den Servern synchronisiert sind.

1. Melden Sie sich an Unica als Unica-Benutzer mit Admin-Berechtigung an (und nicht als Verzeichnisserverbenutzer).
2. Erzwingen Sie die Synchronisation durch Anklicken von **Synchronisieren** auf der Seite **Einstellungen > Benutzer**.
3. Führen Sie die folgenden Überprüfungen durch.
   - Überprüfen Sie, ob Benutzer ordnungsgemäß aus dem LDAP-Server importiert wurden.
   - Wenn Sie die gruppenbasierte Synchronisation verwenden, überprüfen Sie, ob die Unica Platform-Gruppenzugehörigkeiten der erwarteten Zuweisung zu Verzeichnisservergruppen entsprechen.

Einrichten eines Active Directory-Benutzers mit PlatformAdminRole-Berechtigungen

Wenn die NTLMv2-Authentifizierung aktiviert ist, können Sie sich nicht bei Unica als `platform_admin` anmelden. Sie müssen daher die folgende Prozedur ausführen, um Administrator zugriff auf Unica Platform zu erhalten.

1. Melden Sie sich an Unica als interner Benutzer an (also als ein Benutzer, der in Unica Platform erstellt, also nicht aus Active Directory importiert wurde). Es muss ein Benutzer mit den Berechtigungen von „PlatformAdminRole“ in Unica Platform sein.
2. Erstellen Sie eine Unica Platform-Gruppe und ordnen Sie ihr die Rolle „PlatformAdminRole“ zu.
3. Stellen Sie sicher, dass mindestens ein Windows™ Active Directory-Benutzer Mitglied dieser Gruppe ist.

Festlegen des Sicherheitsmodus zum Aktivieren der NTLMv2-Authentifizierung

Nur wenn Sie die NTLMv2-Authentifizierung aktivieren möchten, müssen Sie die Konfigurationseigenschaften wie in der folgenden Prozedur beschrieben festlegen.

NTLMv2-Authentifizierung konfigurieren

Klicken Sie auf **Einstellungen > Konfiguration** und legen Sie die Konfigurationseigenschaften wie in der folgenden Tabelle dargestellt fest.

Tabelle 40. Konfigurationseigenschaftswerte für NTLMv2

Eigenschaft	Wert
Platform | Sicherheit | Anmeldeverfahren	Wählen Sie die Option `Web-zugriffskontrolle` aus.
Platform | Sicherheit | Details zum Anmeldeverfahren | Webzugriffskontrolle | Kopfzeilenvariable für Webzugriffskontrolle	Geben Sie den Namen der Variablen in dem in den Regeln für die Neuerstellung festgelegten Format ein.

Eigenschaft	Wert
**Platform	Sicherheit	Details zum Anmeldeverfahren	Webzugriffskontrolle	Benutzernamenstruktur**	Geben Sie `\w*` ein.
**Allgemeines	Navigation	Platform-URL**	Geben Sie die URL der IIS-Site ein.

Erneutes Starten des Webanwendungsservers

Starten Sie den Webanwendungsserver neu, um zu gewährleisten, dass sämtliche Ihrer Konfigurationsänderungen angewandt werden.

Testen der Anmeldung als Active Directory-Benutzer

Überprüfen Sie die Konfiguration, indem Sie sich bei Unica mit dem entsprechenden Windows™ Active Directory-Benutzerkonto anmelden.

1. Melden Sie sich bei Windows™ als Active Directory-Benutzer an, der Mitglied einer Active Directory-Gruppe ist, die einer Unica Platform-Gruppe zugeordnet ist, der eine Rolle in Unica Platform zugewiesen wurde.
2. Navigieren Sie mit Ihrem Browser zur URL von Unica.

   Wenn Sie die NTLMv2-Authentifizierung aktiviert haben, sollte die Anmeldeanzeige von Unica nicht angezeigt werden. Außerdem sollten Sie in der Lage sein, auf die Unica-Benutzeroberfläche zuzugreifen.

   Wenn Sie die NTLMv2-Authentifizierung nicht aktiviert haben, dann können Sie sich normalerweise mit Ihren Windows-Berechtigungsnachweisen anmelden.

   Hinweise für den Fall, dass Sie sich nicht anmelden können, finden Sie unter restoreAccess (auf Seite 366).

Integration zwischen Unica und LDAP-Servern

Unica Platform kann für die Integration mit Windows™ Active Directory-Server oder einem anderen LDAP-Server (LDAP = Lightweight Directory Access Protocol) konfiguriert werden. Durch Integration von Unica in einen Verzeichnisserver können Sie Benutzer und Gruppen

an einem zentralen Ort verwalten. Die Integration ermöglicht ein flexibles Modell für die Erweiterung der Autorisierungsrichtlinien des Unternehmens in Unica Anwendungen. Durch die Integration werden Unterstützungskosten reduziert, und es wird weniger Zeit für die Implementierung einer Produktionsanwendung benötigt.

Eine Liste der unterstützten Verzeichnisserver finden Sie im Dokument Empfohlene Softwareumgebungen und Mindestsystemvoraussetzungen.

Funktionen bei der Integration in LDAP

Durch die Integration von Unica Platform mit LDAP werden die in diesem Abschnitt beschriebenen Funktionen bereitgestellt.

Authentifizierung bei der Integration in LDAP

Unica-Anwendungen senden eine Abfrage an Unica Platform, um Informationen zur Benutzerautorisierung abzurufen. Wenn die Integration in LDAP implementiert ist, geben die Benutzer Ihren gültigen LDAP-Benutzernamen und das zugehörige Kennwort zur Authentifizierung bei Unica-Anwendungen ein.

Verwalten interner und externer Benutzer

Wenn die Integration konfiguriert wurde, können Sie die importierten Benutzerkonten in Unica Platform nicht hinzufügen, ändern oder löschen. Sie müssen diese Managementaufgaben auf der LDAP-Seite ausführen, und Ihre Änderungen werden bei der Synchronisierung importiert. Wenn Sie importierte Benutzerkonten in Unica Platform ändern, können Benutzer auf Probleme bei der Authentifizierung stoßen.

Benutzerkonten, die Sie auf der LDAP-Seite löschen, werden auf Unica Platform nicht gelöscht. Sie müssen diese Konten in Unica Platform manuell deaktivieren. Es ist sicherer, diese gelöschten Benutzerkonten zu inaktivieren, anstatt sie zu löschen, da Benutzer Eigentumszugriffsrechte auf Ordner in Unica Campaign haben. Wenn Sie ein Benutzerkonto löschen, das Eigentümer eines Ordners ist, sind die Objekte in dem betreffenden Ordner nicht mehr verfügbar.

Synchronisieren

Wenn Unica für die Integration in einen LDAP-Server konfiguriert wurde, werden Benutzer und Gruppen in zuvor festgelegten Intervallen automatisch synchronisiert.

Die automatische Synchronisation verfügt nur über eine eingeschränkte Funktionalität.

- Benutzer, die vom LDAP-Server gelöscht wurden, werden während der automatischen Synchronisation nicht gelöscht.

Sie können eine vollständige Synchronisation aller Benutzer und Gruppen mit der Synchronisationsfunktion im Benutzerbereich von Unica erzwingen. Alternativ hierzu können Sie sich auch an die Services wenden, um das Definieren einer verdeckten Konfigurationseigenschaft anzufordern, durch die bei der automatischen Synchronisation eine vollständige Synchronisation durchgeführt wird.

Importieren von Benutzern auf der Basis von Gruppen oder Attributen

Sie können einen von zwei Filtertypen wählen, um die Benutzerkonten auszuwählen, die vom LDAP-Server in Unica Platform importiert werden.

Sie müssen zwischen gruppenbasiertem und attributbasiertem Import wählen. Mehrere Methoden gleichzeitig werden nicht unterstützt.

Gruppenbasierter Import

Unica Platform importiert Gruppen und die zugehörigen Benutzer aus der Datenbank des Verzeichnisservers über eine regelmäßige Synchronisationsaufgabe, die automatisch Informationen vom Verzeichnisserver abruft. Wenn Unica Platform Benutzer und Gruppen aus der Serverdatenbank importiert, werden die Gruppenzugehörigkeiten nicht geändert. Um diese Änderungen zu erfassen, müssen Sie eine manuelle Synchronisation durchführen.

Anmerkung: Die LDAP-Gruppen müssen einen eindeutigen Namen aufweisen, selbst wenn die Gruppen für separate Partitionen konfiguriert werden.

Sie können Unica-Berechtigungen zuordnen, indem Sie eine LDAP-Gruppe einer Unica-Gruppe zuordnen. Aufgrund dieser Zuweisung können neue Benutzer, die der LDAP-Gruppe

zugeordnet wurden, die Berechtigungen übernehmen, die für die entsprechende Unica-Gruppe festgelegt wurden.

Eine Untergruppe in Unica Platform erbt die LDAP-Zuordnungen oder Benutzerzugehörigkeiten ihrer übergeordneten Gruppen nicht.

Weitere Informationen zum Konfigurieren des gruppenbasierten Imports finden Sie weiter unten in diesem Kapitel.

Attributbasierter Import

Wenn Sie keine Gruppen in Ihrem LDAP-Server erstellen möchten, die sich auf bestimmte Unica-Produkte beziehen, haben Sie die Möglichkeit, die importierten Benutzer durch die Angabe von Attributen zu steuern. Dazu müssen Sie folgende Schritte während des LDAP-Installationsprozesses ausführen.

1. Bestimmen Sie die Zeichenfolge, die in Ihrem LDAP-Server für das Attribut verwendet wird, nach dem Sie filtern möchten.
2. Setzen Sie die Eigenschaft **Platform | Sicherheit | LDAP-Synchronisation | LDAP-Attributname für Benutzerreferenz** auf `DN`.

   Damit wird Unica Platform mitgeteilt, dass die Synchronisation nicht auf einer Gruppe mit Mitgliedsreferenzen basiert, sondern auf einer Organisationseinheit oder Organisation.
3. Wenn Sie die Eigenschaft **Übersicht LDAP-Referenzen** konfigurieren, setzen Sie den Abschnitt "Filter" des Werts auf das Attribut, nach dem Sie suchen möchten. Verwenden Sie für den Filter die Zeichenfolge, die Sie in Schritt 1 festgelegt haben.

Wenn Sie die attributbasierte Synchronisation verwenden, ist die periodische Synchronisation immer eine vollständige Synchronisation und keine partielle Synchronisation, die für die gruppenbasierte Synchronisation ausgeführt wird. Für die attributbasierte Synchronisation sollten Sie die Eigenschaft **LDAP-Synchronisationsintervall** auf einen hohen Wert setzen oder auf `0`, um die automatische Synchronisation zu inaktivieren und sich auf die vollständige Synchronisation zu verlassen, wenn Benutzer zum Verzeichnis hinzugefügt werden.

Informationen zu LDAP und Partitionen

In Umgebungen mit mehreren Partitionen wird die Partitionszugehörigkeit eines Benutzers von der Gruppe bestimmt, zu der der Benutzer gehört, wenn die Gruppe einer Partition zugeordnet wird. Ein Benutzer kann nur zu einer Partition gehören. Folglich gilt: Wenn ein Benutzer Mitglied mehrerer LDAP-Gruppen ist und diese Gruppen Unica-Gruppen zugeordnet sind, die wiederum unterschiedlichen Partitionen zugewiesen sind, muss das System für den betreffenden Benutzer eine einzelne Partition auswählen.

Diese Situation sollte nach Möglichkeit vermieden werden. Tritt sie aber dennoch ein, gilt die Partition der Unica-Gruppe, die zuletzt einer LDAP-Gruppe zugeordnet wurde, als diejenige, der der Benutzer angehört. Informationen dazu, welche LDAP-Gruppe zuletzt zugeordnet wurde, finden Sie in den LDAP-Gruppenzuordnungen, die im Konfigurationsbereich angezeigt werden. Diese werden in chronologischer Reihenfolge mit den letzten Zuweisungen an letzter Stelle angezeigt.

Unterstützung interner und externer Benutzer

Unica unterstützt zwei Benutzerkonten- und Benutzergruppenarten.

- **Intern** - Benutzerkonten und -gruppen, die über die Unica-Sicherheitsbenutzeroberfläche in Unica erstellt wurden. Diese Benutzer werden über Unica Platform authentifiziert.
- **Extern** - Benutzerkonten und -gruppen, die durch Synchronisation mit einem unterstützten LDAP-Server in Unica importiert wurden. Diese Synchronisation geschieht nur dann, wenn Unica für die Integration in den LDAP-Server konfiguriert wurde. Diese Benutzer werden über den LDAP-Server authentifiziert.

Es empfiehlt sich, beide Arten von Benutzern und Gruppen zu verwenden, wenn Sie z. B. Ihren Kunden den Zugriff auf Unica-Anwendungen gewähren, sie jedoch nicht als vollständige Unternehmensbenutzer zu Ihrem LDAP-Server hinzufügen möchten.

Die Verwendung dieses hybriden Authentifizierungsmodells bedeutet mehr Verwaltungsaufwand als ein Modell mit reiner LDAP-Authentifizierung.

Sonderzeichen in Anmeldenamen

Nur die folgenden Sonderzeichen sind in Anmeldenamen zulässig: Punkt (.), Unterstreichungszeichen (_) und Bindestrich (-). Wenn andere Sonderzeichen (einschließlich Leerzeichen) im Anmeldenamen eines Benutzers enthalten sind, den Sie von Ihrem LDAP-Server in Unica Platform importieren wollen, müssen Sie den Anmeldenamen so ändern, dass der Benutzer auf keine Probleme stößt, wenn er sich abmeldet oder administrative Aufgaben ausführt (sofern der Benutzer Administratorberechtigung besitzt).

Voraussetzungen für die LDAP-Integration

Um die LDAP-Integrationsfunktionen nutzen zu können, müssen Unica-Anwendungen in einem unterstützten Betriebssystem installiert werden.

Roadmap für den Konfigurationsprozess: LDAP-Integration

Verwenden Sie diese Roadmap für den Konfigurationsprozess, um die Aufgaben zu suchen, die zur Integration von Unica mit LDAP erforderlich sind. Die Spalte „Abschnitt“ stellt Links zu den Themen bereit, in denen die Aufgaben ausführlich beschrieben werden.

Tabelle 41. Roadmap für den Konfigurationsprozess: LDAP-Integration

Topic	Informationen
Erhalt erforderlicher Informationen *(auf Seite 177)*	Einholen von Informationen über Ihren LDAP-Server, die für die Integration in Unica benötigt werden.
Gruppenzugehörigkeit, Zuordnung und Anwendungszugriff *(auf Seite 180)*	Bei einer gruppenbasierten Synchronisation Identifizieren oder Erstellen der Gruppen in Unica Platform, denen Sie Ihre LDAP-Gruppen zuordnen werden.
Speichern von Berechtigungsnachweisen für Verzeichnisserver in Unica Platform *(auf Seite 180)*	Wenn Ihr Verzeichnisserver anonyme Zugriffe nicht erlaubt (die gängigste Art der Konfiguration), konfigurieren Sie ein Unica-Benutzerkonto und legen Sie dafür einen Be-

Tabelle 41. Roadmap für den Konfigurationsprozess: LDAP-Integration (Fortsetzung)

Topic	Informationen
	nutzernamen mit Administratorberechtigung für den Verzeichnisserver und ein entsprechendes Kennwort fest.
• Festlegen der Verbindungseigenschaften für LDAP-Anmeldung in Unica *(auf Seite 182)* • Festlegen der LDAP-Synchronisationseigenschaften *(auf Seite 183)* • Festlegen von Eigenschaften zur Zuordnung von Benutzerattributen *(auf Seite 184)* • Zuordnung von LDAP-Gruppen zu Unica-Gruppen *(auf Seite 185)*	Konfigurieren von Unica Platform für die Integration, indem Sie die Werte auf der Seite „Konfiguration“ festlegen.
Testen der Synchronisation *(auf Seite 186)*	Überprüfen, ob Benutzer wie erwartet importiert werden, und bei einer gruppenbasierten Synchronisation sicherstellen, dass Gruppen ordnungsgemäß synchronisiert werden.
Festlegen des Sicherheitsmodus in LDAP *(auf Seite 204)*	Festlegen der Sicherheitsmodus-Werte auf der Seite „Konfiguration“.
Erneutes Starten des Webanwendungsservers *(auf Seite 188)*	Dieser Schritt ist erforderlich, um zu gewährleisten, dass sämtliche Ihrer Änderungen angewandt werden.
Testen der Anmeldung als LDAP-Benutzer *(auf Seite 204)*	Vergewissern Sie sich, dass Sie sich in Unica als LDAP-Benutzer anmelden können.

Erhalt erforderlicher Informationen

Rufen Sie die erforderlichen Informationen über den Verzeichnisserver ab, den Sie für die Integration verwenden möchten. Sie verwenden diese Informationen beim Konfigurationsprozess, um Berechtigungsnachweise für Verzeichnisserver zu speichern und Werte von Konfigurationseigenschaften festzulegen.

Beziehen Sie die folgenden Informationen.

- Besorgen Sie sich den Namen und den Port des Server-Hosts.
- Bestimmen Sie einen Benutzer, der über Suchberechtigungen für den Verzeichnisserver verfügt, und tragen Sie die folgenden Informationen über den Benutzer zusammen.
    - Anmeldename.
    - Passwort
    - Definierter Name (DN)
- Besorgen Sie sich die folgenden Informationen für den Verzeichnisserver.
    - Vollständig qualifizierter Hostname oder IP-Adresse
    - Der Port, auf dem der Server empfangsbereit ist.
- Bestimmen Sie die Zeichenfolge, die Ihr Verzeichnisserver für das Benutzerattribut im Gruppenobjekt benutzt. Üblicherweise wird der Wert `uniquemember` in LDAP-Servern und `member` in Windows™ Active Directory-Servern verwendet. Sie sollten dies auf Ihrem Verzeichnisserver überprüfen.
- Fordern Sie die folgenden erforderlichen Benutzerattribute an.
    - Bestimmen Sie die Zeichenfolge, die Ihr Verzeichnisserver für das Benutzeranmeldungsattribut benutzt. Diese Zeichenfolge ist immer erforderlich. Üblicherweise ist der Wert `uid` in LDAP-Servern und `sAMAccountName` in Windows™ Active Directory-Servern. Überprüfen Sie diese Zeichenfolge auf Ihrem Verzeichnisserver.
    - Nur wenn Unica Campaign in einer UNIX™-Umgebung installiert ist, ermitteln Sie die Zeichenfolge, die von Ihrem Verzeichnisserver für das alternative Anmeldeattribut verwendet wird.
- Wenn Sie die attributbasierte Synchronisation verwenden, rufen Sie die Zeichenfolgen für die Attribute (mindestens eins) ab, die Sie für diesen Zweck verwenden möchten.

- Falls Sie mit Unica Platform zusätzliche (optionale), auf Ihrem Verzeichnisserver gespeicherte Benutzerattribute importieren möchten, bestimmen Sie die Zeichenfolgen, die Ihr Verzeichnisserver für Folgendes verwendet.
    - Vorname
    - Nachname
    - Position des Benutzers
    - Department
    - Unternehmen
    - Land
    - E-Mail-Adresse des Benutzers
    - Adresse 1
    - Telefon (geschäftlich)
    - Mobiltelefon
    - Telefon (privat)

Informationen über definierte Namen

Damit die Verzeichnisserver-Integration in Unica aktiviert werden kann, muss der definierte Name (DN) für einen Benutzer und für Gruppen bestimmt werden. Der definierte Name eines Objekts auf dem Verzeichnisserver ist der vollständige Pfad durch Baumstruktur des Verzeichnisservers zu diesem Objekt.

DNs bestehen aus den folgenden Komponenten:

- Organisationseinheit (OE). Dieses Attribut wird verwendet, um einen Namespace auf der Grundlage der Organisationsstruktur anzugeben. Eine OE wird normalerweise einem vom Benutzer erstellten Container oder Ordner auf dem Verzeichnisserver zugeordnet.
- Allgemeiner Name (Common Name, CN). Dieses Attribut stellt das Objekt selbst innerhalb des Verzeichnisservers dar.
- Domänenkomponente (Domain Component, DC). Ein definierter Name, der Domänenkomponentenattribute verwendet, verfügt für jede Domänenebene

unter dem Stammverzeichnis über eine Domänenkomponente. Dies bedeutet, dass ein Domänenkomponentenattribut für jedes Element vorhanden ist, das im Domänennamen durch einen Punkt abgetrennt wird.

Der definierte Name eines Objekts kann über die Administrationskonsole des Verzeichnisservers bestimmt werden.

Gruppenzugehörigkeit, Zuordnung und Anwendungszugriff

Hier werden die Richtlinien beschrieben, die bei der Zuordnung der Verzeichnisservergruppen zu Unica Platform-Gruppen beachtet werden müssen.

- Identifizieren oder Erstellen Sie die Verzeichnisservergruppen, dessen Mitglieder Sie in Unica Platform importieren möchten. Wenn diese Gruppen zu Unica Platform-Gruppen zugeordnet sind, werden Mitglieder dieser Gruppen automatisch als Unica-Benutzer erstellt.

  Mitglieder der Untergruppen Ihres Verzeichnisservers werden nicht automatisch importiert. Um Benutzer aus Untergruppen zu importieren, müssen Sie die untergeordneten Gruppen zu Unica Platform-Gruppen oder -Untergruppen zuordnen.

  Sie dürfen ausschließlich statische Verzeichnisservergruppen zuordnen; dynamische oder virtuelle Gruppen werden nicht unterstützt.
- Identifizieren oder Erstellen Sie die Gruppen in der Unica Platform, denen Sie Verzeichnisservergruppen zuordnen werden.
- Ordnen Sie den zuzuordnenden Gruppen einen entsprechenden Anwendungszugriff zu.

Speichern von Berechtigungsnachweisen für Verzeichnisserver in Unica Platform

Wenn Ihr Verzeichnisserver anonyme Zugriffe nicht erlaubt, müssen Sie ein Unica-Benutzerkonto konfigurieren, das den Benutzernamen und das Kennwort eines Verzeichnisserverbenutzers enthält (siehe Beschreibung in der folgenden Prozedur).

1. Melden Sie sich an Unica als ein Benutzer mit Admin-Zugriff an.
2. Wählen Sie ein Unica-Benutzerkonto aus oder erstellen Sie es, damit dieses Konto über alle Verzeichnisserverberechtigungsnachweise eines LDAP-Benutzers mit Leseberechtigung für alle Benutzer- und Gruppeninformationen auf dem LDAP-Server verfügt. Befolgen Sie diese Richtlinien.
    - In einem nachfolgenden Schritt setzen Sie den Wert der Konfigurationseigenschaft `Unica Platform-Benutzer für LDAP-Berechtigungsnachweis` auf den Benutzernamen für dieses Unica-Benutzerkonto. Der Standardwert dieser Eigenschaft ist `asm_admin`, ein Benutzer, der in jeder neuen Unica Platform-Installation verwendet wird. Sie können das Konto `asm_admin` verwenden, um die Verzeichnisserver-Berechtigungsnachweise dort zu speichern.
    - Der Name dieses Unica-Benutzerkontos darf nicht mit dem Benutzernamen eines Verzeichnisserver-Benutzers übereinstimmen.
3. Fügen Sie eine Datenquelle für dieses Unica-Benutzerkonto hinzu, um die Berechtigungsnachweise zu speichern, die Unica Platform für die Verbindung zum LDAP-Server verwendet. Befolgen Sie diese Richtlinien.

Tabelle 42. Datenquellenfelder zum Speichern von Berechtigungsnachweisen

Feld	Richtlinie
Datenquellenname	Sie können einen beliebigen Namen eingeben. Beachten Sie jedoch, dass in einem späteren Schritt der Wert der Konfigurationseigenschaft `Datenquelle für LDAP-Berechtigungsnachweise` mit diesem Datenquellennamen übereinstimmen muss. Damit Übereinstimmung mit dem Standardwert für diese Eigenschaft besteht und sie den Wert nicht festlegen müssen, geben Sie `LDAPServer` als Datenquellenname ein.
Datenquellenanmeldung	Geben Sie den definierten Namen (DN) des Benutzers mit Verwaltungsaufgaben und mit Leseberechtigung für alle Benutzer- und Gruppeninformationen an, der mit Unica syn-

Feld	Richtlinie

	chronisiert wird. Der neue definierte Name ähnelt dem folgenden:
	`uidcn=user1,ou=someGroup,dc=systemName,dc=com`
	Alternativ können Sie den Rootbenutzernamen verwenden, der Zugriff auf alle Gruppen auf dem LDAP-Server hat. Der Standardrootbenutzer und die Angabe dieses Benutzers für die unterstützten Verzeichnisserver werden nachfolgend gezeigt.
	• Der Rootbenutzer für den Active Directory Server ist Administrator. Sie können diesen Benutzer wie folgt angeben.
	`domain\ldap_admin_username`
	• Der Rootbenutzer für Oracle Directory Server ist Directory Manager. Sie können diesen Benutzer wie folgt angeben.
	`cn=Directory Manager`
	• Der Rootbenutzer für IBM Security Directory Server ist root. Sie können diesen Benutzer wie folgt angeben.
	`cn=root`

Datenquellenkennwort	Geben Sie das Kennwort des Benutzers mit Verwaltungsaufgaben an, dessen Anmeldename Sie in das Feld **Datenquelle für Anmeldung** eingegeben haben.

Festlegen der Verbindungseigenschaften für LDAP-Anmeldung in Unica

In den Eigenschaften für das LDAP-Anmeldeverfahren werden Verbindungsdetails angegeben, die das System verwendet, um die Verbindung zum Verzeichnisserver herzustellen.

1. Klicken Sie auf **Einstellungen > Konfiguration** und navigieren Sie zu der Kategorie **Unica Platform | Sicherheit | Details zum Anmeldeverfahren | LDAP**.
2. Legen Sie Werte der folgenden Konfigurationseigenschaften fest.

   Informationen zum Festlegen der einzelnen Eigenschaften finden Sie in den zugehörigen Referenzinformationen.

   - `Hostname des LDAP-Servers`
   - `LDAP-Server-Port`
   - `Benutzersuchfilter`
   - `In Unica Platform gespeicherte Berechtigungsnachweise verwenden`
   - `Unica Platform-Benutzer für LDAP-Berechtigungsnachweise`
   - `Datenquelle für LDAP-Berechtigungsnachweis`
   - `Basis-DN`
   - `SSL für LDAP-Verbindung verlangen`

Festlegen der LDAP-Synchronisationseigenschaften

Mit den Eigenschaften für die LDAP-Synchronisation werden Details angegeben, die das System verwendet, um sich am Verzeichnisserver anzumelden und Benutzer für den Import zu identifizieren. Einige dieser Eigenschaften steuern auch die Häufigkeit und andere Details des automatischen Synchronisationsprozesses.

1. Klicken Sie auf **Einstellungen > Konfiguration** und navigieren Sie zur Kategorie **Platform | Sicherheit | LDAP-Synchronisation**.
2. Legen Sie im Abschnitt **LDAP-Eigenschaften** die Werte der folgenden Konfigurationseigenschaften fest.

   In der Kontexthilfe der Eigenschaft oder unter dem zugehörigen Themenlink in diesem Abschnitt finden Sie Anweisungen zum Einrichten der Werte.

   - `LDAP-Synchronisation aktiviert`
   - `LDAP-Synchronisationsintervall`
   - `LDAP-Synchronisation verzögert`
   - `LDAP-Synchronisationszeitlimitüberschreitung`
   - `LDAP-Synchronisationsumfang`

- `LDAP-Provider-URL`
- `SSL für LDAP-Verbindung erforderlich` (optional)
- `Unica-Gruppentrennzeichen für LDAP-Konfiguration`
- `LDAP-Trennzeichen für Referenzkonfiguration`
- `Unica Platform-Benutzer für LDAP-Berechtigungsnachweise`
- `Datenquelle für LDAP-Berechtigungsnachweis`
- `LDAP-Attributname für Benutzerreferenz`
- `Regelmäßige LDAP-Basis-DN-Suche inaktiviert`
- `Benutzeranmeldung`
- Verschiedene Benutzerattribute wie Abteilung, Land, und Berufsbezeichnung des Benutzers (optional)

Festlegen von Eigenschaften zur Zuordnung von Benutzerattributen

Diese Eigenschaften geben die Benutzerattribute an, die das System aus dem Verzeichnisserver importiert.

1. Klicken Sie auf **Einstellungen > Konfiguration** und navigieren Sie zur Kategorie **Platform | Sicherheit | LDAP-Synchronisation**.
2. Legen Sie im Abschnitt **Benutzerattribute zuordnen** die Werte für die Zuweisung der aufgelisteten Unica-Benutzerattribute zu den Benutzerattributen auf Ihrem Verzeichnisserver fest.

   Wenn Sie die gruppenbasierte Synchronisation verwenden, ist die einzige Eigenschaft, die Sie zuordnen müssen, `Benutzeranmeldung`. Üblicherweise ist der Wert `uid` in LDAP-Servern und `sAMAccountName` in Windows™ Active Directory-Servern. Verwenden Sie den überprüften Wert (siehe Beschreibung in „Erhalt erforderlicher Informationen").

   Wenn Sie die attributbasierte Synchronisation verwenden, ordnen Sie die Attribute zu, nach denen Sie suchen möchten.

   Beachten Sie Folgendes:

- Die hier zugeordneten Eigenschaften werden für die importierten Benutzer bei jeder Unica Platform-Synchronisation mit Ihrem Verzeichnisserver ersetzt.
- Unica Platform erfordert, dass E-Mail-Adressen der in RFC 821 angegebenen Definition entsprechen. definierten Richtlinien entsprechen. Sollten die E-Mail-Adressen auf Ihrem Verzeichnisserver diesem Standard nicht entsprechen, ordnen Sie diese nicht als zu importierende Attribute zu.
- Falls Ihre Verzeichnisserverdatenbank zulässt, dass ein Attribut mehr Zeichen enthält als in den Unica Platform-Systemtabellen zugelassen werden (siehe nachfolgende Tabelle), wird der Attributtyp entsprechend gekürzt.

Tabelle 43. Anzahl zulässiger Zeichen für Benutzerattribute

Attribut	Zulässi-ge Länge
Benutzeranmeldung (erforderlich)	256
Vorname	128
Nachname	128
Position des Benutzers	128
Department	128
Unternehmen	128
Land	128
E-Mail-Adresse des Benutzers	128
Adresse 1	128
Telefon (geschäftlich)	20
Mobiltelefon	20
Telefon (privat)	20
Alternative Anmeldung (erforderlich unter UN-IX™)	256

Zuordnung von LDAP-Gruppen zu Unica-Gruppen

Benutzer, die den Verzeichnisservergruppen angehören, die Sie hier zuordnen, werden importiert und zu Mitgliedern der hier angegebenen Unica Platform-Gruppen.

Wichtig: Ordnen Sie keine Gruppen zu, die den Benutzer `asm_admin` als Mitglied haben.

1. Klicken Sie auf **Einstellungen > Konfiguration** und navigieren Sie zur Kategorie **Unica | Unica Platform | Sicherheit | LDAP-Synchronisation | LDAP-Referenz auf Unica Platform-Gruppenübersicht**.
2. Erstellen Sie für jede Verzeichnisservergruppe, die Sie einer Unica Platform-Gruppe zuordnen möchten, eine Kategorie **LDAP-Referenz auf Unica Platform-Gruppe**, indem Sie die Vorlage *(LDAP reference to Unica Platform group map)* auswählen. Legen Sie die folgenden Eigenschaften fest.
   - `Neuer Kategoriename`
   - `Übersicht LDAP-Referenzen`
   - `Unica Platform-Gruppe`

   Folgende Werte ordnen beispielsweise die LDAP-Gruppe `MarketingPlatformUsers` den Gruppen Unica Platform `marketingopsUsers` und `campaignUsers` zu (`FILTER` wird nicht verwendet).

   - `LDAP-Referenzen`: `cn=MarketingPlatformUsers,cn=Users, dc=myCompany,dc=com`
   - `Unica Platform-Gruppe`: `marketingopsUsers;campaignUsers`

Testen der Synchronisation

Überprüfen Sie, ob Benutzer und Gruppen ordnungsgemäß zwischen den Servern synchronisiert sind.

1. Melden Sie sich an Unica als Unica-Benutzer mit Admin-Berechtigung an (und nicht als Verzeichnisserverbenutzer).
2. Erzwingen Sie die Synchronisation durch Anklicken von **Synchronisieren** auf der Seite **Einstellungen > Benutzer**.
3. Führen Sie die folgenden Überprüfungen durch.
    - Überprüfen Sie, ob Benutzer ordnungsgemäß aus dem LDAP-Server importiert wurden.
    - Wenn Sie die gruppenbasierte Synchronisation verwenden, überprüfen Sie, ob die Unica Platform-Gruppenzugehörigkeiten der erwarteten Zuweisung zu Verzeichnisservergruppen entsprechen.

Festlegen des Sicherheitsmodus in LDAP

Hier wird beschrieben, wie die Eigenschaften des Sicherheitsmodus gesetzt werden, damit LDAP-Benutzer sich an Unica-Anwendungen anmelden können.

1. Melden Sie sich bei Unica an, klicken Sie auf **Einstellungen > Konfiguration** und navigieren Sie zu **Unica Platform | Sicherheit**.
2. Setzen Sie den Eigenschaftswert `Anmeldeverfahren` auf `LDAP`.

Erneutes Starten des Webanwendungsservers

Starten Sie den Webanwendungsserver neu, um zu gewährleisten, dass sämtliche Ihrer Konfigurationsänderungen angewandt werden.

Testen der Anmeldung als LDAP-Benutzer

Testen Sie Ihre Konfiguration, indem Sie sich in Unica als LDAP-Benutzer anmelden, der Mitglied einer LDAP-Gruppe ist, die einer Unica Platform-Gruppe mit Zugangsberechtigung für Unica Platform angehört.

Integration mit Plattformen zur Webzugriffskontrolle

Plattformen zur Webzugriffskontrolle werden von Organisationen dazu verwendet, die Sicherheitssysteme zu konsolidieren, mit denen ein Portal zur Regulierung des

Benutzerzugriffs auf Webseiten bereitgestellt wird. Dieser Abschnitt liefert einen Überblick über die Unica-Integration in Plattformen zur Webzugriffskontrolle.

Authentifizierung

Wenn Benutzer über ein Portal zur Webzugriffskontrolle auf eine Anwendung zugreifen, wird ihre Authentifizierung über das System zur Webzugriffskontrolle verwaltet. Benutzer der Webzugriffskontrolle, die gleichzeitig einer LDAP-Gruppe angehören, die mit Unica synchronisiert ist, erhalten eine Authentifizierung für alle Unica-Anwendungen, wenn sie sich im System zur Webzugriffskontrolle anmelden. Diesen Benutzern werden die Anmeldeanzeigen der Unica-Anwendungen nicht angezeigt.

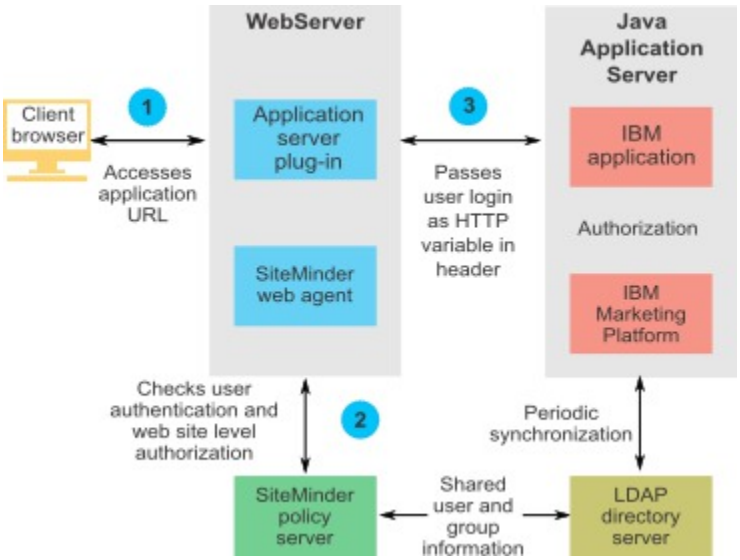
Berechtigung

Unica Anwendungsanfrage Unica Platform für Benutzerautorisierungsinformationen. Unica Platform importiert Gruppen und die zugehörigen Benutzer aus der LDAP-Datenbank über eine regelmäßige Synchronisationsaufgabe, die automatisch Informationen vom LDAP-Server abruft. Wenn Benutzer aus der LDAP-Datenbank in Unica Platform importiert werden, wird die Gruppenzugehörigkeit beibehalten. Diese LDAP-Benutzer werden ebenfalls über das System für die Webzugriffskontrolle bereitgestellt, sodass das System für die Webzugriffskontrolle und Unica auf eine einheitliche Benutzergruppe verweisen.

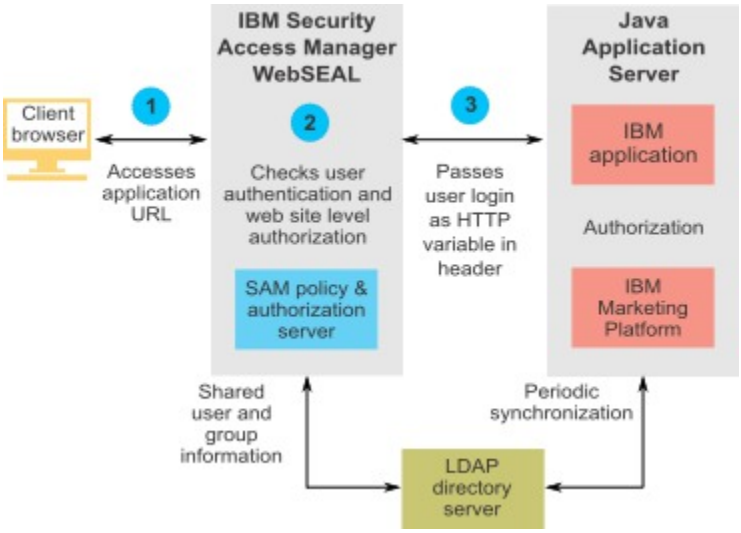
Zusätzliche Autorisierungssteuerelemente (einschließlich der Steuerelemente für die Anwendungs-URLs, auf die Benutzer zugreifen können) sind über die meisten Systeme zur Webzugriffskontrolle verfügbar.

Diagramme zur Integration der Webzugriffskontrolle

Die nachfolgende Abbildung zeigt, wie Unica mit SiteMinder und einem LDAP-Verzeichnisserver verwendet wird, um Benutzer zu authentifizieren und zu autorisieren.



Die nachfolgende Abbildung zeigt, wie Unica mit IBM Security Access Manager und einem LDAP-Verzeichnisserver zusammenarbeitet, um Benutzer zu authentifizieren und zu autorisieren.



Informationen zu Kontextstammverzeichnissen

Sie müssen den Schutz von URLs im System zur Webzugriffskontrolle aufheben, um verschiedene Funktionen in Unica-Produkten zu aktivieren. Zur Ausführung dieser Aufgabe müssen Sie die Kontextstammverzeichnisse des Produkts in die URLs aufnehmen.

Die folgende Tabelle enthält eine Liste der Standard-Kontextstammverzeichnisse für die in diesem Kapitel aufgeführten Unica-Produkte. Ihre Installation verwendet möglicherweise keine Standard-Kontextstammverzeichnisse, die meisten Installationen akzeptieren jedoch den Standardwert.

In den Beispielen in diesem Kapitel werden die Standard-Kontextstammverzeichnisse verwendet. Wenn Ihre Umgebung keine Standard-Kontextstammverzeichnisse verwendet, müssen Sie das Kontextstammverzeichnis in den Beispiel-URLs in das Kontextstammverzeichnis ändern, das in Ihrer Umgebung verwendet wird.

Tabelle 44. Kontextstammverzeichnis für Unica-Produkte

Produkt	Kontextstammverzeichnis
Unica Platform	unica
Unica Campaign	Kampagne
Unica Optimize	Campaign/optimize
Unica Plan	Plan
Unica Collaborate	collaborate
Unica Interact	Campaign/interact

Voraussetzungen für die SiteMinder-Integration

Folgende Voraussetzungen müssen erfüllt werden, damit Unica in Netegrity SiteMinder integriert werden kann.

- SiteMinder muss für die Verwendung eines Web-Agents und eines Richtlinienservers konfiguriert sein.
- SiteMinder muss so konfiguriert sein, dass der Anmeldename als HTTP-Variable in der URL-Anfrage an die Unica-Anwendung übergeben wird.
- Die Unica-Eigenschaft **Kopfzeilenvariable für Webzugriffssteuerung** muss auf den Namen der Variablen gesetzt sein, die SiteMinder für Anmeldenamen verwendet.

  Der Standardname der Variablen für den SiteMinder-Anmeldenamen ist `sm_user`.
- Der SiteMinder-Richtlinienserver muss für die Verwendung von LDAP als Repository zum Speichern von Gruppenmitgliedern und Benutzereigenschaften konfiguriert sein.
- Die Unica-Anwendungs-URLs, die vom Web-Server, der SiteMinder hostet, und vom Java™-Anwendungsserver, der die Unica-Anwendung hostet, bereitgestellt werden, müssen auf denselben Pfad verweisen.
- Der Web-Server, auf dem SiteMinder gehostet wird, muss so konfiguriert sein, dass Anfragen an die Unica-Anwendungs-URL an den Java™-Anwendungsserver umgeleitet werden.
- Allen Benutzern, die Zugriff auf Unica-Anwendungen benötigen, muss in SiteMinder der Zugriff auf die Unica-Webanwendungen für HTTP`GET`- und `POST`-Anforderungen über SiteMinder gewährt werden.

Hinweise zu den für die Aktivierung bestimmter Funktionen oder zu den für die Unterstützung bestimmter Unica-Produkte erforderlichen Einstellungen finden Sie im weiteren Verlauf dieses Abschnitts.

Konfigurieren von SiteMinder für Unica-Produkte

Heben Sie den Schutz von SiteMinder-Objekten wie in dieser Prozedur beschrieben auf, um die korrekte Funktion Ihrer Unica-Produkte zu aktivieren.

1. Melden Sie sich im Bereich **Richtlinienserver verwalten** von SiteMinder an und klicken Sie auf **Domänen**.
2. Wählen Sie den Bereich aus, der Ihre Installationen betrifft, klicken Sie mit der rechten Maustaste auf **unprotecturl** und wählen Sie **Eigenschaften des Bereichs** aus.

3. Wie in der folgenden Tabelle beschrieben, geben Sie für jede der anwendbaren URLs, die URL im Textfeld **Ressourcenfilter** ein und wählen Sie unter **Standardressourcenschutz** die Einstellung **Ungeschützt** aus.

Table 45. Für Unica-Produkte erforderliche ungeschützte Objekte

Produkt oder Komponente	Objekte
Unica Campaign	• `/Campaign/services/CampaignServices30Service` • `/Campaign/api/campaign/rest` • `/Campaign/FlowchartNotifyScheduler` • `/Campaign/OperationMonitor` • `http://host:port/Campaign/api/campaign/rest/deepsearch/partition` Ersetzen Sie Partition durch den Partitionsnamen. Wenn die Integration mit Engage implementiert wird, dann gilt Folgendes. In den folgenden URLs, ersetzen Sie partition durch den Partitionsnamen. • `http://host:port/Campaign/jsp/engage/engageHome.jsp` • `http://host:port/Campaign/api/campaign/rest/engage/offers` • `http://host:port/Campaign/api/campaign/rest/engage/offer` • `http://host:port/Campaign/servlet/EngageUpload` • `http://host:port/Campaign/api/campaign/rest/engageimportlist/partition`

Produkt oder Komponente	Objekte
	• `http://host:port/Campaign/api/campaign/rest/engageimportlist/partition/jobid` Diese URL dient zur Überprüfung des Status eines Importjobs. Ersetzen Sie jobid durch Ihre Job ID. • `http://host:port/Campaign/api/campaign/rest/engageimportlist/partition/schedule` • `http://host:port/Campaign/api/campaign/rest/engageimportlist/partition/channel/schedule` Diese URL dient zum Senden von Push- oder SMS-Nachrichten. Der Kanal ist entweder `sms` oder `push`.
Unica Journey	• `/journey/api/platformlogin` • `/journey/api/datadefinitions` • `/journey/api/entrysources` • `/journey/api/journeys` • `/journey/api/folders` • `/journey/api/permissions` • `/unica/api/manager/authentication/login` • `/unica/api/manager/user/user-details` • `/unica/api/manager/configuration/get` • `/unica/api/manager/policy/roles-permissions` • `/unica/api/manager/license/7` • `/unica/api/manager/datasource` • `/journey/api/thirdpartylogin`

Produkt oder Komponente	Objekte
Unica Collaborate	• /collaborate/affiniumcollaborate.jsp • /collaborate/services/CollaborateIntegrationServices1.0 • /collaborate/flowchartRunNotifyServlet • /collaborate/js/js_messages.jsp • /collaborate/js/format_symbols.jsp • /collaborate/alertsService
Unica Deliver	/Campaign/deliver/eventSinkServlet
Unica Interact	• /Campaign/interact/saveFlowchartAction.udo • /Campaign/interact/flowchartEventPatterns.udo • /Campaign/interact/testRunFlowchart.udo • /Campaign/interact/getProfileDataAction.udo • /Campaign/interact/manageIPB.udo • /Campaign/interact/flowchartRTAttrs.udo • /Campaign/initOfferListResolution.udo • /Campaign/getOfferListResolutionStatus.udo
Unica Plan	• /plan/errorPage.jsp • /plan/alertsService • /plan/services • /plan/services/collabService • /plan/services/PlanIntegrationServices/1.0 • /plan/affiniumplan.jsp • /plan/invalid_user.jsp • /plan/js/js_messages.jsp

Produkt oder Komponente	Objekte
	• `/plan/js/format_symbols.jsp` • `/unica/servlet/AJAXProxy` • `/plan/api/plan/flowchartApproval/flowchartApproval/validate`
Unica Optimize	• `/Campaign/optimize/ext_runOptimizeSession.do` • `/Campaign/optimize/ext_optimizeSessionProgress.do` • `/Campaign/optimize/ext_doLogout.do`
IBM SPSS Modeler Advantage Enterprise Marketing Management Edition	`/unica/rest/spssUser`
Unica Platform Datenfilter	`/unica/servlet/DataFiltering`
Unica Benachrichtigungen	• `unica/servlet/alertAJAXProxy` • `unica/notification/alertsCount`
Unica Scheduler	`/unica/servlet/SchedulerAPIServlet`

Aktivieren von Einzelabmeldungen mit SiteMinder

Damit eine Abmeldung von SiteMinder ermöglicht wird, wenn ein Benutzer sich bei einer Unica-Anwendung abmeldet, muss SiteMinder folgendermaßen konfiguriert sein:

1. Melden Sie sich am SiteMinder-Bereich **Richtlinienserver verwalten** an und setzen Sie die Eigenschaft `logoffUri` auf die URl der Unica-Anmeldeseite.

   Beispiel: `/sm_realm/unica/j_spring_security_logout`, wo *`sm_realm`* der Sicherheitsbereich von SiteMinder ist und `unica` die Kontext-Root Unica Platform ist.
2. Heben Sie den Schutz der Unica-Abmeldeseite `/unica/jsp/frameworklogout.jsp` auf, damit SiteMinder den Benutzer nicht zwingt, sich erneut anzumelden, um die Abmeldeseite anzuzeigen.

Aktivieren benutzerdefinierter Abmeldungen mit SiteMinder

Um benutzerdefinierte Abmeldungen mit SiteMinder zu aktivieren, setzen Sie `unica.sm.logouturl` unter `Affinium|suite|security|loginModes|siteMinderPartitionLogin`, indem Sie die folgenden Schritte ausführen.

1. Rufen Sie die Konfigurations-ID der verborgenen Konfiguration von Platform unica.sm.logouturl mithilfe der folgenden Abfrage ab.

   ```
   select ID from USM_CONFIGURATION where INTERNAL_NAME =
   'unica.sm.logouturl'
   ```
2. Aktualisieren Sie den Wert des Konfigurationselements unica.sm.logouturl:

   ```
   update USM_CONFIGURATION_VALUES set STRING_VALUE='<custom logout url>'
   where CONFIGURATION_ID=<ID obtained from above query>
   ```

Integrationsvoraussetzungen für IBM Security Access Manager

Die folgenden Voraussetzungen müssen erfüllt sein, um die Integration von Unica mit IBM Security Access Manager durchführen zu können.

- Die IBM Security Access Manager-WebSEAL-Junction muss so konfiguriert sein, dass der Benutzername (kurzer Name, nicht vollständig definierter Name) als HTTP-Variable in der URL-Anforderung an die Unica-Anwendung übergeben wird.
- Die Unica-Eigenschaft `Web access control header variable` muss auf den Namen der Variablen gesetzt sein, die Security Access Manager für Anmeldenamen verwendet.

Der Standardname der Variablen für den Security Access Manager-Anmeldenamen ist `iv-user`.

- Der IBM Security Access Manager-Richtlinienserver muss für die Verwendung von LDAP als Repository zum Speichern von Gruppenmitgliedern und Benutzerattributen konfiguriert sein.
- Die Unica-Anwendungs-URLs, die von einer WebSEAL-Verbindung definiert werden, und der Java™-Anwendungsserver, auf dem die Unica-Anwendung gehostet wird, müssen auf denselben Pfad verweisen.
- Alle Benutzer, die Zugriff auf Unica-Anwendungen haben, müssen einer Gruppe angehören, die einer Zugriffssteuerungsliste (Access Control List, ACL) mit entsprechenden Berechtigungen hinzugefügt wurde. Eine WebSEAL-Verbindung, die auf einen Anwendungsserver weist, auf dem Unica Platform bereitgestellt wird, muss dieser ACL zugeordnet sein.
- Um die grundlegenden Authentifizierung auf der ISAM-Konfiguration zu ignorieren, müssen Sie die Einstellung `Ignore HTTP Basic Authentication header` festlegen. Navigieren Sie zu **Junction Management -> <Edit Junction> -> Identität bearbeiten** und wählen Sie **Ignorieren** für HTTP-Basisauthentifizierungsheader aus.

Anmerkung: Wenn sich Benutzer bei einer Unica-Anwendung abmelden, werden sie nicht automatisch bei IBM Security Access Manager abgemeldet. Sie müssen den Browser nach der Abmeldung bei einer Unica-Anwendung schließen, um sich bei IBM Security Access Manager abzumelden.

Konfigurieren von IBM Security Access Manager für Unica-Produkte

Heben Sie den Schutz von IBM Security Access Manager-Objekten wie in dieser Prozedur beschrieben auf, um die korrekte Funktion Ihrer Unica-Produkte zu aktivieren.

1. Verwenden Sie Web Portal Manager, um sich bei der Domäne als Domänenadministrator anzumelden.
2. Klicken Sie auf **ACL > ACL erstellen**, füllen Sie die Felder **Name** und **Beschreibung** aus und klicken Sie auf **Anwenden**.
3. Klicken Sie auf **ACL > ACL auflisten** und auf der Seite 'ACLs verwalten', klicken Sie auf den Link für Ihre ACL-Richtlinien.
4. Auf der Seite 'ACL Eigenschaften' klicken Sie auf **Erstellen** und erstellen Sie folgendermaßen zwei Einträge für Ihre ACL.
    - Für den ersten Eintrag legen Sie den Eintragstyp auf **nicht authentifiziert** fest und erteilen die Berechtigungen **Trx - Traversieren, Lesen, Löschen und Ausführen**.
    - Für den zweiten Eintrag legen Sie den Eintragstyp auf **jede andere** fest und erteilen die Berechtigungen **Trx - Traversieren, Lesen, Löschen und Ausführen**.
5. Auf der Seite ACL-Eigenschaften der ACL, fügen Sie auf der Registerkarte Anhängen ungeschützte Objekte an, wie für Ihre Produktinstallationen erforderlich.

   Verwenden Sie den vollständigen Pfad in IBM Security Access Manager und beginnen Sie bei WebSEAL.

Table 46. Für Unica-Produkte erforderliche ungeschützte Objekte

Produkt oder Komponente	Objekte
Unica Campaign	• `/WebSEAL junction/Campaign/optimize/ext_runOptimizeSession.do` • `/WebSEAL junction/Campaign/optimize/ext_optimizeSessionProgress.do` • `/WebSEAL junction/Campaign/optimize/ext_doLogout.do` • `/WebSEAL junction/Campaign/interact/flowchartEventPatterns.udo` • `/WebSEAL junction/Campaign/interact/saveFlowchartAction.udo`

Produkt oder Komponente	Objekte
	• /WebSEAL junction/Campaign/interact/testRunFlowchart.udo • /WebSEAL junction/Campaign/interact/getProfileDataAction.udo • /WebSEAL junction/Campaign/interact/manageIPB.udo • /WebSEAL junction/Campaign/servlet/EngageUpload • /WebSEAL junction/Campaign/api/campaign/rest/engageimportlist/partition • /WebSEAL junction/Campaign/api/campaign/rest/engageimportlist/partition/schedule • /WebSEAL junction/Campaign/api/campaign/rest/engageimportlist/partition/channel/schedule • /WebSEAL junction/Campaign/interact/interactiveChannelSimulator.do • /WebSEAL junction/Campaign/interact/interactiveChannelOfferMapping.do • /WebSEAL junction/Campaign/services/CampaignServices30Service • /WebSEAL junction/Campaign/FlowchartNotifyScheduler • /WebSEAL junction/Campaign/OperationMonitor • /WebSEAL junction/Campaign/initOfferListResolution.udo • /WebSEAL junction/Campaign/getOfferListResolutionStatus.udo

Produkt oder Komponente	Objekte
	• /WebSEAL junction/Campaign/moveCampaignsSubmit.do • /WebSEAL junction/Campaign/interact/interactiveChannelStrategy.do • /WebSEAL junction/Campaign/api/interact/rest • /WebSEAL junction/Campaign/api/campaign/rest • /WebSEAL junction/Campaign/interact/flowchartRTAttrs.udo • /WebSEAL junction/Campaign/api/campaign/rest/ deepsearch/partition • /WebSEAL junction/Campaign/api/interact/rest/v2 • /WebSEAL junction/Campaign/api/interact/rest/v2/channels?page=0&size=1000 • /WebSEAL junction/journey/api/campaign • WebSEAL junction/Campaign/services/CampaignServices30Service • WebSEAL junction/Campaign/api/campaign/rest • WebSEAL junction/Campaign/FlowchartNotifyScheduler • WebSEAL junction/Campaign/initOfferListResolution.udo • WebSEAL junction/Campaign/getOfferListResolutionStatus.udo • WebSEAL junction/Campaign/OperationMonitor • WebSEAL junction/Campaign/api/campaign/rest • http://*host:port*/Campaign/api/campaign/rest/deepsearch/*partition* Ersetzen Sie Partition durch den Partitionsnamen.

Produkt oder Komponente	Objekte
	Wenn die Integration mit Engage implementiert wird, dann gilt Folgendes. In den folgenden URLs, ersetzen Sie partition durch den Partitionsnamen. • `http://host:port/Campaign/jsp/engage/engage-Home.jsp` • `http://host:port/Campaign/api/campaign/rest/engage/offers` • `http://host:port/Campaign/api/campaign/rest/engage/offer` • `http://host:port/Campaign/servlet/EngageU-pload` • `http://host:port/Campaign/api/campaign/rest/engageimportlist` • `http://host:port/Campaign/api/campaign/rest/engageimportlist/partition` • `http://host:port/Campaign/api/campaign/rest/engageimportlist/partition/jobid` Diese URL dient zur Überprüfung des Status eines Importjobs. Ersetzen Sie jobid durch Ihre Job ID. • `http://host:port/Campaign/api/campaign/rest/engageimportlist/partition/schedule` • `http://host:port/Campaign/api/campaign/rest/engageimportlist/partition/channel/schedule` Diese URL dient zum Senden von Push- oder SMS-Nachrichten. Der Kanal ist entweder `sms` oder `push`.

Produkt oder Komponente	Objekte
Unica Collaborate	• *WebSEAL junction*/collaborate/affiniumcollaborate.jsp • *WebSEAL junction*/collaborate/services/CollaborateIntegrationServices1.0 • *WebSEAL junction*/collaborate/flowchartRunNotifyServlet • *WebSEAL junction*/collaborate/js/js_messages.jsp • *WebSEAL junction*/collaborate/js/format_symbols.jsp • *WebSEAL junction*/collaborate/alertsService
Unica Journey	• /WebSEAL/<instance name>/<junction name>/journey/api/platformlogin • /WebSEAL/<instance name>/<junction name>/journey/api/datadefinitions • /WebSEAL/<instance name>/<junction name>/journey/api/entrysources • /WebSEAL/<instance name>/<junction name>/journey/api/journeys • /WebSEAL/<instance name>/<junction name>/journey/api/folders • /WebSEAL/<instance name>/<junction name>/journey/api/permissions • /WebSEAL/<instance name>/<junction name>/unica/api/manager/authentication/login • /WebSEAL/<instance name>/<junction name>/unica/api/manager/user/user-details • /WebSEAL/<instance name>/<junction name>/unica/api/manager/configuration/get

Produkt oder Komponente	Objekte
	• /WebSEAL/<instance name>/<junction name>/unica/api/manager/policy/roles-permissions • /WebSEAL/<instance name>/<junction name>/unica/api/manager/license/7 • /WebSEAL/<instance name>/<junction name>/unica/api/manager/datasource • /WebSEAL/<instance name>/<junction name>/journey/api/thirdpartylogin
Unica Deliver	*WebSEAL junction*/Campaign/deliver/eventSink-Servlet
Unica Interact	• *WebSEAL junction*/Campaign/interact/flow-chartEventPatterns.udo • *WebSEAL junction*/Campaign/interact/saveFlow-chartAction.udo • *WebSEAL junction*/Campaign/interact/testRun-Flowchart.udo • *WebSEAL junction*/Campaign/interact/getPro-fileDataAction.udo • *WebSEAL junction*/Campaign/interact/manageIP-B.udo • *WebSEAL junction*/Campaign/initOfferListReso-lution.udo • *WebSEAL junction*/Campaign/getOfferListReso-lutionStatus.udo • *WebSEAL junction*/Campaign/interactiveChan-nelOfferMapping.do • *WebSEAL junction*/Campaign/interactiveChan-nelStrategy.do

Produkt oder Komponente	Objekte
	• `WebSEAL junction/Campaign/interact/interactiveChannelOfferMapping.do` • `WebSEAL junction/Campaign/FlowchartNotifyScheduler` • `WebSEAL junction/Campaign/OperationMonitor` • `WebSEAL junction/Campaign/initOfferListResolution.udo` • `WebSEAL junction/Campaign/getOfferListResolutionStatus.udo` • `WebSEAL junction/interact/servlet/InteractJSService` • `WebSEAL junction/interact/servlet/RestServlet` • `WebSEAL junction/interact/services/InteractService` • `WebSEAL junction/Campaign/api/campaign/rest` • `WebSEAL junction/Campaign/moveCampaignsSubmit.do` • `WebSEAL junction/Campaign/interact/flowchartRTAttrs.udo` • `WebSEAL junction/Campaign/interact/interactiveChannelStrategy.do` • `WebSEAL junction/Campaign/api/interact/rest`
Unica Plan	• *`WebSEAL junction`*`/plan/services` • *`WebSEAL junction`*`/plan/errorPage.jsp` • *`WebSEAL junction`*`/plan/alertsService` • *`WebSEAL junction`*`/plan/services/collabService` • *`WebSEAL junction`*`/plan/services/PlanIntegrationServices/1.0` • *`WebSEAL junction`*`/plan/affiniumplan.jsp`

Produkt oder Komponente	Objekte
	• *WebSEAL junction*/plan/invalid_user.jsp • *WebSEAL junction*/plan/js/js_messages.jsp • *WebSEAL junction*/plan/js/format_symbols.jsp • *WebSEAL junction*/unica/servlet/AJAXProxy • *WebSEAL junction*//plan/api/plan/flowchartApproval/flowchartApproval/validate
Unica Optimize	• *WebSEAL junction*/Campaign/optimize/ext_runOptimizeSession.do • *WebSEAL junction*/Campaign/optimize/ext_optimizeSessionProgress.do • *WebSEAL junction*/Campaign/optimize/ext_doLogout.do
IBM SPSS Modeler Advantage Enterprise Marketing Management Edition	*WebSEAL junction*/unica/rest/spssUser
Unica Platform Datenfilter	*WebSEAL junction*/unica/servlet/DataFiltering.
Unica Benachrichtigungen	• *WebSEAL junction*/unica/servlet/DataFiltering • *WebSEAL junction*/unica/servlet/alertAJAXProxy • *WebSEAL junction*/unica/notification/alertsCount
Unica Scheduler	*WebSEAL junction*/unica/servlet/SchedulerAPIServlet

Produkt oder Komponente	Objekte
Aktivieren Sie eine Abmeldung von IBM Security Access Manager, wenn ein Benutzer sich bei einer Unica-Anwendung abmeldet.	• *WebSEAL junction*/unica/j_spring_security_logout • *WebSEAL junction*/unica/jsp/frameworklogout.jsp
Unica Platform	*WebSEAL junction*WebSEAL junction/unica/css/access_control.css

Roadmap für den Konfigurationsprozess: Unica mit einer Webzugriffssteuerung integrieren

Verwenden Sie diese Roadmap für den Konfigurationsprozess, um die Aufgaben zu suchen, die zur Integration von Unica mit einem System zur Webzugriffskontrolle erforderlich sind. Die Spalte „Abschnitt“ stellt Links zu den Themen bereit, in denen die Aufgaben ausführlich beschrieben werden.

Tabelle 47. Roadmap für den Konfigurationsprozess: Unica mit einer Webzugriffssteuerung integrieren

Topic	Informationen
Ausführen der LDAP-Integration *(auf Seite 224)*	Führen Sie die Anweisungen zur LDAP-Integration bis zum Schritt „Testen der Synchronisation“ aus.
Festlegen der Verbindungseigenschaften für Webzugriffskontrolle	Legen Sie Eigenschaften für die Integration in ein Webzugriffskontrollsystem auf der Seite „Konfiguration“ fest.

Tabelle 47. Roadmap für den Konfigurationsprozess: Unica mit einer Webzugriffssteuerung integrieren (Fortsetzung)

Topic	Informationen
in Unica *(auf Seite 224)*	
Erneutes Starten des Webanwendungsservers *(auf Seite 188)*	Dieser Schritt ist erforderlich, um zu gewährleisten, dass sämtliche Ihrer Änderungen angewandt werden.
Testen der Synchronisation der Webzugriffskontrolle und der Unica-Anmeldung *(auf Seite 226)*	Überprüfen Sie, ob Benutzer und Gruppen ordnungsgemäß im Webzugriffskontrollsystem synchronisiert werden und ob Sie sich an Unica anmelden können.

Ausführen der LDAP-Integration

Hier finden Sie die Schritte, die zur LDAP-Integration erforderlich sind.

Festlegen der Verbindungseigenschaften für Webzugriffskontrolle in Unica

Sie müssen einige Konfigurationseigenschaften festlegen, um die Integration der Webzugriffskontrolle zu konfigurieren.

Legen Sie auf der Seite **Einstellungen & Konfiguration** die Werte der Eigenschaften anhand der Beschreibung in der folgenden Tabelle fest.

Informationen zum Festlegen der einzelnen Eigenschaften finden Sie in den zugehörigen Referenzinformationen.

Tabelle 48. Eigenschaften zum Konfigurieren der Integration der Webzugriffskontrolle

Eigenschaften	Wert
Unica | Unica Platform | Sicherheit | Details zum Anmeldeverfahren	Wählen Sie `Webzugriffssteuerung` aus.
Unica | Unica Platform | Sicherheit | Details zur Anmeldemethode | Web-Zugriffskontrolle | Zusätzliche Kopfzeilenvariablen	Die angegebenen kommagetrennten Variablen werden im HTTP-Header gesucht, während Sie sich durch die Web-Zugriffskontrollsoftware anmelden. Wenn das Prüfprotokoll aktiviert ist, werden diese Variablen erfasst und im Authentifizierungsereignis unter Prüfprotokollen gespeichert. Die erfassten HTTP-Variablen können angezeigt werden, indem Sie unter "Ereignisdetails" auf "Mehr" klicken. **Anmerkung:** Diese Eigenschaft ist ab Version 12.1.0.3 verfügbar.
Unica | Unica Platform | Sicherheit | Details zum Anmeldeverfahren | Webzugriffskontrolle | Benutzernamenstruktur	Ein regulärer Java™-Ausdruck, mit dem die Benutzeranmeldedaten aus der HTTP-Kopfzeilenvariablen der für die Webzugriffskontrolle verwendeten Software extrahiert werden. Sie müssen für alle XML-Zeichen im regulären Ausdruck XML-Escape-Zeichen verwenden. Der empfohlene Wert für SiteMinder und IBM Security Access Manager ist `\w*`
Unica | Unica Platform | Sicherheit | Details zum Anmeldeverfahren | Webzugriffskontrolle | Kopfzeilenvariable für Webzugriffskontrolle	Die in der Software zur Steuerung des Webzugriffs konfigurierte HTTP-Kopfzeilenvariable, die an den Webanwendungsserver übermittelt wird. Standardmäßig verwendet SiteMinder `sm_user` und IBM Security Access Manager `iv-user`. Legen Sie für IBM Security Access Manager für diesen Wert die Benutzernamenkomponente der IBM® Raw-Zeichenfolge fest und nicht die IBM® HTTP-Zeichenfolge.

Eigenschaften	Wert
URL für Unica | Allgemeines | Navigation | Unica Platform	Legen Sie diesen auf `http://sm_host:sm_port/sm_realm/unica` fest Dabei gilt Folgendes • *sm_host* ist der Name oder die IP-Adresse des Computers, auf dem SiteMinder installiert ist. • *sm_port* ist die SiteMinder-Portnummer • *sm_realm* ist der SiteMinder-Bereich

Erneutes Starten des Webanwendungsservers

Starten Sie den Webanwendungsserver neu, um zu gewährleisten, dass sämtliche Ihrer Konfigurationsänderungen angewandt werden.

Testen der Synchronisation der Webzugriffskontrolle und der Unica-Anmeldung

Mit dieser Prozedur können Sie die Integration testen.

1. Melden Sie sich mit einem LDAP-Konto am System zur Webzugriffskontrolle an, das im System zur Webzugriffskontrolle synchronisiert wurde und Zugriff auf Unica Platform hat.
2. Prüfen Sie Folgendes:
   - Benutzer werden wie erwartet importiert.
   - Gruppen werden wie erwartet importiert.
   - Unica Gruppenmitgliedschaften entsprechen der erwarteten Zuweisung zu LDAP Gruppen.
3. Navigieren Sie mit Ihrem Browser zur URL von Unica Platform, und melden Sie sich an.

   Sie sollten auf Unica zugreifen können, ohne dass die Anmeldeanzeige von Unica angezeigt wird.
4. Lösen von Problemen mit der Software zur Steuerung des Webzugriffs Netegrity SiteMinder gehen Sie nach den folgenden Anweisungen vor.

- Wenn eine Unica-Anmeldeanzeige angezeigt wird, wurde das zur Anmeldung verwendete Benutzerkonto möglicherweise nicht in SiteMinder synchronisiert.
- Wenn Sie nicht auf Unica zugreifen können, überprüfen Sie die Richtigkeit der SiteMinder-Konfiguration. Mithilfe von SiteMinder TestTool können Sie überprüfen, ob das zur Anmeldung verwendete Benutzerkonto autorisiert wurde und ob ihm Zugriff auf Unica-URLs in SiteMinder gewährt wurde.
- Wenn Sie auf Unica zugreifen können, aber die Navigation nicht richtig funktioniert oder Bilder nicht angezeigt werden, überprüfen Sie, ob der Webserver, auf dem SiteMinder gehostet wird, und der Java™ Anwendungsserver, auf dem Unica Platform gehostet wird, verwenden den gleichen Pfad, um auf Unica Platform zu verweisen.

Überprüfen Sie zusätzliche Header in den Prüfprotokollen

Stellen Sie sicher, dass die Prüfprotokolle aktiviert sind. Unter der Eigenschaft 'Webzugriffssteuerung| Zusätzliche Header Variablen', geben Sie die Namen der HTTP Header Variablen an, die erfasst werden sollen. Nach erfolgreicher Anmeldung, überprüfen Sie die Berichte der Prüfereignisse und die Ereignisdetails auf erfasste Variablen.

Konfigurieren der Integration mit SSL-Typ „WebSEAL-Junction“

Befolgen Sie die hier aufgeführte Prozedur, um die Unica Platform-Integration mit IBM Security Access Manager mit dem SSL-Typ „WebSEAL-Junction“ zu konfigurieren.

Detaillierte Informationen zu diesen Prozeduren finden Sie in der Dokumentation, die mit IBM Security Access Manager und Ihrem Webanwendungsserver bereitgestellt wird.

1. Generieren Sie SSL-Zertifikate oder erwerben Sie sie und konfigurieren Sie dann den Webanwendungsserver für die Verwendung dieser Zertifikate.
2. Erstellen Sie ein WebSEAL-Zertifikat und konfigurieren Sie IBM Security Access Manager zu seiner Verwendung.
3. Importieren Sie Ihr WebSEAL-Zertifikat in Ihren Webanwendungsserver.
4. Importieren Sie das Zertifikat Ihres Webanwendungsservers in IBM Security Access Manager.

5. Erstellen Sie den SSL-Typ „WebSEAL-Junction“ in IBM Security Access Manager.

   Wenn Sie mehrere Unica-Produkte installieren, dann erstellen Sie eine separate Junction für jedes Produkt.
6. Legen Sie für jedes installierte Produkt die Konfigurationseigenschaft für die Navigations-URL auf der Seite **Einstellungen & Konfiguration** fest.

   Der Wert muss die WebSEAL-Junction angeben, die für dieses Produkt verwendet wird. Verwenden Sie das folgende Muster:

   `https://machine_name_or_IP_address.domain_name:port_number/webSEAL_junction/context-root`

   Verwenden Sie für den Zugriff auf Unica eine wie folgt definierte URL:

   `https://machine_name_or_IP_address.domain_name:port_number/webSEAL_junction//unica`
7. Ungeschützte URLs in IBM Security Access Manager werden an anderer Stelle in diesem Handbuch beschrieben.

Alert- und Benachrichtigungsmanagement

Unica Platform stellt Support für Systemalerts und Benutzerbenachrichtigungen bereit, die von Unica-Produkten gesendet werden.

Von Produkten gesendete Systemalerts und Benutzerbenachrichtigungen werden an der Benutzeroberfläche folgendermaßen angezeigt.

- **Alerts** enthalten Informationen über Systemereignisse. Sie werden bei der Benutzeranmeldung in einem Popup-Fenster angezeigt.

  Beispiele sind ein geplantes oder ungeplantes Herunterfahren von Servern.
- **Benachrichtigungen** enthalten benutzerspezifische Informationen über Änderungen, die an Elementen vorgenommen werden, die für den Benutzer von Interesse sind, oder

über vom Benutzer auszuführende Aufgaben. Der Benutzer kann sie anzeigen, indem er auf das Umschlagsymbol oben rechts im Fenster klickt.

Dabei kann es sich z. B. um Aktualisierungen für Ablaufdiagramme oder Mailing-Listen oder um eine Erinnerung an den Stichtag für eine zugewiesene Aufgabe handeln.

Benutzer können auch den Erhalt von Alerts und Benachrichtigungen per E-Mail abonnieren, wenn Unica Platform für den Versand konfiguriert ist.

Innerhalb von Unica Platform verwendet Unica Scheduler die Benachrichtigungsfunktion.

Alert- und Benachrichtigungsabonnements

Benutzer können Systemalerts und Benachrichtigungen auch per E-Mail erhalten, wenn Unica Platform für den Versand konfiguriert ist. Sie können auch die Abonnementebene auswählen.

Beispielsweise können Sie auswählen, nur kritische Systemalerts und alle Benachrichtigungen zu erhalten. Die Abonnementsebenen unterscheiden sich je nach Produkt, das die Systemalerts und Benachrichtigungen sendet.

Anmerkung: Alle Systemalerts werden immer in Popup-Fenstern bereitgestellt, wenn sich der Benutzer an Unica anmeldet. Benutzer können dies nicht ändern, indem sie ihr Abonnement ändern.

Wenn sich Benutzer bei Unica anmelden, wird das Fenster **Systemalerts** nur angezeigt, wenn neue oder ungelesene Alerts vorliegen. Benutzer können einen Alert als gelesen markieren, indem Sie den Alert auswählen und im Fenster **Systemalerts** auf **Als gelesen markieren** klicken.

Festlegen von Systemalert- und Benachrichtigungsabonnements

Benutzer ohne Administratorrechte können mit diesem Verfahren eigene Abonnements für Systemalerts und Benachrichtigungen festlegen.

1. Melden Sie sich bei Unica an und wählen Sie `Einstellungen > Benutzer`.

   Die Seite mit Ihren Kontodetails wird geöffnet.
2. Klicken Sie auf der Seite mit Ihren Kontodetails auf **Benachrichtigungsabonnement**.
3. Wählen Sie mithilfe der Kontrollkästchen die Ebene der Benachrichtigungen aus, die Sie erhalten möchten. Wählen Sie zudem aus, ob Sie die Benachrichtigungen auf der Benutzeroberfläche, per E-Mail, über beide Optionen oder überhaupt nicht erhalten möchten.
4. Klicken Sie auf **Abschicken**, um Ihre Änderungen zu speichern.

Konfigurieren von E-Mail-Benachrichtigungen in Unica

Führen Sie dieses Verfahren aus, um Unica Platform für das Senden von Systemalert- und Benachrichtigungs-E-Mails an Benutzer zu konfigurieren. Vor dem Start muss ein E-Mail-Server eingerichtet worden sein.

Besorgen Sie sich die folgenden Informationen über den E-Mail-Server.

- Das vom E-Mail-Server verwendete Protokoll
- Der vom E-Mail-Server überwachte Port
- Der Name der Maschine, die Ihren E-Mail-Server hostet
- Ob für Ihren E-Mail-Server eine Authentifizierung erforderlich ist
- Wenn für Ihren Mail-Server eine Authentifizierung erforderlich ist, Kontoname und Kennwort auf dem Mail-Server

Tipp: Benötigen Sie zusätzliche Details zur Ausführung dieses Verfahrens, sehen Sie sich die zugehörigen Referenzen an.

1. Wenn für Ihren E-Mail-Server eine Authentifizierung erforderlich ist, speichern Sie den Namen und das Kennwort eines Mail-Server-Kontos als Datenquelle in einem Unica Platform-Benutzerkonto.

   Verwenden Sie ein internes Unica Platform-Benutzerkonto und keinen von einem LDAP-Server importierten Benutzer.

Notieren Sie sich den Unica Platform-Benutzernamen und den Datenquellennamen, da Sie diese Namen in Schritt 3 benötigen.

2. Melden Sie sich bei Unica als Benutzer mit Administratorberechtigungen in Unica Platform an.
3. Legen Sie auf der Seite **Einstellungen > Konfiguration** die Konfigurationseigenschaften in den folgenden Kategorien fest.
    - `Allgemein | Kommunication | E-mail`
    - `Platform | Benachrichtigungen`

    Verwenden Sie die Informationen, die Sie über Ihren E-Mail-Server erhalten haben, um Werte festzulegen.

Implementierung von unidirektionalem SSL

In diesem Abschnitt wird unidirektionales SSL in Unica beschrieben.

Die gesamte Kommunikation, die sicher zwischen zwei über ein Netz verbundenen Anwendungen ablaufen soll, kann über das SSL-Protokoll (Secure Sockets Layer) stattfinden.

SSL stellt auf folgende Weise sichere Verbindungen bereit:

- Eine Anwendung kann die Identität einer anderen Anwendung authentifizieren.
- Mit einem privaten Schlüssel können über die SSL-Verbindung übertragene Daten verschlüsselt und entschlüsselt werden.

Wenn Anwendungen für SSL konfiguriert werden, dann findet der Webdatenverkehr nicht mehr über HTTP, sondern über HTTPS statt. Diese Änderung wird in den URLs angezeigt.

Wenn eine Kommunikation zwischen Prozessen stattfindet, agiert der Prozess, der eine Anforderung sendet, als Client. Der Prozess, der auf die Anforderung antwortet, agiert als Server. Im Interesse einer lückenlosen Sicherheit sollte SSL für alle Arten der Kommunikation mit Unica-Produkten implementiert werden.

SSL kann unidirektional oder bidirektional konfiguriert werden. Mit unidirektionalem SSL muss der Server ein Zertifikat für den Client vorweisen. Der Client benötigt jedoch kein Zertifikat für den Server. Damit die SSL-Verbindung erfolgreich zustande kommt, muss

der Client den Server authentifizieren. Der Server akzeptiert eine Verbindung von einem beliebigen Client.

Übersicht über SSL-Zertifikate

Lesen Sie diesen Abschnitt, um allgemeine Informationen über SSL-Zertifikate zu erhalten.

Was ist ein Zertifikat?

Ein Zertifikat ist eine digitale Signatur, die den Server als benannte Entität identifiziert. Zertifikate können von einer Zertifizierungsstelle (CA) signiert werden, die für die Identität des Servers garantiert, oder sie können selbstsigniert sein. VeriSign oder Thawte sind Beispiele für Zertifizierungsstellen. Ein selbst signiertes Zertifikat ist ein Zertifikat, bei dem die Zertifizierungsstelle mit der Entität, die das Zertifikat identifiziert, übereinstimmt.

Serverseitige Zertifikate

Jeder Server, der SSL-Kommunikation bereitstellen soll – unabhängig davon, ob es sich um einen Anwendungsserver oder um eine Unica-Anwendung, wie beispielsweise den Unica Campaign-Listener, handelt – muss ein Zertifikat vorweisen können.

Clientseitige Truststores

Wenn der Client das Zertifikat des Servers empfängt, muss der Client bestimmen, ob das Zertifikat vertrauenswürdig ist. Ein Client stuft das Zertifikat eines Servers automatisch als vertrauenswürdig ein, wenn es im Truststore (Vertrauensspeicher) des Clients gespeichert ist. Ein Truststore ist eine Datenbank mit den Zertifikaten, die als vertrauenswürdig eingestuft werden.

Moderne Browser verfügen über einen Truststore, in dem allgemeine, von CAs bestätigte Zertifikate gespeichert sind. Deshalb erfolgt keine Nachfrage, wenn Sie die gesicherte Webseite größerer Onlinehändler öffnen, da dort CA-signierte Zertifikate verwendet werden. Wenn ein Benutzer sich jedoch bei einer HCL-Anwendung anmeldet, die ein selbst signiertes Zertifikat vorweist, erhält er eine Nachfrage.

Beachten Sie, dass Browser überprüfen, ob der Hostname des Servers mit dem Anforderernamen des Zertifikats übereinstimmt. (Der Anforderername ist der allgemeine

Name, der im definierten Namen verwendet wird, den sie bei der Anforderung eines Zertifikats angeben). Möglicherweise zeigt der Browser eine Warnung an, wenn diese beiden Namen nicht übereinstimmen.

Wenn ein Browser auf eine HCL-Anwendung zugreift, die über ein nicht erkanntes Zertifikat verfügt (z.B. ein selbst signiertes Zertifikat), wird ein Dialogfenster geöffnet, in dem der Benutzer gefragt wird, ob der Vorgang fortgesetzt werden soll. Wenn der Benutzer das Zertifikat im lokalen Truststore installiert, wird diese Nachfrage nicht wieder angezeigt.

Client- und Serverrollen in Unica

Unica-Anwendungskomponenten können bei einer Kommunikation je nach Situation als Client oder Server agieren.

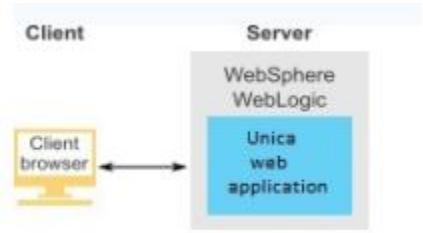
Die meisten Unica-Anwendungen bestehen aus zwei Teilen.

- Die Webanwendung. Dies ist die Komponente, auf die Benutzer über einen Browser zugreifen.
- Der Server (z.B. der Unica Campaign-Listener und der Unica Platform-API-Server). Auf diese Komponente wird programmgesteuert zugegriffen.

Folgende Beispiele und Diagramme veranschaulichen die Rollen, die HCL-Komponenten in verschiedenen Kommunikationssituationen spielen.

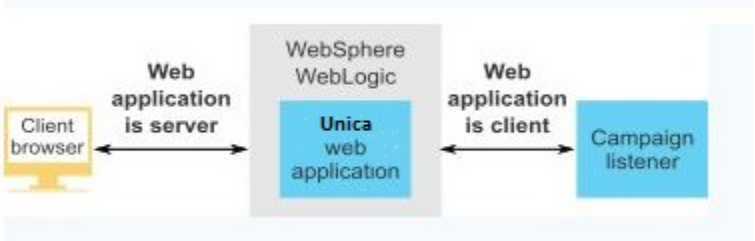
Beispiel 1 - Kommunikation zwischen einem Browser und einer Unica Webanwendung

Wenn Benutzer mit Unica Webanwendungen über einen Browser kommunizieren, agiert der Browser als Client und die Unica-Webanwendung als Server.



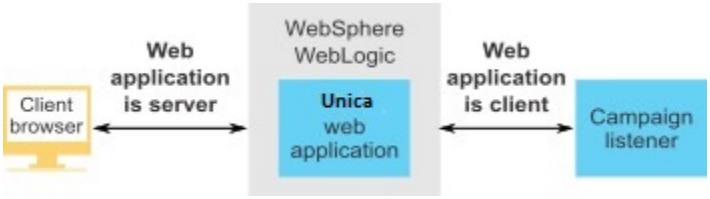
Beispiel 2: Kommunikation zwischen den Komponenten einer Unica Anwendung

Die zwei Komponenten einer einzelnen Unica-Anwendung können auch programmgesteuert miteinander kommunizieren. Wenn z. B. von der Unica Campaign-Webanwendung eine Anforderung an einen Unica Campaign-Listener gesendet wird, agiert die Unica Campaign-Webanwendung als Client und der Listener als Server.



Beispiel 3: Unica-Komponenten übernehmen beide Rollen

Eine Unica-Anwendungskomponente kann in einigen Kommunikationssituationen als Client und in anderen als Server agieren. Im folgenden Diagramm finden Sie ein Beispiel für diese Beziehungen.



SSL in Unica

Viele -Anwendungskomponenten können bei normalen Operationen als Server und Client agieren. Einige -Komponenten sind in Java™ und einige in C++ geschrieben. Diese Tatsache bestimmt, wie die Zertifikate implementiert werden müssen. Sie geben das Format an, wenn Sie ein selbst signiertes Zertifikat erstellen oder von einer Zertifizierungsstelle erwerben.

Für Anwendungen ist kein Truststore erforderlich, wenn sie als Client agieren und unidirektionale SSL-Anforderungen an eine Serverkomponente senden.

Java™ Komponente als Server

Bei in Java™ geschriebenen -Anwendungen, welche die JSSE-SSL-Implementierung verwenden und auf einem Anwendungsserver implementiert sind, müssen Sie den Anwendungsserver so konfigurieren, dass das Zertifikat verwendet werden kann. Das Zertifikat muss im JKS-Format gespeichert werden.

Das mit dem Anwendungsserver bereitgestellte Standardzertifikat kann nicht verwendet werden.

Sie können JKS-Zertifikate für Ihre Java-Anwendungen mit dem Java-Tool „keytool“ erstellen.

C++-Komponente als Server

Der Campaign Listener und die Optimize Serverkomponente, ist in C ++ geschrieben und erfordert ein von OpenSSL generiertes Zertifikat.

Java™ Komponente als Client

Bei -Anwendungen, die in Java™ geschrieben und auf einem Anwendungsserver implementiert werden, ist kein Truststore erforderlich. Zur Vereinfachung der Konfiguration findet bei Java™-Anwendungen, die als Client agieren, keine Authentifizierung des Servers während einer unidirektionalen SSL-Kommunikation statt. Es erfolgt jedoch eine Verschlüsselung.

C/C++-Komponente als Client

Bei Anwendungen, die in C/C++ geschrieben wurden und die eine OpenSSL-Implementierung verwenden, ist kein Truststore erforderlich. Der Campagin-Listener fällt unter diese Kategorie.

Wie viele Zertifikate?

Im Idealfall sollte für jeden Computer, auf dem eine Komponente als Server agiert, ein anderes Zertifikat verwendet werden.

Wenn Sie nicht mehrere Zertifikate verwenden möchten, können Sie dasselbe Zertifikat für alle Komponenten verwenden, die als Server agieren. Wenn Sie ein Zertifikat für alle Anwendungen verwenden, werden Benutzer beim ersten Zugriff auf Anwendungen vom Browser gefragt, ob das Zertifikat akzeptiert werden soll.

Roadmap für den Konfigurationsprozess: SSL implementieren in Unica

Verwenden Sie diese Roadmap für den Konfigurationsprozess, um die Aufgaben zu suchen, die zur Implementierung von SSL in Unica erforderlich sind. Die Spalte „Abschnitt“ stellt Links zu den Themen bereit, in denen die Aufgaben ausführlich beschrieben werden.

Tabelle 49. Roadmap für den Konfigurationsprozess: SSL implementieren in Unica

Topic	Informationen
Erhalten oder Erstellen von Zertifikaten *(auf Seite)*	Wenn Sie nicht die von HCL und Ihrem Anwendungsserver bereitgestellten Standardzertifikate verwenden möchten, müssen Sie Zertifikate abrufen oder erstellen.
Konfigurieren Sie Ihren Webanwendungsserver für SSL *(auf Seite 247)*	Aktivieren Sie einen SSL-Port in jedem Anwendungsserver, auf dem eine HCL-Anwendung bereitgestellt wird. Falls Sie nicht das Standardzertifikat des Anwendungsservers verwenden, konfigurieren Sie ihn so, dass er Ihr Zertifikat nutzt.
HCL Unica für SSL konfigurieren *(auf Seite 248)*	Legen Sie Konfigurationseigenschaften in Unica fest.

Tabelle 49. Roadmap für den Konfigurationsprozess: SSL implementieren in Unica (Fortsetzung)

Topic	Informationen
Überprüfen der SSL-Konfiguration *(auf Seite 263)*	Melden Sie sich an den einzelnen Unica-Anwendungen an.

Zertifikate für SSL

In der vorliegenden Prozedur wird beschrieben, wie eigene Zertifikate erstellt und konfiguriert werden können. Führen Sie eine für jedes Unica-System, das Sie zur Verwendung von SSL konfigurieren, die folgende Prozedur aus. Wenn Sie die Unica Campaign- und Engage-Integration konfigurieren, dann lesen Sie die Informationen im Unica Campaign und Engage-Integrationshandbuch für IBM Marketing Cloud.

Es gibt mehrere Möglichkeiten, Zertifikate anzufordern oder zu erstellen. Sie können selbst signierte Zertifikate erstellen oder Zertifikate von einer Zertifizierungsstelle (Certificate Authority, CA) beziehen.

Selbst signierte Zertifikate

Sie können selbst signierte Zertifikate erstellen.

Für C++-Komponenten, die als Server benutzt werden, verwenden Sie openSSL, um ein `.pem`-Zertifikat zu erstellen. Der Campaign-Listener implementiert SSL mithilfe der HCL openSSL-Bibliothek. openSSL wird mit Campaign installiert und umfasst ein Befehlszeilenprogramm mit dem Namen `openSSL`, das eine Zertifikatsdatei erstellen kann.

Für Java-Komponenten, die als Server benutzt werden, verwenden Sie das Java-Tool „keytool“, um ein JKS-Zertifikat zu erstellen.

Zertifikate von der Zertifizierungsstelle

Sie können Zertifikate von einer Zertifizierungsstelle (CA = Certificate Authority) beziehen.

Sie können openSSL zum Erstellen von Anforderungen verwenden, die Sie dann an eine Zertifizierungsstelle senden können, um signierte Zertifikate zu erstellen. Oder Sie können signierte Zertifikate abrufen, die in vollständiger Form von CA bereitgestellt werden.

Anweisungen zum Abrufen eines signierten Zertifikats finden Sie in der Dokumentation der Zertifizierungsstelle.

Erhalten oder Erstellen von Zertifikaten

Gehen Sie wie folgt vor, um selbst signierte Zertifikatsdateien zu erstellen und mit HCL Unica zu verwenden.

1. Erstellen Sie ein Zertifikat für C++ HCL Unica-Anwendungskomponenten.
2. Erstellen Sie ein Zertifikat für C++ Java Unica-Anwendungskomponenten.

Erstellen Sie ein Zertifikat für C++ HCL Unica-Anwendungskomponenten.

Der Campaign-Listener implementiert SSL mithilfe der OpenSSL-Bibliothek. Die OpenSSL-Verteilung beinhaltet ein Befehlszeilenprogramm namens `openssl`, mit dem eine Zertifikatdatei erstellt werden. Einzelheiten zur Verwendung dieses Programms finden Sie in der OpenSSL-Dokumentation. Sie können die Hilfe auch aufrufen, indem Sie bei der Ausführung des Programms `-help` eingeben.

Führen Sie die folgenden Schritte aus, um ein selbst signiertes Zertifikat zu erstellen und eine C++ HCL Unica-Komponente für SSL zu konfigurieren.

1. Führen Sie `openssl` in der Befehlszeile aus. Dieses Programm und die zugehörige Konfigurationsdatei `openssl.cnf` sind im Verzeichnis bin der Campagin-Installation enthalten. Es steht außerdem in der OpenSSL-Verteilung zur Verfügung.
2. Generieren Sie einen Schlüssel. Hier ist ein Beispiel für einen Befehl, der einen Schlüssel namens `key.pem` erstellt.

   ```
   set OPENSSL_CONF=CAMPAIGN_HOME\bin\openssl.cnf

   openssl genrsa -out key.pem 4096
   ```

3. Generieren Sie eine Anfrage. Hier ist ein Beispiel für einen Befehl, der einen Schlüssel namens `request.pem` erstellt.

```
openssl req -config openssl.cnf -new -key key.pem -out request.pem
```

Das Tool stellt Ihnen einige Fragen. Wenn Sie einen Punkt (.) eingeben, bleibt das Feld leer. Für ein selbst signiertes Zertifikat müssen Sie zumindest den allgemeinen Namen (Common Name) eingeben.

Wenn Sie das Tool openssl aus dem Verzeichnis `Campaign/bin` verwenden, fügen Sie den Parameter `-config` mit einem Wert hinzu, der auf die Datei `openssl.cnf` im gleichen Verzeichnis verweist. Zum Beispiel: `openssl req -config openssl.cnf -x509 -key key.pem -in request.pem -days 1000 -out certificate.pem`

4. Generieren Sie ein Zertifikat. Mit dem folgenden Befehl wird ein Zertifikat namens `certificate.pem` erstellt, das eine Gültigkeit von 10.000 Tagen ab dem Erstellungsdatum hat. Dabei werden die Dateien `request.pem` und `key.pem` verwendet.

   ```
   openssl req -x509 -key key.pem -in request.pem -days 10000 -out certificate.pem
   ```

   Wenn Sie das Tool openssl aus dem Verzeichnis `Campaign/bin` verwenden, fügen Sie den Parameter `-config` mit einem Wert hinzu, der auf die Datei `openssl.cnf` im gleichen Verzeichnis verweist. Zum Beispiel:

   ```
   openssl req -config openssl.cnf -x509 -key key.pem -in request.pem -days 10000 -out certificate.pem
   ```

5. Erstellen Sie ein neues Beispiel für eine Zertifikatsdatei campaign.pem.
6. Kopieren Sie den Inhalt von key.pem und certificate.pem in diese durch eine neue Zeile getrennte Datei.

Erstellen Sie ein Zertifikat für Java HCL Unica-Komponenten.

HCL Unica-Webanwendungskomponenten, die in Java geschrieben sind, verwenden die JSSE-Bibliothek. Der Sun-JDK umfasst ein Programm namens `keytool`, mit dem eine Zertifikatdatei erstellt werden kann. Einzelheiten zur Verwendung dieses Programms finden Sie in der Java-Dokumentation. Sie können die Hilfe auch aufrufen, indem Sie bei der Ausführung des Programms `-help` eingeben.

Führen Sie die folgenden Schritte aus, um ein selbst signiertes Zertifikat zu erstellen und eine Java HCL Unica-Komponente für SSL zu konfigurieren.

1. Führen Sie `keytool` in der Befehlszeile aus. Dieses Programm befindet sich im Verzeichnis bin des Sun Java-JDK.
2. Erstellen Sie einen Identity-Keystore. Mit dem folgenden Beispielbefehl wird ein vertrauenswürdiger Keystore namens `UnicaClientIdentity.jks` erstellt.

   ```
   keytool -genkey -alias UnicaClientIdentity -keyalg RSA -keystore UnicaClientIdentity.jks -keypass clientPwd -validity 1000 -dname "CN=hostName, O=myCompany" -storepass clientPwd
   ```

   Beachten Sie Folgendes:
   - Notieren Sie sich den Wert von `-storepass` (clientPwd im Beispiel), da Sie diesen bei der Konfiguration des Anwendungsservers benötigen.
   - Notieren Sie sich den Wert von `-alias` (UnicaClientIdentity im Beispiel), da Sie diesen für die restlichen Verfahrensschritte benötigen.
   - Der allgemeine Name (CN) im definierten Namen sollte mit dem zum Zugriff auf HCL Unica genutzten Hostnamen übereinstimmen. Wenn z. B. die URL für HCL Unica lautet: https://hostName.companyDomain.com:7002/unica/jsp, dann sollte der CN hostName.companyDomain.com sein. Der CN-Teil des definierten Namens ist der einzige erforderliche Teil; Organisation (O) und Organisationseinheit (OU, Organization Unit) sind nicht erforderlich.
   - In WebSphere 6.0 müssen das Keystore-Kennwort und das Schlüsselkennwort übereinstimmen.
3. Erstellen Sie ein Zertifikat auf Basis des erstellten Identitäts-Keystore. Mit dem folgenden Beispielbefehl wird ein vertrauenswürdiger Keystore namens `UnicaCertificate.cer` erstellt. Der Wert von `-alias` ist der Alias, den Sie für den Identity-Keystore festgelegt haben (UnicaClientIdentity im Beispiel).

   ```
   keytool -export -keystore UnicaClientIdentity.jks -storepass clientPwd-alias UnicaClientIdentity -file UnicaCertificate.cer
   ```
4. Generieren Sie einen vertrauenswürdigen Keystore, der auf dem erstellten Zertifikat basiert. Mit dem folgenden Beispielbefehl wird ein vertrauenswürdiger Keystore namens `UnicaTrust.jks` erstellt.

```
keytool -import -alias UnicaClientIdentity -file UnicaCertificate.cer-
keystore UnicaTrust.jks -storepass trustPwd
```

Beachten Sie Folgendes:

- Geben Sie `Y` ein, wenn Sie aufgefordert werden, die Vertrauenswürdigkeit des Zertifikats zu bestätigen.
- Der Wert von `-alias` ist der Alias, den Sie für den Identity-Keystore festgelegt haben (`UnicaClientIdentity` im Beispiel).
- Notieren Sie sich den Wert von `-storepass` (`trustPwd` im Beispiel), da Sie diesen bei der Konfiguration des Anwendungsservers benötigen.

Open SSL-Zertifikat in Java Key Store importieren

```
keytool -import -alias ListenerKey -file CAMPAIGN_HOME\bin\certificate.pem
-keystore PlatformClientIdentity.jks -storepass password
```

```
keytool -import -file CAMPAIGN_HOME\bin\certificate.pem -alias ListenerKey
-keystore <APP_SERVER_JAVA>\jre\lib\security\cacerts
```

Wie man signierte Zertifikate abruft

Sie können entweder die Programme OpenSSL und keytool verwenden, um Anfragen zur Erstellung von signierten Zertifikaten an CA zu erstellen, oder Sie können vollständig von CA zur Verfügung gestellte signierte Zertifikate erhalten.

Anmerkung:

- Für in C++ geschriebene HCL Unica-Anwendungen fordern Sie ein Zertifikat im PEM-Format an.
- Für alle übrigen HCL Unica-Anwendungen fordern Sie ein Zertifikat im JKS-Format an.

Anweisungen zum Abrufen eines signierten Zertifikats finden Sie in der Dokumentation der Zertifizierungsstelle.

Erstellen und Konfigurieren von Zertifikaten für eine Clusterumgebung

In der folgenden Prozedur wird beschrieben, wie Sie Ihre eigenen Zertifikate für eine Clusterumgebung erstellen und konfigurieren.

Die Campaign-Webanwendung muss mithilfe der Standardzertifikate für SSL konfiguriert werden.

In der folgenden Prozedur wird beschrieben, wie selbst signierte Zertifikate für Unica Campaign und Unica Platform erstellt und konfiguriert werden können.

In einer Clusterumgebung, in der sich ein IBM HTTP Server vor der Unica Campaign-Webanwendung und dem Campaign-Listener befindet, müssen Sie die folgenden Schritte ausführen, um den Campaign-Listener in SSL zu konfigurieren.

Sie können diese Schritte als Anleitung für die Konfiguration von Zertifikaten für andere Unica-Produkte verwenden.

Diese Prozedur ist für die Standardzertifikate anwendbar, die von dem IBM WebSphere Application Server bereitgestellt werden. Wenn Sie benutzerdefinierte Sicherheitszertifikate verwenden, müssen Sie die Schritte für die benutzerdefinierten Zertifikate ausführen, die der IBM WebSphere Application Server verwendet.

Führen Sie die folgenden Schritte aus, um den IBM HTTP Server für SSL zu konfigurieren.

1. Verwenden Sie GSKit zum Generieren von SSL-Zertifikaten wie folgt.
    a. Erstellen und initialisieren Sie eine neue Schlüsseldatenbank.

       Beispiel:

       ```
       gsk8capicmd_64 -keydb -create -populate -db IHS.kdb -pw password
       -stash
       ```

       Die Option `-stash` ist für Unica Campaign erforderlich.

    b. Verwenden Sie GSKit zum Generieren eines selbst signierten Zertifikats für Unica Campaign und speichern Sie es wie folgt in der Schlüsseldatenbank.

Beispiel:

```
gsk8capicmd_64 -cert -create -db IHS.kdb -dn "CN=*.in.ibm.com"
-expire 3650 -pw password -size 1024 -label key -default_cert yes
```

c. Extrahieren Sie den öffentlichen Teil des Zertifikats in eine Datei.

Damit die Clients einem Zertifikat vertrauen können, muss sein öffentlicher Teil an die Clients verteilt und in deren Schlüsseldatenbanken gespeichert werden. In diesem Schritt exportieren Sie den öffentlichen Teil des Unica Campaign-Zertifikats. Es wird in einem späteren Schritt importiert.

Beispiel:

```
gsk8capicmd_64 -cert -extract -db IHS.kdb -stashed -label key
-target IHS.arm
```

d. Aktivieren Sie folgendes Modul in der Datei `httpd.conf`.

Beispiel:

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so

Listen 443
<VirtualHost *:443>
SSLEnable
</VirtualHost>
KeyFile /data/webservers/IBM/IHS/ssl/IHS.kdb
SSLStashFile /data/webservers/IBM/IHS/ssl/IHS.sth
SSLDisable
```

e. Geben Sie in der Datei `httpd.conf` den Schlüsseldateipfad an.

f. Führen Sie einen Neustart von IBM HTTP Server aus.

2. Generieren Sie Schlüsselspeicher-Datenbankdateien für den Server, der den Unica Campaign-Listener hostet.

a. Führen Sie auf dem Server, der den Unica Campaign-Listener hostet, folgende Befehle von einer Position aus und notieren Sie sich den Pfad.

```
gsk8capicmd_64 -keydb -create -populate -db Key.kdb -pw password
 -stash
gsk8capicmd_64 -cert -create -db Key.kdb -dn "CN=*.in.ibm.com"
 -expire 3650 -pw password -size 1024
  -label key -default_cert yes
gsk8capicmd_64 -cert -extract -db Key.kdb -stashed -label key
 -target Key.arm
```

b. Überprüfen Sie, ob die folgenden Dateien an der Position generiert werden, von der aus Sie die oben genannten Befehle ausgeführt haben.
   - `Key.arm`
   - `Key.crl`
   - `Key.kdb`
   - `Key.rdb`
   - `Key.sth`

3. Importieren Sie die Dateien `Key.arm` und `HIS.arm` auf den Anwendungsserver, auf dem die Campaign-Webanwendung bereitgestellt wird.

a. Kopieren Sie die Dateien `Key.arm` und `HIS.arm` auf den Campaign-Webanwendungsserver.

b. Führen Sie die folgenden Schritte aus, um die Dateien `Key.arm` und `HIS.arm` zu **NodeDefaultTrustStore** des WebSphere Application Server hinzuzufügen:
   i. Klicken Sie auf **Sicherheit > Verwaltung von SSL-Zertifikaten und Schlüsseln > Schlüsselspeicher und Zertifikate**.
   ii. Klicken Sie auf **NodeDefaultTrustStore > Unterzeichnerzertifikate**.
   iii. Klicken Sie auf **Hinzufügen** und geben Sie unter Aliasname den **Aliasnamen** für die Dateien `Key.arm` und `HIS.arm` sowie den Pfad an, in den die Datei kopiert werden soll.
   iv. Klicken Sie auf **OK**.

4. Extrahieren Sie die persönlichen Zertifikate und die Unterzeichnerzertifikate für den IBM WebSphere Application Server
    a. Klicken Sie auf **Sicherheit > Verwaltung von SSL-Zertifikaten und Schlüsseln > Schlüsselspeicher und Zertifikate**.
    b. Klicken Sie auf **NodeDefaultTrustStore > Persönliche Zertifikate**.
    c. Wählen Sie das Standardzertifikat aus.
    d. Fügen Sie den Dateinamen für „Persönliche Zertifikate“ und den gültigen Pfad auf dem Unica Campaign-Webanwendungsserver hinzu. Beispiel: `/opt/HCL/HCLUnica101/ClientPersonal.cer`.
    e. Klicken Sie auf **OK**.
    f. Klicken Sie auf **NodeDefaultTrustStore > Unterzeichnerzertifikate**.
    g. Wählen Sie das Standardzertifikat aus.
    h. Fügen Sie den Dateinamen für „Unterzeichnerzertifikate“ und den gültigen Pfad auf dem Unica Campaign-Webanwendungsserver hinzu. Beispiel: `/opt/HCL/HCLUnica101/ClientSigner.cer`.
    i. Navigieren Sie zu dem Ordner und überprüfen Sie, ob beide Zertifikate im Ordner vorhanden sind.
5. Importieren Sie die persönlichen Zertifikate und Unterzeichnerzertifikate in die Unica Campaign-Listener- und die HCL HTTP Server-Schlüsselspeicher-Datenbank.

    a. Kopieren Sie die Zertifikate `ClientPersonal.cer` und `ClientSigner.cer` auf den Listener-Server. Sie können die gleiche Position verwenden, an der die Datei `key.kdb` erstellt wurde.

    b. Importieren Sie die persönlichen Zertifikate und Unterzeichnerzertifikate mithilfe des Befehls gsk8capicmd_64 in die Listener-Keystore-Datenbank, und zwar von der Position, an der die Listener-Keystore-Datenbank (`key.kdb`) erstellt wurde.

```
gsk8capicmd_64 -cert -add -db Key.kdb -stashed -label
 ClientPersonalKey -file ClientPersonal.cer
gsk8capicmd_64 -cert -add -db Key.kdb -stashed -label
 ClientSignerlKey -file ClientSigner.cer
```

c. Kopieren Sie die Zertifikate `ClientPersonal.cer` und `ClientSigner.cer` auf den HCL HTTP-Server. Sie können die gleiche Position verwenden, an der die Datei `IHS.kdb` erstellt wurde.

d. Importieren Sie die persönlichen Zertifikate und Unterzeichnerzertifikate mithilfe des Befehls gsk8capicmd_64 in die Listener-Schlüsselspeicher-Datenbank, und zwar von der Position, an der die HCL HTTP-Server-Schlüsselspeicher-Datenbank (`IHS.kdb`) erstellt wurde.

6. Importieren Sie den Campaign-Listener-Schlüssel in die HCL HTTP Server-Keystore-Datenbank und den HCL HTTP Server-Schlüssel in die Campaign-Keystore-Datenbank.

a. Kopieren Sie den HCL HTTP Server-Schlüssel (`IHS.arm`) auf den Listener-Server.

b. Importieren Sie den HCL HTTP-Server-Schlüsselspeicher mithilfe des Befehls gsk8capicmd_64 in die Listener-Schlüsselspeicher-Datenbank, und zwar von der Position, an der die Campaign-Listener-Schlüsselspeicher-Datenbank (`key.kdb`) erstellt wurde.

```
gsk8capicmd_64 -cert -add -db Key.kdb -stashed -label IHSKey
 -file IHS.arm
```

c. Kopieren Sie den Campaign-Schlüssel (`Key.arm`) auf den Listener-Server.

d. Importieren Sie den Campaign-Listener-Schlüssel mithilfe des Befehls gsk8capicmd_64 in die HCL HTTP-Server-Schlüsselspeicher-Datenbank, und zwar von der Position, an der die HCL HTTP-Server-Schlüsselspeicher-Datenbank (`IHS.kdb`) erstellt wurde.

```
gsk8capicmd_64 -cert -add -db IHS.kdb -stashed -label IHSKey
 -file Key.arm
```

7. Starten Sie den HCL Campaign-Anwendungsserver und den HCL HTTP Server erneut und starten Sie anschließend den Unica Campaign-Listener.

Konfigurieren Sie Ihren Webanwendungsserver für SSL

Konfigurieren Sie auf jedem Anwendungsserver, auf dem eine Unica Anwendung implementiert wird, den Webanwendungsserver so, dass die von Ihnen vorgesehenen Zertifikate genutzt werden.

Weitere Informationen zur Ausführung dieser Schritte entnehmen Sie bitte der Dokumentation Ihres Webanwendungsservers.

Sicherheit von Cookies

Einige Cookies sind im Client-Browser möglicherweise nicht angemessen gesichert. Bei ungesicherten Cookies ist die Anwendung anfällig für Man-in-the-Middle- und Session-Hijacking-Angriffe. Um dies zu verhindern, ergreifen Sie die folgenden Vorsichtsmaßnahmen.

- Erzwingen Sie stets die Verwendung von SSL, um die Gefahr zu verringern, dass Cookies bei der Übertragung abgefangen werden.
- Legen Sie im Webanwendungsserver die Flags `secure` und `httponly` für alle Cookies fest.
    - Das Flag `secure` weist den Browser an, das Cookie ausschließlich über eine HTTPS-Verbindung zu senden. Wenn Sie dieses Flag festlegen, müssen Sie in allen Anwendungen, die miteinander kommunizieren, SSL aktivieren.
    - Das Flag `httponly` verhindern den Zugriff auf Cookies über ein Script auf Clientseite.

Festlegen der Flags für SSL in WebSphere®

Gehen Sie wie folgt vor, um die Flags `secure` und `httponly` in WebSphere® festzulegen.

Sie legen die `secure`- und `httponly`-Flags in der WebSphere®-Administrationskonsole fest.

Tipp: Ausführliche Informationen finden Sie in der Dokumentation zu WebSphere®.

1. Navigieren Sie auf der Unica Platform-Anwendungsebene zu **Sitzungsmanagement** und klicken Sie auf **Cookies aktivieren**.
2. Aktivieren Sie **Cookies auf HTTPS-Sitzungen beschränken** und **Sitzungscookies auf HTTPOnly festlegen, um Cross-Site-Scripting-Angriffe zu verhindern**.
3. Speichern Sie die Änderungen und wenden Sie sie an.
4. Stoppen Sie die Unica Platform-Anwendung und starten Sie sie erneut.

Festlegen der Flags für SSL in WebLogic

Gehen Sie wie folgt vor, um die Flags `secure` und `httponly` festzulegen.

Tipp: Ausführliche Informationen finden Sie in der Dokumentation zu WebLogic.

1. Wenn Unica Platform bereitgestellt wurde und ausgeführt wird, müssen Sie es stoppen und die Bereitstellung zurücknehmen.
2. Extrahieren Sie die WAR-Datei von Unica Platform.
3. Bearbeiten Sie die Datei `weblogic.xml`, um die Flags `secure` und `httponly` festzulegen.
4. Erstellen Sie die WAR-Datei von Unica Platform neu, führen Sie die Bereitstellung erneut aus und starten Sie das Programm erneut.

HCL Unica für SSL konfigurieren

Um Unica-Anwendungen für die Nutzung von SSL zu konfigurieren, müssen Sie einige Konfigurationseigenschaften festlegen. Nutzen Sie für Ihre Installation von Unica-Produkten sowie die durch SSL zu sichernde Kommunikation die in diesem Abschnitt beschriebenen geeigneten Verfahren.

Wenn Sie auf Ihre Unica-Installation über eine gesicherte Verbindung zugreifen und wenn Sie wie in den nachfolgenden Verfahren beschrieben Navigationseigenschaften für Anwendungen festlegen, müssen Sie `https` und die Nummer des gesicherten Ports in der URL verwenden. Der Standard-SSL-Port ist `7002` für WebLogic und `8002` für WebSphere®.

Konfigurieren von SSL in Unica Platform

Mit dieser Prozedur können Sie SSL in Unica Platform konfigurieren.

1. Melden Sie sich in Unica an und klicken Sie auf **Einstellungen > Konfiguration**.
2. Setzen Sie den Wert der Eigenschaft `Allgemeines | Navigation | Unica Platform-URL` auf die URL von Unica Platform.

   Beispiel: `https://host.domain:SSL_port/unica`

   Hierbei gilt:

   - *`host`* ist der Name oder die IP-Adresse des Computers, auf dem Unica Platform installiert ist.
   - *`domain`* ist die Unternehmensdomäne, in der die Unica-Produkte installiert sind.
   - *`SSL_Port`* ist der SSL-Port auf dem Webanwendungsserver, auf dem Unica Platform bereitgestellt wurde.

   Beachten Sie das `https` in der URL.
3. Gehen Sie zu den Eigenschaften unter Kategorie `Navigation` für jedes Ihrer installierten Unica-Produkte und legen Sie dort die HTTP- und HTTPS-Ports fest. Die Namen der Eigenschaften können je nach Produkt variieren, ihr Zweck sollte jedoch deutlich erkennbar sein. Legen Sie diese Werte für jedes Produkt auf den HTTP- und HTTPS-Port des Anwendungsservers fest, auf dem das Produkt bereitgestellt wurde.
4. Führen Sie die in „Konfigurieren von SSL in Unica Platform mit LDAP-Integration“ beschriebene Prozedur durch, wenn die LDAP-Integration implementiert ist.
5. Führen Sie die in „Konfigurieren von SSL in Unica Platform mit Datenfilter“ beschriebene Prozedur durch, wenn Sie die Datenfilterfunktion verwenden wollen.

Konfigurieren von SSL in Platform für eine Clusterumgebung

Mit dieser Prozedur können Sie SSL in Platform für eine Clusterumgebung konfigurieren.

1. Melden Sie sich in HCL Unica an und klicken Sie auf **Einstellungen** > **Konfiguration**.
2. Setzen Sie unter `Affinium | Manager | Navigation` die **Unica Platform**-URL auf die Unica Platform-URL.

   Beispiel: `https://<IHS_Host>/unica`.

3. Legen Sie unter `Affinium | Campaign | Navigation` die **serverURL** auf die Unica Campaign-URL fest.

   Beispiel: `https://<IHS_Host>/Campaign`.
4. Legen Sie unter `Affinium | Campaign | server` die **fullContextPath** auf die Unica Campaign-URL fest.

   Beispiel: `https://<IHS_Host>/Campaign`.
5. Legen Sie unter `Affinium | Campaign | unicaACListener` **serverhost** auf `<IHS Host>` und **useSSL** auf `True` fest.

Konfigurieren von SSL in Unica Platform mit LDAP-Integration

Mit dieser Prozedur können Sie SSL in Unica Platform konfigurieren.

1. Führen Sie die in „Konfigurieren von SSL in Unica Platform“ beschriebene Prozedur durch (falls noch nicht erfolgt).
2. Melden Sie sich in Unica an und klicken Sie auf **Einstellungen > Konfiguration** .

   Die Seite „Konfiguration“ wird angezeigt.
3. Navigieren Sie zur Kategorie `Unica | Unica Platform | Sicherheit | Details zum Anmeldeverfahren | LDAP` und legen Sie für die Eigenschaft `SSL für LDAP-Verbindung erforderlich` den Wert `true` fest.

   Bei dieser Einstellung muss Unica Platform bei der Benutzeranmeldung eine Verbindung zum LDAP-Server über SSL herstellen.
4. Navigieren Sie zur Kategorie `Unica | Unica Platform | Sicherheit | LDAP-Synchronisation` und legen Sie die folgenden Werte fest.
   - Setzen Sie den Wert der Eigenschaft `LDAP provider URL` auf:
     `ldaps://`*`host`*`.`*`domain`*`: `*`SSL_Port`*

     Hierbei gilt:
     - *`host`* ist der Name oder die IP-Adresse des LDAP-Servers
     - *`domain`* ist die Domäne des LDAP-Servers
     - *`SSL_Port`* ist der SSL-Port des LDAP-Servers.

     Beispiel: `ldaps://LDAPMachine.myCompany.com:636`

Beachten Sie das `ldaps` in der URL.

Der Standard-SSL-Port für LDAP-Server lautet `636`.

- Legen Sie den Eigenschaftswert `Erfordert SSL für LDAP-Verbindung` auf `true` fest.

  Bei dieser Einstellung muss Unica Platform bei der Synchronisation mit dem LDAP-Server eine Verbindung zum LDAP-Server über SSL herstellen.

Konfigurieren von SSL in Unica Platform mit Datenfilter

Wenn Unica Platform mit SSL implementiert wird und Sie vorhaben, die Datenfilterfunktion zu nutzen, müssen Sie diese Prozedur ausführen, um die SSL-Optionen für das Handshakeverfahren hinzuzufügen.

1. Führen Sie die in „Konfigurieren von SSL in Unica Platform“ beschriebene Prozedur durch (falls noch nicht erfolgt).
2. Holen Sie folgende Informationen ein.
   - Eine Kopie der Zertifikatsdatei, die Sie in Erhalten oder Erstellen von Zertifikaten *(auf Seite)* erstellt haben
   - Das Kennwort des Zertifikats
3. Speichern Sie die Zertifikatsdatei im Verzeichnis *JAVA_HOME*`jre/lib/security`, wobei *JAVA_HOME* das Java™-Verzeichnis ist, das im Script `tools/bin/setenv` in der Unica Platform-Installation angegeben ist.

   Das Script `setenv` gibt die von Unica Platform-Dienstprogrammen verwendete Java™-Instanz an.
4. Importieren Sie mit dem Programm `keytool` das Zertifikat in die Datei `cacerts` für Ihre Java™-Instanz.

   Verwenden Sie den folgenden Beispielbefehl als Leitfaden.

   ```
   keytool -import -trustcacerts -file name_of_your_certificate.cer
   -keystore cacerts
   ```

   Geben Sie das Kennwort des Zertifikats ein, wenn Sie dazu aufgefordert werden.

Konfigurieren von SSL in Unica Plan

Mit dieser Prozedur können Sie SSL in Unica Plan konfigurieren.

1. Melden Sie sich in Unica an und klicken Sie auf **Einstellungen > Konfiguration** .
2. Setzen Sie den Eigenschaftswert `Marketing Operations | navigation | serverURL` auf die URL der Webanwendung Unica Plan.

   Beispiel: `serverURL=https://host:SSL_port/plan`

   Hierbei gilt:

   - *`host`* ist der Name oder die IP-Adresse des Computers, auf dem Unica Plan installiert ist.
   - *`SSL_Port`* ist der SSL-Port der Unica Plan-Webanwendung

   Beachten Sie das `https` in der URL.
3. Öffnen Sie die Datei `plan_config.xml` in einem Text- oder XML-Editor.

   Die Datei `plan_config.xml` ist im Unterverzeichnis `conf` der Unica Plan-Installation abgelegt.
4. Legen Sie die Eigenschaft `UAPInitParam notifyPlanBaseURL` für Ihre SSL-Verbindung fest.

   Beispiel: `<UAPInitParam notifyPlanBaseURL="https://host:SSL_Port/plan/affiniumplan.jsp"/>`

   Hierbei gilt:

   - *`host`* ist der Name oder die IP-Adresse des Computers, auf dem Unica Plan installiert ist.
   - *`SSL_Port`* ist der SSL-Port der Unica Plan-Webanwendung

   Beachten Sie das `https` in der URL.
5. Um die Adobe™ Adobe Acrobat Online Markup-Funktion für die Arbeit mit Unica Plan über HTTPS zu aktivieren, legen Sie die Eigenschaft `markupServerURL` für Ihre SSL-Verbindung fest.

   Beispiel: `<UAPInitParam markupServerURL="https://host:SSLport/plan/services/collabService?WSDL">`

Hierbei gilt:

- *host* ist der Name oder die IP-Adresse des Computers, auf dem Unica Plan installiert ist.
- *SSL_Port* ist der SSL-Port der Unica Plan-Webanwendung

Beachten Sie das `https` in der URL.

6. Speichern und schließen Sie die Datei `plan_config.xml`.

Konfigurieren von SSL in Unica Campaign

Mit dieser Prozedur können Sie SSL in Unica Campaign konfigurieren.

Anmerkung: Wenn Sie SSL in Unica Campaign konfigurieren, müssen Sie auch den Campaign-Listener in SSL konfigurieren. Wenn Sie den Campaign-Listener in SSL nicht festlegen, wird als Status für das geplante Ablaufdiagramm möglicherweise `Unknown` angezeigt.

1. Öffnen Sie die Datei `config.xml` in einem Text- oder XML-Editor.

   `config.xml file` befindet sich im `conf` -Verzeichnis im Installationsverzeichnis von Unica Campaign.
2. Definieren Sie in der Datei `config.xml` die folgenden Werte.
   - `unicaServerSSLFile = PATH_TO_OPENSSL_PEM/campaign.pem`
3. Speichern und schließen Sie die Datei `config.xml`.
4. Melden Sie sich in Unica Platform an und klicken Sie auf **Einstellungen > Konfiguration**.

   Die Seite „Konfiguration“ wird angezeigt.
5. Legen Sie den Eigenschaftswert `Campaign | unicaACListener | useSSL` auf `yes` fest.
6. Falls Sie die Webanwendung auf einem SSL-Port installiert haben, setzen Sie den Eigenschaftswert `Campaign | Navigation | serverURL` auf die URL der Webanwendung. Beispiel:

   ```
   serverURL=https://host:SSL_port/Campaign
   ```

Hierbei gilt:

- `host` ist der Name oder die IP-Adresse des Computers, auf dem die Webanwendung installiert ist.
- `SSL-Port` ist der SSL-Port der Webanwendung.

Beachten Sie das https in der URL.

7. Wenn Sie Operational Monitoring nutzen, konfigurieren Sie diesen für SSL, indem Sie den Eigenschaftswert `Campaign | Monitoring | serverURL` auf die Verwendung von HTTPS einstellen. Beispiel:

   ```
   serverURL=https://host:SSL_port/Campaign/OperationMonitor
   ```

   Hierbei gilt:

   - `host` ist der Name oder die IP-Adresse des Computers, auf dem die Webanwendung installiert ist.
   - `SSL-Port` ist der SSL-Port der Webanwendung.

   Beachten Sie das `https` in der URL.

Konfigurieren der Chiffren-Liste in Unica Campaign

Voraussetzung: Unica Campaign muss mit SSL konfiguriert werden.

Wenn die Unica Campaign-Anwendung und der Listener so konfiguriert sind, dass die SSL-Optionen auf `TRUE` festgelegt sind, dann werden standardmäßig 98 Chiffren unterstützt, um die SSL-Kommunikation zwischen der Unica Campaign-Anwendung bzw. dem Unica Campaign-Anwendungsserver und dem Listener zu ermöglichen.

Um schwache Chiffren von dieser Standardchiffrenliste auszuschließen, können Benutzer das Tag `<SSLCipherList>` oder die Eigenschaft in der Datei config.xml verwenden.

Um die Unterstützung für schwache Chiffren zu entfernen, müssen Benutzer die folgende Zeile in der Datei config.xml hinzufügen. Sie legt fest, dass die Unterstützung für Standardchiffren `AES256-SHA, CAMELLIA256-SHA, AES128-SHA, SEED-SHA, CAMELLIA128-SHA, DES-CBC3-SHA, IDEA-CBC-SHA` ausschließt.

```
<property name="SSLCipherList"><value>DEFAULT:!AES256-SHA:!CAMELLIA256-SHA:!AES128-SHA:!SEED-SHA:!CAMELLIA128-SHA:!DES-CBC3-SHA:!IDEA-CBC-SHA</value></property>
```

Dadurch werden die oben genannten Chiffren deaktiviert, die im Tag `<SSLCipherList>` der Datei config.xml enthalten sind.

Wenn Clients oder Benutzer das SSLCipherList-Tag in der Datei config.xml nicht erwähnen, dann wird die Standardchiffrenliste berücksichtigt und 98 Chiffren werden unterstützt.

Anmerkung: Der Listener startet nicht und die folgenden Fehler werden in der Datei unica_aclsnr.log generiert, wenn Benutzer oder Clients irgendeine Chiffre deaktivieren, die für das Zertifikat oder den Browser erforderlich ist.

```
Error enabling SSL connection.

SOCKET BIND port=4664: ERRNO 10048: Unknown error
```

Konfigurieren von SSL in Unica Campaign für eine Clusterumgebung

Mit dieser Prozedur können Sie SSL auf dem Unica Campaign-Listener-Server in einer Clusterumgebung konfigurieren.

1. Öffnen Sie die Datei `config.xml` für den Listener-Server in einem Text- oder XML-Editor.

   `config.xml file` befindet sich im `conf` -Verzeichnis im Installationsverzeichnis von Unica Campaign.
2. Definieren Sie in der Datei `config.xml` die folgenden Werte.
   - Legen Sie **configurationServerBaseURL** auf die Campaign-SSL-URL fest. Dies ist die HCL HTTP Server-URL.
   - Legen Sie **unicaServerSSLFile** auf den Pfad fest, in dem die Datei "Kennwort" gespeichert ist.
   - Legen Sie **unicaServerSSLFile** auf den Pfad fest, in dem die Datei "Kennwort" gespeichert ist.

Beispiel:

```
<configuration name="bootstrap">
   <category name="bootstrap">
      <property name="suiteName"><value>Affinium</value></property>
      <property name="clientType"><value>HTTP</value></property>
      <!-- configurationServerBaseURL value will be set by
 AffiniumSuite assembly installer -->
      <property
 name="configurationServerBaseURL"><value>https://<IHS_Host>/Campaign<
/value></property>
      <property
 name="trustedApplication"><value>false</value></property>
      <property name="unicaClientKeystore"><value></value></property>
      <property
 name="unicaClientKeystorePwd"><value></value></property>
      <property
 name="unicaServerSSLFile"><value>/PATH_TO_OPENSSL_PEM/campaign.pem</v
alue></property>
   <property name="unicaServerSSLFilePwd"><value></value></property>
   </category>
</configuration>
```

3. Speichern und schließen Sie die Datei `config.xml`.

Konfigurieren von Campaign mit SSL und dem Campaign-Listener ohne SSL

Sie müssen Einstellungen konfigurieren, damit die Anwendungen nahtlos arbeiten, wenn Ihre Einrichtung Campaign mit SSL und den Campaign-Listener ohne SSL umfasst.

Die Campaign-Webanwendung muss mithilfe der Standardzertifikate in SSL konfiguriert werden.

Alle Konfigurationen sind auf den WebSphere Application Server für Campaign anwendbar. Für die Einrichtung mit und ohne SSL sind mehrere Schritte erforderlich. Jedem Schritt sind möglicherweise weitere Unterschritte zugeordnet, die ausgeführt werden müssen.

Führen Sie die folgenden Schritte aus, um Campaign mit SSL und den Campaign-Listener ohne SSL zu konfigurieren:
Führen Sie die folgenden Schritte aus.

Tabelle 50. Konfigurieren von Campaign mit SSL und dem Campaign-Listener ohne SSL

#	Schritt	Unterschritte

1	Generieren und verwenden Sie die Datei `.pem` (Zertifikat).	Führen Sie den folgenden Befehl von einer Position aus und notieren Sie sich die Pfade. Erstellen Sie ein neues Beispiel für eine Zertifikatsdatei campaign.pem (Kopieren Sie den Inhalt von key.pem und certificate.pem in diese durch eine neue Zeile getrennte Datei)
		`set OPENSSL_CONF=CAMPAIGN_HOME\bin\openssl.cnf`
		`openssl genrsa -out key.pem 4096`
		`openssl req -config openssl.cnf -new -key key.pem -out request.pem`
		`openssl req -config openssl.cnf -x509 -key key.pem -in request.pem -days 1000 -out certificate.pem`
		Die folgenden Dateien werden an der Position generiert, von der aus Sie die Befehle ausgeführt haben.
		• key.pem
		• request.pem
		• certificate.pem
		• campaign.pem

#	Schritt	Unterschritte
2	Importieren Sie die Datei `campaign.pem` auf den Anwendungsserver, auf dem die Campaign-Webanwendung bereitgestellt wird.	a. Kopieren Sie die Datei `campaign.pem` auf den Campaign-Webanwendungsserver. b. Führen Sie die folgenden Schritte aus, um die Datei `campaign.pem` zu **NodeDefaultTrustStore** des WebSphere Application Server hinzuzufügen: i. Klicken Sie auf **Sicherheit > Verwaltung von SSL-Zertifikaten und Schlüsseln > Schlüsselspeicher und Zertifikate**. ii. Klicken Sie auf **NodeDefaultTrustStore > Unterzeichnerzertifikate**. iii. Klicken Sie auf **Hinzufügen** und geben Sie unter Aliasname den **Aliasnamen** für die Datei `campaign.pem` sowie den Pfad an, in den die Datei kopiert werden soll. iv. Klicken Sie auf **OK**. Der Listener-Schlüssel wird zum Anwendungsserver hinzugefügt.

3	Ändern Sie die Datei `config.xml` auf dem Listener-Server.	Stellen Sie folgende Informationen bereit:
		
		• **configurationServerBaseURL**: Geben Sie die Campaign-SSL-URL an.
		• **unicaServerSSLFile**: Geben Sie den `PATH_TO_OPENSSL_PEM/campaign.pem`-Dateipfad an.
		• **unicaServerSSLFilePwd**: Geben Sie den entsprechenden `password`-Dateipfad an.
		
		`<configuration name="bootstrap">`
		`<category name="bootstrap">`

#	Schritt	Unterschritte
		<property name="suiteName"><value>Affinium</value></property> <property name="clientType"><value>HTTP</value></property> <!-- configurationServerBaseURL value will be set by AffiniumSuite assembly installer --> <property name="configurationServerBaseURL"> <value>https://eagle191.hcl.com:9447/Campaign</value> </property> <property name="trustedApplication"><value>false</value></property> <property name="unicaClientKeystore"><value></value></property> <property name="unicaClientKeystorePwd"><value></value></property> <property name="unicaServerSSLFile"> <value>PATH_TO_OPENSSL_PEM/campaign.pem</value> </property> <property name="unicaServerSSLFilePwd"> <value> password </value> </property>

#	Schritt	Unterschritte
		</category> </configuration>
4	Legen Sie bei den Einstellungen für **unicaACListener** den Parameter **useSSL** auf **TRUE** fest.	-
5	Starten Sie Campaign Application Server und den Campaign-Listener erneut.	-

Konfigurieren von SSL in Unica Optimize

Mit dieser Prozedur können Sie SSL in Unica Optimize konfigurieren.

1. Öffnen Sie die Datei `config.xml` aus dem Verzeichnis `conf` der Unica Optimize-Installation in einem Text- oder XML-Editor.
2. Legen Sie als Wert für `unicaServerSSLFile` den vollständigen Pfad des verwendeten Zertifikats fest.
3. Speichern und schließen Sie die Datei `config.xml`.
4. Legen Sie den Wert der Konfigurationseinstellung `Campaign| unicaACOListener | useSSL` auf `yes` fest.
5. Wenn Sie das Unica Optimize-Befehlszeilentool `ACOOptAdmin` verwenden, führen Sie die folgenden Schritte aus.

a. Holen Sie folgende Informationen ein.
   - Eine Kopie der Zertifikatsdatei, die Sie in Erhalten oder Erstellen von Zertifikaten *(auf Seite)* erstellt haben
   - Das Kennwort des Zertifikats

b. Speichern Sie die Zertifikatsdatei im Verzeichnis `JAVA_HOME/jre/lib/security`, wobei *JAVA_HOME* das Java™-Verzeichnis ist, das im Script `ACOOptAdmin` angegeben ist.

c. Importieren Sie mit dem Programm `keytool` das Zertifikat in die Datei `cacerts` für Ihre Java™-Instanz.

   Verwenden Sie den folgenden Beispielbefehl als Leitfaden.

   ```
   keytool -import -trustcacerts -file name_of_your_certificate.cer
   -keystore cacerts
   ```

   Geben Sie das Kennwort des Zertifikats ein, wenn Sie dazu aufgefordert werden.

Konfigurieren von SSL in Unica Interact

Sie können die SSL-Kommunikation für Unica Interact in drei verschiedenen Bereichen konfigurieren, auch wenn dies zu erheblichen Leistungseinbußen führt.

SSL kann in den folgenden Bereichen verwendet werden:

- Designumgebung als Client und Laufzeitumgebung als Server.

  Nutzen Sie https in der URL, die auf den Unica Interact-Laufzeitserver verweist. Beispiel: Setzen Sie `Campaign | partitions | partition[n] | Interact | ServerGroups | [serverGroup] | instanceURLs | [instanceURL] | instanceURL` auf `https://myserver.domain.com:7007/interact`.
- Laufzeitumgebung als Client und Unica Platform als Server.
- Ihr Touchpoint als Client und die Laufzeitumgebung als Server.

Legen Sie die HTTPS-URL mit der Methode `getInstance` fest. Bei Verwendung eines Lastenausgleichs müssen Sie den Lastenausgleich möglicherweise ebenfalls für SSL konfigurieren.

- Wenn der Unica Interact-Design-Server und der entsprechende Laufzeitserver sich auf separaten Hosts befinden, die mit SSL arbeiten, dann importieren Sie die Sicherheitszertifikate auf den beiden Servern, um den SSL-Handshake zu ermöglichen.

Wichtig: Wenn Sie einen beliebigen Teil von Unica Interact für die Kommunikation mittels SSL konfigurieren, treten Leistungseinbußen auf. Es wird nicht empfohlen, Unica Interact für die Verwendung von SSL zu konfigurieren.

Konfigurieren von SSL in Unica Collaborate

Nachdem Unica Campaign für die Nutzung von SSL konfiguriert wurde, ist keine weitere Konfiguration erforderlich, um Unica Collaborate für SSL zu konfigurieren.

Konfigurieren von SSL in Berichten

Mit dieser Prozedur können Sie SSL in Berichten konfigurieren.

1. Konfigurieren Sie Cognos® mit SSL, wie in der Cognos®-Dokumentation beschrieben.
2. Konfigurieren Sie Apache mit SSL, wie in der Apache-Dokumentation beschrieben.
3. Registrieren Sie das Cognos®-Zertifikat mit Unica, wie in der Cognos®-Dokumentation beschrieben.
4. Registrieren Sie die Unica-Zertifikate mit Cognos®, wie in der Cognos®-Dokumentation beschrieben.

Konfigurieren von SSL in Digital Analytics for On Premises

Digital Analytics for On Premises akzeptiert keine Anfragen: Es agiert stets als Client in der HTTP- und HTTPS-Kommunikation zur Auflösung von Seitentiteln auf den zu analysierenden Webseiten. Wenn Sie Seitentitel für eine Site auflösen müssen, die SSL verwendet, müssen Sie lediglich sicherstellen, dass die richtige URL in die Profiloptionen für die analysierte

Webseite oder die analysierten Cluster-Server eingegeben wurde und dass die URL das Protokoll HTTPS beinhaltet.

Digital Analytics for On Premises kommuniziert nicht mit Unica Platform.

Überprüfen der SSL-Konfiguration

Mit dieser Prozedur können Sie die SSL-Konfiguration überprüfen.

1. Starten Sie Ihre einzelnen Unica-Anwendungen.
2. Melden Sie sich an Unica an und greifen Sie auf alle installierten Unica-Webanwendungen zu.
3. Nur bei Unica Interact-Laufzeitservern: Testen Sie die Verbindung mit der URL `https://host:port/interact/jsp/admin.jsp`.
4. Wenn Sie ein selbst signiertes Zertifikat nutzen, richten Sie Ihren Browser auf jede einzelne Unica-Serverkomponente und prüfen Sie, dass die empfangenen Zertifikat-Informationen den erwarteten Daten entsprechen.

   Beispiel: Wenn der Unica Campaign-Listener auf Port 4664 eines Hosts namens `campaignHost` ausgeführt wird, geben Sie im Browser folgende Adresse ein: `https://campaignHost:4664`

   Der Browser öffnet ein Fenster, in dem Sie gefragt werden, ob Sie das Zertifikat akzeptieren, und Sie können die Zertifikatdetails anzeigen.

Nützliche SSL-Links

Diese Links enthalten weitere Informationen zu den Aufgaben, die zur Implementierung von SSL in Unica erforderlich sind.

- OpenSSL-Dokumentation - https://www.openssl.org/
- Dokumentation zum Java-Tool "keytool" - http://docs.oracle.com/javase/7/docs/technotes/tools/solaris/keytool.html
- Liste der Zertifizierungsstellen - https://curlie.org/Computers/Security/Public_Key_Infrastructure/PKIX/Tools_and_Services/Third_Party_Certificate_Authorities/

Datenschutzniveau-Einstellungen für WebLogic

Sie müssen die Datenschutzniveau-Einstellungen festlegen, wenn Sie HCL Unica-Anwendungen für die Verwendung von SSL konfigurieren.

Folgende Datenschutzniveau-Einstellungen werden für WebLogic unterstützt:

- TLS11
- TLS12

Führen Sie die folgenden Schritte aus, um die Datenschutzniveau-Einstellungen zu ändern: Hängen Sie folgende Option an die Variable `JAVA_OPTIONS` an:

- For TLS11- `-Dweblogic.security.SSL.protocolVersion=TLSv1.1`
- For TLS12- `-Dweblogic.security.SSL.protocolVersion=TLSv1.2`

Datenschutzniveau-Einstellungen für WebSphere

Sie müssen die Datenschutzniveau-Einstellungen festlegen, wenn Sie HCL Unica-Anwendungen für die Verwendung von SSL konfigurieren.

Folgende Datenschutzniveau-Einstellungen werden für WebSphere unterstützt:

- SSL_TLS
- SSL
- TLS
- TLSv1
- SSL_TLSv2
- TLSv1.1
- TLSv1.2

Führen Sie die folgenden Schritte aus, um die Datenschutzniveau-Einstellungen zu ändern:

1. Navigieren Sie zu **Sicherheit > Verwaltung von SSL-Zertifikaten und Schlüsseln > SSL-Konfigurationen**
2. Wählen Sie die erforderliche SSL-Konfiguration aus.

3. Klicken Sie unter **Weitere Eigenschaften** auf **Datenschutzniveau-Einstellungen**.
4. Wählen Sie im Bereich **Datenschutzniveau-Einstellungen** aus der Dropdown-Liste für **Protokoll** die erforderlichen Datenschutzniveau-Einstellungen aus.
5. Klicken Sie auf **Speichern**.
6. Aktualisieren Sie in der Datei `ssl.client.props`, die sich im Verzeichnis `WAS_install\profiles\AppSrv01\properties` befindet, Folgendes:

   ```
   com.ibm.ssl.protocol=<Specify required QoP settings>
   ```

7. Starten Sie den Anwendungsserver erneut.

Sicherheitsframework für Unica-APIs

Unica Platform stellt das Sicherheitsframework für durch Unica-Produkte implementierte APIs bereit.

Mithilfe eines Satzes Konfigurationseigenschaften auf der Seite **Einstellungen > Konfiguration** können Entwickler die Sicherheit der durch Unica-Produkte bereitgestellten APIs folgendermaßen festlegen.

- Für eine bestimmte Produkt-API kann der Zugriff auf das Produkt blockiert werden.
- Für eine bestimmte Produkt-API kann festgelegt werden, dass HTTPS für die Kommunikation zwischen der angegebenen API und dem Produkt erforderlich ist.
- Für eine bestimmte Produkt-API kann festgelegt werden, dass Authentifizierung für die Kommunikation zwischen der angegebenen API und dem Produkt erforderlich ist.

Die Konfigurationseigenschaften, mit der die API-Sicherheit gesteuert wird, befinden sich in der Kategorie **Unica Marketing Platform | Sicherheit |API-Management**. Zu jedem Produkt gibt es eine Konfigurationseigenschaftsvorlage, mit der Sie neue Sicherheitseinstellungen für die durch das Produkt bereitgestellten APIs erstellen können.

Sie können die Sicherheitseinstellungen für eine API festlegen und ändern, z.B. zum Testen oder Bereitstellen einer Einheit oder auch allgemein während des Lebenszyklus der APIs.

Das Sicherheitsframework unterstützt momentan APIs nur für Unica Campaign.

Das Unica Platform-Sicherheitsframework unterstützt die folgenden Authentifizierungsoptionen für den Zugriff auf geschützte APIs. Sie können je nach Umgebung eine dieser Optionen verwenden.

- Interne Benutzer, die bei Unica Platform registriert sind, können mit ihren Unica Platform-Anmeldeberechtigungsnachweisen authentifiziert werden, um ein sicheres Token zu erhalten.
- Externe Benutzer, die einer Föderation angehören, die von Unica Platform verwendet wird, können über den Identitätsproviderserver authentifiziert werden.

Authentifizierung interner Benutzer mit der Unica Platform-Anmeldungs-API

Um interne Benutzer in Clientanwendungen zu authentifizieren, verwenden Sie die Unica Platform `login`-API zum Erstellen des sicheren Tokens. Sie können dann jede beliebige geschützte API aufrufen, indem Sie zusätzlich zu den von der API selbst erwarteten Parametern die erforderlichen Parameter im Anforderungsheader übergeben.

Der Sicherheitsfilter fängt diese geschützten Anforderungen ab, prüft sie und gibt sie dann zur Verarbeitung weiter.

Nachdem der Unica Platform-Benutzer authentifiziert wurde, fügt der Unica Platform-Sicherheitsfilter der Anforderung den Anmeldenamen als Attribut des Schlüssels `USER_NAME_STRING` hinzu, bevor er ihn zur Verarbeitung an das Produkt übergibt.

Die sicheren Tokens haben eine Standardlebensdauer von 15 Sekunden. Wenn die Lebensdauer des Tokens abgelaufen ist, kann es nicht mehr zum Aufrufen einer geschützten API verwendet werden. Jedes Mal, wenn die Unica Platform `login`-API für einen Benutzer aufgerufen wird, werden die vorherigen Sicherheitstokens des Benutzers inaktiviert.

Sie können die Lebensdauer von sicheren Tokens ändern, indem Sie den Wert der Eigenschaft **Tokenlebensdauer** auf der Seite **Einstellungen > Konfiguration** in der Kategorie **Allgemein | Sonstiges** festlegen.

Beispiel-URL

`http[s]://host:port/unica/api/manager/authentication/login/`

Headerparameter

Tabelle 51. Headerparameter für die Anmeldungs-API bei internen Benutzern

Parameter	Beschreibung
`m_user_name`	Der Unica Platform-Anmeldename des internen Benutzers.
`m_user_password`	Das Unica Platform-Kennwort des internen Benutzers als Klartext.

Antwort

Wenn die Anmeldung erfolgreich ist, lautet die Antwort HTTP 200 mit folgenden JSON-Daten.

- `m_tokenId` - zufällig generiertes Token
- `m_user_name` - Benutzername des angemeldeten Benutzers
- `createDate` - Zeitmarke in folgendem Format, wobei die Zeitzone IST ist:

```
Mon Jul 06 18:23:35 IST 2015
```

Wenn die Anmeldung wegen falscher Berechtigungsnachweise fehlschlägt, lautet die Antwort HTTP 401 (nicht berechtigt). Wenn festgelegt wurde, dass die `login`-API geblockt wird, lautet die Antwort 403 (unzulässig). Wenn die Konfiguration der `login`-API die Verwendung von HTTPS vorsieht und die API über HTTP aufgerufen wird, lautet die Antwort 403 (unzulässig).

Um interne Benutzer abzumelden, verwenden Sie die Unica Platform `logout`-API.

Abmeldung interner Benutzer mithilfe der Unica Platform-Abmeldungs-API

Verwenden Sie die Unica Platform `logout`-API, um interne Benutzer abzumelden und das Sicherheitstoken zu löschen.

Die `logout`-API ist standardmäßig geschützt. Die Authentifizierungsparameter werden im Anforderungsheader zu vordefinierten Schlüsseln erwartet.

Beispiel-URL

`http[s]://host:port/unica/api/manager/authentication/logout/`

Headerparameter

Tabelle 52. Headerparameter für die Abmeldungs-API

Parameter	Beschreibung
`m_user_name`	Der Unica Platform-Anmeldename des internen Benutzers.
`m_tokenId`	Das durch die Authentifizierung erhaltene sichere Token.
`api_auth_mode`	Verwenden Sie für interne Benutzer den Wert `manager`.

Antwort

Wenn die Authentifizierung erfolgreich ist, lautet die Antwort `HTTP 200` und das Sicherheitstoken wird gelöscht. Wenn die Antwort HTTP 200 lautet, sollte die Clientanwendung die Abmeldung bestätigen.

Wenn die Authentifizierung fehlschlägt, lautet die Antwort `HTTP 401`.

Authentifizierung und Abmeldung externer Benutzer über eine Föderation

Wenn Unica Platform in eine unterstützte Föderation integriert ist, können sich Benutzer bei ihrem eigenen System anmelden und die Clientanwendung erhält über den Identitäts-Provider-Server von Unica Platform ein Token.

Nachdem ein föderierter Benutzer authentifiziert wurde, wird sein Unica Platform-Anmeldename der Anforderung als Attribut des Schlüssels `USER_NAME_STRING` hinzugefügt.

Die Abmeldung sollte am Identitäts-Provider-Server stattfinden.

Headerparameter

In der folgenden Tabelle werden die Headerparameter beschrieben, die bei der Authentifizierung über den Identitäts-Provider-Server von Unica Platform verwendet werden.

Tabelle 53. Headerparameter bei einer Föderation

Parameter	Beschreibung
f_userId	Benutzer-ID in der Föderation.
f_clientId	Client-ID in der Föderation.
f_spId	Service-Provider-ID in der Föderation.
f_tokenId	Single-Sign-on-Token des Identitäts-Provider-Servers.
api_auth_mode	Verwenden Sie für die föderierte Authentifizierung den Wert `fsso`.

Antwort

Die Antwort lautet `HTTP 200` mit zusätzlichen API-abhängigen Elementen.

Erzeugung und Management von Datenfiltern

Datenfilter ermöglichen es, die Kundendaten zu beschränken, die ein Unica-Benutzer in Unica Anwendungen anzeigen und bearbeiten kann. Die mit einem Datenfilter gesicherten Daten stellen einen Datensatz dar, der über die Felder in den von Ihnen angegebenen Kundentabellen definiert wird.

Die verschiedenen Unica-Anwendungen verwenden Datenfilter auf unterschiedliche Art und Weise. Um zu bestimmen, ob ein bestimmtes Produkt Datenfilterung verwendet und wie diese ggf. im Produkt angewendet wird, finden Sie in der jeweiligen Produktdokumentation.

Übersicht über das Erstellen von Datenfiltern

Unica Platform stellt die folgenden Features bereit, mit denen Unica-Administratoren Datenfilter einrichten können.

- Ein Dienstprogramm für das Definieren von Datenfiltern
- Eine Benutzeroberfläche für das Zuweisen von Benutzern und Gruppen zu Datenfiltern und zum Anzeigen zugeordneter Datenfilter.

Datenfilterzuweisungen zur Einschränkung des Benutzerzugriffs

Wenn der Datenzugriff einzelner Benutzer oder Benutzergruppen eingeschränkt werden soll, müssen Sie diese Benutzer oder Benutzergruppen Datenfiltern zuordnen. Allen Unica-Benutzern und -Gruppen können Datenfilter zugewiesen werden.

Sie können einem einzelnen Datenfilter mehrere Benutzer und Gruppen zuordnen und einen Benutzer oder eine Benutzergruppe mehreren Datenfiltern zuordnen.

Anmerkung: Gruppen übernehmen die Datenfilterzuweisungen ihrer Untergruppen nicht.

Ein Benutzer, der mehreren Datenfiltern zugewiesen wurde, kann alle Datensätze anzeigen, die von den Datenfiltern zugelassen werden.

Zwei Möglichkeiten, Datenfilter zu erstellen: automatische Generierung und manuelle Spezifikation

Unica Platform stellt das Dienstprogramm `datafilteringScriptTool` bereit, das XML verarbeitet, um Datenfilter in den Unica Platform-Systemtabellen zu erstellen. Abhängig von der Art, wie XML geschrieben wird, können Sie dieses Dienstprogramm auf zweierlei Weise verwenden: automatische Generierung und manuelle Spezifikation.

Automatische Generierung

Mit dem Dienstprogramm `datafilteringScriptTool` können Datenfilter automatisch aus einer Datenbanktabelle generiert oder mit JDBC angezeigt werden. Das Dienstprogramm erstellt automatisch Datenfilter auf Grundlage eindeutiger Wertekombinationen in Feldern, die Sie in der XML angeben (ein Datenfilter für jede eindeutige Kombination).

Diese Methode empfiehlt sich, wenn Sie viele Datenfilter erstellen müssen, die auf eindeutigen Kombinationen von Werten in verschiedenen Feldern basieren.

Manuelle Angabe

Mit dem Dienstprogramm `datafilteringScriptTool` können Datenfilter einzeln und nacheinander auf Grundlage der angegebenen Feldwerte bereitgestellt werden.

Diese Methode empfiehlt sich, wenn Sie eine Gruppe von Datenfiltern erstellen möchten, der nicht jede eindeutige Kombination der Feldwerte umfasst.

Zwei Möglichkeiten, Benutzer und Gruppen zuzuordnen: in der Benutzerschnittstelle und in der XML

Sie haben zwei Möglichkeiten, Benutzern und Gruppen zu Datenfiltern zuzuweisen: über die Benutzerschnittstelle oder in dem XML, das Sie zur Erstellung der Datenfilter verwenden. Das Zuweisen von Benutzern in der XML stellt eine nützliche Methode dar, wenn Sie über viele Benutzer verfügen, von denen jeder einen separaten Filter erfordert.

Das Zuweisen von Benutzern in der XML ist nur möglich, wenn Sie Datenfilter mit der **manuellen Spezifikation** erzeugen. Wenn Sie Benutzer in der XML zuweisen, müssen die Datenfilter-IDs die Zuweisung angeben. Und diese IDs sind nur verfügbar, wenn Sie Datenfilter mit der manuellen Spezifikation angeben und nicht mit der automatischen Spezifikation.

Details zur Verwendung dieser beiden Methoden zum Zuweisen von Benutzern und Gruppen finden Sie in diesem Kapitel.

Datenfilterkonzepte

Damit Sie verstehen, wie Datenfilter eingerichtet werden, müssen Sie mit einigen Konzepten vertraut sein, die in der Datenfilterfunktion, allgemein in Datenbanken und im Besonderen in Unica Campaign verwendet werden, wenn Sie Datenfilter zur Verwendung in einer Anwendung der Unica Campaign-Produktreihe einrichten.

- **Datenkonfiguration** - Mit einer Datenkonfiguration werden Datenfiltergruppen gruppiert. Alle Datenfilter, die ähnliche Daten sichern, werden derselben Datenkonfiguration zugeordnet.
- **Zielgruppe** - Felder in Kundentabellen mit der Kennzeichnung als Zielgruppenebene in Unica Campaign. Typische Zielgruppenebenen sind Haushalte und Einzelpersonen.
- **Physischer Feldname** - Die physischen Namen von Feldern in einer Datenbanktabelle sind die Namen, die angezeigt werden, wenn Sie die Tabellen direkt im Datenbankclient anzeigen. Wenn die Datenfilterung aktiv ist, wird der physische Name zum Abrufen von Daten aus der Kundendatenbank verwendet.

- **Logischer Feldname** - Wenn Sie Datenfilter definieren, ordnen Sie physischen Feldern logische Namen zu. Beim Einrichten von Datenfiltern, die in einer Anwendung der Unica Campaign-Produktreihe verwendet werden, müssen diese logischen Namen mit den Namen übereinstimmen, die den Feldern in Unica Campaign zugewiesen wurden. Dieser Name wird vom Dienstprogramm verwendet, wenn es Datenfilter generiert.

Roadmap für den Konfigurationsprozess: Datenfilter erstellen

Verwenden Sie diese Roadmap für den Konfigurationsprozess, um die Aufgaben zu suchen, die zum Konfigurieren von Datenfiltern erforderlich sind. Die Spalte „Abschnitt“ stellt Links zu den Themen bereit, in denen die Aufgaben ausführlich beschrieben werden.

Tabelle 54. Roadmap für Prozess zur Konfiguration von Datenfiltern

Topic	Informationen
• Planung der Datenfilterkriterien: automatische Generierung *(auf Seite 273)* • Planung der Datenfilterkriterien: manuelle Generierung *(auf Seite 275)*	Entscheiden, welche Kundendaten Sie sichern wollen.
Abrufen des JDBC-Treibers für Ihre Datenbank: Nur für die automatische Generierung *(auf Seite 276)*	Nur für die automatische Generierung: Herunterladen des JDBC-Treibers vom Typ 4, der Konnektivität zu der Datenbank gewährleistet, die die Tabelle beinhaltet, die die Basis für Ihre Datenfilter darstellt.
Erhalt erforderlicher Informationen *(auf Seite 276)*	Sammeln der erforderlichen Datenbankinformationen sowie, falls Sie die Datenfilter mit einer Anwendung in der Unica Campaign-Familie verwenden möchten, der Unica Campaign-bezogenen Informationen.

Tabelle 54. Roadmap für Prozess zur Konfiguration von Datenfiltern (Fortsetzung)

Topic	Informationen
Erzeugen der XML-Datei zur Angabe von Datenfiltern *(auf Seite 277)*	Erstellen Sie die XML-Datei, die die Kundendaten festlegt, die als Kriterien für jeden Datenfilter verwendet werden.
Festlegen der erforderlichen Konfigurationseigenschaften für Datenfilter *(auf Seite 278)*	Festlegen der Konfigurationseigenschaften, die die Datenfilterung aktivieren.
Füllen der Datenfilter-Systemtabellen *(auf Seite 279)*	Ausführen des Dienstprogramms `datafilteringScriptTool`, das Ihre XML-Datei verwendet, um die Unica Platform-Systemtabellen zu füllen, die für Ihre Datenfilter verwendet werden.
Zuweisen von Benutzern und Gruppen zu Datenfiltern *(auf Seite 279)*	Wenn Sie Benutzer und Gruppen nicht in der XML zu Datenfiltern zuweisen, verwenden Sie die Unica-Datenfilter-Benutzerschnittstelle, um nach Benutzern, Gruppen und Datenfiltern zu suchen sowie anschließend Elemente aus den Suchergebnissen auszuwählen und diese zuzuordnen.

Planung der Datenfilterkriterien: automatische Generierung

Datenfilterkriterien basieren auf Ihren Kundendaten. Bevor Sie Datenfilter festlegen können, müssen Sie entscheiden, welche Kundendaten Sie sichern möchten.

Sie könnten z. B. den Zugriff auf Kundendaten, basierend auf dem Wohnort der Kunden nach Ländern, Städten oder Bundesländern beschränken. Falls Ihre Kundendatenbank über eine Tabelle mit Land-, Stadt- und Bundesland-Feldern verfügt, könnten Sie eine Gruppe Datenfilter auf diese Felder basieren. Diese Werte würden Sie dann bei der Definierung Ihrer Datenfilter verwenden.

Folgende Konzepte sollten Sie für die Planung der Erstellung von Datenfiltern durch automatische Generierung kennen.

- **Profilfeld** - Ein Feld, dessen Wert berücksichtigt wird, wenn das Dienstprogramm zur Datenfiltergenerierung nach eindeutigen Kombinationen von Werten sucht. Das Dienstprogramm erstellt für jede eindeutige Wertekombination einen Datenfilter. Wenn der Datenfilter in einer Anwendung von Unica verwendet wird, wird dieser Wert in einer Abfrage von Kundendaten als WHERE-Klausel verwendet. Da der Klauselsatz nach Übereinstimmungen sucht, müssen Profilfelder mit den Feldern, die einen festen Satz an eindeutigen Werten unterstützen, übereinstimmen.
- **Festes Feld** - Ein optionales Feld, das die Sätze begrenzt, die das Dienstprogramm zur Datenfiltergenerierung bei der Abfrage eindeutiger Kombinationen von Profilfeldwerten sucht. Der von Ihnen festgelegte Wert ist außerdem in jedem generierten Datenfilter enthalten. Wenn der Datenfilter in einer Anwendung von Unica verwendet wird, wird dieser Wert in einer Abfrage von Kundendaten als WHERE-Klausel verwendet. Da der Klauselsatz nach Übereinstimmungen sucht, müssen Festgelegte Felder mit den Feldern, die einen festen Satz an eindeutigen Werten unterstützen, übereinstimmen.

In dem Beispiel oben würden Sie wahrscheinlich für ein Land ein festgelegtes Feld und für die Stadt und das Bundesland ein Profilfeld festlegen. Das Dienstprogramm zur Datenfiltergenerierung erstellt einen Datenfilter für jede eindeutige Wertekombination, die es in diesen Feldern findet.

Ein Benutzer von Unica, der einem oder mehreren Datenfiltern zugeordnet ist, könnte ausschließlich mit den Daten arbeiten, die zu Kunden gehören, die in dem bzw. den Vertriebsgebiet/en leben, die dem entsprechenden Datenfilter bzw. -filtern zugewiesen sind.

Es kann sein, dass Ihre Kundentabellen nicht alle Werte beinhalten, für die Sie einen Datenfilter erstellen möchten. So kann es z. B. sein, dass Sie nicht in jedem Land und Bundesland Kunden haben, jedoch für die zukünftige Nutzung Datenfilter für jedes Land und jedes Bundesland erstellen möchten. In diesem Fall können Sie auf eine Tabelle verweisen, die jedes Land und jedes Bundesland beinhaltet, und diese im Bereich GenerateDataFilters

Ihrer XML-Spezifikation verwenden. Wenn Sie die Erstellung Ihrer Datenfilter mit dem Dienstprogramm abgeschlossen haben, können Sie diese Testtabelle löschen.

Planung der Datenfilterkriterien: manuelle Generierung

Datenfilterkriterien basieren auf Ihren Kundendaten. Bevor Sie Datenfilter festlegen können, müssen Sie entscheiden, welche Kundendaten Sie sichern möchten.

Sie könnten z.B. den Zugriff auf Kundendaten, basierend auf dem geografischen Vertriebsgebiet, dem der Benutzer von Unica zugewiesen ist, beschränken. Falls ein Bezug zwischen dem Regionsfeld in Ihrer Kundendatenbank und Ihren Vertriebsgebieten besteht, könnten Sie eine Gruppe Datenfilter auf dieses Feld basieren.

Für die Planung der Erstellung von Datenfiltern durch manuelle Spezifikation sollten Sie das Konzept der **Feldeinschränkungen** kennen. Eine Feldeinschränkung ist ein Felder-/Wertepaar, das zur Festlegung eines Datenfilters eingesetzt wird. Dieser Wert wird bei einer Abfrage von Kundendaten als WHERE-Klausel verwendet. Da der Klauselsatz nach Übereinstimmungen sucht, müssen Feldeinschränkungen mit den Feldern, die einen festen Satz an eindeutigen Werten unterstützen, übereinstimmen.

In dem Beispiel könnte das Feld Region die folgenden Werte enthalten: Asien, Europa, Naher Osten, Nordamerika und Südamerika. Diese Werte verwenden Sie bei der Definierung von Feldeinschränkungen für Ihre Datenfilter. Sie würden für jedes Ihrer Vertriebsgebiete einen anderen Filter definieren, indem Sie die Werte im Regionsfeld Ihrer Kundendatenbanken als Feldeinschränkungen verwenden.

Ein Benutzer von Unica, der einem oder mehreren Datenfiltern zugeordnet ist, könnte ausschließlich mit den Daten arbeiten, die zu Kunden gehören, die in dem bzw. den Vertriebsgebieten leben, die dem entsprechenden Datenfilter bzw. -filtern zugewiesen sind.

Die Datenfilter, die Sie mit der manuellen Methode erzeugen, können über die Benutzerschnittstelle oder durch Zuweisungen in der XML zu Benutzern zugewiesen werden.

Abrufen des JDBC-Treibers für Ihre Datenbank: Nur für die automatische Generierung

Wenn Sie mit dem Dienstprogramm zur Datenfiltergenerierung (`datafilteringScriptTool`) Datenfilter automatisch generieren, benötigen Sie einen JDBC-Treiber.

1. Herunterladen des JDBC-Treibers vom Typ 4, der Konnektivität zu der Datenbank gewährleistet, die die Tabelle beinhaltet, die die Basis für Ihre Datenfilter darstellt.
2. Installieren Sie den Treiber auf dem Rechner, auf dem auch Unica Platform installiert ist.
3. Notieren Sie sich den Klassennamen und das Verzeichnis.

Erhalt erforderlicher Informationen

Zum Erzeugen von Datenfiltern müssen Sie Informationen zu Ihren Daten und deren Zuordnung in Ihren Unica-Produkten zusammenstellen.

Nur für die **manuelle Spezifikation**: Beziehen Sie die folgenden Informationen.

- Physischer Name der Tabelle, die die Felder enthält, die Sie benutzen möchten.
- Den festen Satz an Daten der Felder, die Sie für Feldeinschränkungen benutzen möchten.
- Falls Sie die Datenfilter mit einer Anwendung der Unica Campaign-Familie verwenden möchten, besorgen Sie sich die Namen, die in Unica Campaign den folgenden Feldern zugewiesen sind.
    - Die Zielgruppenfelder
    - Die Felder, die Sie für Feldeinschränkungen verwenden möchten.

Nur für die **automatische Generierung**: Beziehen Sie die folgenden Informationen.

- Datenbanktyp, Name bzw. IP-Adresse und Port der Datenbank, die die Tabelle enthält, die Sie zur Definierung Ihrer Datenfilter verwenden möchten.
- Berechtigungsnachweise (Benutzername und Kennwort) für den Verbindungsaufbau zur Datenbank.
- Physischer Name der Tabelle, die die Felder enthält, die Sie benutzen möchten.

- Physische Namen der Felder, die Sie für Profilfelder und festgelegte Felder (festgelegte Felder sind optional) verwenden möchten.
- Falls Sie die Datenfilter mit einer Anwendung der Unica Campaign-Familie verwenden möchten, besorgen Sie sich die Namen, die in Unica Campaign den folgenden Feldern zugewiesen sind.
    - Die Zielgruppenfelder.
    - Die Felder, die Sie für Profilfelder und festgelegte Felder nutzen möchten.

Anmerkung: Beim Einrichten von Datenfiltern, die in einer Anwendung der Unica Campaign-Produktreihe verwendet werden, müssen die logischen Namen der Felder, die Sie in der datenfilterdefinierenden XML-Datei festlegen, mit den Namen übereinstimmen, die diesen Feldern in Unica Campaign zugewiesen wurden.

Erzeugen der XML-Datei zur Angabe von Datenfiltern

Erstellen Sie die XML-Datei, die die Kundendaten festlegt, die als Kriterien für jeden Datenfilter verwendet werden. Im nächsten Schritt werden Sie ein Dienstprogramm ausführen, das die Systemtabellen mit diesen Generierungen ausfüllt.

Zum Erzeugen der Datenfilter verwendet das Dienstprogramm `datafilteringScriptTool` eine XML-Darstellung der Daten, um Einträge in die Unica Platform-Systemtabellendatenbank einzufügen.

Im Folgenden ist ein Überblick der Elemente in der XML-Datei angegeben, die Sie erzeugen.

- `<Execute Batch>` Befehl, der den Dateneinfügeprozess initiiert. Dieser Befehl wird mehrmals innerhalb der XML-Datei wiederholt.
- `<AddDataConfiguration>` - Definiert die Datenkonfigurationen, bei denen es sich um Gruppen verwandter Datenfilter handelt.
- `<AddLogicalFields>` - Definiert die zu filternden Feldern und den Datentyp der Felder.
- `<AddDataFilter>` - Wenn Sie die **manuelle Spezifikation** verwenden, werden ein definiertes logisches Feld referenziert und die Feldeinschränkungen angegeben.
- `<GenerateDataFilters>` - Wenn Sie die **automatische Spezifikation** verwenden, werden die Felder und Werte referenziert, mit denen die Datensätze eingeschränkt

werden, die für eindeutige Kombinationen von Werten berücksichtigt werden, um eine Reihe von Datenfiltern zu definieren.
- `<AddDataTable>` - Definiert die Beziehung zwischen logischen Feldern und deren physischen Tabellen und Spalten. Ein logisches Feld kann auf unterschiedliche physische Tabellen angewendet werden, sodass ein Filter auf mehrere Tabellen angewendet werden kann.
- `<addAudiences>` - Referenziert ein definiertes logisches Feld und gibt die Zielgruppenebene wie in Unica Campaign definiert an.
- `<addAudienceTableAssociations>` - Definiert die Beziehung zwischen einer Zielgruppenebene und der definierten Tabelle und der definierten Datenfilterkonfiguration.
- `<AddAssignments>` - Wenn Sie **Zuweisungen innerhalb der XML-Datei erzeugen, anstatt die Benutzerschnittstelle** zu verwenden, werden einzelne Benutzer oder Gruppen zu definierten Datenfiltern zugewiesen.

Weitere Informationen und Beschreibungen zusätzlicher Elemente, die in den oben beschriebenen Elementen verschachtelt sind, finden Sie in den Themen dieses Kapitels:

- Detaillierte Beschreibungen jedes Elements in der XML
- Die XML für Beispielszenarios

Festlegen der erforderlichen Konfigurationseigenschaften für Datenfilter

Legen Sie die erforderlichen Konfigurationseigenschaften fest, um die Datenfilterung zu aktivieren.

Navigieren Sie auf der Seite **Einstellungen & Konfiguration** zur Kategorie **Allgemeines | Datenfilterung** und legen Sie die folgenden Eigenschaften fest.

- Standardtabellenname
- Standardzielgruppenname

In der Kontexthilfe der Eigenschaft oder unter dem zugehörigen Themenlink in diesem Abschnitt finden Sie Anweisungen zum Einrichten der Werte.

Optionale Konfigurationseigenschaft zum Verbessern der Datenfilterleistung

Sie können den Datenfiltercache zur Verbesserung der Leistung aktivieren.

Setzen Sie zur Verbesserung der Leistung den Wert der Eigenschaft **Allgemeines | Datenfilter | Datenfiltercache aktivieren** auf **true**. Diese Eigenschaft gibt an, ob Unica Platform Datenfilterdefinitionen aus der Datenbank oder aus einem Cache abruft. Wenn Sie diesen Wert auf **true** setzen, werden die Datenfilterdefinitionen im Cache gespeichert, und der Cache wird bei jeder Änderung der Datenfilterdefinitionen aktualisiert.

Sie müssen einen Neustart der Unica Platform-Webanwendung durchführen, nachdem Sie Änderungen an diesem Eigenschaftswert vorgenommen haben, damit die Änderungen wirksam werden.

Füllen der Datenfilter-Systemtabellen

Ausführen des Dienstprogramms `datafilteringScriptTool`, das Ihre XML-Datei verwendet, um die Datenfilter-Systemtabellen zu füllen.

Details zur Verwendung des Dienstprogramms `datafilteringScriptTool` können Sie der vollständigen Beschreibung an anderer Stelle in diesem Handbuch entnehmen.

Anmerkung: Wenn Sie Datenfilter löschen müssen, führen Sie das Skript `ManagerSchema_PurgeDataFiltering.sql` aus, das an anderer Stelle in diesem Handbuch beschrieben wird.

Zuweisen von Benutzern und Gruppen zu Datenfiltern

Wenn Sie Benutzer oder Gruppen nicht in der XML zuweisen, die Sie erzeugen, verwenden Sie die Unica-Datenfilter-Benutzerschnittstelle, um nach Benutzern, Gruppen und Datenfiltern zu suchen sowie anschließend Elemente aus den Suchergebnissen auszuwählen und diese zuzuordnen.

XML-Datenfilterreferenz

In diesem Abschnitt werden die XML-Elemente beschrieben, für die Werte angegeben werden müssen.

Informationen über die IDs in der XML

Einige Objekte erfordern IDs. Die Angabe von IDs ist z.B. für Datenkonfigurationen, logische Felder und Datentabellen erforderlich. Die angegebenen IDs müssen innerhalb einer Objektkategorie eindeutig sein.

Einige Objekte verweisen auf andere Objekte, die IDs verwenden. Tabellen verweisen beispielsweise auf logische Felder. Wenn Sie auf ein anderes Objekt verweisen möchten, verwenden Sie dazu die ID, die Sie für das Objekt angegeben haben.

Die XML verwendet die folgende Konvention für ID-Elementnamen. Diese Konvention erleichtert es zu verstehen, wann eine eindeutige ID erstellt und wann auf eine andere ID in der XML verwiesen werden muss.

- Wenn eine eindeutige ID erstellt werden muss, erhält das Element den Namen `id`.
- Wenn auf eine andere Objekt-ID verwiesen werden muss, wird das Element nach dem Objekt benannt. Das ID-Element, mit dem Sie auf ein logisches Feld verweisen, erhält z.B. den Namen `logicalFieldId`.

Beachten Sie, dass die einem Objekt zugewiesenen IDs nicht die IDs sind, die Unica Platform dem Objekt zuordnet. Die zugewiesenen IDs werden nur für die Referenz auf das Objekt in der XML verwendet.

AddDataConfiguration | dataConfiguration

Mit dieser Gruppe von Elementen werden die Datenkonfigurationen definiert, die Sie mit gruppenbezogenen Datenfiltern verwenden. Für jede Gruppe mit zugehörigen Datenfiltern sollte eine Datenkonfiguration erstellt werden.

Tabelle 55. AddDataConfiguration | dataConfiguration

Element	Beschreibung	Systemtabelle
`id`	Eindeutige ID, die dieser Datenkonfiguration zugewiesen wird.	Nicht zutreffend
`name`	Name, der dieser Gruppe von Datenfiltern zugewiesen wird.	Tabelle: df_config Feld: config_name

AddLogicalFields | logicalFields | LogicalField

Mit dieser Gruppe von Elementen werden die logischen Felder definiert, die den Feldern in der Kundentabelle entsprechen, mit denen die Datenfelder definiert werden. Erstellen Sie ein logisches Feld für jedes Feld, aus dem Sie Feldeinschränkungen erstellen möchten, sowie ein logisches Feld für jede Zielgruppe.

Tabelle 56. AddLogicalFields | logicalFields | LogicalField

Element	Beschreibung	Systemtabelle
`id`	Eindeutige ID, die diesem logischen Feld zugewiesen wird.	Nicht zutreffend
`name`	Logischer Name dieses Felds oder dieser Zielgruppe. Bei Verwendung mit einer Anwendung der Unica Campaign-Reihe muss der logische Name mit dem Feld- oder Zielgruppennamen in Unica Campaign übereinstimmen.	Tabelle: df_logical_field Feld: logical_name
`type`	Datentyp dieses Felds in der Kundentabelle. Zulässige Werte sind: • java.lang.String • java.lang.Long	Tabelle: df_logical_field Feld: Typ

Tabelle 56. AddLogicalFields | logicalFields | LogicalField (Fortsetzung)

Element	Beschreibung	Systemtabelle
	• java.lang.Double • java.lang.Boolean • java.lang.Date (Das Datumsformat ist Monat/Tag/Jahr, wobei Monat, Tag und Jahr jeweils in Zahlen ausgedrückt werden.)	

GenerateDataFilters

Diese Gruppe von Elementen wird zur Generierung eines Datenfilters bei Verwendung der **manuellen Spezifikation** verwendet.

Tabelle 57. GenerateDataFilters

Element	Beschreibung	Systemtabelle
`tableName`	Physischer Name der Tabelle, von der aus die Datenfilter generiert werden sollen, einschließlich des Namens des Datenbankschemas. Wenn in der Datenbank die Groß- und Kleinschreibung beachtet wird, muss sie mit der Groß- und Kleinschreibung in der Datenbank übereinstimmen.	Tabelle: df_table Feld: table_name
`configurationName`	Name der Datenkonfiguration im Element `AddDataConfiguration | dataConfigurati-`	Nicht zutreffend

Tabelle 57. GenerateDataFilters (Fortsetzung)

Element	Beschreibung	Systemtabelle
	on, dem dieser Filter zugeordnet ist.	
jdbcUrl	Die URL-Referenz für die Kundendatenbank, die die Tabelle beinhaltet, die die Basis für Ihre Datenfilter darstellt.	Nicht zutreffend
jdbcUser	Der Benutzername eines Kontos mit Zugriff auf die Kundendatenbank.	Nicht zutreffend
jdbcPassword	Das Kennwort des Kontos mit Zugriff auf die Kundendatenbank.	Nicht zutreffend
jdbcDriverClass	Der Name des JDBC-Treibers, unter den die Konnektivität mit der Kundendatenbank hergestellt wird.	Nicht zutreffend
jdbcDriverClass-Path | string	Der Pfad des JDBC-Treibers.	Nicht zutreffend

GenerateDataFilters | fixedFields | FixedField

Mit dieser Gruppe von Elementen werden die optionalen Felder und die Werte anzugeben, mit denen die Datensätze eingeschränkt werden, die berücksichtigt werden, wenn das Dienstprogramm zur Datenfiltergenerierung nach eindeutigen Kombinationen von Werten sucht, um eine Reihe von Datenfiltern zu definieren. Wird nur zusammen mit der **automatischen Generierung** verwendet.

Tabelle 58. GenerateDataFilters | fixedFields | FixedField

Element	Beschreibung	Systemtabelle
`expression`	Ein Element der Daten im Feld, die in einer WHERE-Klausel verwendet werden, wenn Daten für Datenfilter erstellt und Daten für einen Benutzer, der diesem Filter zugewiesen ist, abgerufen werden. Wenn in der Datenbank die Groß- und Kleinschreibung beachtet wird, muss sie mit der Groß- und Kleinschreibung in der Datenbank übereinstimmen.	Tabelle: df_fieldconstraint Feld: expression
`logicalFieldName`	Name des logischen Felds im Element AddLogicalFields | logicalFields | LogicalField. Dieser Name wird als Beschriftung im Feld für die erweiterte Suche in der Datenfilter-Benutzeroberfläche in Unica Platform verwendet.	Tabelle: df_logical_field Feld: logical_name
`physicalFieldName`	Physischer Name des Felds. Wenn in der Datenbank die Groß- und Kleinschreibung beachtet wird, muss sie mit der Groß- und Kleinschreibung in der Datenbank übereinstimmen.	Nicht zutreffend

GenerateDataFilters | ProfilField | ProfileField

Mit dieser Gruppe von Elementen können Sie die Felder angeben, mit deren eindeutigen Kombinationen von Werten eine Reihe von Datenfiltern definiert wird. Wird nur zusammen mit der **automatischen Generierung** verwendet.

Tabelle 59. GenerateDataFilters | ProfilField | ProfileField

Element	Beschreibung	Systemtabelle
`logicalFieldName`	Name des logischen Felds im Element `AddLogicalFields | logicalFields | Logical-Field`.	Tabelle: df_logical_field Feld: logical_name
`physicalFieldName`	Physischer Name des Felds. Wenn in der Datenbank die Groß- und Kleinschreibung beachtet wird, muss sie mit der Groß- und Kleinschreibung in der Datenbank übereinstimmen.	Nicht zutreffend

AddDataTable | dataTable

Diese Gruppe von Elementen wird verwendet, um IDs an Kundentabellen zuzuordnen.

Tabelle 60. AddDataTable | dataTable

Element	Beschreibung	Systemtabelle
`id`	Eindeutige ID, die dieser Tabelle zugewiesen wird.	Nicht zutreffend
`name`	Physischer Name der Kundentabelle, die gesichert werden soll. Wenn in der Datenbank die Groß- und Kleinschreibung beachtet	Tabelle: df_table Feld: table_name

Tabelle 60. AddDataTable | dataTable (Fortsetzung)

Element	Beschreibung	Systemtabelle
	wird, muss sie mit der Groß- und Kleinschreibung in der Datenbank übereinstimmen.	

AddDataFilters | dataFilters | DataFilter

Diese Gruppe von Elementen wird zum Erzeugen eines Datenfilters bei Verwendung der **manuellen Spezifikation** verwendet.

Tabelle 61. AddDataFilters | dataFilters | DataFilter

Element	Beschreibung	Systemtabelle
`configId`	ID der Datenkonfiguration im Element AddDataConfiguration | dataConfiguration, dem dieser Filter zugeordnet ist.	Nicht zutreffend
`id`	Eindeutige ID, die Sie zuordnen.	Nicht zutreffend

AddDataFilters | dataFilters | DataFilter | fieldConstraints | FieldConstraint

Mit dieser Gruppe von Elementen können Sie die Daten in einem Feld angeben, mit dem ein Datenfilter bei Verwendung der **manuellen Spezifikation** definiert wird.

Tabelle 62. AddDataFilters | dataFilters | DataFilter | fieldConstraints | FieldConstraint

Element	Beschreibung	Systemtabelle
`logicalField-Id`	Name des logischen Felds im Element `AddLogicalFields |`	Nicht zutreffend

Tabelle 62. AddDataFilters | dataFilters | DataFilter | fieldConstraints | FieldConstraint (Fortsetzung)

Element	Beschreibung	Systemtabelle
	`logicalFields | Logical-Field`.	
`expression`	Ein Element der Daten im Feld, die in einer `WHERE`-Klausel verwendet werden, wenn Daten für Datenfilter erstellt und Daten für einen Benutzer, der diesem Filter zugewiesen ist, abgerufen werden. Wenn in der Datenbank die Groß- und Kleinschreibung beachtet wird, muss sie mit der Groß- und Kleinschreibung in der Datenbank übereinstimmen.	Tabelle: df_fieldconstraint Feld: expression

AddDataTable | dataTable | fields | TableField

Mit dieser Gruppe von Elementen werden physische Felder in der Kundentabelle logischen Feldern zugeordnet, die Sie definiert haben.

Tabelle 63. AddDataTable | dataTable | fields | TableField

Element	Beschreibung	Systemtabelle
`name`	Physischer Name des Felds in der Kundentabelle. Wenn in der Datenbank die Groß- und Kleinschreibung beachtet wird, muss sie mit der Groß- und Kleinschreibung in der Datenbank übereinstimmen.	Tabelle: df_table_field Feld: physical_name

Tabelle 63. AddDataTable | dataTable | fields | TableField (Fortsetzung)

Element	Beschreibung	Systemtabelle
`logicalField-Id`	Name des logischen Felds im Element `AddLogicalFields | logicalFields | Logical-Field`.	Nicht zutreffend

AddAudience | audience

Mit dieser Gruppe von Elementen wird der Name angegeben, der in Unica Campaign einer Zielgruppenebene zugewiesen ist, die in der Unica Campaign-Produktreihe verwendet wird.

Tabelle 64. AddAudience | audience

Element	Beschreibung	Systemtabelle
`id`	Eindeutige ID, die dieser Zielgruppe zugewiesen wird.	Nicht zutreffend
`name`	Name der Zielgruppe, wie in Unica Campaign angegeben.	Tabelle: df_audience Feld: audience_name

AddAudience | audience | fields | AudienceField

Mit dieser Gruppe von Elementen erfolgt die Angabe des Felds oder der Felder in den Kundentabellen, die als Zielgruppenfelder verwendet werden.

Tabelle 65. AddAudience | audience | fields | AudienceField

Element	Beschreibung	Systemtabelle
`logicalField-Id`	Name des logischen Felds im Element `AddLogicalFields | logicalFields | Logical-Field`. Bei Verwendung mit ei-	Nicht zutreffend

Tabelle 65. AddAudience | audience | fields | AudienceField (Fortsetzung)

Element	Beschreibung	Systemtabelle
	ner Anwendung der Unica Campaign-Reihe muss derselbe logische Name in Unica Campaign verwendet werden.	
`fieldOrder`	Für die zukünftige Verwendung. Setzen Sie den Wert auf `0`.	Nicht zutreffend

addAudienceTableAssociations | addAudienceTableAssociation | audienceTableAssociation

Diese Gruppe von Elementen wird dazu verwendet, jeweils ein Zielgruppenfeld und eine Tabelle Datenkonfigurationen zuzuordnen. Erstellen Sie eine Zuordnung für jedes Zielgruppenfeld.

Tabelle 66. addAudienceTableAssociations | addAudienceTableAssociation | audienceTableAssociation

Element	Beschreibung	Systemtabelle
`audienceId`	ID der Zieltruppe, die in dieser Zuordnung verwendet wird. Der ID-Wert muss dem Element `AddAudience | audience` angehören.	Nicht zutreffend
`tableId`	ID der Tabelle, die in dieser Zuordnung verwendet wird. Der ID-Wert muss dem Element `AddDataTable | dataTable` angehören. Die Tabelle muss die Zielgruppe enthalten, die im audienceID-Element angegeben wird.	Nicht zutreffend

Tabelle 66. addAudienceTableAssociations | addAudienceTableAssociation | audienceTableAssociation (Fortsetzung)

Element	Beschreibung	Systemtabelle
	Wenn die Zielgruppe in mehr als einer Tabelle enthalten ist, erstellen Sie mehrere Zuweisungen.	
`configId`	ID der Datenkonfiguration, die in dieser Zuordnung verwendet wird. Der ID-Wert muss dem Element `AddDataConfiguration | dataConfiguration` angehören.	Nicht zutreffend

AddAssignments | assignments | AssignmentByName

Sie können diese Gruppe von Elementen verwenden, um Benutzer oder Gruppen mit Datenfiltern zuzuweisen. Optional. Sie können diese Zuweisungen auch über die Benutzerschnittstelle vornehmen.

Tabelle 67. AddAssignments | assignments | AssignmentByName

Element	Beschreibung	Systemtabelle
`namespaceId`	Name der Datenkonfiguration im Element `AddDataConfiguration | dataConfiguration`, dem dieser Filter zugeordnet ist.	Nicht zutreffend
`dataObjectId`	ID des Filters, der in dieser Zuordnung verwendet wird. Der ID-Wert muss dem Element `DataFilter` angehören.	Nicht zutreffend
`principalType`	Der Typ der Zuweisung	Tabelle: ols_assignment Feld: principal_type

Tabelle 67. AddAssignments | assignments | AssignmentByName (Fortsetzung)

Element	Beschreibung	Systemtabelle
	• 1 steht für das Zuweisen eines Datenfilters zu einem einzelnen Benutzer • 2 steht für das Zuweisen eines Datenfilters zu einer Gruppe von Benutzern	
`principalName`	• Wenn der für principalType verwendete Wert `1` lautet, legen Sie den Wert auf die Unica Platform-Anmeldung des Benutzers fest, die Sie dem referenzierten Datenfilter zuweisen möchten. • Wenn der für principalType verwendete Wert `2` lautet, legen Sie den Wert auf den Namen der Unica Platform-Gruppe fest, deren Mitglieder Sie dem referenzierten Datenfilter zuweisen möchten.	Tabelle: ols_assignment Feld: principal_id

Beispiel: Manuelles Angeben von Datenfiltern

Jim muss eine Gruppe von Datenfiltern basierend auf Vertriebsgebieten erstellen.

In Unica Campaign wurden die Kundentabellen bereits zugeordnet und Zielgruppenebenen definiert.

Abrufen von Informationen

Jim stellt fest, dass die Gebietstabelle die Felder enthält, die als Feldeinschränkung für die Datenfilter angegeben werden müssen.

Die folgende Tabelle enthält die Informationen, die Jim zu den Kundenfeldern und ihrer Unica Campaign-Zuweisung abruft.

Tabelle 68. Felder der Gebietstabelle

Felder (physischer Name)	Felder (Name in Unica Campaign)	Daten	Datentyp
cust_region	CustomerRegion	• Ostafrika • Asien • Europa • Naher Osten • Nordameri-ka	java.lang-.String
hh_id	HouseholdID	Nicht zutreffend	java.lang.Long
indiv_id	IndividualID	Nicht zutreffend	java.lang.Long

Jim erfährt, dass die in Unica Campaign verwendeten Zielgruppennamen „household“ (Haushalt) und „individual“ (Einzelperson) sind. Er stellt fest, dass die Gebietstabelle zwei Zielgruppenfelder enthält. Das Feld hh_id entspricht der Zielgruppe household. Das Feld indiv_id in der Tabelle „Territory“ entspricht der Zielgruppe „individual“.

Da Jim ein logisches Feld für jede Zielgruppe und eines für jede Feldeinschränkung erstellen muss, sind insgesamt drei logische Felder erforderlich.

Jim ist außerdem bewusst, dass die Datenfilter in einer Datenkonfiguration angeordnet werden müssen. Er beschließt, die Datenkonfiguration „Territory“ zu nennen.

Jim kann jetzt die XML-Datei erstellen.

Erstellen der XML-Datei

Nachfolgend wird die XML-Datei angezeigt, die Jim erstellt. Die Werte, die er auf Grundlage der abgerufenen Informationen verwendet, sind **`fettgedruckt`** .

```
<ExecuteBatch>
                <!-- ********************************* -->
                <!--          Data configuration       -->
                <!-- ********************************* -->
  <name>SeedData</name>
  <operations>
      <ExecuteBatch>
        <name>DataFilters</name>
        <operations>
          <AddDataConfiguration>
            <dataConfiguration>
                <id>1</id>
                <name>Territory</name>
            </dataConfiguration>
           </AddDataConfiguration>
         </operations>
       </ExecuteBatch>
                <!-- ********************************* -->
                <!--         Logical fields            -->
                <!-- ********************************* -->
      <AddLogicalFields>
        <logicalFields>
            <LogicalField>
                <id>1</id>
                <name>CustomerRegion</name>
                <type>java.lang.String</type>
            </LogicalField>
            <LogicalField>
                <id>2</id>
```

```
            <name>HouseholdID</name>
            <type>java.lang.Long</type>
        </LogicalField>
        <LogicalField>
            <id>3</id>
            <name>IndividualID</name>
            <type>java.lang.Long</type>
        </LogicalField>
        </logicalFields>
 </AddLogicalFields>
            <!-- ********************************* -->
            <!--    Territory field constraints    -->
            <!-- ********************************* -->
<AddDataFilters>
  <dataFilters>
    <DataFilter>
      <configId>1</configId>
      <id>1</id>
      <fieldConstraints>
        <FieldConstraint>
          <logicalFieldId>1</logicalFieldId>
          <expression>Africa</expression>
        </FieldConstraint>
      </fieldConstraints>
    </DataFilter>
    <DataFilter>
      <configId>1</configId>
      <id>2</id>
      <fieldConstraints>
        <FieldConstraint>
          <logicalFieldId>1</logicalFieldId>
          <expression>Asia</expression>
```

```
        </FieldConstraint>
      </fieldConstraints>
    </DataFilter>
    <DataFilter>
      <configId>1</configId>
      <id>3</id>
      <fieldConstraints>
        <FieldConstraint>
          <logicalFieldId>1</logicalFieldId>
          <expression>Europe</expression>
        </FieldConstraint>
      </fieldConstraints>
    </DataFilter>
    <DataFilter>
      <configId>1</configId>
      <id>4</id>
      <fieldConstraints>
        <FieldConstraint>
          <logicalFieldId>1</logicalFieldId>
          <expression>Middle East</expression>
        </FieldConstraint>
      </fieldConstraints>
    </DataFilter>
    <DataFilter>
      <configId>1</configId>
      <id>5</id>
      <fieldConstraints>
        <FieldConstraint>
          <logicalFieldId>1</logicalFieldId>
          <expression>North America</expression>
        </FieldConstraint>
      </fieldConstraints>
```

```
        </DataFilter>
      </dataFilters>
    </AddDataFilters>
            <!-- ********************************* -->
            <!--   Map physical to logical fields   -->
            <!-- ********************************* -->
    <ExecuteBatch>
      <name>addTables</name>
      <operations>
        <AddDataTable>
          <dataTable>
          <id>1</id>
          <name>Territory</name>
          <fields>
            <TableField>
              <name>cust_region</name>
              <logicalFieldId>1</logicalFieldId>
            </TableField>
            <TableField>
              <name>hh_id</name>
              <logicalFieldId>2</logicalFieldId>
            </TableField>
            <TableField>
              <name>indiv_id</name>
              <logicalFieldId>3</logicalFieldId>
            </TableField>
          </fields>
          </dataTable>
        </AddDataTable>
      </operations>
    </ExecuteBatch>
```

```
                <!--
**********************************************************  -->
                <!--              Audience table associations
   -->
                <!--
**********************************************************  -->
      <ExecuteBatch>
             <name>addAudiences</name>
             <operations>
             <AddAudience>
               <audience>
               <id>1</id>
               <name>household</name>
               <fields>
                 <AudienceField>
                   <logicalFieldId>2</logicalFieldId>
                   <fieldOrder>0</fieldOrder>
                 </AudienceField>
               </fields>
             </audience>
           </AddAudience>
           <AddAudience>
               <audience>
               <id>2</id>
               <name>individual</name>
               <fields>
                 <AudienceField>
                   <logicalFieldId>3</logicalFieldId>
                   <fieldOrder>0</fieldOrder>
                 </AudienceField>
               </fields>
               </audience>
```

```
              </AddAudience>
              </operations>
       </ExecuteBatch>
                <!--
 ******************************************************* -->
                <!--            Associate table-audience pairs
  -->
                <!--               with data configuration
  -->
                <!--
 ******************************************************* -->
       <ExecuteBatch>
             <name>addAudienceTableAssociations</name>
             <operations>
             <AddAudienceTableAssociation>
                 <audienceTableAssociation>
                   <audienceId>1</audienceId>
                   <tableId>1</tableId>
                   <configId>1</configId>
               </audienceTableAssociation>
             </AddAudienceTableAssociation>
             <AddAudienceTableAssociation>
                 <audienceTableAssociation>
                   <audienceId>2</audienceId>
                   <tableId>1</tableId>
                   <configId>1</configId>
                 </audienceTableAssociation>
             </AddAudienceTableAssociation>
             </operations>
       </ExecuteBatch>
    </operations>
</ExecuteBatch>
```

Ausfüllen der Systemtabellen

Jim hat die XML-Datenfilterdatei `regionDataFilters.xml` genannt und in der Unica Platform-Installation im Verzeichnis `tools/bin` gespeichert. Er öffnet eine Eingabeaufforderung und füllt die Systemtabellen des Datenfilters mithilfe des Dienstprogramms datafilteringScriptTool aus.

Zuweisen von Benutzern und Gruppen zu den Datenfiltern

Am Schluss meldet sich Jim mit einem Konto mit Unica-Administratorberechtigungen an Unica Platform an.

Er weiß, dass bereits Gruppen in Unica eingerichtet wurden und diese Benutzer enthalten, die nach Stadt zugeordnet wurden.

Jim navigiert zum Bereich mit den Datenfiltern und stellt fest, dass die Feldeinschränkungen aus seinen Datenfiltern in der erweiterten Suche als Datenfilter verfügbar sind. Er führt eine Suche für einen Datenfilter aus und gibt „Africa“ als Suchkriterium an. Der von ihm eingerichtete Datenfilter für das Gebiet Africa wird in den Suchergebnissen angezeigt.

Danach führt Jim eine Suche für die Benutzergruppe Africa aus, die in Unica eingerichtet wurde, um alle dezentrale Marketiers aufzuführen, die in Afrika für das Kundenmarketing zuständig sind. Die Gruppe Africa wird in den Suchergebnissen angezeigt.

Jim wählt daraufhin die Gruppe und die Datenfilter in den Suchergebnissen aus und weist die Gruppe dem Datenfilter zu, indem er auf Zuweisen klickt.

Er führt weitere Suchläufe für Datenfilter und Gruppen aus, bis alle Zuweisungen abgeschlossen sind.

Beispiel: Gruppe von Datenfiltern automatisch generieren

Jim muss eine Gruppe von Datenfiltern basierend auf Ländern, Städten und Bundesländern erstellen.

In Unica Campaign wurden die Kundentabellen bereits zugeordnet und Zielgruppenebenen definiert.

Herunterladen des JDBC-Treibers

Jim weiß, dass die Kundendatenbank des Unternehmens eine Microsoft™ SQL Server-Datenbank ist. Er lädt den entsprechenden Treiber vom Typ 4 herunter und legt ihn auf dem Computer mit der Unica Platform-Installation ab, wobei er den Namen und Pfad des Treibers dokumentiert.

- Name der JDBC-Treiberklasse - `com.microsoft.sqlserver.jdbc.SQLServerDriver`
- Pfade des JDBC-Treibers - `C:\tools\Java\MsJdbc\sqljdbc.jar`

Abrufen von Informationen

Jim ruft den Namen, Host und Port der Kundendatenbank sowie die Berechtigungsnachweise ab, die für die Herstellung der Verbindung erforderlich sind.

- Datenbankname - Kunden
- Datenbankhostname - companyHost
- Datenbankport - 1433
- Benutzername - sa
- Kennwort - myPassword

Jim sichtet die Daten in der Kundendatenbank des Unternehmens und stellt fest, dass es in allen Ländern, Städten und Bundesländern, für die ein Filter erstellt werden soll, Kunden gibt. Er bemerkt, dass die geografische Tabelle die Felder enthält, die als festgelegte Felder und Profilfelder für die Datenfilter angegeben werden müssen.

Die folgende Tabelle enthält die Informationen, die Jim zu den Kundenfeldern und ihrer Unica Campaign-Zuweisung abruft.

Tabelle 69. Felder der geografischen Tabelle

Felder (physischer Name)	Felder (Name in Unica Campaign)	Daten	Datentyp
Land	Land	• USA • Frankreich • Großbritannien	java.lang.String
Ort	Ort	Ein fester Satz mit verschiedenen Städten	java.lang.String
STATUS	Status	Ein fester Satz mit verschiedenen Bundesländern (bzw. anders benannten Regionen, je nach Land)	java.lang.String
hh_id	HouseholdID	Nicht zutreffend	java.lang.Long
indiv_id	IndividualID	Nicht zutreffend	java.lang.Long

Jim erfährt, dass die in Unica Campaign verwendeten Zielgruppennamen „household“ (Haushalt) und „individual“ (Einzelperson) sind. Er stellt fest, dass die geographische Tabelle zwei Zielgruppenfelder enthält.

- Das Feld `hh_id` entspricht der Zielgruppe household.
- Das Feld `indiv_id` in der Tabelle „Geographic“ entspricht der Zielgruppe „individual“.

Da Jim ein logisches Feld für jede Zielgruppe und eines für jedes festgelegte Feld und Profilfeld erstellen muss, sind insgesamt fünf logische Felder erforderlich.

Jim ist außerdem bewusst, dass die Datenfilter in einer Datenkonfiguration angeordnet werden müssen. Er beschließt, die Datenkonfiguration „Geographic“ zu nennen.

Jim kann jetzt die XML-Datei erstellen.

Erstellen der XML-Datei

Nachfolgend wird die XML-Datei angezeigt, die Jim erstellt. Die Werte, die er auf Grundlage der abgerufenen Informationen verwendet oder für die er sich entscheidet, sind **`fettgedruckt`**.

```
<ExecuteBatch>
               <!-- ********************************* -->
               <!--          Data configuration       -->
               <!-- ********************************* -->
  <name>SeedData</name>
  <operations>
      <ExecuteBatch>
        <name>DataFilters</name>
        <operations>
            <AddDataConfiguration>
                <dataConfiguration>
                    <id>1</id>
                    <name>Geographic</name>
                <</dataConfiguration>
                <</AddDataConfiguration>
        </operations>
      </ExecuteBatch>
               <!-- ********************************* -->
               <!--         Logical fields            -->
               <!-- ********************************* -->
      <AddLogicalFields>
```

```
        <logicalFields>
            <LogicalField>
                <id>1</id>
                <name>Country</name>
                <type>java.lang.String</type>
            </LogicalField>
            <LogicalField>
                <id>2</id>
                <name>City</name>
                <type>java.lang.String</type>
            </LogicalField>
            <LogicalField>
                <id>3</id>
                <name>State</name>
                <type>java.lang.String</type>
            </LogicalField>
            <LogicalField>
                <id>4</id>
                <name>HouseholdID</name>
                <type>java.lang.Long</type>
            </LogicalField>
            <LogicalField>
                <id>5</id>
                <name>IndividualID</name>
                <type>java.lang.Long</type>
            </LogicalField>
            </logicalFields>
    </AddLogicalFields>
                <!-- ********************************* -->
                <!--       Generate data filters       -->
                <!-- ********************************* -->
    <GenerateDataFilters>
```

```
               <!--
****************************************************** -->
               <!-- Specify the table to be scanned for unique
combinations -->
               <!-- of values  from which data filters will be defined.
 -->
               <!--
****************************************************** -->
             <tableName>Geographic</tableName>
               <!--
****************************************************** -->
               <!-- Identify the data configuration  with which
 -->
               <!-- generated data filters will be associated.
 -->
               <!--
****************************************************** -->
            <configurationName>Geographic</configurationName>
             <!-- Specify the data source connection information. -->
            <jdbcUrl>
              jdbc:sqlserver://localhost:1433;databaseName=Customers
            </jdbcUrl>
            <jdbcUser>sa</jdbcUser>
            <jdbcPassword>myPassword</jdbcPassword>
            <jdbcDriverClass>

 com.microsoft.sqlserver.jdbc.SQLServerDriver</jdbcDriverClass>
            <jdbcDriverClassPath>
                  <string>C:\tools\Java\MsJdbc\sqljdbc.jar</string>
            </jdbcDriverClassPath>
               <!-- ********************************** -->
               <!--      Specify the fixed fields      -->
```

```
            <!-- ********************************* -->
        <fixedFields>
            <FixedField>
               <expression>USA</expression>
               <logicalFieldName>Country</logicalFieldName>
               <physicalFieldName>country</physicalFieldName>
            </FixedField>
            <FixedField>
               <expression>France</expression>
               <logicalFieldName>Country</logicalFieldName>
               <physicalFieldName>country</physicalFieldName>
            </FixedField>
            <FixedField>
               <expression>Britain</expression>
               <logicalFieldName>Country</logicalFieldName>
               <physicalFieldName>country</physicalFieldName>
            </FixedField>
        </fixedFields>
        <!-- Specify the profile fields. -->
        <profileFields>
            <ProfileField>
               <logicalFieldName>State</logicalFieldName>
               <physicalFieldName>state</physicalFieldName>
            </ProfileField>
            <ProfileField>
               <logicalFieldName>City</logicalFieldName>
               <physicalFieldName>city</physicalFieldName>
            </ProfileField>
        </profileFields>
    </GenerateDataFilters>
            <!-- ********************************* -->
            <!--   Map physical to logical fields   -->
```

```
            <!-- ******************************** -->
    <ExecuteBatch>
        <name>addTables</name>
        <operations>
        <AddDataTable>
            <dataTable>
            <id>1</id>
            <name>Geographic</name>
            <fields>
               <TableField>
                    <name>country</name>
                    <logicalFieldId>1</logicalFieldId>
               </TableField>
               <TableField>
                    <name>city</name>
                    <logicalFieldId>2</logicalFieldId>
               </TableField>
               <TableField>
                    <name>state</name>
                    <logicalFieldId>3</logicalFieldId>
               </TableField>
               <TableField>
                    <name>hh_id</name>
                    <logicalFieldId>4</logicalFieldId>
               </TableField>
               <TableField>
                    <name>indiv_id</name>
                    <logicalFieldId>5</logicalFieldId>
               </TableField>
            </fields>
            </dataTable>
            </AddDataTable>
```

```
            </operations>
      </ExecuteBatch>
               <!--
*******************************************************  -->
               <!--              Audience table associations
   -->
               <!--
*******************************************************  -->
      <ExecuteBatch>
            <name>addAudiences</name>
            <operations>
            <AddAudience>
                <audience>
                <id>1</id>
                <name>household</name>
                <fields>
                   <AudienceField>
                      <logicalFieldId>4</logicalFieldId>
                      <fieldOrder>0</fieldOrder>
                   </AudienceField>
                </fields>
                </audience>
            </AddAudience>
            <AddAudience>
                <audience>
                <id>2</id>
                <name>individual</name>
                <fields>
                   <AudienceField>
                     <logicalFieldId>5</logicalFieldId>
                     <fieldOrder>0</fieldOrder>
                   </AudienceField>
```

```
                </fields>
                </audience>
            </AddAudience>
            </operations>
      </ExecuteBatch>
               <!--
*************************************************** -->
               <!--            Associate table-audience pairs
 -->
               <!--               with data configuration
 -->
               <!--
*************************************************** -->
      <ExecuteBatch>
            <name>addAudienceTableAssociations</name>
            <operations>
            <AddAudienceTableAssociation>
               <audienceTableAssociation>
                   <audienceId>1</audienceId>
                   <tableId>1</tableId>
                   <configId>1</configId>
               </audienceTableAssociation>
            </AddAudienceTableAssociation>
            <AddAudienceTableAssociation>
               <audienceTableAssociation>
                   <audienceId>2</audienceId>
                   <tableId>1</tableId>
                   <configId>1</configId>
               </audienceTableAssociation>
            </AddAudienceTableAssociation>
            </operations>
      </ExecuteBatch>
```

```
   </operations>
</ExecuteBatch>
```

Ausfüllen der Systemtabellen

Jim hat die XML-Datenfilterdatei `geographicDataFilters.xml` genannt und in der Unica Platform-Installation im Verzeichnis `tools/bin` gespeichert. Er öffnet eine Eingabeaufforderung und füllt die Systemtabellen des Datenfilters mithilfe des Dienstprogramms `datafilteringScriptTool` aus.

Das Dienstprogramm erstellt viele Datenfilter. In jedem Datenfilter sind die Kriterien ein Land (das festgelegte Feld) und eine eindeutige Kombination einer Stadt und eines Bundeslandes, die vom Dienstprogramm aus der Datenbank als Datensätze mit enthaltenem festgelegtem Feldwert abgerufen wurden. Alle eindeutigen Kombinationen einer Stadt und eines Bundeslands werden für die einzelnen Länder, die als festgelegtes Feld angegeben wurden, verwendet.

Zuweisen von Benutzern und Gruppen zu den Datenfiltern

Am Schluss meldet sich Jim mit einem Konto mit Administratorberechtigungen in Unica Platform an Unica Platform an.

Er weiß, dass bereits Gruppen in Unica Platform eingerichtet wurden und diese Benutzer enthalten, die nach Stadt zugeordnet wurden.

Jim navigiert zum Bereich mit den Datenfiltern und stellt fest, dass die Werte für Land, Stadt und Bundesland aus seinen Datenfiltern in der erweiterten Suche als Datenfilter verfügbar sind. Er führt eine Suche für einen Datenfilter aus und gibt die Stadt Boston in den USA als Suchkriterium an. Der Datenfilter für Boston wird in den Suchergebnissen angezeigt.

Danach führt Jim eine Suche für die Benutzergruppe „Boston“ aus, die in Unica Platform eingerichtet wurde, um alle dezentralen Marketiers aufzuführen, die in Boston für das Kundenmarketing zuständig sind. Die Gruppe Boston wird in den Suchergebnissen angezeigt.

Jim wählt daraufhin die Gruppe und die Datenfilter in den Suchergebnissen aus und weist die Gruppe dem Datenfilter zu, indem er auf Zuweisen klickt.

Er führt weitere Suchläufe für Datenfilter und Gruppen aus, bis alle Zuweisungen abgeschlossen sind.

Informationen zum Zuweisen von Benutzern und Gruppen in der XML

Alternativ zur Verwendung der Benutzerschnittstelle können Sie Benutzer oder Gruppen auch in der XML zu Datenfiltern zuweisen. Das Zuweisen von Benutzern und Gruppen zu Datenfiltern in der XML ist nur möglich, wenn Sie zum Erzeugen der Datenfilter die manuelle Spezifikation verwenden.

Sie können den Platzhalter `#user_login#` verwenden, der Datenfilter automatisch basierend auf dem Unica Platform-Anmeldenamen des Benutzers erzeugt.

Sie verwenden den XML-Elementblock `AddAssignments`, um Benutzer und Gruppen mit Ihren Datenfiltern zuzuweisen.

In dem Beispiel verwendetes Szenario

In dem Beispiel wird das folgende Szenario verwendet.

Eine Organisation verwendet Unica Collaborate und möchte Datenfilter erzeugen, mit denen dezentrale Marketiers nur die Kunden in der Region anzeigen können, denen sie zugewiesen sind. Deshalb benötigt jeder Benutzer seinen eigenen Datenfilter.

In Unica Collaborate werden die Listenanzeige und die Formularvorlagen basierend auf der Region eingerichtet. Informationen zur Konfiguration der Integration finden Sie im Unica CollaborateAdministratorhandbuch.

Die Zielgruppenebene ist der Kunde.

Die Datenfilter werden für vier Tabellen in der `exampleSchema`-Datenbank erstellt, wie in der folgenden Tabelle erläutert.

Tabelle 70. In den Beispielen verwendete Tabellen und Felder

Tabelle	Felder
`exampleSchema.Corporate_Lists`	`UserID`, `State`, und `RegionID`

Tabelle 70. In den Beispielen verwendete Tabellen und Felder (Fortsetzung)

Tabelle	Felder
	Dies ist die Tabelle für die Listenanzeige, die in Unica Collaborate eingerichtet ist. Die Spalte „UserID“ enthält die Unica Platform-Anmeldenamen der dezentralen Marketiers. Diese weist die Unica Platform-Anmeldenamen der dezentralen Marketiers den jeweiligen Regionen zu.
`exampleSchema.customer_contact`	`Indiv_ID`, `Region_ID`, und `State` Felder für Kunden
`exampleSchema.lkup_state`	Eine Lookup-Tabelle für das Feld `state_name`
`exampleSchema.lkup_region`	Eine Lookup-Tabelle für das Feld `region_id`

Beispiel: Platzhalter zum Zuweisen von Gruppenmitgliedern zu Datenfiltern verwenden

Um einen separaten Datenfilter für jedes Mitglied einer angegebenen Gruppe zu erzeugen, gehen Sie folgendermaßen vor.

- Erzeugen Sie logische Felder wie gewöhnlich.
- Erzeugen Sie einen einzelnen Datenfilter mit dem Platzhalter `#user_login#` im Element `expression`.
- Legen Sie unter dem Element `AssignmentByName` das Element `principalType` auf `2`, das Element `principalName` auf den Gruppennamen und das Element `dataObjectId` auf die ID des Platzhalter-Datenfilters fest.
- Erzeugen Sie Zuordnungen von Zielgruppen wie gewöhnlich.

Diese Methode ist in der folgenden XML mithilfe des oben beschriebenen Szenarios dargestellt.

```
<ExecuteBatch>
                <!-- ********************************* -->
                <!--          Data configuration       -->
                <!-- ********************************* -->
    <name>SeedData</name>
    <operations>
        <ExecuteBatch>
            <name>DataFiltering</name>
            <operations>
                <AddDataConfiguration>
                    <dataConfiguration>
                        <id>1</id>
                        <name>collaborate</name>
                    </dataConfiguration>
                </AddDataConfiguration>
            </operations>
        </ExecuteBatch>
                <!-- ********************************* -->
                <!--         Logical fields            -->
                <!-- ********************************* -->
        <AddLogicalFields>
            <logicalFields>
                <LogicalField>
                    <id>1</id>
                    <name>Customer_ID</name>
                    <type>java.lang.String</type>
                </LogicalField>

                <LogicalField>
                    <id>2</id>
                    <name>AudienceLevel</name>
                    <type>java.lang.String</type>
```

```
            </LogicalField>

            <LogicalField>
                <id>3</id>
                <name>UserID</name>
                <type>java.lang.String</type>
            </LogicalField>

            <LogicalField>
                <id>4</id>
                <name>State_code</name>
                <type>java.lang.String</type>
            </LogicalField>

            <LogicalField>
                <id>5</id>
                <name>Region</name>
                <type>java.lang.Long</type>
            </LogicalField>
        </logicalFields>
    </AddLogicalFields>
            <!-- ********************************* -->
            <!--       Wild card data filter       -->
            <!-- ********************************* -->
    <AddDataFilters>
        <dataFilters>
            <DataFilter><
                <configId>1</configId>
                <id>1</id>
                <fieldConstraints>
                    <FieldConstraint>
                        <logicalFieldId>3</logicalFieldId>
```

```
                        <expression>#user_login#</expression>
                    </FieldConstraint>
                </fieldConstraints>
            </DataFilter>
        </dataFilters>
    </AddDataFilters>
            <!--
*********************************************************** -->
            <!--                    Add data tables
   -->
            <!--
*********************************************************** -->

    <ExecuteBatch>
        <name>addTables</name>
        <operations>
            <!--
*********************************************************** -->
            <!--           Table exampleSchema.Corporate_Lists
   -->
            <!--
*********************************************************** -->
             <AddDataTable>
                <dataTable>
                    <id>1</id>
                    <name>exampleSchema.Corporate_Lists</name>
                    <fields>
                        <TableField>
                            <tableId>1</tableId>
                            <name>UserID</name>
                            <logicalFieldId>3</logicalFieldId>
                        </TableField>
```

```
                            <TableField>
                                <tableId>1</tableId>
                                <name>State</name>
                                <logicalFieldId>4</logicalFieldId>
                            </TableField>
                            <TableField>
                                <tableId>1</tableId>
                                <name>Region_ID</name>
                                <logicalFieldId>5</logicalFieldId>
                            </TableField>
                        </fields>
                    </dataTable>
                </AddDataTable>
                <!--
****************************************************** -->
                <!--           Table exampleSchema.customer_contact
   -->
                <!--
****************************************************** -->
                <AddDataTable>
                    <dataTable>
                        <id>2</id>
                        <name>exampleSchema.customer_contact</name>
                        <fields>
                            <TableField>
                                <tableId>2</tableId>
                                <name>Indiv_ID</name>
                                <logicalFieldId>1</logicalFieldId>
                            </TableField>
                            <TableField>
                                <tableId>2</tableId>
                                <name>Region_ID</name>
```

```
                            <logicalFieldId>5</logicalFieldId>
                        </TableField>
                        <TableField>
                            <tableId>2</tableId>
                            <name>State</name>
                            <logicalFieldId>4</logicalFieldId>
                        </TableField>
                    </fields>
                </dataTable>
            </AddDataTable>
            <!--
*********************************************************** -->
            <!--              Table exampleSchema.lkup_state
   -->
            <!--
*********************************************************** -->
            <AddDataTable>
                <dataTable>
                    <id>3</id>
                    <name>example.schema.lkup_state</name>
                    <fields>
                        <TableField>
                            <tableId>3</tableId>
                            <name>state_name</name>
                            <logicalFieldId>4</logicalFieldId>
                        </TableField>
                    </fields>
                </dataTable>
            </AddDataTable>
            <!--
*********************************************************** -->
```

```
                <!--              Table exampleSchema.lkup_region
   -->
                <!--
********************************************************* -->
                <AddDataTable>
                    <dataTable>
                        <id>4</id>
                        <name>exampleSchema.lkup_region</name>
                        <fields>
                            <TableField>
                                <tableId>4</tableId>
                                <name>Region_ID</name>
                                <logicalFieldId>5</logicalFieldId>
                            </TableField>
                        </fields>
                    </dataTable>
                </AddDataTable>
            </operations>
        </ExecuteBatch>
                <!--
******************************************************** -->
                <!--              Audience table associations
   -->
                <!--
******************************************************** -->
        <ExecuteBatch>
            <name>addAudiences</name>
            <operations>
                <AddAudience>
                    <audience>
                        <id>1</id>
                        <name>Customer</name>
```

```
                    <fields>
                        <AudienceField>
                            <logicalFieldId>2</logicalFieldId>
                            <fieldOrder>0</fieldOrder>
                        </AudienceField>
                    </fields>
                </audience>
            </AddAudience>

            <AddAudience>
                <audience>
                    <id>2</id>
                    <name>default</name>
                    <fields>
                        <AudienceField>
                            <logicalFieldId>2</logicalFieldId>
                            <fieldOrder>0</fieldOrder>
                        </AudienceField>
                    </fields>
                </audience>
            </AddAudience>
        </operations>
    </ExecuteBatch>

    <ExecuteBatch>
        <name>addAudienceTableAssociations</name>
        <operations>
            <AddAudienceTableAssociation>
                <audienceTableAssociation>
                    <audienceId>1</audienceId>
                    <tableId>1</tableId>
                    <configId>1</configId>
```

```
                </audienceTableAssociation>
            </AddAudienceTableAssociation>

            <AddAudienceTableAssociation>
                <audienceTableAssociation>
                    <audienceId>1</audienceId>
                    <tableId>2</tableId>
                    <configId>1</configId>
                </audienceTableAssociation>
            </AddAudienceTableAssociation>

            <AddAudienceTableAssociation>
                <audienceTableAssociation>
                    <audienceId>2</audienceId>
                    <tableId>3</tableId>
                    <configId>1</configId>
                </audienceTableAssociation>
            </AddAudienceTableAssociation>

            <AddAudienceTableAssociation>
                <audienceTableAssociation>
                    <audienceId>2</audienceId>
                    <tableId>4</tableId>
                    <configId>1</configId>
                </audienceTableAssociation>
            </AddAudienceTableAssociation>

        </operations>
    </ExecuteBatch>
            <!--
********************************************************** -->
```

```
                <!--           Link filters (dataObjectId) to group
    -->
                <!--
 ******************************************************** -->
        <AddAssignments>
            <assignments>
                 <AssignmentByName>
                    <namespaceId>1</namespaceId>
                    <dataObjectId>1</dataObjectId>
                    <principalType>2</principalType>
                    <principalName>FieldMarketer</principalName>
                </AssignmentByName>
            </assignments>
        </AddAssignments>
    </operations>
</ExecuteBatch>
```

Informationen zum Zuweisen von Benutzern und Gruppen über die Benutzerschnittstelle

Sie können Benutzer und Gruppen auf den Seiten **Einstellungen > Datenfilter** bestimmten Datenfiltern zuweisen.

Um auf den Seiten **Einstellungen > Datenfilter mit Datenfiltern** arbeiten zu können, müssen die folgenden Bedingungen erfüllt sein.

- Die Datenfilter müssen in den Unica Platform-Systemtabellen konfiguriert sein.
- Sie müssen sich als Unica Platform-Benutzer mit der Berechtigung Seite **Datenfilter verwalten** anmelden. Die vorkonfigurierte Rolle Unica Platform **AdminRole** hat diese Berechtigung.

Erweiterte Suche

Unica Platform bietet eine Benutzeroberfläche, über die Benutzer und Gruppen Datenfiltern zugeordnet werden können. Diese Benutzeroberfläche verwendet eine erweiterte Suchfunktion, um Benutzer-, Gruppen- und Datenfilterlisten abzurufen. Sie können Benutzer und Gruppen aus diesen Listen auswählen und sie den gewünschten Datenfiltern zuordnen.

Suche mit Datenfilter

Die Suchfunktion für Datenfilter stellt Suchkriterien bereit, die mit den Kriterien übereinstimmen, die bei der Datenfiltereinrichtung angegeben wurden. Beispiel: Angenommen, eine Gruppe von Datenfiltern basiert auf einem Feld mit den folgenden Daten zu Vertriebsgebieten.

- Ostafrika
- Asien
- Europa
- Naher Osten
- Nordamerika

Bei der erweiterten Suche mit Datenfiltern würden diese Daten in einer Dropdown-Liste bereitgestellt, aus der Sie beim Suchen nach Datenfiltern eine Auswahl treffen könnten.

Benutzer- und Gruppensuche

Die erweiterte Suchfunktion für Benutzer und Gruppen enthält ein Textfeld, in das Sie Text eingeben könnten, nach dem gesucht werden soll.

Wenn eine Registerkarte mit der erweiterten Benutzer- und Gruppensuche erstmals geladen wird, enthalten die beiden Textfelder „Benutzer“ und „Gruppe“ jeweils ein Platzhalterzeichen (*). Eine Suche, die mit diesem Platzhalterzeichen ausgeführt wird, gibt als Suchergebnis alle Datensätze zurück.

Wenn Sie das Platzhalterzeichen löschen und keinen anderen Text eingeben, sodass das Feld leer bleibt, werden keine Datensätze zurückgegeben. Führen Sie etwa eine Suche mit einem leeren Benutzertextfeld und einem Stern im Gruppentextfeld aus, werden in den Ergebnissen ausschließlich Gruppen aufgeführt.

Wenn Sie auf der Registerkarte „Zuweisungen anzeigen“ die Felder Benutzer und Gruppe leer lassen, werden unabhängig davon, welche Datenfilterkriterien ausgewählt wurden, keine Datensätze zurückgegeben.

Bei Eingabe von Text in das Feld wird nach Übereinstimmungen mit den eingegebenen Zeichen im Textfeld gesucht. Dies geschieht nach der Reihenfolge, in der die Zeichen eingegeben wurden. Wenn Sie z.B. eine Gruppe namens „Nordamerika“ abrufen möchten, können Sie jeden Buchstaben oder jede Buchstabengruppe (in der richtigen Reihenfolge) eingeben, die in dem Namen vorkommt. Nordamerika wird unter den Ergebnissen angezeigt, wenn Sie „nord“ oder „d“ eingegeben haben, jedoch nicht bei Eingabe von „dron“.

Bei der Suche wird die Groß-/Kleinschreibung nicht beachtet. Dies bedeutet, dass „Nord“ gleich „nord“ ist.

Anzeigen zugewiesener Datenfilter

Verwenden Sie diese Prozedur, um zugewiesene Datenfilter anzuzeigen.

1. Melden Sie sich an Unica als Benutzer mit der Unica Platform-Rolle AdminRole an und klicken Sie auf **Datenfilterung**.

   Die Seite „Datenfilter“ wird angezeigt.
2. Anzeigen **zugewiesener Datenfilter**.
3. Führen Sie eine erweiterte Suche nach zugewiesenen Datenfiltern durch, um Suchergebnisse zu erhalten.

Eine Liste mit Datenfiltern, die den Suchkriterien entsprechen, wird angezeigt.

Zuweisen von Benutzern und Gruppen zu Datenfiltern

Verwenden Sie diese Prozedur, um Datenfiltern Benutzer und Gruppen zuzuordnen.

1. Melden Sie sich bei Unica als Benutzer mit der Unica Platform-Rolle „AdminRole“ an und klicken Sie auf **Einstellungen > Datenfilter**.

   Die Seite „Datenfilter“ wird angezeigt.

2. Klicken Sie auf **Benutzer oder Gruppen zuweisen**.
3. Führen Sie eine erweiterte Suche nach Datenfiltern durch, um eine Liste mit Datenfiltern zu erhalten.
4. Führen Sie eine erweiterte Suche nach Benutzern und/oder Gruppen durch, um eine Liste mit Benutzern und/oder Gruppen zu erhalten.
5. Wählen Sie in der Liste der Suchergebnisse Datenfilter und die Benutzer und Gruppen aus, die Sie diesen Datenfiltern zuweisen möchten.
6. Klicken Sie auf **Zuweisen**.

Die ausgewählten Benutzer und Gruppen werden den ausgewählten Datenfiltern zugewiesen.

Entfernen von Datenfilterzuweisungen

Verwenden Sie diese Prozedur, um Datenfilterzuweisungen zu entfernen.

1. Melden Sie sich bei Unica als Benutzer mit der Unica Platform-Rolle „AdminRole“ an und klicken Sie auf **Einstellungen > Datenfilter**.

   Die Seite „Datenfilter“ wird angezeigt.
2. Anzeigen **zugewiesener Datenfilter**.
3. Führen Sie eine erweiterte Suche nach zugewiesenen Datenfiltern durch, um aus den Suchergebnissen auswählen zu können.
4. Wählen Sie in Ihrer Liste mit den Suchergebnissen die Datenfilter aus, dessen Zuweisungen Sie löschen möchten.
5. Klicken Sie auf **Zuweisung aufheben**.

Die ausgewählten Zuweisungen werden gelöscht. Die Datenfilter selbst werden nicht gelöscht.

Hinzufügen von Datenfiltern nach Erstellung des ersten Satzes

Nachdem Sie den ersten Satz erstellt haben können Sie mit dem Hinzufügen von Datenfiltern fortfahren. Sie können beispielsweise einen Datenfiltersatz erstellen, der auf

Ländern und Städten/Bundesländern basiert und später einen anderen Satz erstellen, der auf Postleitzahlen basiert.

Sie haben folgende Möglichkeiten zum Beziehen der XML-Datei für zusätzliche Datenfilter:

- Modifizieren Ihrer ursprünglichen XML-Datei, um neue Filter hinzuzufügen. Wenn Sie die Datenbank mit dem Dienstprogramm `dataFilteringScriptTool` senden, erstellt Unica Platform lediglich die neuen Datenfilter.
- Erstellen Sie eine XML-Datei, indem Sie neue Datenfilter festlegen. Wenn Sie die Datenbank mit dem Dienstprogramm `dataFilteringScriptTool` senden, werden bestehende Datenfilter nicht gelöscht.

Füllen Sie die Datenfiltertabellen aus und weisen Sie Benutzer und Gruppen wie in diesem Handbuch beschrieben zu, nachdem Sie die XML-Datei erstellt haben.

Prüfereignisüberwachung in Unica

Sie können konfigurieren, welche Prüfereignisse überwacht werden, und jedem überwachten Ereignis eine Bewertungsstufe zuweisen.

Es werden zwei Arten von Prüfereignissen überwacht:

- Sicherheitsbezogene Ereignisse wie Änderungen des Benutzerstatus, der Gruppenzugehörigkeit und von Berechtigungen
- Änderungen der Unica-Konfigurationseigenschaften, die auf der Seite **Einstellungen > Konfiguration** verwaltet werden

Die Prüfereignisinformationen sind vom Systemprotokoll unabhängig, und die ausgeführte Konfiguration für das Systemprotokoll hat keine Auswirkungen auf die Prüfereignisüberwachung.

Mithilfe des Prüfereignisberichts können die überwachten Ereignisse passend angezeigt werden. Sie können den Inhalt des Berichts konfigurieren, die im Bericht angezeigten Informationen filtern und Berichtsdaten exportieren.

Sie müssen die Rolle „AdminRole“ oder „PlatformAdminRole“ in Unica Platform besitzen, um den Prüfereignisbericht und die Prüfungssicherungen zu konfigurieren oder um den Bericht anzuzeigen.

Einschränkungen bei der Prüfereignisüberwachung

Wenn Sie die Überwachung von Prüfereignissen für Konfigurationseigenschaften konfigurieren, werden diese Änderungen nur überwacht, wenn sie über die Seite **Einstellungen > Konfiguration** vorgenommen wurden.

Beispielsweise werden die folgenden Änderungen an Konfigurationseigenschaften nicht überwacht.

- Änderungen mit dem Unica Platform-Dienstprogramm `configTool`
- Änderungen, die bei einer Installation oder einem Upgrade von Unica-Produkten vorgenommen wurden.

Auch wenn Sie Standardbenutzer, Rollen und Berechtigungen für Unica Platform und Unica Campaign über das Dienstprogramm Unica Platform `populateDB` manuell hinzufügen, werden diese Änderungen nicht überwacht.

Traditionelle Prüfereignisse

In früheren Unica Platform-Releases wurden Prüfereignisse in den Unica Platform-Systemtabellen gesichert, auch wenn kein Bericht verfügbar war. Bei einem Upgrade von einer Version vor 9.1.1 enthält dieser Prüfereignisbericht diese Ereignisse der Vorversion.

Prüfereignisse der Vorversion werden in dem Bericht wie folgt angezeigt.

- Die Spalte **Priorität** enthält **Keine Priorität (Vorversion)**, um anzugeben, dass diese Prüfsätze gespeichert wurden, bevor der Prüfbericht verfügbar war.
- In einer Umgebung mit einer einzigen Partition enthält die Spalte **Partition** die ID der Standardpartition.
- In einer Umgebung mit mehreren Partitionen enthält die Spalte **Partition** den Wert **-1 (Vorversion)**, um anzugeben, dass die Partition, zu der das Ereignis gehört, nicht bestimmt werden kann.

Die folgenden Ereignisse der Vorversion können nach dem Upgrade erscheinen.

- Die Benutzerauthentifizierung war erfolgreich.
- Die Benutzerauthentifizierung ist fehlgeschlagen.
- Die Authentifizierung ist fehlgeschlagen, da ein Benutzer versucht hat, sich mit zu vielen gleichzeitigen Sitzungen anzumelden.
- Der Benutzer hat sich abgemeldet, und die entsprechende Sitzung wurde beendet.
- Das Benutzerkennwort hat sich geändert.

Prüfereignisse der Vorversion sind in den Berichten nur sichtbar, wenn Sie mit einem Konto auf den Bericht zugreifen, der die Rolle PlatformAdminRole in Unica Platform hat. Der vordefinierte Benutzer platform_admin hat diese Rolle.

Rückwirkende Änderungen

Wird der Vorname, der Nachname oder die E-Mail-Adresse eines Benutzerkontos geändert, wird diese Änderung in allen überwachten Prüfereignissen für diesen Benutzer widergespiegelt. Dies gilt auch für Ereignisse, die vor den Änderungen am Benutzerprofil vorgenommen wurden.

Berechtigungen zum Anzeigen des Prüfereignisberichts in Umgebungen mit mehreren Partitionen

In einer Umgebung mit mehreren Partitionen wirkt sich die Partitionsmitgliedschaft des Administrators, der den Prüfereignisbericht anzeigt, auf die Ereignisse aus, die aufgenommen werden, wenn der Administrator den Bericht anzeigt.

Für alle Prüfereignisse außer Konfigurationsereignissen zeigt der Bericht nur die Ereignisse an, die in der Partition des Administrators aufgetreten sind, der den Bericht angezeigt hat. Ereignisse, die in anderen Partitionen aufgetreten sind, werden im Bericht nicht angezeigt.

Eine Ausnahme sind lediglich Administratoren mit der Rolle PlatformAdminRole, die Ereignisse sehen können, die in allen Partitionen auftreten.

Alle Konfigurationsereignisse sind für alle Administratoren sichtbar, die den Bericht anzeigen können.

Aktivieren und Inaktivieren der Ereignisprüfung

Standardmäßig ist die Ereignisprüfung inaktiviert. Soll die Ereignisprüfung aktiviert werden, setzen Sie die Konfigurationseigenschaft **Unica Platform | Prüfereignisse | Ereignisprüfung ist aktiviert** auf True.

Diese Konfigurationseigenschaft wirkt sich nur auf die unter **Unica Platform | Prüfereignisse** der Seite „Konfiguration“ aufgelisteten Prüfereignisse aus. Die im Systemprotokoll überwachten Ereignisse sind nicht betroffen.

Sie können die Ereignisprüfung jederzeit inaktivieren, indem Sie den Wert der Konfigurationseigenschaft **Ereignisprüfung ist aktiviert** auf False setzen.

Der Prüfereignisbericht enthält nicht die über die Eigenschaft **Ereignisprüfung ist aktiviert** gesteuerten Ereignisse, die in dem Zeitraum aufgetreten sind, in dem die Eigenschaft auf **False** gesetzt war.

Die Prüfereignisse konfigurieren, die im Bericht erscheinen sollen

Um die Prüfereignisse einschließlich ihres Schweregrads anzugeben, die im Prüfbericht verfügbar sind, werden Eigenschaften auf der Seite **Einstellungen > Konfiguration** festgelegt.

1. Gehen Sie zur Seite **Einstellungen > Konfiguration** und erweitern Sie die **Unica Platform | Prüfungsereignisse | Konfigurationskategorie für Überwachungsereignisse**.
2. Wählen Sie die Ereignisse aus, die Sie überwachen möchten.

   Die überwachten Ereignisse können in den Prüfbericht aufgenommen werden.
3. Erweitern Sie die Ansicht der Kategorie **Unica Platform | Prüfereignisse | Konfiguration der Priorität von Prüfereignissen** und klicken Sie dann auf **Einstellungen bearbeiten**.
4. Geben Sie den Schweregrad an, den Sie den einzelnen überwachten Ereignissen zuordnen wollen.

   Treffen Sie eine Auswahl aus den folgenden Optionen.

- Keine Priorität
- Informationsnachrichten
- Warnung
- Kritisch

Der angegebene Schweregrad erscheint im Prüfbericht und kann beim Filtern des Berichts verwendet werden.

Wenn Sie das Benutzersitzungsereignis **An- und Abmeldeereignisse für Mitglieder der Gruppe „HighSeverityAccounts“ erfassen** überwachen möchten, fügen Sie die Benutzer, deren Anmelde- und Abmeldeereignisse Sie überwachen möchten, der Gruppe **highSeverityAccounts** hinzu. Diese Aktion kann auf der Seite **Einstellungen > Benutzergruppen** ausgeführt werden.

Diese Gruppe wird bei der Installation automatisch in der Standardpartition erstellt. In einer Umgebung mit mehreren Partitionen wird diese Gruppe automatisch erstellt, wenn mit dem Dienstprogramm Unica Platform `partitionTool` eine neue Partition erstellt wird.

Inhalt und Anzeige des Prüfberichts ändern

Sie können Ereignisse und Spalten hinzufügen und entfernen, Spalten neu anordnen und sortieren, die Zeitspanne neu festlegen, angeben, welche überwachten Ereignisse im Bericht gezeigt werden sollen, und die Informationen filtern.

Wenn Sie den Prüfbericht öffnen, ohne Berichtsparameter festzulegen, werden die folgenden Standardeinstellungen verwendet.

- Alle auf der Seite **Einstellungen > Konfiguration** in der Kategorie **Unica Platform | Prüfereignisse | Konfiguration der Prüfereignisse** ausgewählten Ereignisse werden gezeigt, bei Bedarf auch auf mehreren Seiten.
- Es werden keine Datumskriterien angewendet.
- Ereignisse werden wie folgt sortiert: Ereignis Datum/Uhrzeit (absteigend), Anmeldename (aufsteigend), Bewertungsstufe (aufsteigend)

Verwenden Sie die folgende Prozedur, um diese Einstellungen zu ändern.

1. Rufen Sie **Analyse > Platform** auf.
2. Soll der Inhalt des Berichts geändert werden, gehen Sie wie folgt vor:

    a. Klicken Sie auf die Schaltfläche **Berichtsparameter**.

    Das Fenster „Berichtsparameter“ wird geöffnet.

    b. Füllen Sie die Felder aus.

    Wollen Sie die Sortierreihenfolge im Bericht festlegen, können Sie in diesem Fenster aus vordefinierten Sortierreihenfolgen auswählen. Sie können auch auf Spaltenüberschriften im Bericht klicken, um nach diesen Spalten zu sortieren.

    c. Klicken Sie auf **Weiter**, um auf eine Seite zu gelangen, auf der Sie auswählen können, welche Ereignisse im Bericht gezeigt werden sollen.

    d. Klicken Sie auf **Speichern und schließen**, um Ihre Auswahl auf den Bericht anzuwenden.
3. Soll der Bericht gefiltert werden, geben Sie Text oder Zahlen in das Feld **Filtern** ein und klicken Sie auf die Schaltfläche **Filtern**.

    Im Bericht werden nur die Ereignisse angezeigt, die die Filterzeichen in einer beliebigen im Bericht angezeigten Spalte enthalten.

    Wollen Sie den Filter löschen, klicken Sie auf das **X** im Feld „Filtern“.

Felder im Fenster „Berichtsparameter“

Verwenden Sie die Felder auf der Seite „Berichtsparameter“, um die Art und Weise zu konfigurieren, in welcher der Prüfbericht angezeigt wird.

Tabelle 71. Felder im Fenster „Berichtsparameter“

Feld	Beschreibung
Sortieren	Wählen Sie eine Sortierreihenfolge im Dropdown-Menü aus. Es werden verschiedene Kombinationen von Spaltensortierungen aufgelistet. Zudem kann ausgewählt werden, ob die Sortierung absteigend oder aufsteigend erfolgen soll.

Tabelle 71. Felder im Fenster „Berichtsparameter“ (Fortsetzung)

Feld	Beschreibung
	Sie können Spalten auch über die Steuerelemente auf der Berichtsseite sortieren.
Zeitraum	Wählen Sie in der Dropdown-Liste einen der vordefinierten Zeiträumen aus oder geben Sie das Start- und Enddatum eines benutzerdefinierten Bereichs an.
Ereignisse	Wählen Sie die optionalen Ereignisse aus, die in den Bericht aufgenommen werden sollen. Damit ein Ereignis im Bericht verfügbar ist, muss es in der Kategorie **Unica Platform | Prüfereignisse | Konfiguration der Prüfereignisse** der Seite **Einstellungen > Konfiguration** ausgewählt werden.
Spalten	Verwenden Sie die Schaltflächen **Hinzufügen** und **Entfernen**, um die optionalen Spalten anzugeben, die im Bericht erscheinen sollen.

Felder und Schaltflächen im Prüfereignisbericht

Die Felder im Prüfereignisbericht enthalten Details über System- und Benutzerereignisse in Unica.

Tabelle 72. Felder und Schaltflächen im Prüfereignisbericht

Feld oder Schaltfläche	Beschreibung
Filter	Soll der Bericht gefiltert werden, geben Sie Text oder Zahlen in das Feld Filtern ein und klicken Sie auf die Schaltfläche Filtern. Im Bericht werden nur die Ereignisse angezeigt, die die Filterzeichen in einer beliebigen im Bericht angezeigten Spalte enthalten.
	Klicken Sie auf dieses Symbol, um ein Fenster zu öffnen, in dem Sie die im Bericht angezeigten Spalten ändern, einen Zeitraum

Tabelle 72. Felder und Schaltflächen im Prüfereignisbericht (Fortsetzung)

Feld oder Schaltfläche	Beschreibung
Berichtsparameter	festlegen und eine vordefinierte Sortierreihenfolge auswählen können.
 Exportieren	Klicken Sie auf dieses Symbol, um ein Fenster zu öffnen, in dem Sie den Bericht in CSV-Format oder Textformat exportieren können.
 Aktualisieren	Klicken Sie auf dieses Symbol, um die Berichtsdaten zu aktualisieren.
Vorgegebene Felder	
Ereignis Datum/Zeit (kurz)	Datum und Uhrzeit des Ereignisses auf dem Server, auf dem Unica Platform implementiert ist.
Ereignisname	Das überwachte Ereignis. Überwachte Ereignisse werden auf der Seite **Einstellungen > Konfiguration** angegeben.
Einzelheiten zum Ereignis	Details zu dem überwachten Ereignis. Ist ein Link vorhanden, können Sie den Link anklicken, um ausführliche Informationen einzusehen.
Anmeldename	Der Anmeldename des Benutzers, der die Aktion ausgeführt hat.
Nachname, Vorname	Der Vor- und Nachname des Benutzers, der die Aktion ausgeführt hat.
Severity	Der Schweregrad, der dem Ereignis auf der Seite **Unica Platform | Prüfereignisse | Konfiguration der Priorität von Prüfereignissen** zugeordnet wurde.
Im Fenster „Berichtsparameter“ festgelegte optionale Felder.	

Tabelle 72. Felder und Schaltflächen im Prüfereignisbericht (Fortsetzung)

Feld oder Schaltfläche	Beschreibung
Browser	Der Browser, den die Person verwendet hat, die die Aktion ausgeführt hat.
Hostname	Der Name oder die IP-Adresse der Maschine, auf der die Aktion ausgeführt wurde.
Anfrage von	Die URI, von der die HTTP-Anforderung stammt.
Ereignis Datum/Zeit (lang)	Datum und Uhrzeit des Ereignisses auf dem Server, auf dem Unica Platform implementiert ist (einschließlich der Zeitzone).
E-Mail-Adresse des Benutzers	Die E-Mail-Adresse des Benutzers, der die Aktion ausgeführt hat.
Partition	Die Partitionsmitgliedschaft des Benutzers, der die Aktion ausgeführt hat.

Archivierte Prüfereignisse

Sie können Sicherungen von Prüfereignissen durch das Festlegen der Werte von Konfigurationseigenschaften auf der Seite **Einstellungen > Konfiguration** in der Kategorie **Unica Platform | Prüfereignisse | Konfiguration der Prüfereignisse** konfigurieren.

Die archivierten Daten werden in der Tabelle `USM_AUDIT_BACKUP` gespeichert Tabelle und können in den Prüfereignisbericht aufgenommen werden, wenn Sie einen benutzerdefinierten Datumsbereich mit Daten aus dem Archiv festlegen. Das Laden eines Berichts, der archivierte Daten enthält, kann länger dauern als das Laden eines Berichts ohne archivierte Daten.

Das System sendet eine Benachrichtigung, wenn ein Prozess zur Sicherung von Prüfereignissen beendet ist. Sie können auch eine Gruppe von Benutzern konfigurieren, die diese Benachrichtigungen in Form von E-Mails erhalten.

Legen Sie die folgenden Eigenschaften fest, um Prüfereignissicherungen zu konfigurieren.

- **Sicherung der Prüfung aktivieren**
- **Archivieren der Daten nach der hier angegebenen Anzahl an Tagen**
- **Prüfdatensätze für die hier angegebene Anzahl an Tagen im primären Bereich behalten**
- **Archivstartzeit**
- **Name der die Benachrichtigungen über die Prüfung der Sicherung erhaltenden Gruppe**

Konfigurieren der Benachrichtigungen über die Sicherung von Prüfereignissen

Um Benutzer über den Status der Benachrichtigungen über die Sicherung von Prüfereignissen zu informieren, machen Sie sie zu Mitgliedern einer Gruppe, die Sie in einer Konfigurationseigenschaft angeben.

1. Legen Sie die Gruppe fest, deren Mitglieder E-Mail-Benachrichtigungen von Sicherungen der Prüfdaten erhalten sollen.

   Sie können eine vorhandene Gruppe verwenden oder auf der Seite **Einstellungen > Benutzergruppen** eine neue Gruppe erstellen.

   Sie können nur eine einzelne Gruppe für den Empfang von Benachrichtigungen angeben.
2. Rufen Sie die Seite **Einstellungen > Konfiguration** auf und erweitern Sie die Kategorie **Unica Platform | Prüfereignisse | Konfiguration der Prüfereignisse**.
3. Setzen Sie die Einstellung **Name der die Benachrichtigungen über die Prüfung der Sicherung erhaltenden Gruppe** auf den Namen der ausgewählten Gruppe.
4. Fügen Sie der Gruppe die Benutzer hinzu, die Benachrichtigungen erhalten sollen.
5. Die Benutzer, die Sie der Gruppe hinzugefügt haben, müssen die Benachrichtigungen auf der Seite **Einstellungen > Benutzer** abonnieren.

   Ein Administrator kann diese Aufgabe für die einzelnen Benutzer übernehmen oder die Benutzer darüber informieren, dass sie Ihr Konto aufrufen, dann auf **Benachrichtigungsabonnements** klicken und dann **Benachrichtigungen der Sicherung der Prüfung** abonnieren müssen.

Immer, wenn das System Prüfdaten sichert, wird eine E-Mail-Benachrichtigung und eine Benachrichtigung der Benutzeroberfläche für die angegebenen Mitglieder der Gruppe generiert, wenn sie die Benachrichtigungen für Prüfereignisse abonniert haben.

Exportieren des Prüfereignisberichts

Sie können den Sicherheitsprüfungsbericht in eine Textdatei oder in eine CSV-Datei exportieren.

1. Rufen Sie **Analyse > Marketing Platform** auf.
2. Klicken Sie auf die Schaltfläche **Exportieren**.
3. Geben Sie im Fenster Prüfberichtexport einen Namen für den exportierten Bericht ein und wählen Sie das Exportformat aus.

   Es gibt folgende Formatoptionen:

   - **CSV** (eine durch Kommata getrennte Liste, die Microsoft™ Excel öffnen kann)
   - **TXT** (Text)

     Wenn Sie das Textformat ausgewählt haben, müssen Sie auch ein Trennzeichen auswählen. Mögliche Optionen:

     - **#**
     - **|**
     - **TAB**
4. Klicken Sie auf **Exportieren**, geben Sie an, ob Sie den exportierten Bericht öffnen oder speichern wollen und schließen Sie dann das Berichtsfenster.

Optimieren des Exports des Prüfereignisberichts für große Ereignisvolumen

Wollen Sie große Prüfereignisberichte exportieren, beispielsweise Berichte mit mehr als 65.000 Sätzen, die Ihren Filterkriterien für Prüfereignisberichte entsprechen, kann es beim Export zu einer Überschreitung des Zeitlimits kommen. Führen Sie die folgende Prozedur aus, um dieses Problem zu umgehen.

Diese Prozedur gilt, wenn Sie mit Internet Explorer auf den Prüfereignisbericht zugreifen.

1. Bearbeiten Sie die Windows™-Registrierungsdatenbank wie folgt.
    a. Öffnen Sie den Windows™ Registrierungseditor und rufen Sie `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings` auf.
    b. Wenn der DWORD-Eintrag `ReceiveTimeout` nicht vorhanden ist, erstellen Sie einen Eintrag.

       Gehen Sie wie folgt vor, um einen neuen DWORD-Eintrag zu erstellen.
        - Klicken Sie mit der rechten Maustaste auf `Internet Settings` und wählen Sie **Neu > DWORD-Wert (32-Bit)** aus.
        - Geben Sie `ReceiveTimeout` als Name für den neuen Eintrag ein.

    c. Geben Sie für den vorhandenen oder neuen Eintrag `ReceiveTimeout` wie folgt einen Wert ein:
        - Klicken Sie mit der rechten Maustaste auf den Eintrag `ReceiveTimeout` und wählen Sie **Ändern** aus.
        - Wählen Sie unter **Basis** den **Dezimal** aus.
        - Geben Sie das Zeitlimitintervall in Millisekunden an.

          Wollen Sie beispielsweise 3 Stunden eingeben, müssen Sie als Wert 10800000 eingeben (180 Minuten * 60 Sekunden * 1000).
2. Konfigurieren Sie Internet Explorer wie folgt.
    a. Wählen Sie **Extras > Internetoptionen** aus und klicken Sie auf die Registerkarte „Sicherheit“.
    b. Wählen Sie die Zone aus, in der Sie auf Unica Platform zugreifen. Sie können beispielsweise Vertrauenswürdige Sites auswählen.
    c. Klicken Sie auf **Stufe anpassen**.
    d. Aktivieren Sie unter **Downloads** die Option **Automatische Eingabeaufforderung für Dateidownloads**.
    e. Starten Sie Internet Explorer erneut.

Unica Platform-Systemprotokoll

Überprüfen Sie als Erstes das Systemprotokoll, wenn die Unica Platform-Anwendung nicht ordnungsgemäß funktioniert. Das Systemprotokoll ist unabhängig von den Informationen zur Sicherheitsprüfung, die in den Systemtabellen gespeichert werden. Das Systemprotokoll überwacht einige der Informationen, die auch in den Sicherheitsprüfungsberichten enthalten sind, und enthält zudem Informationen, die bei der Fehlerbehebung in Unica Platform hilfreich sind.

Das Systemprotokoll enthält die folgenden Informationen.

- Konfigurationsinformationen und sämtliche Informationen zu Fehlern und Debug-Vorgängen für Unica Platform
- Einträge zu wichtigen Ereignissen direkt bei deren Auftreten auf dem Unica Platform-Server (Anforderungen, Gewährungen, Aufhebungen und Fehler)

Informationen über die im Systemprotokoll angezeigten Konfigurationseinstellungen

Anmerkung: Bei einem Problem während eines Schreibversuchs in die Systemprotokolldatei wird statt in eine Datei in stdout (Befehlszeile) geschrieben.

Das Format von Systemprotokolleinträgen

Die Systemprotokolleinträge erfolgen im folgenden Format.

```
Zeitmarke | Prioritätsstufen des Ereignisseisses | Nachricht
```

- **Zeitmarke** – Die Zeit, zu der das Ereignis aufgetreten ist.
- **Prioritätsstufen des Ereignisseisses** – Die Protokollebene des Ereignisses.
- **Nachricht** – Beschreibung des Ereignisses. Wenn der Eintrag eine Anforderung an den Server darstellt, enthält die Nachricht normalerweise die Funktion, die von der Anforderung aufgerufen wird. In den Antworteinträgen werden die Ergebnisse der Anforderungen aufgezeichnet.

Konfiguration des Systemprotokolls

Das Systemprotokoll kann mit der Datei `log4j.properties` konfiguriert werden, die sich standardmäßig im Verzeichnis `conf` der Unica Platform Installation befindet. An dieser Datei vorgenommene Änderungen werden innerhalb von 30 Sekunden, nachdem die Datei gespeichert wurde, wirksam.

Note: Das Systemprotokoll kann mit der Datei `log4j.xml` konfiguriert werden, die sich standardmäßig im Verzeichnis `conf` der Unica Platform Installation befindet. An dieser Datei vorgenommene Änderungen werden innerhalb von 30 Sekunden, nachdem die Datei gespeichert wurde, wirksam.

Die Konfiguration für das Systemprotokoll hat keine Auswirkungen auf die Sicherheitsprüfungsberichte.

Standardeinstellungen des Systemprotokolls

Standardmäßig ist das Systemprotokoll folgendermaßen konfiguriert:

- Protokolldateiname: `platform.log`
- Protokollverzeichnis: `Unica/Platform/logs`
- Protokollebene: `WARN`
- Anzahl der Sicherungen: 10
- Maximale Größe der Protokolldateien: 10 MB

Beachten Sie Folgendes:

- Achten Sie darauf, dass der Computer, auf dem die Protokolle gespeichert werden, über genügend Speicherplatz verfügt, wenn Sie die Anzahl der Sicherungen oder die Größe der Protokolldateien erhöhen.
- Wird die Protokollebene höher als in der Standardeinstellung vorgesehen eingestellt, kann dadurch die Leistung beeinträchtigt werden.

Protokollebenen im Systemprotokoll

Folgende Protokollebenen im Systemprotokoll sind möglich (in aufsteigender Reihenfolge).

- ERROR
- WARN
- INFO
- DEBUG
- TRACE

Die höheren Ebenen enthalten die Informationen aus sämtlichen niedrigeren Ebenen. Z.B wird die Ebene auf DEBUG gesetzt, wird die Verfolgung von DEBUG, INFO, WARN und ERROR aktiviert.

Wenn als Protokollebene DEBUG festgelegt wurde, enthalten die Antwortnachrichten alle SQL-Abfragen, die an den Unica Platform-Datenspeicher gesendet wurden.

Protokollebene für gesamtes Unica Platform-System

Sie können die Protokollebene für alle Komponenten von Unica Platform ändern, indem Sie die gewünschte Zeile im Beispielbereich der Datei auskommentieren. Um eine Zeile auszukommentieren, entfernen Sie das Zeichen <userinput>#</userinput> am Anfang der Zeile. Bei dieser Änderung, achten Sie darauf, dass das Symbol <userinput>#</userinput> am Anfang der Zeile eingefügt wird, in der die vorhergehende Protokollebene angegeben wird.

Note: Sie können die Protokollebene für alle Komponenten von Unica Platform ändern, indem Sie die Protokollebene im unter dem Loggers-Tag definierten Root-Tag ändern.

Festlegen der Protokollebenen für Unica Platform-Komponenten

Sie können die Protokollebene im Systemprotokoll für bestimmte Komponenten von Unica Platform festlegen. Dazu zählen folgende Komponenten:

- Lokalisierung
- Benutzer- und Gruppenverarbeitung
- Datenmigration
- LDAP-Integration

- Authentifizierung (serverseitige Verarbeitung)
- Die Seiten „Konfiguration“
- Datenbankzugriff
- Verschiedene Bibliotheken von Drittanbietern (z. B. iBATIS)

Standardmäßig ist die Protokollierung auf Komponentenebene inaktiviert. Wenn Debugging für ein bestimmtes Modul ausgeführt werden soll, entfernen Sie das Zeichen # am Anfang jeder Zeile des Moduls in der Datei log4j.properties.

Note: Um ein bestimmtes Modul zu debuggen, entfernen Sie das Symbol `<!--` am Anfang jedes <Logger> Tags und `-->` am Ende jedes <Logger> Tags des Moduls in der Datei log4j.xml.

Informationen zu log4j

Zusätzliche Informationen zu log4j finden Sie auf folgende Weise.

- Siehe Kommentare in der Datei `log4j.properties`.
- Siehe http://logging.apache.org/log4j/docs/documentation.html..
- Siehe Kommentare in der Datei `log4j.xml`.
- Weitere Informationen hierzu finden Sie unter . https://logging.apache.org/log4j/2.x/manual/configuration.html

Note: Die Benutzer können Warnungen von JDBC deaktivieren, indem sie die folgende Eigenschaft `hibernate.jdbc.log.warnings=false` in der Datei `platform_home/tools/bin/jdbc.properties` setzen.

Aktivieren der Protokollierung für einzelne Benutzer

Sie können die Protokollierung für einzelne Benutzer aktivieren, indem Sie die Protokollierung für die Verwendung der XML-Datei konfigurieren und anschließend die XML-Datei bearbeiten.

Die Protokollierung wird mit einer von den zwei Dateien konfiguriert: log4j.properties oder log4j.xml. Standardmäßig wird die Datei log4j.properties verwendet.

Sie können die Protokollierung für einzelne Benutzer aktivieren, indem Sie die Protokollierung für die Verwendung der XML-Datei konfigurieren und anschließend die XML-Datei bearbeiten. Wird Unica Platform in einer Cluster Bereitstellung konfiguriert, kopieren Sie die XML Datei auf jeden Knoten.

- Sie können die Einzelbenutzer-Protokollierung aktivieren, indem Sie die XML Datei bearbeiten.
- Die Protokollierung wird mit der standardmäßigen Konfigurationsdatei `log4j.xml` konfiguriert.
- Wenn Unica Platform in einer Clusterbereitstellung konfiguriert wird, kopieren Sie die XML-Datei in die einzelnen Knoten.

Wenn die XML-Protokollierung aktiviert ist, wird ein Thread erstellt, der in regelmäßigen Zeitabständen prüft, ob die XML-Konfigurationsdatei erstellt oder geändert worden ist. Wird eine Änderung oder Dateierstellung erkannt, wird die XML-Datei für die Konfiguration von "log4j" gelesen. Das Abfrageintervall beträgt 60 Sekunden.

1. Konfigurieren Sie die Protokollierung für die Verwendung von log4j.xml, indem Sie den folgenden JVM Parameter festlegen.

   ```
   -DENABLE_PLATFORM_LOG4J_XML_LOGGING=true
   ```

   Der Wert muss auf 'true' gesetzt werden, um die Protokollierung pro Benutzer zu aktivieren.

   Wird Unica Platform in einer Cluster Bereitstellung konfiguriert, legen Sie diesen JVM Parameter in den einzelnen Knoten des Clusters fest.
2. Um das Benutzerkonto anzugeben, das für die Protokollierung pro Benutzer angemeldet werden soll, bearbeiten Sie die Datei log4j.xml und fügen Sie die Benutzer zum Filter-Tag hinzu. Die Protokolle für die Benutzer, die im Filter-Tag hinzugefügt werden.

- Sie können der Datei `log4j.xml` mehrere Tags hinzufügen, um benutzerspezifische Protokolldateien zu erstellen. Sie müssen für jede neue benutzerspezifische Protokolldatei einen neuen Appender hinzufügen.
- Standardmäßig wird die Protokolldatei im Ordner `Platform_Home / Platform/logs` erstellt und hat den Namen `platform.log`. Sie können einen anderen gültigen Pfad und Dateinamen angeben. Sie müssen den absoluten oder den vollständigen Pfad angeben, um die Protokolldateien in den entsprechenden Ordnern generieren zu können.
- Wenn benutzerspezifische Protokolle und Protokolle für alle Benutzer erforderlich sind, fügen Sie einen Appender-Tag mit einem neuen Namen und ohne definierten Filtertag hinzu. Der Appender muss einen eindeutigen Namen haben.
- Fügen Sie unter dem Root-Tag für diesen neuen Appender einen entsprechenden Eintrag hinzu.

3. Wird Unica Platform in einer Cluster-Bereitstellung konfiguriert, kopieren Sie die bearbeitete XML Datei auf jeden Knoten des Clusters.

   Sie können einen Befehl wie den im folgenden Beispiel angezeigten Befehl verwenden.

   `-DPLATFORM_LOG4J_XML_FILE=log4j_node1.xml`

   Die Datei `log4j_node1.xml` ist eine Kopie der Datei `log4j.xml`. Sie können einen beliebigen Namen für die kopierte Datei verwenden. Die Protokolldatei wird auch automatisch mit diesem neuen Namen log4j_node1.log anstelle des Standardnamens platform.log erstellt.

   Betrachten Sie das folgende Beispiel, in dem die Protokolle für den Benutzer asm_admin und für alle anderen Benutzer erfasst werden.

```
<appender name="Console" class="org.apache.log4j.ConsoleAppender">
<param name="ImmediateFlush" value="true"/> <layout
class="org.apache.log4j.PatternLayout"> <param
name="ConversionPattern" value="%-5p %c - %m%n"/> </layout>
<filter class="com.unica.manager.logger.UserMatchFilter"> <param
name="StringToMatch" value="asm_admin" /> </filter> </appender>
<appender name="Console" class="org.apache.log4j.ConsoleAppender">
```

```
<param name="ImmediateFlush" value="true"/> <layout
class="org.apache.log4j.PatternLayout"> <param
name="ConversionPattern" value="%-5p %c - %m%n"/> </layout>
<filter class="com.unica.manager.logger.UserMatchFilter">
<param name="StringToMatch" value="asm_admin" />
</filter> </appender> </appender> <!-- <logger
name="com.unica.manager.configuration.ConfigurationManager">
<level value="TRACE"/> </logger> <logger
name="com.unica.suite.scheduler.server.manager.TaskManager">
<level value="DEBUG"/> </logger> <logger
name="org.hibernate.util.JDBCExceptionReporter"> <level
value="ERROR"/> </logger> --> <root> <level value="WARN"/>
<appender-ref ref="System"/> <appender-ref ref="Console"/>
<appender-ref ref="SystemAllUsers"/> </root>
```

1. Um das Benutzerkonto anzugeben, das bei der Protokollierung pro Benutzer angemeldet werden soll, bearbeiten Sie die Datei `log4j.xml` und entfernen Sie das RollingFile-Tag mit dem Namen UserLogAppender. Fügen Sie die Benutzer-ID im Filter-Tag hinzu. Die Protokolle für den im Filter-Tag hinzugefügten Benutzer werden in der Datei gespeichert, die in diesem Appender erwähnt wird. Setzen Sie den folgenden JVM Parameter, soweit er nicht bereits gesetzt ist

   `-DUNICA_PLATFORM_HOME= <platform_home_directory_path>`

   - Sie können der Datei `log4j.xml` mehrere Tags hinzufügen, um benutzerspezifische Protokolldateien zu erstellen. Sie müssen für jede neue benutzerspezifische Protokolldatei einen neuen Appender hinzufügen.
   - Standardmäßig wird die Protokolldatei im Ordner `Platform_Home / Platform/logs` erstellt und hat den Namen `platform.log`. Sie können einen anderen gültigen Pfad und Dateinamen angeben. Sie müssen den absoluten oder den vollständigen Pfad angeben, um die Protokolldateien in den entsprechenden Ordnern generieren zu können.
   - Wenn benutzerspezifische Protokolle und Protokolle für alle Benutzer erforderlich sind, fügen Sie einen Appender-Tag mit einem neuen Namen und

ohne definierten Filtertag hinzu. Der Appender muss einen eindeutigen Namen haben.
- Fügen Sie unter dem Root-Tag für diesen neuen Appender einen entsprechenden Eintrag hinzu.

2. Wenn Unica Platform in einer Clusterbereitstellung konfiguriert wird, kopieren Sie die bearbeitete XML-Datei in die einzelnen Knoten des Clusters.

   Sie können einen Befehl wie den im folgenden Beispiel angezeigten Befehl verwenden.

   `-DPLATFORM_LOG4J_XML_FILE=log4j_node1.xml`

   Die Datei `log4j_node1.xml` ist eine Kopie der Datei `log4j.xml`. Sie können einen beliebigen Namen für die kopierte Datei verwenden. Die Protokolldatei wird auch automatisch mit diesem neuen Namen log4j_node1.log anstelle des Standardnamens platform.log erstellt.

Betrachten Sie das folgende Beispiel, in dem die Protokolle für den Benutzer `asm_admin` und für alle anderen Benutzer erfasst werden.

```
<?xml version="1.0" encoding="UTF-8"?> <Configuration
 packages="com.unica.manager.logger" monitorInterval="60">
 <Appenders> <!-- Console Log Appender -> <Console name="CONSOLE_LOG"
 target="SYSTEM_OUT" immediateFlush="true"> <PatternLayout
 pattern="%-5p %c - %m%n"/> </Console> <!-- System Log Appender
 --> <!-- The following section is for logs for all the user-->
 <RollingFile name="SYS_LOG" fileName="${sys:UNICA_PLATFORM_LOG_FILE}"
 filePattern="${sys:UNICA_PLATFORM_LOG_FILE}.%d{yyyy-MM-dd}-%i"
 immediateFlush="true" append="true" > <PatternLayout pattern="%d{DATE}
 - %-5p - %m%n" /> <Policies> <TimeBasedTriggeringPolicy interval="1"
 modulate="true"/> <SizeBasedTriggeringPolicy size="10 MB" />
 </Policies> <DefaultRolloverStrategy max="10"/> </RollingFile>
 <!-- The following section is for user specific logs for
 the user asm_admin--> <RollingFile name="UserLogAppender"
 fileName="${sys:UNICA_PLATFORM_HOME}/logs/asm_admin.log"
 filePattern="${sys:UNICA_PLATFORM_HOME}/logs/asm_admin.log.%d{yyyy-MM-dd}"
```

```
immediateFlush="true" append="true" > <PatternLayout
pattern="%d{yyyy-MM-dd HH:mm:ss} [%X{user}] %-5p %F.%M:%L: %m%n" />
<Policies> <SizeBasedTriggeringPolicy size="10 MB" /> </Policies>
<DefaultRolloverStrategy max="10"/> <UserMatchFilter user="asm_admin"
onMatch="ACCEPT" onMismatch="NEUTRAL"/> </RollingFile> </Appenders>
<Loggers> <Root level="WARN" includeLocation="true"> <AppenderRef
ref="SYS_LOG"/> <AppenderRef ref="CONSOLE_LOG"/> <!-- <AppenderRef
ref="UserLogAppender"/> --> </Root> <!-- <Logger name="com.unicacorp"
level="INFO"> --> <!-- <AppenderRef ref="UserLogAppender"/> --> <!--
</Logger> --> <!-- <Logger name="com.unica" level="INFO"> --> <!--
<AppenderRef ref="UserLogAppender"/> --> <!-- </Logger> --> </Loggers>
</Configuration>
```

Unica Platform -Dienstprogramme

Dieser Abschnitt enthält eine Übersicht über die Unica Platform-Dienstprogramme und einige Details zu allen Dienstprogrammen, die nicht in den Beschreibungen der einzelnen Dienstprogramme enthalten sind.

Speicherort der Dienstprogramme

Unica Platform Dienstprogramme befinden sich im Verzeichnis `tools/bin` der Unica Platform-Installation.

Liste und Beschreibungen von Dienstprogrammen

Unica Platform stellt die folgenden Dienstprogramme bereit.

- Clientdetails *(auf Seite 356)* -Generiert einen Schlüssel für eine Clientanwendung wie Unica Journey, um sich mit einer Unica Platform zu authentifizierten.
- alertConfigTool *(auf Seite 349)* - registriert Alerts und Konfigurationen für Unica-Produkte
- configTool *(auf Seite 349)* - importiert, exportiert und löscht Konfigurationseinstellungen, einschließlich Produktregistrierungen.

- datafilteringScriptTool *(auf Seite 357)* - erstellt Datenfilter.
- encryptPasswords *(auf Seite 359)* - verschlüsselt und speichert Kennwörter.
- encryptTomcatDBPasswords *(auf Seite 361)* - encrypt wird zur Verschlüsselung der Datenbankpasswörter verwendet, die der Tomcat-Anwendungsserver intern verwendet.
- partitionTool *(auf Seite 362)* - erstellt Datenbankeinträge für Partitionen.
- populateDb *(auf Seite 366)* - füllt die Unica Platform-Datenbank auf.
- quartzjobtool *(auf Seite 372)* - Aktualisieren Sie die in Version 11.1 und älteren Versionen erstellten Scheduler-Jobs
- restoreAccess *(auf Seite 366)* - stellt einen Benutzer mit der Rolle „PlatformAdminRole“ wieder her.
- scheduler_console_client *(auf Seite 369)* - Führt Unica Scheduler-Jobs aus oder startet sie, die zur Überwachung auf einen Trigger konfiguriert wurden.
- insightsdbutil - Das Installationsprogramm platziert Berichtsentwurfsdateien, die über Datenbankverbindungstoken verfügen. Sie müssen sie für Ihre Systemdatenbank aktualisieren. Sie müssen das `insightsdbutil.sh/bat`-Dienstprogramm ausführen, um es zu aktualisieren. Siehe das Unica Insights-Installations- und Konfigurationshandbuch für weitere Einzelheiten.

Voraussetzungen für die Ausführung von Unica Platform-Dienstprogrammen

Folgende Voraussetzungen gelten für die Ausführung aller Unica Platform-Dienstprogramme.

- Führen Sie alle Dienstprogramme in dem Verzeichnis aus, in dem diese gespeichert sind (standardmäßig das `tools/bin-` Verzeichnis Ihrer Unica Platform-Installation).
- Unter UNIX™ starten Sie die Dienstprogramme am besten über dasselbe Benutzerkonto wie für den Anwendungsserver, auf dem Unica Platform installiert ist. Wenn Sie ein Dienstprogramm mit einem anderen Benutzerkonto ausführen, passen Sie die Berechtigungen für die Datei `platform.log` so an, dass das Benutzerkonto über Schreibberechtigungen dafür verfügt. Wenn Sie die Berechtigungen nicht anpassen, kann das Dienstprogramm keine Schreibvorgänge in die Protokolldatei durchführen und es werden möglicherweise einige Fehlermeldungen angezeigt, obwohl das Tool ordnungsgemäß ausgeführt wird.

Authentifizierung der Dienstprogramme

Dienstprogramme wie `configTool` und weitereUnica-Back-End-Dienstprogramme sind für die Verwendung durch Systemadministratoren konzipiert und erfordern den physischen Zugriff auf die Host-Server, damit sie aufgerufen werden können. Aus diesem Grund wurde die Authentifizierung für diese Dienstprogramme so entworfen, dass sie unabhängig vom Authentifizierungsmechanismus der Benutzeroberfläche ist. Der Zugriff auf diese Dienstprogramme steht für Benutzer zur Verfügung, die über Unica Platform-Administratorberechtigungen verfügen. Der Zugriff auf diese Dienstprogramme ist normalerweise lokal in Unica Platform definiert. Die Authentifizierung erfolgt für dieselbe Komponente.

Fehlerbehebung bei Verbindungsproblemen

Alle Unica Platform-Dienstprogramme mit Ausnahme von `encryptPasswords` interagieren mit den Unica Platform-Systemtabellen. Um eine Verbindung mit der Systemtabellendatenbank herzustellen, verwenden diese Dienstprogramme die folgenden Informationen, die vom Installationsprogramm mithilfe der bei der Unica Platform-Installation bereitgestellten Informationen festgelegt werden. Diese Informationen sind in der Datei `jdbc.properties` gespeichert, die sich im Verzeichnis `tools/bin` Ihrer Unica Platform-Installation befindet.

- Name des JDBC-Treibers
- JDBC-Verbindungs-URL (einschließlich Host, Port und Datenbankname)
- Datenquellenanmeldung
- Datenquellenkennwort (verschlüsselt)

Legen Sie die Umgebungsvariable `JAVA_HOME` fest, entweder im Script `setenv` im Verzeichnis `tools/bin` der Unica Platform-Installation. Normalerweise wird diese Variable automatisch durch das Unica Platform-Installationsprogramm im Script `setenv` festgelegt. Es empfiehlt sich jedoch, zu überprüfen, ob die Variable `JAVA_HOME` festgelegt ist, wenn Probleme bei der Ausführung eines Dienstprogramms auftreten. Das JDK muss der Sun-Version entsprechen (nicht etwa das JRockit JDK, das mit WebLogic bereitgestellt wird).

Sonderzeichen

Zeichen, die im Betriebssystem als reservierte Zeichen gekennzeichnet sind, müssen mit Escapezeichen verwendet werden. Eine Liste der reservierten Zeichen und zugehörigen Escapezeichen finden Sie in der Dokumentation Ihres Betriebssystems.

Standardoptionen in Unica Platform-Dienstprogrammen

Folgende Optionen sind in allen Unica Platform-Dienstprogrammen verfügbar.

`-l logLevel`

Festlegen der Ebene für in der Konsole angezeigte Protokollinformationen. Die verfügbaren Optionen sind `high`, `medium` und `low`. Der Standardwert ist `low`.

`-L`

Festlegen des Gebietsschemas für Konsolennachrichten. Die Voreinstellung für die Ländereinstellung ist en_US. Die verfügbaren Optionswerte werden von den Sprachen bestimmt, in die Unica Platform übersetzt wurde. Geben Sie die Ländereinstellung mithilfe der ICU-Ländereinstellungs-ID gemäß ISO 639-1 und ISO 3166 an.

`-h`

Anzeigen einer kurzen Verwendungsnachricht in der Konsole.

`-m`

Anzeigen der Handbuchseite für dieses Dienstprogramm in der Konsole.

`-v`

Anzeigen weiterer Ausführungsdetails in der Konsole.

Unica Platform-Dienstprogramme auf zusätzlichen Maschinen einrichten

Sie können die Unica Platform-Dienstprogramme ohne zusätzliche Konfiguration auf der Maschine ausführen, auf der Unica Platform installiert ist. Möglicherweise möchten Sie die Dienstprogramme jedoch von einer anderen Maschine im Netz ausführen. In der folgenden Vorgehensweise werden die erforderlichen Schritte dafür beschrieben.

Überprüfen Sie, ob die zu verwendende Maschine die folgenden Voraussetzungen erfüllt.

- Der korrekte JDBC-Treiber muss auf der Maschine vorhanden oder von dieser aus zugänglich sein.
- Die Maschine muss über das Netz auf die Unica Platform-Systemtabellen zugreifen können.
- Die Java™-Laufzeitumgebung muss auf der Maschine installiert oder von dieser aus zugänglich sein.

1. Sammeln Sie die folgenden Informationen zu Unica Platform-Systemtabellen.
    - Der vollständig qualifizierte Pfad für die JDBC-Treiberdatei(en) auf Ihrem System.
    - Der vollständig qualifizierte Pfad zu einer Installation der Java™-Laufzeitumgebung.

      Standardmäßig ist im Installationsprogramm der Pfad zur unterstützten Version der JRE angegeben, die das Installationsprogramm unter dem Unica-Installationsverzeichnis ablegt. Sie können diesen Standardwert übernehmen oder einen anderen Pfad angeben.
    - Datenbanktyp
    - Datenbankhost
    - Datenbankport
    - Datenbankname/System-ID
    - Datenbankbenutzername
    - Datenbankkennwort
2. Führen Sie das Unica Installationsprogramm aus und installieren Sie Unica Platform.

   Geben Sie die Informationen zur Datenbankverbindung ein, die Sie für die Unica Platform-Systemtabellen ermittelt haben. Falls Sie mit dem Unica Installationsprogramm nicht vertraut sind, lesen Sie das Installationshandbuch zu Unica Campaign oder Unica Plan.

   Sie müssen die Unica Platform-Webanwendung nicht bereitstellen, wenn Sie nur die Dienstprogramme installieren.

Dienstprogramme

In diesem Abschnitt werden die Unica Platform-Dienstprogramme mit funktionsbezogenen Einzelheiten, Syntax und Beispielen beschrieben.

alertConfigTool

Für die verschiedenen Unica-Produkte gibt es bestimmte Benachrichtigungstypen. Verwenden Sie das Dienstprogramm `alertConfigTool`, um die Benachrichtigungstypen zu registrieren, falls das Installationsprogramm dies nicht automatisch während der Installation oder dem Upgrade durchgeführt hat.

Syntax

`alertConfigTool -i -f *importFile*`

Commands

`-i -f *importFile*`

Alert- und Benachrichtigungstypen aus einer angegebenen XML-Datei importieren.

Beispiel

- Importieren von Alert- und Benachrichtigungstypen aus der Datei `Platform_alerts_configuration.xml` im Verzeichnis `tools\bin` der Unica Platform-Installation.

  ```
  alertConfigTool -i -f Platform_alerts_configuration.xml
  ```

configTool

Die Eigenschaften und Werte auf der Seite **Konfiguration** werden in den Unica Platform Systemtabellen gespeichert. Sie können das Dienstprogramm `configTool` verwenden, um Konfigurationseinstellungen in und aus den Systemtabellen zu importieren und zu exportieren.

Einsatzmöglichkeiten für „configTool“

Möglicherweise möchten Sie `configTool` aus den folgenden Gründen verwenden.

- Um die Partitions- und Datenquellenvorlagen, die mit Unica Campaigngeliefert werden, zu importieren, die Sie dann auf der Seite **Konfiguration** ändern und duplizieren können.
- Registrieren von (Importieren der Konfigurationseinstellungen für) Unica-Produkten, wenn das Installationsprogramm die Eigenschaften nicht automatisch zur Datenbank hinzufügen kann.
- Exportieren einer XML-Version der Konfigurationseinstellungen für die Sicherung oder zum Importieren in eine andere Installation von Unica.
- Um die Kategorien zu löschen, die nicht über den Link **Kategorie löschen** verfügen. Dabei verwenden Sie `configTool`, um die Konfiguration zu exportieren. Anschließend löschen Sie die XML Datei, welche die Kategorie erstellt hat, und verwenden Sie `configTool`, um die bearbeitete XML Datei zu importieren.

Important: Dieses Dienstprogramm ändert die Tabellen `usm_configuration` und `usm_configuration_values` in der Unica Platform Systemtabellendatenbank, die die Konfigurationseigenschaften und ihre Werte enthält. Um optimale Ergebnisse zu erzielen, erstellen Sie entweder Sicherheitskopien dieser Tabellen oder exportieren Sie die aktuellen Konfigurationen über `configTool` und sichern Sie dann die resultierende Datei. Damit haben Sie die Möglichkeit, die Konfiguration wieder herzustellen, falls der Import über `configTool` fehlschlägt.

Syntax

```
configTool -d -p "elementPath" [-o]

configTool -i -p "parent ElementPath" -f importFile [-o]

configTool -x -p "elementPath" -f exportFile

configTool -vp -p "elementPath" -f importFile [-d]

configTool -r productName -f registrationFile [-o] configTool -u productName
```

Befehle

`-d -p "elementPath" [o]`

Löschen von Konfigurationseinstellungen und den entsprechenden Einstellungen durch Festlegen eines Pfads in der Konfigurationseigenschaftenhierarchie.

Im Elementpfad müssen die internen Namen von Kategorien und Eigenschaften verwendet werden. Diese können Sie abrufen, indem Sie zu der Seite **Konfiguration** navigieren, die gewünschte Kategorie oder Eigenschaft und den Pfad auswählen, der im rechten Teilfenster in Klammern angezeigt wird. Begrenzen Sie einen Pfad in der Hierarchie der Konfigurationseigenschaft mit dem Zeichen `|` und setzen Sie den Pfad in doppelte Anführungszeichen.

Beachten Sie Folgendes:

- Mit diesem Befehl können keine vollständigen Anwendungen, sondern nur Kategorien und Eigenschaften in einer Anwendung gelöscht werden. Verwenden Sie den Befehl `-u`, um die gesamte Anwendung zu deregistrieren.
- Verwenden Sie die Option `-o`, um die Kategorien zu löschen, die auf der Seite **Konfiguration** nicht über den Link **Kategorie löschen** verfügen.

Wird `-d` zusammen mit dem Befehl `-vp` verwendet, löscht configTool alle untergeordneten Knoten im angegebenen Pfad, wenn diese Knoten in der angegebenen XML Datei nicht enthalten sind.

`-i -p "`*`parentElementPath`*`" -f` ***`importFile`*** **`[o]`**

Importieren von Konfigurationseinstellungen mit den entsprechenden Einstellungswerten aus einer festgelegten XML-Datei.

Zum Importieren geben Sie den Pfad zu dem übergeordneten Element an, unter welchem Sie die Kategorien speichern möchten. Das Dienstprogramm `configTool` importiert die Eigenschaften in der Kategorie, die Sie im Pfad angegeben haben.

Sie können Kategorien auf jeder Ebene unter der obersten Ebene speichern. In die Ebene der obersten Kategorie können Sie jedoch keine Kategorie hinzufügen.

Im übergeordneten Elementpfad müssen die internen Namen von Kategorien und Eigenschaften verwendet werden. Diese können Sie abrufen, indem Sie zu der Seite **Konfiguration** navigieren, die gewünschte Kategorie oder Eigenschaft und den Pfad auswählen, der im rechten Teilfenster in Klammern angezeigt wird. Begrenzen Sie einen

Pfad in der Hierarchie der Konfigurationseigenschaft mit dem Zeichen | und setzen Sie den Pfad in doppelte Anführungszeichen.

Sie können den Speicherort der Importdatei relativ zum Verzeichnis `tools/bin` oder einen vollständigen Verzeichnispfad angeben. Unabhängig davon, ob Sie einen relativen Pfad oder keinen Pfad festlegen, sucht `configTool` zuerst nach der Datei relativ zum Verzeichnis `tools/bin`.

Standardmäßig werden bestehende Kategorien über diesen Befehl nicht überschrieben. Aber Sie können die Option `-o` verwenden, um eine Überschreibung zu erzwingen.

`-x -p "`*`elementPath`*`" -f` ***`exportFile`***

Exportieren von Konfigurationseinstellungen und deren Einstellungswerten in eine XML-Datei mit festgelegtem Namen.

Sie können alle Konfigurationseinstellungen exportieren oder den Export auf eine bestimmte Kategorie beschränken, indem Sie einen Pfad in der Konfigurationseigenschaftenhierarchie festlegen.

Für den Elementpfad müssen die internen Namen der Kategorien und Eigenschaften verwendet werden. Diese können Sie abrufen, indem Sie zu der Seite **Konfiguration** navigieren, die gewünschte Kategorie oder Eigenschaft und den Pfad auswählen, der im rechten Teilfenster in Klammern angezeigt wird. Begrenzen Sie einen Pfad in der Hierarchie der Konfigurationseigenschaft mit dem Zeichen | und setzen Sie den Pfad in doppelte Anführungszeichen.

Sie können die Speicherposition der Exportdatei relativ zum aktuellen Verzeichnis oder einen vollständigen Verzeichnispfad angeben. Wenn der Dateipfad kein Trennzeichen (/ in UNIX™, / oder \ in Windows™) enthält, speichert `configTool` die Datei im Verzeichnis `tools/bin` der Unica Platform Installation. Falls Sie die Erweiterung `xml` nicht angeben, wird sie von `configTool` hinzugefügt.

`-vp -p "`*`elementPath`*`" -f` ***`importFile`*** **`[-d]`**

Dieser Befehl wird hauptsächlich bei manuellen Upgrades verwendet, um Konfigurationseigenschaften zu importieren. Wenn Sie ein Fixpack angewendet haben, das eine neue Konfigurationseigenschaft enthält, und dann ein Upgrade durchführen, können beim Importieren einer Konfigurationsdatei als Teil des manuellen Upgrades Werte

überschrieben werden, die beim Anwenden des Fixpacks festgelegt wurden. Der Befehl `-vp` stellt sicher, dass der Import keine zuvor festgelegten Konfigurationswerte überschreibt.

Important: Nachdem Sie das Dienstprogramm `configTool` mit der Option -vp verwendet haben, müssen Sie den Webanwendungsserver, auf dem Unica Platform bereitgestellt wird, erneut starten, damit die Änderungen angewendet werden.

Wird `-d` zusammen mit dem Befehl `-vp` verwendet, löscht configTool alle untergeordneten Knoten im angegebenen Pfad, wenn diese Knoten in der angegebenen XML Datei nicht enthalten sind.

`-r productName -f registrationFile`

Registrieren Sie die Anwendung. Der Speicherort der Registrierungsdatei kann relativ zum Verzeichnis `tools/bin` oder als vollständiger Verzeichnispfad angegeben werden. Standardmäßig wird die bestehende Konfiguration über diesen Befehl nicht überschrieben. Aber Sie können die Option `-o` verwenden, um eine Überschreibung zu erzwingen. Der Parameter *`productName`* muss einer der oben aufgelisteten Parameter sein.

Beachten Sie Folgendes:

- Wenn Sie den Befehl `-r` verwenden, muss die Registrierungsdatei `<application>` als erstes Tag in der XML Datei enthalten.

  Zusammen mit dem Produkt können andere Dateien zur Verfügung gestellt werden, mit deren Hilfe Sie Konfigurationseinstellungen in die Unica Platform-Datenbank einfügen können. Für diese Dateien, verwenden Sie den Befehl `-i`. Nur die Datei, die das Tag `<application>` als erstes Tag enthält, kann mit dem Befehl `-r` verwendet werden.
- Die Registrierungsdatei für Unica Platform lautet `Manager_config.xml` und der erste Tag lautet `<Suite>`. Um diese Datei in einer neuen Installation zu registrieren, verwenden Sie das Dienstprogramm `populateDb`, oder führen Sie das Unica Platform

Installationsprogramm erneut aus, wie im *Unica Platform Installationshandbuch* beschrieben.

- Zur erneuten Registrierung aller Produkte außer Unica Platform nach der Erstinstallation, verwenden Sie `configTool` mit den Befehlen `-r` und `-o`, um die bestehenden Eigenschaften zu überschreiben.

Das Dienstprogramm `configTool` verwendet Produktnamen als Parameter mit den Befehlen, die Produkte registrieren und deregistrieren. Mit dem Release 8.5.0 von Unica haben sich viele Produktnamen geändert. Die in `configTool` verwendeten Namen haben sich jedoch nicht geändert. Die gültigen Produktnamen für die Verwendung in `configTool` sowie die aktuellen Produktnamen sind nachfolgend aufgeführt.

Table 73. Produktnamen für die Registrierung und die Aufhebung der Registrierung mit configTool

Produktname	In configTool verwendeter Name
Unica Platform	`Manager`
Unica Campaign	`Campaign`
Unica Collaborate	`Online zusammenarbeiten`
Unica Deliver	`Zustellen`
Unica Journey	`Journey`
Unica Insights	`UnicaInsights`
Unica Content Integration	`assetPicker`
Unica Offer	`Angebot`
Unica Interact	`interact`
Unica Optimize	`Optimieren`
Unica Plan	`Plan`

Table 73. Produktnamen für die Registrierung und die Aufhebung der Registrierung mit configTool (continued)

Produktname	In configTool verwendeter Name
Opportunity Detect	`Detect`
IBM SPSS Modeler Advantage Enterprise Marketing Management Edition	`SPSS`
Digital Analytics	`Coremetrics`

`-u` *`productName`*

Deregistrieren Sie eine durch *`productName`* angegebenen Anwendung. Sie müssen der Produktkategorie keinen Pfad hinzufügen, der Produktname ist ausreichend und erforderlich. Der Prozess entfernt alle Eigenschaften und Konfigurationseinstellungen für das Produkt.

Optionen

`-o`

Bei Verwendung mit `-i` oder `-r` wird eine vorhandene Kategorie oder Produktregistrierung (Knoten) überschrieben.

Bei Verwendung mit `-d` können Sie eine Kategorie (Knoten) löschen, die auf der Seite **Konfiguration** über den Link **Kategorie löschen** nicht verfügt.

Beispiele

- Importieren Sie die Konfigurationseinstellungen aus der Datei `Product_config.xml` im Verzeichnis `conf` der Unica PlatformInstallation.

  ```
  configTool -i -p "Affinium" -f Product_config.xml
  ```
- Importieren von einer der Unica Campaign-Datenquellenvorlagen in die Unica Campaign-Standardpartition: partition1. Das Beispiel geht davon aus, dass Sie die

Oracle Datenquellenvorlage `OracleTemplate.xml` im Verzeichnis `tools/bin` der Unica Platform Installation gespeichert haben.

```
configTool -i -p "Affinium|Campaign|partitions|partition1|dataSources" -f
OracleTemplate.xml
```

- Exportieren Sie alle Konfigurationseinstellungen in die Datei `myConfig.xml` im Verzeichnis `D:\backups`.

  ```
  configTool -x -f D:\backups\myConfig.xml
  ```

- Exportieren Sie eine bestehenden Unica Campaign Partition (vollständig, mit Datenquelleneinträgen). Speichern Sie in der Datei `partitionTemplate.xml` und danach im Standardverzeichnis `tools/bin` der Unica Platform Installation.

  ```
  configTool -x -p "Affinium|Campaign|partitions|partition1" -f
  partitionTemplate.xml
  ```

- Registrieren Sie manuell die Anwendung productName mit der Datei `app_config.xml`, die im Standardverzeichnis `tools/bin` der Unica Platform Installation gespeichert ist und überschreiben Sie die bestehende Registrierung dieser Anwendung.

  ```
  configTool -r product Name -f app_config.xml -o
  ```

- Aufheben der Registrierung einer Anwendung „productName“.

  ```
  configTool -u productName
  ```

- Führen Sie den folgenden Befehl aus, um die encodeCSV-Funktion zu aktivieren:

  ```
  configTool -vp -p "Affinium|Plan|umoConfiguration" -f Plan_Home\conf
  \Plan_encodeProperty_11.1.xml
  ```

- Registrieren Sie die Einstellungen von Unica Interact als Konfigurationsmenü unter `AffiniumWebApps\Campaign\interact\conf \interact_setup_navigation.xml` mit

  ```
  configTool.bat -v -i -p "Affinium|suite|uiNavigation|settingsMenu" -f
  "interact_setup_navigation.xml"
  ```

Clientdetails

Dieses Dienstprogramm generiert Schlüssel für die Clientanwendung, wie z. B. Unica Journey zur Authentifizierung mit einer Platform-Instanz.

Er registriert den Schlüssel in der Platform-Datenbank und druckt ihn in der Konsole. Der Schlüssel kann dann kopiert und in die Zielanwendung eingefügt werden.

Syntax

```
clientDetails -a appName
```

Befehle

```
-a appName
```

Generieren Sie den Schlüssel für die angegebene Anwendung. Mögliche Werte für appName sind Manager (für Unica Platform) und Journey (für Unica Journey)

Beispiele

Schlüssel für Unica Journey generieren

```
clientDetails -a Journey
```

datafilteringScriptTool

Das Dienstprogramm `datafilteringScriptTool` liest eine XML-Datei, um die Datenfiltertabellen in der Unica Platform-Systemtabellendatenbank zu füllen.

Abhängig von der Art, wie XML geschrieben wird, können Sie dieses Dienstprogramm auf zweierlei Weise verwenden:

- Mit einem Satz XML-Elemente können Sie Datenfilter automatisch auf Grundlage eindeutiger Wertekombinationen in Feldern erstellen (ein Datenfilter für jede eindeutige Kombination).
- Mit einem etwas unterschiedlichen Satz XML-Elemente können Sie jeden Datenfilter angeben, den das Dienstprogramm erstellt.

Informationen zum Erstellen der XML-Elemente finden Sie im Unica Platform-Administratorhandbuch.

Wann „datafilteringScriptTool“ verwendet werden sollte

Sie benötigen `datafilteringScriptTool` bei der Erstellung neuer Datenfilter.

Voraussetzungen

Unica Platform muss bereitgestellt und ausgeführt werden.

„datafilteringScriptTool“ mit SSL verwenden

Bei der Bereitstellung von Unica Platform mit One-Way-SSL müssen Sie das Script „datafilteringScriptTool“ so ändern, dass Sie die SSL-Optionen für das Handshakeverfahren hinzufügen. Um das Script ändern zu können, benötigen Sie die folgenden Informationen:

- Truststore-Dateiname und -Pfad
- Truststore-Kennwort

Öffnen Sie das „datafilteringScriptTool“ (`.bat` oder `.sh`) in einem Texteditor, und suchen Sie nach den folgenden Zeilen (Beispiele aus der Windows™-Version):

```
:callexec

"%JAVA_HOME%\bin\java" -DUNICA_PLATFORM_HOME="%UNICA_PLATFORM_HOME%"

com.unica.management.client.datafiltering.tool.DataFilteringScriptTool %*
```

Bearbeiten Sie diese Zeilen entsprechend, sodass sie wie folgt aussehen (neuer Text in **fettgedruckt**): Ersetzen Sie Ihren Truststore-Pfad und -Dateinamen und das Truststore-Kennwort durch `myTrustStore.jks` und `myPassword`.

```
:callexec

SET SSL_OPTIONS=-Djavax.net.ssl.keyStoreType="JKS"

-Djavax.net.ssl.trustStore="C:\security\myTrustStore.jks"

-Djavax.net.ssl.trustStorePassword=myPassword

"%JAVA_HOME%\bin\java" -DUNICA_PLATFORM_HOME="%UNICA_PLATFORM_HOME%"
%SSL_OPTIONS%

com.unica.management.client.datafiltering.tool.DataFilteringScriptTool %*
```

Syntax

`datafilteringScriptTool -r` *`path`*`file`

Commands

`-r path_file`

Importieren Sie Datenfilterspezifikationen aus einer ausgewählten XML-Datei. Falls sich die Datei nicht im Verzeichnis `tools/bin` in Ihrem Installationsordner befindet, geben Sie einen Pfad an und schließen Sie den Parameter *`path`*`_file` in doppelte Anführungszeichen ein.

Beispiel

- Verwenden Sie eine Datei mit dem Namen `collaborateDataFilters.xml`, die sich im Verzeichnis `C:\unica\xml` befindet, um die Datenfiltersystemtabellen zu füllen.

  ```
  datafilteringScriptTool -r "C:\unica\xml\collaborateDataFilters.xml"
  ```

encryptPasswords

Das Dienstprogramm `encryptPasswords` wird zum Verschlüsseln und Speichern von einem der zwei Kennwörter verwendet, die in Unica Platform intern verwendet werden.

Die zwei Kennwörter, die das Dienstprogramm verschlüsseln kann, lauten wie folgt.

- Das Kennwort, das in Unica Platform verwendet wird, um auf die Systemtabellen zuzugreifen. Das Dienstprogramm ersetzt ein bestehendes verschlüsseltes Kennwort (gespeichert in der Datei `jdbc.properties` im Verzeichnis `tools\bin` der Unica Platform-Installation) durch ein neues Kennwort.
- Das Keystore-Kennwort, das von Unica Platform verwendet wird, wenn diese für den Einsatz von SSL mit einem anderen Zertifikat als dem von Unica Platform oder dem Webanwendungsserver bereitgestellten konfiguriert ist. Das Zertifikat kann entweder ein selbst signiertes Zertifikat oder ein Zertifikat einer Zertifizierungsstelle sein.

Verwendung von „encryptPasswords“

In folgenden Situationen können Sie `encryptPasswords` verwenden:

- Wenn Sie das Kennwort des Kontos ändern, das Sie für den Zugriff auf Ihre Unica Platform-Systemtabellendatenbank verwenden.
- Wenn Sie ein selbst signiertes Zertifikat erstellt oder ein Zertifikat einer Zertifizierungsstelle erhalten haben.

Voraussetzungen

- Bevor Sie `encryptPasswords` zum Verschlüsseln und Speichern eines neuen Datenbankkennworts verwenden, erstellen Sie eine Sicherheitskopie der Datei `jdbc.properties`, die sich im Verzeichnis `tools/bin` in Ihrer Unica Platform-Installation befindet.
- Bevor Sie `encryptPasswords` zum Verschlüsseln und Speichern des Keystore-Kennworts einsetzen, müssen Sie ein digitales Zertifikat erstellt oder erhalten haben und das Keystore-Kennwort kennen.

Syntax

`encryptPasswords -d databasePassword`

`encryptPasswords -k keystorePassword`

Befehle

`-d databasePassword`

Datenbankkennwort verschlüsseln.

`-k keystorePassword`

Verschlüsseln des Keystore-Kennworts und Speichern in der Datei `pfile`.

Beispiele

- Bei der Installation von Unica Platform wurde `myLogin` als Anmeldename für das Konto der Systemtabellendatenbank festgelegt. Nach einiger Zeit haben Sie das Kennwort in `newPassword` geändert. Führen Sie `encryptPasswords` wie folgt aus, um das Datenbankkennwort zu verschlüsseln und zu speichern.

  ```
  encryptPasswords -d newPassword
  ```

- Sie konfigurieren eine Unica-Anwendung, um SSL verwenden zu können, und haben ein digitales Zertifikat erstellt oder erhalten. Führen Sie `encryptPasswords` wie folgt aus, um das Datenbankkennwort zu verschlüsseln und zu speichern.

  ```
  encryptPasswords -k myPassword
  ```

encryptTomcatDBPasswords

Das Dienstprogramm `encryptTomcatDBPasswords` wird zur Verschlüsselung der Datenbankpasswörter verwendet, die der Tomcat-Anwendungsserver intern verwendet. Es wird zur Verschlüsselung von Datenbankkennwörtern verwendet, die in Campaign.xml und unica.xml verwendet werden. Dieses Dienstprogramm kann das Kennwort der Unica-Anwendungsdatenbank verschlüsseln. Das Dienstprogramm gibt das verschlüsselte Kennwort in der Befehlszeile aus.

Wann sollte man encryptTomcatDBPasswords verwenden?

Verwenden Sie das Dienstprogramm `encryptTomcatDBPasswords`, wenn Sie ein verschlüsseltes Kennwort unter Tomcat-Konfigurationen verwenden möchten. Es kann verwendet werden, wenn das Campaign- oder Unica System DB-Kennwort abgelaufen ist oder geändert wurde. Sie können dieses Dienstprogramm verwenden und das Kennwort verschlüsseln, welches in Campaign.xml, unica.xml und plan.xml ersetzt wird, die sich unter `<instanceHome>\conf\Catalina\localhost` befinden.

Syntax

```
encryptTomcatDBPasswords -d databasePassword
```

Befehle

`-d databasePassword`

Datenbankkennwort verschlüsseln.

Anmerkung:

Dieses Dienstprogramm ist nur verfügbar, wenn der Benutzer bei der Installation von Unica Platform als Anwendungsserver Tomcat auswählt.

Dieses Dienstprogramm kann nur dann verwendet werden, wenn der Benutzer unter Tomcat-Konfigurationen verschlüsselte Kennwörter anstelle von Kennwörtern im Klartext verwenden möchte.

Ausführliche Informationen finden Sie in der Tomcat-Dokumentation.

partitionTool

Partitionen sind Unica Campaign-Richtlinien und -Rollen zugeordnet. Diese Richtlinien und Rollen sowie die ihnen zugeordnete Partition sind in den Unica Platform-Systemtabellen gespeichert. Das Dienstprogramm `partitionTool` initialisiert die Unica PlatformSystemtabellen mit grundlegenden Informationen zu Richtlinien und Rollen für Partitionen.

Wann „partitionTool“ verwendet werden sollte

Für jede von Ihnen erstellten Partition, müssen Sie `partitionTool` verwenden, um die Unica Platform Systemtabellen mit grundlegenden Informationen zu Richtlinien und Rollen zu initialisieren.

Ausführliche Informationen zur Einrichtung mehrerer Partitionen in Unica Campaign finden Sie im Installationshandbuch zu Ihrer Version von Unica Campaign.

Sonderzeichen und Leerzeichen

Partitionsbeschreibungen oder Benutzer-, Gruppen- oder Partitionsnamen, die Leerzeichen enthalten, müssen in doppelten Anführungszeichen angegeben werden.

Syntax

```
partitionTool -c -s sourcePartition -n newPartitionName [-u admin_user_name]
[-d partitionDescription] [-g groupName] [-a application]
```

Befehle

Folgende Befehle sind im Dienstprogramm `partitionTool` verfügbar.

`-c`

Kopiert (klont) die Richtlinien und Rollen für eine bereits vorhandene Partition, die mithilfe der Option `-s` angegeben wurde und verwendet den Namen, der mithilfe der Option `-n` angegeben wurde. Die beiden Optionen sind bei `c` erforderlich. Dieser Befehl bewirkt Folgendes.

- Er erstellt einen neuen Unica-Benutzer mit der Rolle „Admin“ in der Richtlinie „Administratorrollen“ sowie in der globalen Richtlinie in Unica Campaign. Der von Ihnen angegebene Partitionsname wird automatisch als Kennwort dieses Benutzers eingerichtet.
- Er erstellt eine neue Unica Platform-Gruppe und macht den neuen Benutzer „Admin“ zum Mitglied dieser Gruppe.
- Er erstellt ein neues Partitionsobjekt.
- Er repliziert sämtliche Richtlinien, die der Quellpartition zugewiesen sind und weist diese der neuen Partition zu.
- Er repliziert für jede replizierte Richtlinie sämtliche dieser Richtlinien zugewiesenen Rollen.
- Er ordnet jeder replizierten Richtlinie sämtliche Funktionen auf die gleiche Weise zu, wie diese in der ursprünglichen Rolle zugeordnet waren.
- Er weist die neue Unica Platform-Gruppe der letzten systemdefinierten Rolle „Admin“ zu, die während der Rollenreplikation erstellt wurde. Wenn Sie die Standardpartition (partition1) klonen, ist diese Rolle die Standard-Administratorrolle (Admin).

Optionen

`-d` *`partitionDescription`*

Optional, wird nur in Verbindung mit `-c` verwendet. Gibt eine Beschreibung an, die in der Ausgabe des Befehls `-list` angezeigt wird. Darf maximal 256 Zeichen enthalten. Falls die Beschreibung Leerzeichen enthält, muss sie in doppelten Anführungszeichen angegeben werden.

`-a` *`Anwendung`*

Optional, wird nur mit `-c`, `-n`, `-g` und `-u` verwendet. Klont Daten von der Quellpartition für die angegebene reine Anwendungspartition. Die Anwendung muss zu den Unica Suite Anwendungen gehören.

`-g` *`groupName`*

Optional, wird nur in Verbindung mit `-c` verwendet. Gibt den Namen der Unica Platform-Administratorgruppe an, die vom Dienstprogramm erstellt wird. Der Name muss eindeutig sein, innerhalb der Instanz Unica Platform

Falls kein Name angegeben wird, wird standardmäßig der Name `partition_nameAdminGroup` verwendet.

`-n` *`partitionName`*

Optional mit `-list`, obligatorisch mit `-c`. Darf maximal 32 Zeichen enthalten.

In Verbindung mit `-list`, gibt die Partition an, deren Informationen gelistet sind.

Bei der Verwendung mit `-c`, gibt den Namen der neuen Partition an und der von Ihnen angegebene Partitionsname wird als Passwort für den Admin Benutzer verwendet. Der Partitionsname muss mit dem Namen übereinstimmen, mit dem Sie die Partition bei der Konfiguration benannt haben (mithilfe der Partitionsvorlage auf der Konfigurationsseite).

`-s` *`sourcePartition`*

Pflichtig, wird nur mit `-c` verwendet. Der Name der Quellpartition, die repliziert werden soll.

`-u` *`adminUserName`*

Optional, wird nur in Verbindung mit `-c` verwendet. Gibt den Benutzernamen des Admin-Benutzers für die replizierte Partition an. Der Name muss innerhalb dieser Instanz von Unica Platform eindeutig sein.

Falls kein Name angegeben wird, wird standardmäßig der Name *`partitionName`*`AdminUser` verwendet.

Der Partitionsname wird automatisch als Kennwort dieses Benutzers eingerichtet.

Beispiele

- Erstellt eine Partition mit folgenden Merkmalen:
    - Geklont von partition1
    - Der Partitionsname lautet `myPartition`

    - Verwendet den Standardbenutzernamen (`myPartitionAdminUser`) und das Passwort (`myPartition`)
    - Verwendet den Standardgruppennamen (`myPartitionAdminGroup`)
    - Beschreibung lautet „ClonedFromPartition1“
    - `partitionTool -c -s partition1 -n myPartition -d "ClonedFromPartition1"`
- Erstellt eine Partition mit folgenden Merkmalen:
    - Geklont von partition1
    - Der Partitionsname lautet `partition2`
    - Gibt den Benutzernamen `customerA`mit dem automatisch zugeordneten Passwort `partition2` an
    - Gibt den Gruppennamen `customerAGroup` an
    - Beschreibung lautet „PartitionForCustomerAGroup“
    - `partitionTool -c -s partition1 -n partition2 -u customerA -g customerAGroup -d "PartitionForCustomerAGroup"`
- Aktualisieren Sie eine Partition mit den folgenden Merkmalen.
    - Geklont von partition1
    - Der Partitionsname lautet partition2
    - Geben Sie den Admin Benutzernamen und die Admin Benutzergruppe von Partition2 an
    - `partitionTool -c -s partition1 -n partition2 -u partition2AdminUser -a Journey`

Note: Bei der Verwendung von Option `-a`, stellen Sie sicher, dass Sie den Gruppennamen angeben, falls der Gruppenname explizit bei der Erstellung von der Partition vom Dienstprogramm angegeben wurde.

`partitionTool -c -s partition1 -n partition2 -u partition2AdminUser -g [partition2 group name] -a Journey`

populateDb

Das Dienstprogramm `populateDb` fügt Standarddaten (Seed) in die Unica Platform-Systemtabellen ein.

Das Unica-Installationsprogramm kann die Unica Platform-Systemtabellen mit Standarddaten für Unica Platform und Unica Campaign auffüllen. Falls Ihre Unternehmensrichtlinien nicht zulassen, dass das Installationsprogramm die Datenbank ändert, oder das Installationsprogramm keine Verbindung zu den Unica Platform-Systemtabellen herstellen kann, müssen Sie mithilfe dieses Dienstprogramms Standarddaten in die Unica Platform-Systemtabellen einfügen.

Für Unica Campaign zählen hierzu Sicherheitsrollen und Berechtigungen für die Standardpartition. Für Unica Platform zählen hierzu Standardbenutzer und -gruppen sowie Sicherheitsrollen und Berechtigungen für die Standardpartition.

Syntax

`populateDb -n productName`

Commands

`-n productName`

Einfügen von Standarddaten in die Unica Platform-Systemtabellen. Gültige Produktnamen sind `Manager` (für Unica Platform) und `Campaign` (für Unica Campaign).

Beispiele

- Manuelles Einfügen von Unica Platform-Standarddaten.

  ```
  populateDb -n Manager
  ```

- Manuelles Einfügen von Unica Campaign-Standarddaten.

  ```
  populateDb -n Campaign
  ```

restoreAccess

Das Dienstprogramm `restoreAccess` ermöglicht die Wiederherstellung des Zugriffs auf Unica Platform, falls alle Benutzer mit der Berechtigung „PlatformAdminRole“ unbeabsichtigt gesperrt wurden oder wenn alle Möglichkeiten, eine Anmeldung an Unica Platform durchzuführen, verlorengegangen sind.

Verwenden von „restoreAccess“

Sie können `restoreAccess` einsetzen, falls einer der beiden folgenden Fälle eintritt.

PlatformAdminRole-Benutzer sind inaktiviert

Es kann vorkommen, dass alle Benutzer mit PlatformAdminRole-Berechtigungen in Unica Platform im System inaktiviert werden. Nachfolgend ein Beispiel für eine Inaktivierung des Benutzerkontos „platform_admin“. Angenommen, nur ein Benutzer verfügt über die PlatformAdminRole-Berechtigungen (der Benutzer „platform_admin“). Nehmen Sie weiterhin an, dass für die Eigenschaft `Maximal zulässige fehlgeschlagene Anmeldeversuche` in der Kategorie **Allgemein | Kennworteinstellungen** auf der Seite „Konfiguration“ der Wert `3` festgelegt ist. Nun gibt ein Benutzer, der versucht, sich als „platform_admin“ anzumelden, drei Mal in Folge ein falsches Kennwort ein. Diese fehlgeschlagenen Anmeldeversuche führen zur Inaktivierung des Kontos „platform_admin“ im System.

In diesem Fall können Sie `restoreAccess` einsetzen, um den Unica Platform-Systemtabellen einen Benutzer mit PlatformAdminRole-Berechtigungen hinzuzufügen, ohne auf die Internetschnittstelle zugreifen zu müssen.

Wenn Sie `restoreAccess` auf diese Art ausführen, erstellt das Dienstprogramm einen Benutzer mit PlatformAdminRole-Berechtigungen sowie dem von Ihnen angegebenen Anmeldenamen und -kennwort.

Falls der von Ihnen angegebene Anmeldename des Benutzers in Unica Platform bereits als interner Benutzer existiert, wird das Kennwort des Benutzers geändert.

Nur ein Benutzer mit dem Anmeldenamen „PlatformAdmin“ und mit PlatformAdminRole-Berechtigungen kann alle Dashboards universell verwalten. Wenn also der Benutzer „platform_admin“ deaktiviert ist und Sie mit `restoreAccess` einen neuen Benutzer erstellen, sollten Sie einen Benutzer mit dem Anmeldenamen „platform_admin“ erstellen.

Falsche Konfiguration der NTLMv2-Authentifizierung

Wenn Sie die NTLMv2-Authentifizierung mit einer fehlerhaften Konfiguration implementieren und sich deshalb nicht mehr anmelden können, dann verwenden Sie `restoreAccess`, um die Fähigkeit zur Anmeldung wiederherzustellen.

Wenn Sie `restoreAccess` auf diese Weise ausführen, dann ändert das Dienstprogramm den Wert der Eigenschaft `Platform | Sicherheit | Anmeldeverfahren` in `Unica Platform`. Diese Änderung ermöglicht es Ihnen, sich mit jedem Benutzerkonto anzumelden, das vor der Sperrung des Zugangs bestanden hat. Sie können auch einen neuen Anmeldenamen und ein neues Kennwort festlegen. Sie müssen den Webanwendungsserver, auf dem Unica Platform bereitgestellt wird, neu starten, wenn Sie das Dienstprogramm `restoreAccess` auf diese Art verwenden.

Hinweise zum Kennwort

Bei der Verwendung von `restoreAccess` sollten Sie Folgendes zum Thema „Kennwörter“ beachten.

- Das Dienstprogramm `restoreAccess` unterstützt keine leeren Kennwörter und setzt keine Kennwortregeln durch.
- Falls Sie einen Anmeldenamen angeben, der bereits verwendet wird, setzt das Dienstprogramm das Kennwort des Benutzers zurück.

Syntax

`restoreAccess -u` *`loginName`* `-p` *`password`*

`restoreAccess -r`

Commands

`-r`

Setzt bei Verwendung ohne die Option `-u`*`loginName`* den Eigenschaftswert `Platform | Sicherheit | Anmeldemethode` zurück auf `Unica Platform`. Erfordert einen Neustart des Webanwendungsservers, um in Kraft zu treten.

Erstellt bei der Verwendung mit der Option `-u`*`loginName`* einen PlatformAdminRole-Benutzer.

Optionen

`-u` *`loginNname`*

Erstellt einen Benutzer mit dem angegebenen Anmeldenamen und den PlatformAdminRole-Berechtigungen. Muss in Verbindung mit der Option `-p` verwendet werden.

`-p` *`password`*

Legt das Kennwort für den zu erstellenden Benutzer fest. Erforderlich mit `-u`.

Beispiele

- Erstellen eines Benutzers mit PlatformAdminRole-Berechtigungen. Der Anmeldename lautet `tempUser` und das Kennwort `tempPassword`.

  ```
  restoreAccess -u tempUser -p tempPassword
  ```
- Ändern des Werts der Anmeldemethode auf `Platform` und Erstellen eines Benutzers mit PlatformAdminRole-Berechtigungen. Der Anmeldename lautet `tempUser` und das Kennwort `tempPassword`.

  ```
  restoreAccess -r -u tempUser -p tempPassword
  ```

scheduler_console_client

Jobs, die im Unica-Scheduler konfiguriert wurden, können mithilfe dieses Dienstprogramms aufgelistet und gestartet werden, wenn sie für die Überwachung eines Auslösers konfiguriert wurden.

Vorgehensweise bei aktiviertem SSL

Wird die Unica Platform Webanwendung zur Verwendung von SSL konfiguriert, muss die vom Dienstprogramm `scheduler_console_client` verwendete JVM dasselbe SSL Zertifikat verwenden, das vom Webanwendungsserver verwendet wird, auf dem Unica Platform bereitgestellt wird.

Führen Sie die folgenden Schritte aus, um das SSL-Zertifikat zu importieren:

- Bestimmen Sie den Speicherort der JRE, die von `scheduler_console_client` verwendet wird.
    - Wird `JAVA_HOME` als Systemumgebungsvariable gesetzt, verweist sie auf die JRE, die vom Dienstprogramm `scheduler_console_client` verwendet wird.
    - Wird `JAVA_HOME` nicht als Systemumgebungsvariable gesetzt, verwendet das Dienstprogramm `scheduler_console_client` die JRE, die entweder im unter dem Verzeichnis `tools/bin` der Unica Platform Installation befindeten Skript `setenv` oder in der Befehlszeile gesetzt wurde.
- Importieren Sie das SSL Zertifikat, das von dem Webanwendungsserver verwendet wird, auf dem Unica Platform für die von `scheduler_console_client` verwendete JRE bereitgestellt wird.

  Sun JDK beinhaltet ein Programm `keytool`, das zu dem Import des Zertifikats verwendet werden kann. Für Einzelheiten zur Verwendung dieses Programms, siehe Java™ Dokumentation oder greifen Sie auf Hilfe zu, indem Sie `-help` eingeben, wenn Sie das Programm ausführen.

  Note: Bei Upgrades wird die mit Unica gelieferte JRE überschrieben. Stellen Sie daher sicher, dass Sie die Zertifikate erneut in JRE importieren, wenn Sie dieselbe JRE verwenden.

- Öffnen Sie die Datei `tools/bin/schedulerconsoleclient` in einem Texteditor und fügen Sie die folgenden Eigenschaften hinzu. Diese variieren je nach Webanwendungsserver, auf dem Unica Platform bereitgestellt wird.
    - Für WebSphere®, fügen Sie diese Eigenschaften zur Datei hinzu.

      -Djavax.net.ssl.keyStoreType=JKS

      -Djavax.net.ssl.keyStore="Pfad zu der Schlüsselspeicher JKS Datei"

      -Djavax.net.ssl.keyStorePassword="Passwort Ihres Schlüsselspeichers"

      -Djavax.net.ssl.trustStore="Pfad zur Truststore JKS Datei"

      -Djavax.net.ssl.trustStorePassword="Ihr Truststore Passwort"

      -DisUseIBMSSLSocketFactory=false
    - Fügen Sie für WebLogic dies Eigenschaften zu der Datei hinzu.

-Djavax.net.ssl.keyStoreType="JKS"

-Djavax.net.ssl.trustStore="Pfad zur Truststore JKS Datei"

-Djavax.net.ssl.trustStorePassword="Ihr Truststore Passwort"

Wenn die Zertifikate nicht übereinstimmen, enthält die Unica Platform-Protokolldatei einen Fehler, der dem folgenden ähnelt.

```
Verursacht durch: sun.security.provider.certpath.SunCertPathBuilderException:
Es konnte kein gültiger Zertifizierungspfad zum angeforderten Ziel gefunden
werden
```

Voraussetzungen

Unica Platform muss installiert und bereitgestellt sein und ausgeführt werden.

Syntax

```
scheduler_console_client -v -t trigger_name user_name
```

```
scheduler_console_client -s -t trigger_name user_name
```

Befehle

`-v`

Listet die Scheduler-Jobs auf, die für die Überwachung auf den angegebenen Trigger konfiguriert wurden.

Kann nur in Verbindung mit der Option `-t` eingesetzt werden.

`-s`

Sendet einen bestimmten Trigger.

Kann nur in Verbindung mit der Option `-t` eingesetzt werden.

Optionen

`-t trigger_name`

Der Name des Triggers, wie im Scheduler konfiguriert.

Beispiel

- Listen Sie Jobs auf, die zur Überwachung eines Triggers `trigger1` konfiguriert sind.

  ```
  scheduler_console_client -v -t trigger1 myLogin
  ```
- Führen Sie Jobs aus, die zur Überwachung eines Triggers `trigger1` konfiguriert sind.

  ```
  scheduler_console_client -s -t trigger1 myLogin
  ```

quartzjobtool

Scheduler-Jobs, die in Version 11.1 oder älteren Versionen erstellt wurden, müssen aktualisiert werden, damit sie in Version 12.0 ausgeführt werden können. Verwenden Sie das Dienstprogramm quartzjobtool, um die Scheduler-Jobs zu aktualisieren, wenn das Installationsprogramm dies nicht automatisch während der Installation oder des Upgrades getan hat. Dieses Tool liest Umgebungsvariablen aus dem Script `setenv_quartz`. Normalerweise wird diese Variable automatisch durch das Unica Platform-Installationsprogramm festgelegt. Es empfiehlt sich jedoch, zu überprüfen, ob die Variable `JAVA_HOME` festgelegt ist, wenn Probleme bei der Ausführung eines Dienstprogramms auftreten. Das JDK muss der Sun-Version entsprechen (nicht etwa das JRockit JDK, das mit WebLogic bereitgestellt wird).

Syntax

quartzjobtool

Verwenden Sie das quartzjobtool, um Planer-Jobs zu aktualisieren. Dieser Schritt ist erforderlich. Wenn dieses Upgrade-Tool nicht ausgeführt wird, kann kein vorhandener geplanter Job gestartet werden. Das quartzjobtool befindet sich im Verzeichnis „tools\bin“ unter der Installation von Unica Platform. Führen Sie dieses Dienstprogramm im Verzeichnis `tools\bin` aus.

Beispielbefehl (Windows): quartzjobtool.bat

Beispielbefehl (Unix): ./quartzjobtool.sh

Beispiel

Dienstprogramm quartzjobtool zum Aktualisieren von Scheduler-Jobs

Unica Platform-SQL-Scripts

In diesem Abschnitt werden die SQL-Scripts beschrieben, die in Unica Platform für verschiedene Aufgaben in Verbindung mit Unica Platform-Systemtabellen bereitgestellt werden.

Die Unica Platform-SQL-Scripts befinden sich im Verzeichnis `db` der Unica Platform-Installation.

Die Scripts sind dazu gedacht, für Unica Platform-Systemtabellen unter Verwendung des Datenbankclients ausgeführt zu werden.

ManagerSchema_DeleteAll.sql

Das Script `Manager_Schema_DeleteAll.sql` entfernt alle Daten aus den Unica Platform-Systemtabellen, ohne die Tabellen selbst zu entfernen. Das Script entfernt alle Benutzer, Gruppen, Sicherheitsberechtigungsnachweise, Datenfilter und Konfigurationseinstellungen aus Unica Platform.

Verwendung von „ManagerSchema_DeleteAll.sql“

Sie können `ManagerSchema_DeleteAll.sql` verwenden, wenn Sie aufgrund beschädigter Daten nicht auf bestimmte Instanzen von Unica Platform zugreifen können.

Zusätzliche Voraussetzungen

Um Unica Platform nach dem Einsatz von `ManagerSchema_DeleteAll.sql` betriebsbereit zu machen, führen Sie die folgenden Schritte aus.

- Führen Sie das Dienstprogramm `populateDB` aus. Das Dienstprogramm `populateDB` stellt die Standardkonfigurationseigenschaften, -benutzer, -rollen und -gruppen wieder her, jedoch keine Benutzer, Rollen und Gruppen, die Sie nach der erstmaligen Installation erstellt oder importiert haben.
- Verwenden Sie das Dienstprogramm configTool mit der Datei `config_navigation.xml`, um Menüelemente zu importieren.

- Haben Sie nach der Installation Konfigurationsaufgaben ausgeführt, beispielsweise das Erstellen von Datenfiltern oder die Integration mit einem LDAP-Server oder einer Plattform zur Webzugriffskontrolle, müssen Sie diese Aufgaben erneut durchführen.
- Falls Sie vormals existierende Datenfilter wiederherstellen möchten, führen Sie das Dienstprogramm `datafilteringScriptTool` mithilfe der XML aus, die ursprünglich zur Erstellung und Bestimmung der Datenfilter verwendet wurde.

ManagerSchema_PurgeDataFiltering.sql

Das Script `ManagerSchema_PurgeDataFiltering.sql` entfernt alle Datenfilterungsdaten aus den Unica Platform-Systemtabellen, ohne die Datenfiltertabellen selbst zu entfernen. Das Script entfernt alle Datenfilter, Datenfilterkonfigurationen, Zielgruppen und Datenfilterzuweisungen aus Unica Platform.

Verwendung von „ManagerSchema_PurgeDataFiltering.sql“

Sie können `ManagerSchema_PurgeDataFiltering.sql` verwenden, um alle Datenfilter zu entfernen, ohne andere Daten aus den Unica Platform-Systemtabellen zu entfernen.

Wichtig: Das Script `ManagerSchema_PurgeDataFiltering.sql` setzt die Werte der zwei Datenfiltereigenschaften `Standardtabellenname` und `Standardzielgruppenname` nicht zurück. Falls diese Werte für die Datenfilter, die Sie verwenden möchten, nicht mehr gültig sind, müssen Sie die Werte auf der Seite „Konfiguration“ manuell (neu) festlegen.

ManagerSchema_DropAll.sql

Das `Script ManagerSchema_DropAll.sql` entfernt alle Unica Platform-Systemtabellen aus einer Datenbank. Das Script entfernt alle Tabellen, Benutzer, Gruppen, Sicherheitsberechtigungsnachweise und Konfigurationseinstellungen aus Unica Platform.

Anmerkung: Falls Sie dieses Script auf eine Datenbank anwenden, die eine frühere Version der Unica Platform-Systemtabellen enthält, erhalten Sie eventuell

Fehlernachrichten in Ihrem Datenbankclient, die aussagen, dass keine Bedingungen existieren. Diese Nachrichten können ignoriert werden.

Verwenden von „ManagerSchema_DropAll.sql“

Sie können `ManagerSchema_DropAll.sql` einsetzen, wenn Sie eine Instanz von Unica Platform deinstalliert haben, in der die Systemtabellen sich in einer Datenbank befinden, die andere Tabellen beinhalten, die Sie eventuell weiterhin nutzen möchten.

Zusätzliche Voraussetzungen

Führen Sie die folgenden Schritte aus, um Unica Platform nach dem Einsatz dieses Scripts betriebsbereit zu machen.

- Führen Sie das entsprechende SQL-Script aus, um die Systemtabellen neu zu erstellen.
- Führen Sie das Dienstprogramm `populateDB` aus. Durch Ausführen des Dienstprogramms `populateDB` werden die Standardkonfigurationseigenschaften, Benutzer, Rollen und Gruppen, jedoch nicht solche, die Sie nach der erstmaligen Installation erstellt oder importiert haben, wiederhergestellt.
- Verwenden Sie das Dienstprogramm `configTool` mit der Datei `config_navigation.xml`, um Menüelemente zu importieren.
- Haben Sie nach der Installation Konfigurationsaufgaben ausgeführt, beispielsweise das Erstellen von Datenfiltern oder die Integration mit einem LDAP-Server oder einer Plattform zur Webzugriffskontrolle, müssen Sie diese Aufgaben erneut durchführen.

SQL-Scripts für die Erstellung von Systemtabellen

Verwenden Sie die in der nachfolgenden Tabelle angegebenen Scripts, um Unica Platform-Systemtabellen manuell zu erstellen, falls Ihre Unternehmensrichtlinien die automatische Erstellung mithilfe des Installationsprogramms nicht erlauben.

Die Scripts sind in der Reihenfolge aufgeführt, in der sie ausgeführt werden müssen.

Tabelle 74. Scripts für die Erstellung von Systemtabellen

Datenquellentyp	Scriptnamen
IBM® DB2®	• `ManagerSchema_DB2.sql` Wenn Sie planen, Multi-Byte-Zeichen zu unterstützen (z. B. Chinesisch, Japanisch oder Koreanisch), verwenden Sie das Script `ManagerSchema_DB2_unicode.sql`. • `ManagerSchema__DB2_CeateFKConstraints.sql` • `active_portlets.sql` • `notification_rules.sql`
Microsoft™ SQL-Server	• `ManagerSchema_SqlServer.sql` • `ManagerSchema__SqlServer_CeateFKConstraints.sql` • `active_portlets.sql` • `notification_rules.sql`
MariaDB	• `ManagerSchema_MariaDB.sql` • `ManagerSchema_MariaDB_StoredProcedures.sql` • `ManagerSchema_MariaDB_CreateFKConstraints.sql` • `active_portlets.sql` • `notification_rules.sql`
Oracle	• `ManagerSchema_Oracle.sql` • `ManagerSchema__Oracle_CeateFKConstraints.sql` • `active_portlets.sql` • `notification_rules_Oracle.sql`

Falls Sie den Einsatz der Scheduler-Funktion planen, mit der Sie ein Ablaufdiagramm konfigurieren können, das in vordefinierten Intervallen ausgeführt wird, müssen Sie zudem die Tabellen erstellen, die diese Funktion unterstützen. Wollen Sie die Scheduler-Tabellen erstellen, führen Sie das entsprechende Script aus (siehe Beschreibung in der folgenden Tabelle).

Tabelle 75. Scripts zur Aktivierung des Unica-Schedulers

Datenquellentyp	Scriptname
DB2®	`quartz_db2.sql`
Microsoft™ SQL-Server	`quartz_sqlServer.sql`
Oracle	`quartz_oracle.sql`
MariaDB	`quartz_MariaDB.sql`

Wann die Scripts zum Erstellen von Systemtabellen verwendet werden sollten

Sie müssen diese Scripts ausführen, wenn Sie Unica Platform installieren oder ein Upgrade durchführen und Sie nicht zugelassen haben, dass das Installationsprogramm die Systemtabellen automatisch erstellt, oder wenn Sie `ManagerSchema_DropAll.sql` verwendet haben, um alle Unica Platform-Systemtabellen aus Ihrer Datenbank zu löschen.

Unica-Konfigurationseigenschaften

Dieser Abschnitt beschreibt die Konfigurationseigenschaften, auf der Seite **Einstellungen > Konfiguration**.

Unica Platform-Konfigurationseigenschaften

Dieser Abschnitt beschreibt die Unica Platform-Konfigurationseigenschaften, die auf der Seite "Konfiguration" zur Verfügung stehen.

Unica Platform

Eigenschaften in dieser Kategorie ermöglichen das Festlegen der Standardländereinstellung und das Setzen von Flags, mit denen angegeben wird, ob die Unica Platform-Installation eine Cluster-Installation ist, ob Unica Plan mit Unica Campaign integriert ist und ob die Angebotsintegration für die Integration aktiviert wird.

Region

Beschreibung

Gibt die Ländereinstellung für Unica-Benutzer an. Wenn Sie diese Eigenschaft auf der Seite "Konfiguration" einstellen, wird die von Ihnen vorgenommene Einstellung innerhalb von Unica zur Standardeinstellung für alle Benutzer. Eine Ausnahme bilden lediglich die Benutzer, deren Ländereinstellung einzeln über die Unica Platform-Benutzerseite eingestellt wurde. Wenn Sie diese Einstellung für einen einzelnen Benutzer festlegen, wird die Standardeinstellung dadurch überschrieben.

Diese Voreinstellung wirkt sich auf die Anzeige der Sprache, Uhrzeit, Zahlen und Datumsangaben in Unica-Anwendungen aus.

Die Verfügbarkeit der Ländereinstellungen kann je nach Unica-Anwendung variieren, und nicht alle Anwendungen unterstützen diese Benutzervorgabe für die Ländereinstellung in Unica Platform. Informationen zum Bestimmen der Verfügbarkeit und Unterstützung der Eigenschaft `Bereichseinstellung` finden Sie in der jeweiligen Produktdokumentation.

Standardwert

`Englisch (Vereinigte Staaten)`

Hilfeserver

Beschreibung

Die URL des Servers, auf dem die von gehostete Onlinehilfe installiert ist. Wenn Unica-Benutzer über einen Interzugang verfügen, sollten Sie den Standardwert, der zu dem von gewarteten und aktualisierten Onlinehilfe-Server führt, nicht ändern.

Standardwert

Die URL des gehosteten Hilfe-Servers.

Gültige Werte

Jeder Server, auf dem von gehostete Hilfe installiert ist.

Unica Plan - Unica Campaign-Integration

Beschreibung

Ein Flag zeigt an, ob Unica Plan und Unica Campaign zusammen installiert und integriert sind. Weitere Informationen zum Konfigurieren dieser Integration finden Sie im Unica PlanUnica Campaign-Integrationshandbuch.

Standardwert

Falsch

Gültige Werte

True | False

Unica Plan - Angebotsintegration

Beschreibung

Bei Systemen, die Unica Plan mit Unica Campaign integrieren, gibt dieses Flag an, ob die Angebotsintegration ebenfalls aktiviert ist. Die Angebotsintegration ermöglicht die Verwendung von Unica Plan zur Durchführung von Lifecycle-Management-Aufgaben für Angebote. Weitere Informationen zum Konfigurieren dieser Integration finden Sie im Unica PlanUnica Campaign-Integrationshandbuch.

Standardwert

Falsch

Gültige Werte

True | False

Startseite

Beschreibung

Die URL der Seite, die Benutzern bei der Anmeldung an Unica angezeigt wird. Der Standardwert ist das Standarddashboard.

Standardwert

Die Standardübersicht.

Gültige Werte

Jede Unica-URL, außer Seiten zur Formulareinreichung, Seitenbearbeitung und Darstellung von Suchergebnissen.

Domänenname

Beschreibung

Der Name der Domäne, in der Unica installiert ist. Der Wert wird während der Installation festgelegt. Dies sollte nicht verändert werden, außer wenn sich der Domänenname ändert.

Wenn Benutzer mit dem Chrome-Browser auf Unica-Produkte zugreifen, verwenden Sie den vollständig qualifizierten Domänennamen (Fully Qualified Domain Name, FQDN). Der Chrome-Browser kann nicht auf die Produkt-URLs zugreifen, wenn der FQDN nicht verwendet wird.

Standardwert

Nicht definiert

Seitentagging inaktivieren

Beschreibung

Bei dem Standardwert `False` verwendet den Site-ID-Code, der während der Unica Platform-Installation eingegeben wurde, um Basisstatistiken zu sammeln, die allgemeine Produktnutzungstrends erfassen, um Produkte zu entwickeln und zu verbessern. sendet die Informationen über HTTP an `http://pt200201.unica.com`.

Wenn solche Informationen nicht gesammelt werden sollen, legen Sie diese Eigenschaft auf `True` fest.

Standardwert

`Falsch`

Gültige Werte

`True | False`

Ist diese Bereitstellung in Gruppen zusammengefasst

Beschreibung

Wenn Sie Unica Platform in einer Clusterbereitstellung installieren, dann legen Sie für diese Eigenschaft den Wert `True` fest. Behalten Sie andernfalls den Standardwert `False` bei.

Wenn Sie diese Eigenschaft während der Unica Platform-Ausführung ändern, müssen Sie Unica Platform neu starten, damit die Änderungen wirksam werden.

Standardwert

`Falsch`

Gültige Werte

`True | False`

Sicherheit bei allen Anwendungen auf statische Inhalte anwenden

Beschreibung

Wird dieser Wert auf `Yes` gesetzt und versucht ein authentifizierter Benutzer, direkt auf statische Inhalte wie z.B. ein Bild zuzugreifen, dann wird eine Überprüfung durchgeführt, um die Authentifizierung des Benutzers zu verifizieren. Wurde der Benutzer authentifiziert, dann werden die Inhalte wiedergegeben. Wurde der Benutzer nicht authentifiziert, dann wird er an die Anmeldeseite weitergeleitet. Diese Einstellung gilt für alle Unica-Produkte.

Standardwert

`Nein`

Gültige Werte

`Yes | No`

Unica | Allgemein | Navigation

Eigenschaften in dieser Kategorie geben Werte an, die intern zum Navigieren zwischen Unica-Produkten verwendet werden.

TCP-Port für sichere Verbindungen

Beschreibung

Gibt den SSL-Port auf dem Webanwendungsserver an, auf dem Unica Platform bereitgestellt wurde. Diese Eigenschaft wird intern für die Kommunikation zwischen den Unica-Produkten verwendet.

Standardwert

`7001`

TCP-Port für Standardverbindungen

Beschreibung

Gibt den HTTP-Port auf dem Webanwendungsserver an, auf dem Unica Platform bereitgestellt wurde. Diese Eigenschaft wird intern für die Kommunikation zwischen Unica-Produkten verwendet.

Standardwert

`7001`

Unica Platform-URL

Beschreibung

Gibt die für Unica Platform verwendete URL an. Diese Einstellung wird bei der Installation vorgenommen und sollte normalerweise nicht geändert werden. Hinweis: Die URL umfasst den Domänennamen (siehe folgendes Beispiel).

```
protocol://machine_name_or_IP_address.domain_name:port_number/
context-root
```

Der Name der Maschine sollte nicht `localhost` sein.

Verwenden Sie den vollständig qualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) in der URL, wenn Benutzer mit dem Chrome-Browser auf Unica-Produkte zugreifen. Der Chrome-Browser kann nicht auf die Produkt-URLs zugreifen, wenn der FQDN nicht verwendet wird.

Wichtig: Wenn Unica-Produkte in einer dezentralen Umgebung installiert werden, müssen Sie für alle Anwendungen der Suite den Namen der Maschine anstatt der IP-Adresse in der Navigations-URL verwenden. Zudem sollten Sie, wenn Sie sich in einer Clusterumgebung befinden und vom Standardport `80` oder `443` abweichende Ports für Ihre Bereitstellung verwenden möchten, keine Portnummer im Wert dieser Eigenschaft verwenden.

Standardwert

Nicht definiert

Beispiel

In einer für SSL konfigurierten Umgebung lautet die URL folgendermaßen:

`https://machineName.companyDomain.com:8080/unica`

Unica | Allgemein | Datenfilterung

Eigenschaften in dieser Kategorie geben Werte an, die benutzt werden, wenn Datenfilter implementiert werden.

Standardtabellenname

Beschreibung

Diese Konfigurationseigenschaft ist zum Aktivieren von Datenfiltern erforderlich.

Legen Sie den Wert dieser Eigenschaft so fest, dass er genau mit dem Namen des Elements `addTables | AddDataTable | dataTable | name` in der XML-Datei übereinstimmt, die zum Erstellen der Datenfilter verwendet wird.

Standardwert

Nicht definiert

Gültige Werte

Maximal 50 Zeichen des Typs "varchar".

Standardzielgruppenname

Beschreibung

Diese Konfigurationseigenschaft ist zum Aktivieren von Datenfiltern erforderlich.

Legen Sie den Wert dieser Eigenschaft so fest, dass er genau mit dem Namen des Elements `AddAudience | Zielgruppe | Name` in der XML-Datei übereinstimmt, die zum Erstellen der Datenfilter verwendet wird.

Standardwert

Nicht definiert

Gültige Werte

Maximal 50 Zeichen des Typs "varchar".

Datenfiltercache aktivieren

Beschreibung

Diese Eigenschaft ist optional und kann eingestellt werden, um die Datenfilterleistung zu verbessern.

Diese Eigenschaft gibt an, ob Unica Platform Datenfilterdefinitionen aus der Datenbank oder aus einem Cache abruft. Wenn Sie diesen Wert auf **true** setzen, werden die Datenfilterdefinitionen im Cache gespeichert, und der Cache wird bei jeder Änderung der Datenfilterdefinitionen aktualisiert.

Sie müssen einen Neustart der Unica Platform-Webanwendung durchführen, nachdem Sie Änderungen an diesem Eigenschaftswert vorgenommen haben, damit die Änderungen wirksam werden.

Standardwert

Falsch

Unica | Allgemein | Passworteinstellungen

Die Eigenschaften unter der Kategorie **Allgemein** | **Passworteinstellungen** geben die Richtlinien an, die für die Unica Passwörter gelten. Die meisten dieser Kennwortoptionen gelten nur für Kennwörter interner Benutzer (in Unica Platform erstellt) und nicht für externe Benutzer, die aus einem externen System importiert wurden.

Eine Ausnahme ist die Eigenschaft `Maximal zulässige fehlgeschlagene Anmeldeversuche`, die sowohl interne als auch externe Benutzer betrifft. Beachten Sie auch, dass diese Eigenschaft keine ähnliche Einschränkung außer Kraft setzt, die in einem externen System festgelegt wurde.

Maximal zulässige fehlgeschlagene Anmeldeversuche

Beschreibung

Gibt an, wie oft bei jeder Anmeldung ein ungültiges Kennwort eingegeben werden kann. Wenn die maximal zulässige Anzahl erreicht ist, wird der Benutzer im Unica-System inaktiviert, und eine Anmeldung mit diesem Benutzernamen ist nicht möglich.

Wenn der Wert auf null oder weniger festgelegt wird, ist eine unendliche Anzahl von aufeinanderfolgenden Fehlversuchen im System zulässig.

Standardwert

3

Gültige Werte

Beliebige Ganzzahl

Kennwortprotokollzähler

Beschreibung

Gibt die Anzahl alter Kennwörter an, die das System für einen Benutzer speichert. Ein Benutzer darf keine Kennwörter wiederverwenden, die in

dieser Liste mit alten Kennwörtern enthalten sind. Wenn der Wert auf null oder weniger festgelegt ist, werden keine alten Kennwörter gespeichert, und der Benutzer kann dasselbe Kennwort wiederholt verwenden. Hinweis: Das Kennwort, das einem Benutzerkonto bei der Erstellung zunächst zugewiesen wurde, ist im Kennwortprotokollzähler nicht enthalten.

Standardwert

`0`

Gültige Werte

Beliebige Ganzzahl

Gültigkeit (in Tagen)

Beschreibung

Gibt die Anzahl der Tage bis zum Ablauf eines Benutzerkennworts an.

Beträgt der Wert 0 oder weniger, läuft das Kennwort nie ab.

Wenn der Wert größer als 0 (Null) ist, muss ein Benutzer das Kennwort bei der ersten Anmeldung ändern, und das Ablaufintervall beginnt mit dem Datum der ersten Anmeldung.

Wenn dieser Wert geändert wird, nachdem Benutzer und Kennwörter erstellt wurden, tritt das neue Ablaufdatum für bestehende Benutzer in Kraft, wenn sie ihr Kennwort das nächste Mal ändern.

Standardwert

`30`

Gültige Werte

Beliebige Ganzzahl

Leere Kennwörter sind zulässig

Beschreibung

Gibt an, ob leere Passwörter zulässig sind. Wenn diese Eigenschaft auf true gesetzt ist, sollten Sie auch `Minimale Zeichenlänge=0` festlegen.

Standardwert

`true`

Gültige Werte

`true | false`

Identische Benutzernamen und Kennwörter sind zulässig

Beschreibung

Gibt an, ob das Kennwort eines Benutzers und der Anmeldename des Benutzers identisch sein dürfen.

Standardwert

`false`

Gültige Werte

`true | false`

Minimale Anzahl Ziffern

Beschreibung

Gibt an, wie viele Ziffern ein Kennwort mindestens enthalten muss. Wenn der Wert gleich null oder kleiner ist, ist keine Mindestanforderung festgelegt.

Standardwert

`0`

Gültige Werte

Beliebige Ganzzahl

Minimale Anzahl Buchstaben

Beschreibung

Gibt an, wie viele Buchstaben ein Kennwort mindestens enthalten muss. Wenn der Wert gleich null oder kleiner ist, ist keine Mindestanforderung festgelegt.

Standardwert

`0`

Gültige Werte

Beliebige Ganzzahl

Minimale Zeichenlänge

Beschreibung

Gibt an, wie viele Zeichen ein Kennwort mindestens enthalten muss. Wenn der Wert gleich null oder kleiner ist, ist keine Mindestanforderung festgelegt. Wenn der Wert auf größer als `0` gesetzt ist, sollten Sie auch `Leere Passwörter erlaubt=false` festlegen.

Standardwert

`4`

Gültige Werte

Beliebige Ganzzahl

Mindestanzahl an Sonderzeichen

Beschreibung

Gibt die Mindestanzahl an Sonderzeichen an, die in einem Passwort erforderlich sind. Dies gilt für Werte größer Null. Bei der Erstellung Passworts können Sie nur die folgenden Sonderzeichen verwenden.

- Stern (*)
- Ausrufezeichen "!"
- At-Zeichen "@"
- Dollar "$"
- Et-Zeichen "&"
- Rautenzeichen "#"

Standardwert

0

Gültige Werte

Beliebige Ganzzahl

Mindestanzahl von Kleinbuchstaben

Beschreibung

Gibt die Mindestanzahl an Kleinbuchstaben an, die in einem Passwort erforderlich sind. Es gilt für Werte größer als 0, indem Sie den entsprechenden Wert für `Mindestanzahl von Buchstabenzeichen` festlegen müssen.

Standardwert

0

Gültige Werte

Beliebige Ganzzahl

Mindestanzahl von Großbuchstaben

Beschreibung

Gibt die Mindestanzahl an Großbuchstaben an, die in einem Passwort erforderlich sind. Es gilt für Werte größer als 0, indem Sie den entsprechenden Wert für `Mindestanzahl von Buchstabenzeichen` festlegen müssen.

Standardwert

0

Gültige Werte

Beliebige Ganzzahl

Maximale Zeichenlänge

Beschreibung

Gibt die maximale Länge eines Passworts an. Es gilt für Werte größer als 0.

Standardwert

0

Gültige Werte

Beliebige Ganzzahl

Unica | Allgemein | Verschiedenes

Eigenschaften in dieser Kategorie geben Werte, die intern verwendet werden, sowie einen Wert an, der u. U. für die Ländereinstellung festgelegt werden muss.

Tokenlaufzeit

Beschreibung

Gibt die Dauer in Sekunden an, über die ein in Unica Platform generiertes Token gültig ist. Dies ist ein Bestandteil der Anmeldungsimplementierung der Suite und Sie sollten diesen Wert nicht ändern.

Standardwert

`15`

Gültige Werte

Beliebige positive Ganzzahl

Vorgabesprache

Beschreibung

Gibt die Standardsprache für Unica Platform an. Wenn Sie Unica Campaign installieren möchten, sollten Sie den Wert so festlegen, dass er den Ländereinstellungen entspricht, die für Unica Campaign in der Eigenschaft `defaultLocale` für Unica Campaign festgelegt wurden.

Standardwert

`Englisch`

Gültige Werte

Unterstützte Ländereinstellungen

Unica | Allgemein | Kommunikation | E-Mail

Eigenschaften dieser Kategorie werden verwendet, um Unica Platform so zu konfigurieren, dass bei Systemalerts und Benachrichtigungen E-Mails an Benutzer gesendet werden.

E-Mail-Kommunikation aktivieren

Beschreibung

Bei dem Wert `True` versucht Unica Platform, E-Mails mit Systemalerts und Benachrichtigungen an Benutzer zu senden. Die anderen Eigenschaften in dieser Kategorie müssen entsprechend eingestellt werden, um diese Funktion zu aktivieren.

Standardwert

`Falsch`

E-Mail-Serverprotokoll

Beschreibung

Gibt das Protokoll auf dem E-Mail-Server an, das zum Senden von Systemalerts und Benachrichtigungen an Benutzer verwendet wird. Wird für E-Mail-Benachrichtigungen benötigt.

Standardwert

`smtp`

E-Mail-Server-Host

Beschreibung

Gibt den Namen des E-Mail-Servers an, der zum Senden von Systemalerts und Benachrichtigungen an Benutzer verwendet wird. Wird für E-Mail-Benachrichtigungen benötigt.

Standardwert

`localhost`

E-Mail-Server-Port

Beschreibung

Gibt den Port des E-Mail-Servers an, der zum Senden von Systemalerts und Benachrichtigungen an Benutzer verwendet wird. Wird für E-Mail-Benachrichtigungen benötigt.

Standardwert

`25,0`

Absenderadresse für E-Mails

Beschreibung

Gibt das Konto an, von dem E-Mails mit Systemalerts und Benachrichtigungen gesendet werden. Wenn auf Ihrem E-Mail-Server eine Authentifizierung erforderlich ist, verwenden Sie die E-Mail-Adresse des Kontos, das Sie beim Speichern eines Mail-Server-Kontonamens und -Kennworts als Datenquelle in einem Unica Platform-Benutzerkonto verwendet haben. Wird für E-Mail-Benachrichtigungen benötigt.

Standardwert

Nicht definiert

Authentifizierung für E-Mail-Server erforderlich?

Beschreibung

Gibt an, ob der E-Mail-Server eine Authentifizierung erfordert.

Standardwert

`Falsch`

Unica-Benutzer für E-Mail-Konten

Beschreibung

Gibt den Benutzernamen des Unica Platform-Kontos an, in dem die E-Mail-Identifikationsdaten als Datenquelle gespeichert sind.

Wird nur für Benachrichtigungen benötigt, wenn der E-Mail-Server Authentifizierung erfordert.

Standardwert

`asm_admin`

Datenquelle für E-Mail-Konto

Beschreibung

Gibt den Namen der Datenquelle in dem Unica Platform-Konto an, in dem die E-Mail-Identifikationsdaten gespeichert sind.

Wird nur für Benachrichtigungen benötigt, wenn der E-Mail-Server Authentifizierung erfordert.

Standardwert

`emailDS`

Unica Platform | Scheduler

Eigenschaften in dieser Kategorie ermöglichen das Aktivieren und Optimieren der Leistung des Unica-Zeitplaners (Scheduler).

Clientabfrageintervall (ms)

Konfigurationskategorie

`Platform|Scheduler`

Beschreibung

Unica Campaign fragt in regelmäßigen Intervallen Jobs vom Unica-Scheduler ab. Das Intervall wird durch diesen Wert in Millisekunden angegeben. Der Standardwert ist 60 Sekunden. Sie sollten diese Eigenschaft nicht auf einen kleineren Wert als 10000 (10 Sekunden) festlegen, weil dies möglicherweise den Kampagnenerfolg verringert.

Standardwert

`60000`

Clientinitialisierungsverzögerung (ms)

Beschreibung

Gibt an, wie lange (in Millisekunden) der Unica Campaign-Scheduler-Thread wartet, bevor er den Unica-Scheduler nach Jobs abfragt, wenn Unica Campaign zum ersten Mal gestartet wird. Stellen Sie einen Wert ein, der mindestens so lange dauert, wie der vollständige Start von Unica Campaign auf Ihrem System. Der Standardwert liegt bei fünf Minuten.

Standardwert

`300000`

Gültige Werte

Beliebige Ganzzahl

Maximale Anzahl Abfragen des unbekannten Status

Beschreibung

Gibt an, wie oft der Zeitplaner den Status einer geplanten Ausführung überprüft, deren Status nicht ermittelt werden kann. Wenn dieser Grenzwert erreicht wird, dann listet das System den Ausführungsstatus auf der Seite **Einstellungen > Zeitplanmanagement** als "Unbekannt" auf.

Standardwert

5

Gültige Werte

Beliebige Ganzzahl

Zeitplaner aktivieren

Beschreibung

Gibt an, ob der Zeitplaner aktiviert wurde. Setzen Sie diese Eigenschaft auf "False", wenn sie verhindern wollen, dass Benutzer den Zeitplaner verwenden können. Die Einstellung "False" inaktiviert den Zeitplaner für alle Produkte, die ihn verwenden.

Sie müssen die Unica Platform-Webanwendung erneut starten, wenn Sie den Zeitplaner aktivieren oder inaktivieren.

Standardwert

`Wahr`

Gültige Werte

`True | False`

Unica Platform | Scheduler | Wiederholungsdefinitionen

Eigenschaften in dieser Kategorie legen die Wiederholungsstruktur für den Unica-Zeitplaner (Scheduler) fest. Diese erscheinen im Dialogfenster, das Sie zum Festlegen einer Wiederholungsstruktur verwenden, wenn Sie einen Zeitplan erstellen. Sie können die Wiederholungsvorlage verwenden, um Ihre eigene Wiederholungsstruktur mithilfe eines gültigen Cron-Ausdrucks zu erstellen.

Jede Stunde

Beschreibung

Der Jobablauf wird stündlich ausgelöst.

Standardwert

`0 0 0/1 * * ?`

Jeden Tag

Beschreibung

Der Job wird alle 24 Stunden ausgelöst.

Standardwert

`0 0 0 * * ?`

Jeden [Wochentag] um 00:00 Uhr

Beschreibung

Der Job wird an dem angegebenen Wochentag um 00:00 Uhr ausgelöst.

Standardwert

- Montag - `0 0 0 ? * MON`
- Dienstag - `0 0 0 ? * TUE`
- Mittwoch - `0 0 0 ? * WED`
- Donnerstag - `0 0 0 ? * THU`
- Freitag - `0 0 0 ? * FRI`
- Samstag - `0 0 0 ? * SAT`
- Sonntag - `0 0 0 ? * SUN`

Am [ersten|letzten] Tag jedes Monats um 00:00 Uhr

Beschreibung

Der Job wird an dem angegebenen Tag des Monats (ersten oder letzten) um 00:00 Uhr ausgelöst.

Standardwert

- Erster Tag jedes Monats - `0 0 0 1 * ?`
- Letzter Tag jedes Monats - `0 0 0 L * ?`

Am [ersten|letzten] Tag jedes Quartals um 00:00 Uhr

Beschreibung

Der Job wird an dem angegebenen Tag des Quartals (am ersten oder letzten Tag) um 00:00 Uhr ausgelöst.

Standardwert

- Erster Tag jedes Quartals- `0 0 0 1 * JAN,APR,JUL,OCT`
- Letzter Tag jedes Quartals - `0 0 0 L * MAR,JUN,SEP,DEC`

Am [ersten|letzten] Tag jedes Jahres um 00:00 Uhr

Beschreibung

Der Job wird an dem angegebenen Tag des Jahres (ersten oder letzten) um 00:00 Uhr ausgelöst.

Standardwert

- Erster Tag jedes Jahres - `0 0 0 1 ? JAN *`
- Letzter Tag jedes Jahres - `0 0 0 L ? DEC *`

Jeden [Monat]um 00:00 Uhr

Beschreibung

Der Job wird an dem ersten Tag des angegebenen Monats um 00:00 Uhr ausgelöst.

Standardwert

- Jeden Januar - `0 0 0 1 ? JAN *`
- Jeden Februar - `0 0 0 1 ? FEB *`
- Jeden März - `0 0 0 1 ? MAR *`
- Jeden April - `0 0 0 1 ? APR *`
- Jeden Mai - `0 0 0 1 ? MAY *`
- Jeden Juni - `0 0 0 1 ? JUN *`
- Jeden Juli - `0 0 0 1 ? JUL *`
- Jeden August - `0 0 0 1 ? AUG *`
- Jeden September - `0 0 0 1 ? SEP *`
- Jeden Oktober - `0 0 0 1 ? OCT *`
- Jeden November - `0 0 0 1 ? NOV *`
- Jeden Dezember - `0 0 0 1 ? DEC *`

Unica Platform | Scheduler | Zeitplanregistrierungen | [Produkt] | [Objekttyp]

Es gibt unterschiedliche Kategorien für jeden der Objekttypen, die mit dem Unica-Zeitplaner (Scheduler) geplant werden können. Die Eigenschaften in diesen Kategorien sollten normalerweise nicht geändert werden.

Klassenname des Steuerprogramms

Beschreibung

Die Klasse, die der Unica-Zeitplaner (Scheduler) verwendet, um eine Ablaufdiagramm- oder Mailing-Ausführung auszulösen.

Standardwert

Statusabfrageintervall

Konfigurationskategorie

`Platform|Scheduler|Schedule registrations|[Product]|[Object type]`

Bei Unica Campaign-Ablaufdiagrammen ist der Pfad für diese Eigenschaft `Platform|Scheduler|Schedule registrations|Campaign|Flowchart`

Beschreibung

Der Unica-Zeitplaner (Scheduler) fragt das Produkt in regelmäßigen Intervallen ab, um den Ausführungsstatus geplanter Objekte (beispielsweise Ablaufdiagramme oder Mailings) zu erhalten, die keinen Status berichtet haben. Das Intervall wird in Millisekunden angegeben. Der Standardwert liegt bei 10 Minuten. Wird ein kürzeres Abfrageintervall (ein geringerer Wert) angegeben, kann die Systemleistung beeinträchtigt werden. Wird ein längeres Abfrageintervall (ein höherer Wert) angegeben, wird die Belastung des Systems reduziert. Legen Sie für Unica Campaign ein weniger häufigeres Abfrageintervall fest, wenn viele Unica Campaign-Ablaufdiagramme vorhanden sind, die länger als 10 Minuten dauern.

Standardwert

`600000`

Name der die Jobbenachrichtigungen erhaltenden Gruppe

Beschreibung

Es werden Benachrichtigungen für alle Zeitpläne und jeden Objekttyp an alle Mitglieder der Gruppe gesendet, die Sie hier angeben.

Unica Platform | Scheduler | Zeitplanregistrierungen | [Produkt] | [Objekttyp] | [Richtgruppe]

Standard-Richtgruppen existieren für jeden Objekttyp, der mit dem Unica-Zeitplaner (Scheduler) geplant werden kann. Berücksichtigen Sie hierbei, dass diese Standardgruppen nicht auf der Seite "Benutzergruppen" erscheinen. Sie können die Vorlage für Richtgruppen verwenden, um zusätzliche Gruppen zu erstellen.

Richtwert

Beschreibung

Die höchste Anzahl der dieser Gruppe zugeordneten Zeitpläne, die gleichzeitig ausgeführt werden können. Die von Ihnen hier angegebenen Gruppen erscheinen in der Dropdown-Liste **Planergruppe** in der Benutzeroberfläche des Schedulers zum Erstellen und Bearbeiten von Zeitplänen. Die Standardrichtgruppe ist auf 999 gesetzt, was bedeutet, dass es effektiv keine Grenze gibt. Da alle Zeitpläne zu einer Richtgruppe gehören müssen, sollten Sie diesen Wert unverändert lassen, damit Zeitpläne, die Sie nicht regulieren möchten, dieser Gruppe zugeordnet werden können.

Standardwert

Gültige Werte

Eine beliebige positive Ganzzahl.

Unica Platform | Sicherheit

Die Eigenschaft in dieser Kategorie gibt den Anmeldemodus für Unica-Produkte an.

Anmeldeverfahren

Beschreibung

Gibt den Authentifizierungsmodus für alle installierten und zur Zusammenarbeit konfigurierten Unica-Produkte wie folgt an:

- Wenn Sie den Wert auf `Unica Platform` setzen, verwenden Unica-Produkte Unica Platform zur Authentifizierung und Autorisierung.
- Wenn Sie den Wert auf `LDAP` setzen, verwenden Unica-Produkte einen LDAP-Server zur Authentifizierung.
- Wenn Sie diesen Wert auf `Web access control` setzen, verwenden Unica-Produkte eine Software zur Webzugriffskontrolle zur Authentifizierung.
- Wenn Sie den Wert auf `SAML 2.0` setzen, verwenden Unica-Produkte einen IdP-Server zur Authentifizierung.

Wird diese Einstellung geändert, dann müssen Sie die Unica Platform-Webanwendung stoppen und erneut starten, damit Ihre Änderung wirksam wird.

Standardwert

`Unica Platform`

Gültige Werte

`Unica Platform | LDAP | Webzugriffskontrolle`

Unica Platform | Sicherheit | Details zum Anmeldeverfahren | LDAP

Mit den Eigenschaften in dieser Kategorie wird die LDAP-Integration konfiguriert.

Hostname des LDAP-Servers

Beschreibung

Gibt den Namen oder die IP-Adresse des LDAP-Servers an. Stellen Sie den Wert auf den Namen der Maschine oder die IP-Adresse des LDAP-Servers ein. Zum Beispiel: `machineName.companyDomain.com`

Verwenden Sie bei der Integration mit Windows™ Active Directory den Servernamen anstelle des DNS-Namens.

Standardwert

Nicht definiert

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

LDAP-Server-Port

Beschreibung

Gibt den Port an, den der LDAP-Server überwacht. Stellen Sie den Wert entsprechend ein. Die Portnummer ist üblicherweise `389` (`636`, wenn SSL verwendet wird).

Standardwert

`389`

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

Benutzersuchfilter

Beschreibung

Gibt den Filter an, der für die Benutzersuche verwendet wird. Gültige Werte sind jeder gültige LDAP-Suchfilter (siehe RFC 2254). Beachten Sie, dass Sie für alle XML-Zeichen in diesem Wert XML-Escape-Zeichen verwenden müssen.

Typischerweise ist der Wert für dieses Attribut `uid` in LDAP-Servern und `sAMAccountName` bei Windows™ Active Directory-Servern. Bitte überprüfen Sie dies jedoch auf Ihrem LDAP- oder Active Directory-Server. Wenn Ihr LDAP-

Server Windows™ Active Directory ist, sollten Sie den Standardwert dieser Eigenschaft ändern und eher `sAMAccountName` als `uid` verwenden. Zum Beispiel:

```
(&(|(objectClass=user)(objectClass=person))(sAMAccountName={0}))
```

Standardwert

```
(&(|(objectClass=user)(objectClass=person))(uid={0}))
```

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

In gespeicherte Berechtigungsnachweise verwenden Unica Platform

Beschreibung

Gibt an, ob Unica Platform in der Unica Platform-Datenbank gespeicherte Benutzerberechtigungsnachweise verwendet, wenn der LDAP- oder Windows™ Active Directory-Server während der Benutzerauthentifizierung (bei der Anmeldung) durchsucht wird.

Bei dem Wert `true` verwendet Unica Platform Berechtigungsnachweise aus der Unica Platform-Datenbank, und Sie müssen die entsprechenden Werte für die Eigenschaften `Unica PlatformBenutzer für LDAP-Berechtigungsnachweise` und `Datenquelle für LDAP-Berechtigungsnachweise` in dieser Kategorie angeben.

Sollte Ihr LDAP- oder Windows™ Active Directory-Server keinen anonymen Zugriff erlauben, setzen Sie den Wert auf `true`.

Ist dieser Wert `false`, verbindet sich Unica Platform anonym mit dem LDAP- oder Windows™ Active Directory-Server. Sollte Ihr LDAP- oder Windows™ Active Directory-Server anonymen Zugriff erlauben, setzen Sie den Wert auf `false`.

Standardwert

`falsch`

Gültige Werte

`true | false`

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

Unica Platform-Benutzer für LDAP-Berechtigungsnachweise

Beschreibung

Legt den Namen des Unica-Benutzers fest, dem die LDAP-Administratorzugangsdaten zugeteilt wurden. Legen Sie diesen Wert fest, wenn Sie die Eigenschaft `Use credentials stored inUnica Platform` in dieser Kategorie auf `true` setzen.

Legen Sie den Wert dieser Eigenschaft auf den Benutzernamen fest, den Sie für den Unica-Benutzer erstellt haben, als Sie die LDAP-Integration konfigurierten. Diese Eigenschaft funktioniert zusammen mit der Eigenschaft `Datenquelle für LDAP-Berechtigungsnachweis` in dieser Kategorie.

Standardwert

`asm_admin`

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

Datenquelle für LDAP-Berechtigungsnachweis

Beschreibung

Gibt die Unica Platform-Datenquelle für die LDAP-Administratorzugangsdaten an. Legen Sie diesen Wert fest, wenn Sie die Eigenschaft `Use credentials stored inUnica Platform` in dieser Kategorie auf `true` setzen.

Legen Sie den Wert dieser Eigenschaft auf den Datenquellennamen fest, den Sie für den Unica-Benutzer erstellt haben, als Sie die LDAP-Integration konfigurierten. Diese Eigenschaft funktioniert zusammen mit der Eigenschaft `Unica Platform Benutzer für LDAP-Berechtigungsnachweise` in dieser Kategorie.

Standardwert

Nicht definiert

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

Basis-DN

Beschreibung

Gibt den definierten Basisnamen (DN) an, der auf den Stamm der LDAP-Verzeichnisstruktur verweist.

Standardwert

`[CHANGE ME]`

Gültige Werte

Jeder gültige DN (siehe RFC 1779, RFC 2253)

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

SSL für LDAP-Verbindung verlangen

Pfad

`Unica Platform | Sicherheit | LDAP`

Beschreibung

Legt fest, ob Unica Platform SSL verwendet, wenn es sich mit dem LDAP-Server verbindet, um Benutzer zu authentifizieren. Wenn Sie den Wert auf `true` einstellen, wird die Verbindung mit SSL gesichert.

Standardwert

`falsch`

Gültige Werte

`true | false`

Platform | Sicherheit | Details zum Anmeldeverfahren | Web access control

Mit den Eigenschaften in dieser Kategorie wird die Integration mit der Software zur Webzugriffskontrolle konfiguriert.

Benutzernamenmuster

Beschreibung

Ein regulärer Java ™ Ausdruck, mit dem die Benutzeranmeldedaten aus der HTTP Header-Variablen der für die Webzugriffskontrolle verwendeten Software extrahiert werden. Beachten Sie, dass Sie für alle XML-Zeichen im regulären Ausdruck XML-Escape-Zeichen verwenden müssen. Der empfohlene Wert für SiteMinder und IBM Security Access Manager ist `\w*`

Diesen Wert sollten Sie auch verwenden, wenn Sie einen angepassten Proxy benutzen, um ein vor Ort gehostetes Unica Campaign-System mit einem cloudbasierten Digital Analytics-System zu integrieren.

Standardwert

Nicht definiert

Gültige Werte

Ein beliebiger regulärer Java™ Ausdruck.

Verfügbarkeit

Diese Eigenschaft wird verwendet, wenn die Integration von Unica Platform in eine Software zur Steuerung des Webzugriffs konfiguriert wurde.

Kopfzeilenvariable für Webzugriffskontrolle

Beschreibung

Gibt die in der Software zur Steuerung des Webzugriffs konfigurierte HTTP-Kopfzeilenvariable an, die an den Webanwendungsserver übermittelt wird. Standardmäßig wird `sm_user` von SiteMinder und `iv-user` von IBM Security Access Manager (SAM) verwendet. Setzen Sie diesen Wert für SAM auf die Benutzernamenkomponente der unformatierten Zeichenfolge und nicht der HTTP-Zeichenfolge.

Standardwert

Nicht definiert

Gültige Werte

Jede Zeichenfolge

Verfügbarkeit

Diese Eigenschaft wird verwendet, wenn die Integration von Unica Platform in eine Software zur Steuerung des Webzugriffs konfiguriert wurde.

Zusätzliche Header-Variablen

Beschreibung

Gibt eine durch Kommas getrennte Liste zusätzlicher HTTP-Header Variablen an, die während der Protokollierung über die Webzugriffskontrollsoftware erfasst werden sollen. Die angegebenen HTTP-Header Variablen werden erfasst und im Überwachungsprotokoll der Authentifizierung gespeichert, falls die Überwachungsprotokolle aktiviert sind.

Standardwert

Nicht definiert

Gültige Werte

Jede durch Kommas getrennte Zeichenfolge

Verfügbarkeit

Diese Eigenschaft wird verwendet, wenn die Integration von Unica Platform in eine Webzugriffskontrollsoftware konfiguriert wurde.

Platform | Sicherheit | Details zum Anmeldeverfahren | SAML 2.0

Die Eigenschaften in dieser Kategorie dienen zur Konfiguration der einmaligen Anmeldung (SSO = Single Sign-on) über einen SAML 2.0-IdP-Server.

IdP-Server-URL für einmalige Anmeldung

Beschreibung

Die URL der Seite, die angezeigt wird, wenn Benutzer die Single Sign-on-URL für Unica öffnen.

Standardwert

```
[CHANGE ME]
```

IdP-Server-URL für einmalige Abmeldung

Beschreibung

Diese Angabe ist optional. Wenn sich Benutzer abmelden, dann können Sie an die Seite weitergeleitet werden, die Sie hier angeben, sodass ihre Abmeldung auch die Abmeldung beim IdP-Server bewirkt. Ihr IdP-Server stellt zu diesem Zweck normalerweise eine URL bereit.

Standardwert

```
[CHANGE ME]
```

Fehlerseiten-URL für SSO-Fehler

Beschreibung

Wenn beim Single Sign-on ein Fehler aufgrund eines Konfigurations- oder Integrationsproblems auftritt, dann können Benutzer an die hier angegebene Seite weitergeleitet werden. Diese Einstellung überschreibt die Standardfehlerseite, die von Unica Platform bereitgestellt wird.

Standardwert

[CHANGE ME]

Ziel-URL

Beschreibung

Die URL des Service-Providers (Anwendung), an die der Benutzer nach erfolgreicher Authentifizierung über den IdP-Server weitergeleitet wird. Diese URL wird in jeder SAML-Anforderung unter dem Tag <AuthnRequest Destination> aufgeführt.

Standardwert

[CHANGE ME]

Konsumentenservice-URL

Beschreibung

Die Konsumentenservice-URL für Zusicherungen, die der Service-Provider (Anwendung) für SAML-Zusicherungen verarbeitet und parst. Diese URL wird in jeder SAML-Anforderung unter dem Tag <AuthnRequest AssertionConsumerServiceURL> aufgeführt. Dieser Wert kann mit dem Wert der Eigenschaft **Ziel URL** identisch sein.

Standardwert

[CHANGE ME]

Anwendungs-ID

Beschreibung

Die Anwendungs-ID, die Unica Platform auf dem IdP-Server zugeordnet ist. Diese ID ist in jeder SAML-Anforderung an den IdP-Server angegeben. Diese ID wird in jeder SAML-Anforderung unter dem Tag <Issuer> aufgeführt.

Standardwert

[CHANGE ME]

Qualifikationsmerkmal für Namen von Service-Providern

Beschreibung

Das Qualifikationsmerkmal für den Namen des Service-Providers. Dieses Qualifikationsmerkmal für den Namen wird in jeder SAML-Anforderung unter dem Tag <NameIDPolicy SPNameQualifier> aufgeführt.

Standardwert

[CHANGE ME]

Pfad der Metadaten

Beschreibung

Der Speicherort der Datei von IDP-Metadaten auf dem Unica Platform Server. Diese Datei von IDP-Metadaten wird vom IDP-Server bereitgestellt.

Standardwert

[CHANGE ME]

Entitäts-ID

Beschreibung

Die Entitäts-ID des IdP-Servers. Setzen Sie diese Eigenschaft auf den Wert von *entityID* in der XML-Deklaration am Anfang der vom IdP-Server erzeugten Metadaten-Datei.

Unica Platform verwendet diese ID während der Zusicherungsvalidierung zum Laden der IdP-Konfigurationen und des entsprechenden digitalen Zertifikats.

Standardwert

```
[CHANGE ME]
```

Attribute-NVP für Antwortparsing

Beschreibung

Die Benutzerkontenattribute werden vom IdP-Server an Unica Platform gesendet. Sie können diese Konfigurationseigenschaft verwenden, um die in Unica Platform automatisch erstellten Attribute für Benutzer zu erfassen, wenn die Eigenschaft **Authentifizierte Benutzer zu Platform hinzufügen** aktiviert wird.

Der IdP-Server kann einen anderen Namen für ein Attribut in Bezug auf den Namen verwenden, der von Unica Platform benutzt wird. Sie können diese Eigenschaft verwenden, um das IdP-Attribut dem entsprechenden Attribut in Unica Platform zuzuordnen. Dadurch sind keine Codeänderungen mehr erforderlich.

Der IdP-Server kann beispielsweise die Zeichenfolge **emailAddress** als Name für ein Attribut verwenden, das in Unica Platform **Email** lautet. In diesem Fall wird **Email=emailAddress** als Wert in dieser Eigenschaft zur Attributzuordnung eingegeben.

Verwenden Sie für die Benutzerattribute in Unica Platform die folgenden Werte.

- FirstName
- LastName
- Abteilung
- Organisation
- Country
- Email
- Address1
- Address2
- Phone1

  Verwendung für Geschäftstelefon.

- Phone2

  Verwendung für Mobiltelefon.
- Phone3

  Verwendung für Privattelefon.
- AltLogin
- ExternalUsersGroup

  Wird die Eigenschaft **Authentifizierte Benutzer zur Unica Platform hinzufügen** aktiviert, wird ein vom IdP Server authentifizierter Benutzer in der Unica Platform erstellt, falls dieser Benutzer nicht bereits über ein Unica Platform Konto verfügt. Diese Benutzer werden automatisch zur Standardbenutzergruppe **ExternalUsersGroup** hinzugefügt. Sie können allerdings auch eine benutzerdefinierte Gruppe angeben, zu der die Benutzer hinzugefügt werden sollen. Wird diese Option implementiert, legen Sie den Namen der benutzerdefinierten Benutzergruppe als Wert für das Attribut **ExternalUsersGroup** fest. Sollte beispielsweise ein Benutzer zu einem Gruppennamen hinzugefügt werden, der durch das SAML Attribut MyGroup identifiziert wird, würden Sie diesen Wert auf **ExternalUsersGroup=MyGroup setzen.** Die Benutzer werden dem Gruppennamen hinzugefügt, der im SAML Attribut MyGroup angegeben ist.

Trennen Sie dabei mehrere Name-/Wert-Paare durch ein Semikolon.

Standardwert

```
omit-xml-declaration=yes;
```

Verschlüsselte IdP-Antwort verarbeiten

Beschreibung

Wenn Ihr IdP-Server zum Senden verschlüsselter Antworten konfiguriert wurde, dann aktivieren Sie diese Eigenschaft, um anzugeben, dass die SAML-Antwort des IdP-Servers mithilfe eines konfigurierten gemeinsam

genutzten Schlüssels entschlüsselt werden muss, bevor sie von Unica Platform verarbeitet werden kann.

Wird diese Eigenschaft aktiviert, müssen Sie den Wert **Geteilter geheimer Schlüssel** auf den geheimen Schlüssel setzen, der zur Entschlüsselung der Antwort verwendet wird.

Standardwert

`Inaktiviert`

Geheimer Schlüssel für gemeinsame Nutzung

Beschreibung

Wird die Option **Verschlüsselte IdP-Antwort verarbeiten** aktiviert, setzen Sie für diesen Eigenschaftswert den Pfad der Keystore-Datei.

Standardwert

`[CHANGE ME]`

Inhaber des Keystoreberechtigungsnachweises

Beschreibung

Legen Sie für diesen Wert den Anmeldenamen des Unica-Benutzerkontos fest, der den geheimen SAML-Schlüssel in einer Datenquelle speichert.

Standardwert

`[CHANGE ME]`

Datenquelle des Keystoreberechtigungsnachweises

Beschreibung

Legen Sie für diesen Wert den Namen der Datenquelle fest, die zur Speicherung des geheimen Schlüssels für die gemeinsame Nutzung erstellt wurde, der für die Entschlüsselung eingesetzt wird. Das Kennwort in der Datenquelle ist das Kennwort für die Keystore-Datei.

Standardwert

[CHANGE ME]

Zertifikatsalias

Beschreibung

Wird die Option **Verschlüsselte IdP-Antwort verarbeiten** aktiviert, setzen Sie für diesen Eigenschaftswert den Zertifikatsaliasnamen des privaten Schlüssels, der in der Keystore-Datei gespeichert wird. Dieser Name wird für die Entschlüsselung der verschlüsselten SAML-Antwort verwendet, die vom IdP-Server gesendet wird.

Standardwert

[CHANGE ME]

Authentifizierte Benutzer zur Platform hinzufügen

Beschreibung

Wenn diese Option aktiviert ist, wird in Unica Platform ein über den IdP-Server authentifizierter Benutzer erstellt, wenn dieser Benutzer noch nicht über ein Unica Platform-Konto verfügt.

Die neu erstellten Benutzer werden automatisch der Standardgruppe **ExternalUsersGroup** hinzugefügt.

Die Gruppe **ExternalUsersGroup** verfügt lediglich über die Unica Platform **UserRole**. Ein Administrator muss zusätzliche Berechtigungen für die neu erstellten Benutzer erteilen, sodass diese Benutzer auf die Unica-Produkte zugreifen und diese Produkte nutzen können. Ein Administrator kann weiterführende Berechtigungen erteilen, indem er Benutzer als Mitglieder von Gruppen mit unterschiedlichen Anwendungszugriffsebenen definiert.

Alternativ hierzu kann die SAML-Antwort auch einen angepassten Benutzergruppennamen enthalten und neu erstellte Benutzer werden zu dieser Gruppe hinzugefügt.

Wenn diese Option inaktiviert ist, kann ein über den IdP-Server authentifizierter Benutzer nicht auf Unica Platform zugreifen, wenn dieser Benutzer noch nicht über ein Unica Platform-Konto verfügt.

Standardwert

`Inaktiviert`

Weiterleitung an SSO

Beschreibung

Falls dieser Wert **True** ist, gilt Folgendes:

- Benutzer, die sich bei Unica anmelden, werden an die IdP-Seite für die einmalige Anmeldung (SSO = Single Sign-on) weitergeleitet.
- Nachdem Benutzer die Anmeldung durchgeführt haben, wechseln sie zur standardmäßigen Unica Platform-Landing-Page.
- Der Standard Unica Platform Anmeldebildschirm ist nie verfügbar.

Note:

- **NameID-Format einstellen**

  Standardmäßig wird eine SAML Anfrage mit dem NameID-Format als vorübergehend generiert. Wenn Sie eine SAML Anfrage mit persistentem NameID-Format erstellen müssen, müssen Sie diesen JVM Parameter festlegen.

  `-DENABLE_PERSISTENT_NAMEID_FORMAT=true`

- **Konfiguration von SAML-authentifizierten Benutzererstellung für eine nicht standardmäßige Partition**

  Wird die Eigenschaft `Authentifizierte Benutzer zur Unica Platform hinzufügen` aktiviert, wird ein vom IdP Server authentifizierter Benutzer in der Unica Platform erstellt, falls dieser Benutzer nicht bereits über ein

Unica Platform Konto verfügt. Diese Benutzer werden automatisch der Standardpartition hinzugefügt, d.h. der Partition mit ID 1.

Möchten Sie jedoch, dass ein Benutzer einer anderen Partition hinzugefügt wird, muss dies als SAML Attribut angegeben werden

Beispiel: `PartitionId=<partitionid>`

- **Konfiguration von RequestedAuthnContext in SAML Anfrage**

  Standardmäßig wird eine SAML Anfrage mit `RequestedAuthnContext` in der SAML Anfrage generiert.

  `RequestedAuthnContext` wird von einigen IDP Servern in der SAML Anfrage nicht erfordert. Um dies aus der Anfrage zu entfernen, müssen Sie diesen JVM Parameter festlegen.

  `-REMOVE_REQUESTED_AUTHN_CONTEXT=true`

Platform | Sicherheit | LDAP-Synchronisierung

Mit den Eigenschaften für die LDAP-Synchronisation werden Details angegeben, die das System verwendet, um sich am Verzeichnisserver anzumelden und Benutzer für den Import zu identifizieren. Einige dieser Eigenschaften steuern auch die Häufigkeit und andere Details des automatischen Synchronisationsprozesses.

LDAP-Synchronisation aktiviert

Beschreibung

Setzen Sie den Wert auf `true`, um die LDAP- oder Active Directory-Synchronisierung zu aktivieren.

Standardwert

`falsch`

Gültige Werte

`true | false`

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

LDAP-Synchronisationsintervall

Beschreibung

Unica Platform wird in regelmäßigen Intervallen, hier in Sekunden angegeben, mit dem LDAP- oder Active Directory-Server synchronisiert. Beträgt der Nullwert oder weniger, führt Unica Platform keine Synchronisation durch. Ist der Wert eine positive Ganzzahl, tritt der neue Wert ohne Neustart innerhalb von zehn Minuten in Kraft. Folgeänderungen treten innerhalb der konfigurierten Intervallzeit in Kraft.

Standardwert

`600`, oder 10 Minuten

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

LDAP-Synchronisation verzögert

Beschreibung

Dies ist die Angabe der Zeit (im 24-Stunden-Format), nach der die regelmäßige Synchronisation mit dem LDAP-Server beginnt, nachdem Unica Platform gestartet wurde. Beispielsweise bedeuten der Wert 23:00 für `LDAP sync delay` und der Wert 600 für `LDAP sync interval`, dass beim Start von Unica Platform die regelmäßige Synchronisation um 23:00 Uhr gestartet wird und danach alle 10 Minuten (600 Sekunden) durchgeführt wird.

Standardwert

`23:00` oder 11:00pm

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

LDAP-Synchronisationszeitlimitüberschreitung

Beschreibung

Die Eigenschaft für die LDAP-Synchronisationzeitlimitüberschreitung legt die maximale Dauer (in Minuten) nach dem Start einer Synchronisation fest, bevor Unica Platform den Prozess als beendet markiert. Die Platform erlaubt die Durchführung von nur jeweils einem Synchronisationsprozess. Schlägt eine Synchronisation fehl, wird sie als beendet markiert, ungeachtet dessen, ob sie erfolgreich abgeschlossen wurde oder nicht.

Dies ist besonders praktisch in Clusterumgebungen. Wird die Unica Platform beispielsweise in einem Cluster eingesetzt, könnte ein Server innerhalb des Clusters eine LDAP-Synchronisation starten und dann herunterfahren, ehe der Prozess als beendet markiert wurde. In diesem Fall wartet Unica Platform für die in dieser Eigenschaft angegebene Dauer und startet dann die nächste geplante Synchronisation.

Standardwert

`600` (600 Minuten bzw. zehn Stunden)

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

LDAP-Synchronisationsumfang

Beschreibung

Steuert den Umfang der ersten Anfrage, um die Gruppe von Benutzern abzurufen. Sie sollten den Standardwert von SUBTREE für die Synchronisation mit den meisten LDAP-Servern beibehalten.

Standardwert

SUBTREE

Gültige Werte

Die Werte sind standardmäßige LDAP-Suchbereichsbegriffe.

- OBJECT – Ausschließliche Suche nach dem Eintrag im definierten Basisnamen. Nur dieser Eintrag wird zurückgegeben.
- ONE_LEVEL – Suche nach allen Einträgen eine Ebene unter dem definierten Basisnamen, ohne den definierten Basisnamen selbst.
- SUBTREE – Suche nach allen Einträgen auf allen Ebenen unter und einschließlich des festgelegten definierten Basisnamens.

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

LDAP-Provider-URL

Beschreibung

Bringen Sie die LDAP-URL des LDAP- oder Active Directory-Servers für die meisten Implementierungen in eines der folgenden Formate:

- `ldap://IP_address:port_number`
- `ldap://machineName.domain.com:port_number`

Auf LDAP-Servern ist die Portnummer üblicherweise 389 (636, wenn SSL verwendet wird).

Wenn Unica mit einen Active Directory-Server integriert ist und Ihre Active Directory-Implementierung serverlose Bindung verwendet, stellen Sie den Wert dieser Eigenschaft auf die URL für Ihren Active Directory-Server ein, indem Sie das folgende Format verwenden:

`ldap:///dc=example,dc=com`

Standardwert

Nicht definiert

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

SSL für LDAP-Verbindung verlangen

Pfad

`Marketing Platform | Sicherheit | LDAP-Synchronisierung`

Beschreibung

Legt fest, ob Unica Platform SSL verwendet, wenn es sich mit dem LDAP-Server verbindet, um Benutzer zu synchronisieren. Wenn Sie den Wert auf `true` einstellen, wird die Verbindung mit SSL gesichert.

Standardwert

`falsch`

Gültige Werte

`true | false`

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

Unica Platform-Gruppentrennzeichen für LDAP-Konfiguration

Beschreibung

Verwenden Sie in der Kategorie `LDAP-Referenz auf Unica Platform-Gruppenzuordnung` das hier festgelegte Trennzeichen, wenn Sie eine LDAP-

oder Active Directory-Gruppe mehreren Unica Platform-Gruppen zuordnen möchten. Dazu kann jedes einzelne Zeichen dienen, das nicht in den Namen erscheint, die es voneinander trennt.

Standardwert

; (Semikolon)

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

LDAP-Trennzeichen für Referenzkonfiguration

Beschreibung

Gibt das Trennzeichen an, das die Komponenten SEARCHBASE und FILTER trennt, aus denen sich die LDAP- oder Active Directory-Referenz zusammensetzt (beschrieben in der Kategorie `LDAP-Referenzen für die Erstellung von Unica Platform-Benutzern`).

FILTER ist optional: Wenn dies weggelassen wird, erstellt der Unica Platform-Server dynamisch den Filter basierend auf dem Eigenschaftswert `LDAP-Attributname für Benutzerreferenz`.

Standardwert

; (Semikolon)

Gültige Werte

Dazu kann jedes einzelne Zeichen dienen, das nicht in den Namen erscheint, die es voneinander trennt.

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

Unica Platform -Benutzer für LDAP-Berechtigungsnachweise

Beschreibung

Legt den Namen des Unica-Benutzers fest, dem die LDAP-Administratorzugangsdaten zugeteilt wurden.

Legen Sie den Wert dieser Eigenschaft auf den Benutzernamen fest, den Sie für den Unica-Benutzer erstellt haben, als Sie die LDAP-Integration konfigurierten. Diese Eigenschaft funktioniert zusammen mit der Eigenschaft `Datenquelle für LDAP-Berechtigungsnachweis` in dieser Kategorie.

Standardwert

`asm_admin`

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

Datenquelle für LDAP-Berechtigungsnachweis

Beschreibung

Gibt die Unica Platform-Datenquelle für die LDAP-Administratorzugangsdaten an.

Legen Sie den Wert dieser Eigenschaft auf den Datenquellennamen fest, den Sie für den Unica-Benutzer erstellt haben, als Sie die LDAP-Integration konfigurierten. Diese Eigenschaft funktioniert zusammen mit der Eigenschaft `Unica Platform Benutzer für LDAP-Berechtigungsnachweise` in dieser Kategorie.

Standardwert

Nicht definiert

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

LDAP-Attributname für Benutzerreferenz

Beschreibung

Gibt für den Import von Benutzern auf Gruppenbasis den Namen an, den Ihr LDAP- oder Active Directory-Server für das Benutzerattribut im Gruppenobjekt benutzt. Üblicherweise wird der Wert `uniquemember` in LDAP-Servern und `member` in Windows™ Active Directory-Servern verwendet.

Setzen Sie bei einem Import von Benutzern auf Attributbasis diese Eigenschaft auf `DN`, und wenn Sie die Eigenschaft **Übersicht LDAP-Referenzen** konfigurieren, setzen Sie den Teil FILTER des Werts auf die Zeichenfolge, die der LDAP-Server für das Attribut verwendet, nach dem gesucht werden soll.

Standardwert

`Mitglied`

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

Regelmäßige LDAP-Basis-DN-Suche inaktiviert

Beschreibung

Wenn diese Eigenschaft auf `True` gesetzt wird, führt Unica Platform die LDAP-Synchronisationssuche mit dem definierten Namen aus der Eigenschaft `Base DN` in der Kategorie **Unica Platform | Sicherheit | LDAP** durch. Wenn die Eigenschaft auf `False` gesetzt ist, führt Unica Platform die LDAP-Synchronisationssuche mit den Gruppen durch, die LDAP-Gruppen unter **LDAP-Referenz auf IBM Marketing Platform-Gruppenübersicht** zugeordnet sind.

In der folgenden Tabelle wird beschrieben, ob Änderungen in Abhängigkeit von dem Wert für diese Eigenschaft bei der regelmäßigen Synchronisation berücksichtigt werden.

Tabelle 76. Auswirkung dieser Eigenschaft auf das Verhalten bei der regelmäßigen Synchronisation

Ändern	Wird die Änderung berücksichtigt, wenn der Wert auf True steht?	Wird die Änderung berücksichtigt, wenn der Wert auf False steht?
In Unica Platform wird ein Benutzer gelöscht, der vom LDAP-Server synchronisiert wird.	Ja	Nein
Ein Benutzer wird aus einer LDAP-Gruppe gelöscht, die einer Unica Platform-Gruppe zugeordnet ist.	Nein	Nein
In Unica Platform wird ein Benutzer aus einer Unica Platform-Gruppe gelöscht, die einer LDAP-Gruppe zugeordnet ist.	Nein	Nein
Ein neuer Benutzer wird dem LDAP-Server hinzugefügt. Die Änderung wird nur dann mit dem Anmeldeverfahren LDAP. Wenn das Anmeldeverfahren LDAP ist, importiert das System neue Benutzer aus LDAP durch Auto Sync.	Ja	Ja

Tabelle 76. Auswirkung dieser Eigenschaft auf das Verhalten bei der regelmäßigen Synchronisation (Fortsetzung)

Ändern	Wird die Änderung berücksichtigt, wenn der Wert auf True steht?	Wird die Änderung berücksichtigt, wenn der Wert auf False steht?
Ein Benutzer wird einer LDAP-Gruppe hinzugefügt, die einer Unica Platform-Gruppe zugeordnet ist.	Ja	Nein
Es werden Benutzerattribute auf dem LDAP-Server geändert.	Ja	Ja

Standardwert

`Falsch`

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

Benutzeranmeldung

Beschreibung

Ordnet die Anmeldung der Unica-Benutzer dem äquivalenten Benutzerattribut in Ihrem LDAP- oder Active Directory-Server zu. `Benutzeranmeldung` ist die einzige erforderliche Zuweisung. Typischerweise ist der Wert für dieses Attribut `uid` in LDAP-Servern und `sAMAccountName` in Windows™ Active Directory-Servern. Bitte überprüfen Sie dies jedoch auf Ihrem LDAP- oder Active Directory-Server.

Standardwert

`uid`

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

Vorname

Beschreibung

Ordnet das Benutzerattribut "Vorname" in Unica Platform dem entsprechenden Benutzerattribut in Ihrem LDAP- oder Active Directory-Server zu.

Standardwert

`givenName`

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

Nachname

Beschreibung

Ordnet das Benutzerattribut "Nachname" in Unica Platform dem entsprechenden Benutzerattribut in Ihrem LDAP- oder Active Directory-Server zu.

Standardwert

`sn`

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

Position des Benutzers

Beschreibung

Ordnet das Attribut "Position des Benutzers" in Unica Platform dem entsprechenden Benutzerattribut in Ihrem LDAP- oder Active Directory-Server zu.

Standardwert

`TITEL`

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

Abteilung

Beschreibung

Ordnet das Benutzerattribut "Abteilung" in Unica Platform dem entsprechenden Benutzerattribut in Ihrem LDAP- oder Active Directory-Server zu.

Standardwert

Nicht definiert

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

Unternehmen

Beschreibung

Ordnet das Benutzerattribut "Unternehmen" in Unica Platform dem entsprechenden Benutzerattribut in Ihrem LDAP- oder Active Directory-Server zu.

Standardwert

Nicht definiert

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

Land

Beschreibung

Ordnet das Benutzerattribut "Land" in Unica Platform dem entsprechenden Benutzerattribut in Ihrem LDAP- oder Active Directory-Server zu.

Standardwert

Nicht definiert

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

E-Mail-Adresse des Benutzers

Beschreibung

Ordnet das Benutzerattribut "E-Mail-Adresse des Benutzers" in Unica Platform dem entsprechenden Benutzerattribut in Ihrem LDAP- oder Active Directory-Server zu.

Standardwert

`mail`

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

Adresse 1

Beschreibung

Ordnet das Benutzerattribut "Adresse" in Unica Platform dem entsprechenden Benutzerattribut in Ihrem LDAP- oder Active Directory-Server zu.

Standardwert

Nicht definiert

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

Telefon (geschäftlich)

Beschreibung

Ordnet das Benutzerattribut "Telefon (geschäftlich)" in Unica Platform dem entsprechenden Benutzerattribut in Ihrem LDAP- oder Active Directory-Server zu.

Standardwert

`telephoneNumber`

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

Mobiltelefon

Beschreibung

Ordnet das Benutzerattribut "Telefon (mobil)" in Unica Platform dem entsprechenden Benutzerattribut in Ihrem LDAP- oder Active Directory-Server zu.

Standardwert

Nicht definiert

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

Telefon (privat)

Beschreibung

Ordnet das Benutzerattribut "Telefon (privat)" in Unica Platform dem entsprechenden Benutzerattribut in Ihrem LDAP- oder Active Directory-Server zu.

Standardwert

Nicht definiert

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

Alternative Anmeldung

Beschreibung

Ordnet das Benutzerattribut "Alternative Anmeldung" in Unica Platform dem entsprechenden Benutzerattribut in Ihrem LDAP- oder Active Directory-Server zu.

Standardwert

Nicht definiert

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

Platform | Sicherheit | LDAP-Synchronisation | LDAP-Referenz auf Unica Platform-Gruppenzuordnung.

Mit den Eigenschaften in dieser Kategorie wird die LDAP-Integration konfiguriert.

Übersicht LDAP-Referenzen

Beschreibung

Benutzer, die Mitglieder der hier festgelegten LDAP- oder Active Directory-Gruppe sind, werden in die Unica Platform-Gruppe importiert, die in der Eigenschaft `Unica Platformgroup` angegeben ist.

Legen Sie den Wert dieser Eigenschaft mit der folgenden Syntax fest: `SEARCHBASE DELIMITER FILTER`, wobei Folgendes gilt:

`SEARCHBASE` ist der definierte Name (DN) des Objekts.

`DELIMITER` ist der Wert der Eigenschaft `LDAP-Trennzeichen für AM-Gruppe`.

`FILTER` ist der LDAP- oder Active Directory-Attributfilter. `FILTER` ist optional, wenn Sie den gruppenbasierten Import verwenden: Wenn dies weggelassen wird, erstellt der Unica Platform-Server dynamisch den Filter basierend auf dem Eigenschaftswert `LDAP-Attributname für Benutzerreferenz`.

Setzen Sie bei einem Import auf Attributbasis den Wert von `FILTER` auf die Zeichenfolge, die der LDAP-Server für das Attribut verwendet, nach dem gesucht werden soll. Zudem müssen Sie den Wert für **LDAP-Attributname für Benutzerreferenz** auf `DN` setzen.

Standardwert

Nicht definiert

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

Unica Platform Gruppe

Beschreibung

Benutzer, die in der `DAP-Referenzgruppe`-Eigenschaft als Mitglieder der LDAP- oder Active Directory-Gruppe festgelegt sind, werden in die hier festgelegte Unica Platform-Gruppe importiert.

Standardwert

Nicht definiert

Verfügbarkeit

Diese Eigenschaft wird nur verwendet, wenn die Unica Platform-Integration mit dem Windows™ Active Directory-Server oder einem anderen LDAP-Server konfiguriert wurde.

Platform | Sicherheit | Föderierte Authentifizierung

Eigenschaften in dieser Kategorie werden bei der Implementierung der föderierten Authentifizierung auf der Basis von SAML (Security Assertion Markup Language) 2.0 verwendet, wodurch eine einmalige Anmeldung (Single Sign-on) an mehreren Anwendungen möglich ist.

Föderierte Anmeldung ermöglichen

Beschreibung

Wählen Sie das Kontrollkästchen in dieser Eigenschaft aus, um eine föderierte Authentifizierung in einer integrierten Umgebung zu ermöglichen.

Standardwert

Inaktiviert

Identitätsprovider-URL

Beschreibung

Die URL des Identitätsprovider-Servers.

Zertifikatsaussteller

Beschreibung

Die URL der Zertifizierungsstelle, die das Zertifikat auf dem Identitätsprovider-Server ausgegeben hat. Wenn Sie Ihre eigenen Zertifikate mit dem Java™-Dienstprogramm 'keytool' generieren, legen Sie für diesen Wert die IdP-Server-URL fest.

Platform | Sicherheit | Föderierte Authentifizierung | Partitionen | Partition[n]

Die Eigenschaften in dieser Kategorie werden bei der Implementierung der föderierten Authentifizierung auf der Basis von SAML (Security Assertion Markup Language) 2.0 zwischen Unica-Anwendungen und anderen - und Drittanbieteranwendungen verwendet.

Keystore-Pfad

Beschreibung

Die Position der vertrauenswürdigen Keystore-Datei im Webanwendungsserver.

Keystore-Hauptschlüssel

Beschreibung

Der Hauptschlüssel für den Keystore im Webanwendungsserver.

Keystore-Alias

Beschreibung

Der Alias für den Keystore im Webanwendungsserver.

Unica Platform | Sicherheit | API-Verwaltung

Die Eigenschaften in dieser Kategorie dienen zur Konfiguration des Authentifizierungsverhaltens, das für alle Unica-APIs gilt.

Sitzungsbasierte API-Authentifizierung aktivieren

Beschreibung

Wenn Sie das Kontrollkästchen dieser Eigenschaft auswählen, um sie zu aktivieren, dann werden Benutzer, die durch Anmeldung bei Unica authentifiziert wurden, nicht zur erneuten Anmeldung aufgefordert, wenn sie über eine Unica-Anwendung während der Sitzung, für die sie authentifiziert wurden, auf eine sichere API zugreifen.

Wird diese Eigenschaft aktiviert und ein authentifizierter Unica Interact-Benutzer ruft eine Unica Campaign-API während der Sitzung auf, dann ist keine weitere Anmeldung erforderlich.

Standardwert

Inaktiviert

Sicherheitstoken nach einmaliger Verwendung löschen

Beschreibung

Wenn Sie das Kontrollkästchen für diese Eigenschaft auswählen, um die Eigenschaft zu aktivieren, dann wird das für einen authentifizierten Benutzer generierte Token zerstört, wenn es zum ersten Mal für den Zugriff auf eine sichere API verwendet wird. Dadurch wird die Sicherheit verbessert, da die weitere Verwendung dieses Tokens verhindert wird.

Standardwert

Aktiviert

Platform | Sicherheit | API Verwaltung | [Produkt] | (API Konfigurationsvorlage)

Verwenden Sie die Vorlage in dieser Kategorie, um die Authentifizierung für die Unica-APIs zu konfigurieren. Sie können den Zugriff blockieren oder HTTPS oder die Authentifizierung für APIs als erforderlich festlegen.

API-URI

Beschreibung

Für jedes Produkt wird der erste Teil des URI durch den Sicherheitsrahmen wie folgt aufgelöst: `http[s]://host:port/context root/api/product`

Deshalb sollten Sie in diesem Feld nur die Ressourcennamen der zu konfigurierenden API eingeben. Die einzugebende Zeichenfolge finden Sie in der API-Dokumentation des Produkts.

Der für diese Eigenschaft verwendete Wert muss mit einem / (Schrägstrich) beginnen, andernfalls wird die Konfiguration vom Sicherheitsframework ignoriert.

Diese Eigenschaft unterstützt sowohl die exakte URL-Übereinstimmung als auch die Musterübereinstimmung für die konfigurierten APIs.

- Für die exakte Übereinstimmung kann die URI mit einem Schrägstrich (/) oder dem Ressourcennamen enden.
- Für die Musterübereinstimmung muss die URI mit einem Stern (*) enden.

Wenn Sie den Wert dieser Eigenschaft auf `/*` festlegen, werden die Einstellungen, die Sie für andere Einstellungen in dieser Kategorie verwenden, auf alle APIs des Produkts angewendet.

Note: Bei der API Unica Platform `login` ist diese Konfigurationseigenschaft schreibgeschützt.

Standardwert

Nicht definiert

API-Zugriff blockieren

Beschreibung

Wählen Sie diese Option aus, wenn Sie eine API daran hindern möchten, auf ein Produkt zuzugreifen. Diese Option ist standardmäßig nicht ausgewählt.

Wenn eine API geblockt ist, gibt der Sicherheitsfilter den HTTP-Statuscode 403 (unzulässig) zurück.

Sicherer API-Zugriff über HTTPS

Beschreibung

Wählen Sie diese Option aus, wenn Sie einer API den Zugriff auf ein Produkt nur über HTTPS ermöglichen möchten. Diese Option ist standardmäßig ausgewählt.

Wenn auf eine API, bei der diese Eigenschaft aktiviert ist, über HTTP statt HTTPS zugegriffen wird, gibt der Sicherheitsfilter den HTTP-Statuscode 403 (unzulässig) zurück.

Authentifizierung für API-Zugriff erfordern

Beschreibung

Wählen Sie diese Option aus, wenn Sie als erforderlich festlegen möchten, dass eine API authentifiziert wird, bevor sie auf ein Produkt zugreifen kann. Diese Option ist standardmäßig ausgewählt.

Wenn auf eine API, bei der diese Eigenschaft aktiviert ist, mit ungültigen Berechtigungsnachweisen zugegriffen wird, gibt der Sicherheitsfilter den HTTP-Statuscode 401 (nicht berechtigt) zurück.

Note: Bei der API Unica Platform `login` ist diese Konfigurationseigenschaft deaktiviert, da diese API als erste für die API Authentifizierung aufgerufen wird.

Standardwert

(Deaktiviert)

Authentifizierungsmodus

Beschreibung

Wählen Sie diese Option aus, wenn Sie die API mit Standardauthentifizierung oder Bearer-Token Authentifizierung authentifizieren möchten. Wird die Option Basisauthentifizierung oder Bearer-Token ausgewählt, müssen die entsprechende Benutzer-ID und Passwort in der Datenquelle des Benutzers verwaltet werden. Für den Authentifizierungsmodus Manager verhält es sich genauso, wenn der Parameter `api_auth_mode = Manager` im Anforderungsheader verwendet wird. Diese Dropdown-Auswahl ist gültig nur wenn 'Authentifizierung für API Zugriff erforderlich' ausgewählt wird.

Standardwert

Manager

Berechtigungsinhaber der Datenquelle

Beschreibung

Geben Sie den Benutzernamen an, der die Datenquelle mit den erforderlichen Authentifizierungsdaten enthält. Die Datenquelle enthält die Benutzer ID und das Passwort bei der Auswahl von Standardauthentifizierung in der Dropdown-Liste vom Authentifizierungsmodus. Die Datenquelle enthält Bearer-Token bei der Auswahl von Bearer-Token in der Dropdown-Liste vom Authentifizierungsmodus.

Standardwert

asm_admin

Datenquelle

Beschreibung

Geben Sie den Namen der Datenquelle an, der unter dem in dem Feld 'Berechtigungsinhaber der Datenquelle' angegebenen Benutzer erstellt wird.

Standardwert

API_SECRET_DS

Unica Platform | Sicherheit | API-Verwaltung | [Produkt] | Unica Platform | Authentifizierung

(Affinium|suite|security|apiSecurity|manager|managerAuthentication) Verwenden Sie die Vorlagen in dieser Kategorie, um die Authentifizierung für Unica APIs zu konfigurieren. Sie können den Zugriff blockieren oder HTTPS oder die Authentifizierung für APIs als erforderlich festlegen.

API-URI

Beschreibung

Für jedes Produkt wird der erste Teil des URI durch den Sicherheitsrahmen wie folgt aufgelöst: `http[s]://host:port/context root/api/product`

Deshalb sollten Sie in diesem Feld nur die Ressourcennamen der zu konfigurierenden API eingeben. Die einzugebende Zeichenfolge finden Sie in der API-Dokumentation des Produkts.

Der für diese Eigenschaft verwendete Wert muss mit einem / (Schrägstrich) beginnen, andernfalls wird die Konfiguration vom Sicherheitsframework ignoriert.

Diese Eigenschaft unterstützt sowohl die exakte URL-Übereinstimmung als auch die Musterübereinstimmung für die konfigurierten APIs.

- Für die exakte Übereinstimmung kann die URI mit einem Schrägstrich (/) oder dem Ressourcennamen enden.
- Für die Musterübereinstimmung muss die URI mit einem Stern (*) enden.

Wenn Sie den Wert dieser Eigenschaft auf `/*` festlegen, werden die Einstellungen, die Sie für andere Einstellungen in dieser Kategorie verwenden, auf alle APIs des Produkts angewendet.

Note: Bei der API Unica Platform `login` ist diese Konfigurationseigenschaft schreibgeschützt.

Standardwert

/authentication/login

API-Zugriff blockieren

Beschreibung

Wählen Sie diese Option aus, wenn Sie eine API daran hindern möchten, auf ein Produkt zuzugreifen. Diese Option ist standardmäßig nicht ausgewählt.

Wenn eine API geblockt ist, gibt der Sicherheitsfilter den HTTP-Statuscode 403 (unzulässig) zurück.

Standardwert

(Deaktiviert)

Sicherer API-Zugriff über HTTPS

Beschreibung

Wählen Sie diese Option aus, wenn Sie einer API den Zugriff auf ein Produkt nur über HTTPS ermöglichen möchten. Diese Option ist standardmäßig ausgewählt.

Wenn auf eine API, bei der diese Eigenschaft aktiviert ist, über HTTP statt HTTPS zugegriffen wird, gibt der Sicherheitsfilter den HTTP-Statuscode 403 (unzulässig) zurück.

Standardwert

(Deaktiviert)

Authentifizierung für API-Zugriff erfordern

Beschreibung

Wählen Sie diese Option aus, wenn Sie als erforderlich festlegen möchten, dass eine API authentifiziert wird, bevor sie auf ein Produkt zugreifen kann. Diese Option ist standardmäßig ausgewählt.

Wenn auf eine API, bei der diese Eigenschaft aktiviert ist, mit ungültigen Berechtigungsnachweisen zugegriffen wird, gibt der Sicherheitsfilter den HTTP-Statuscode 401 (nicht berechtigt) zurück.

Note: Bei der API Unica Platform `login` ist diese Konfigurationseigenschaft deaktiviert, da diese API als erste für die API Authentifizierung aufgerufen wird.

Standardwert

(Deaktiviert)

Authentifizierungsmodus

Beschreibung

Wählen Sie diese Option aus, wenn Sie die API mit Standardauthentifizierung oder Bearer-Token Authentifizierung authentifizieren möchten. Wird die Option Basisauthentifizierung oder Bearer-Token ausgewählt, müssen die entsprechende Benutzer-ID und Passwort in der Datenquelle des Benutzers verwaltet werden. Für den Authentifizierungsmodus Manager verhält es sich genauso, wenn der Parameter `api_auth_mode = Manager` im Anforderungsheader verwendet wird. Diese Dropdown-Auswahl ist gültig nur wenn 'Authentifizierung für API Zugriff erforderlich' ausgewählt wird.

Standardwert

Manager

Berechtigungsinhaber der Datenquelle

Beschreibung

Geben Sie den Benutzernamen an, der die Datenquelle mit den erforderlichen Authentifizierungsdaten enthält. Die Datenquelle enthält die Benutzer ID

und das Passwort bei der Auswahl von Standardauthentifizierung in der Dropdown-Liste vom Authentifizierungsmodus. Die Datenquelle enthält Bearer-Token bei der Auswahl von Bearer-Token in der Dropdown-Liste vom Authentifizierungsmodus.

Standardwert

asm_admin

Datenquelle

Beschreibung

Geben Sie den Namen der Datenquelle an, der unter dem in dem Feld 'Berechtigungsinhaber der Datenquelle' angegebenen Benutzer erstellt wird.

Standardwert

API_SECRET_DS

Related information

Sicherheitsframework für Unica-APIs *(on page 265)*

Unica Platform | Sicherheit | API management | [Produkt] | Unica Platform | Benutzer

(Affinium|suite|security|apiSecurity|manager|managerUser) Verwenden Sie die Vorlagen in dieser Kategorie, um die Authentifizierung für Unica APIs zu konfigurieren. Sie können den Zugriff blockieren oder HTTPS oder die Authentifizierung für APIs als erforderlich festlegen.

API-URI

Beschreibung

Für jedes Produkt wird der erste Teil des URI durch den Sicherheitsrahmen wie folgt aufgelöst: `http[s]://host:port/context root/api/product`

Deshalb sollten Sie in diesem Feld nur die Ressourcennamen der zu konfigurierenden API eingeben. Die einzugebende Zeichenfolge finden Sie in der API-Dokumentation des Produkts.

Der für diese Eigenschaft verwendete Wert muss mit einem / (Schrägstrich) beginnen, andernfalls wird die Konfiguration vom Sicherheitsframework ignoriert.

Diese Eigenschaft unterstützt sowohl die exakte URL-Übereinstimmung als auch die Musterübereinstimmung für die konfigurierten APIs.

- Für die exakte Übereinstimmung kann die URI mit einem Schrägstrich (/) oder dem Ressourcennamen enden.
- Für die Musterübereinstimmung muss die URI mit einem Stern (*) enden.

Wenn Sie den Wert dieser Eigenschaft auf `/*` festlegen, werden die Einstellungen, die Sie für andere Einstellungen in dieser Kategorie verwenden, auf alle APIs des Produkts angewendet.

Note: Bei der API Unica Platform `login` ist diese Konfigurationseigenschaft schreibgeschützt.

Standardwert

/user/partitions/*

API-Zugriff blockieren

Beschreibung

Wählen Sie diese Option aus, wenn Sie eine API daran hindern möchten, auf ein Produkt zuzugreifen. Diese Option ist standardmäßig nicht ausgewählt.

Wenn eine API geblockt ist, gibt der Sicherheitsfilter den HTTP-Statuscode 403 (unzulässig) zurück.

Standardwert

(Deaktiviert)

Sicherer API-Zugriff über HTTPS

Beschreibung

Wählen Sie diese Option aus, wenn Sie einer API den Zugriff auf ein Produkt nur über HTTPS ermöglichen möchten. Diese Option ist standardmäßig ausgewählt.

Wenn auf eine API, bei der diese Eigenschaft aktiviert ist, über HTTP statt HTTPS zugegriffen wird, gibt der Sicherheitsfilter den HTTP-Statuscode 403 (unzulässig) zurück.

Standardwert

(Aktiviert)

Authentifizierung für API-Zugriff erfordern

Beschreibung

Wählen Sie diese Option aus, wenn Sie als erforderlich festlegen möchten, dass eine API authentifiziert wird, bevor sie auf ein Produkt zugreifen kann. Diese Option ist standardmäßig ausgewählt.

Wenn auf eine API, bei der diese Eigenschaft aktiviert ist, mit ungültigen Berechtigungsnachweisen zugegriffen wird, gibt der Sicherheitsfilter den HTTP-Statuscode 401 (nicht berechtigt) zurück.

Note: Bei der API Unica Platform `login` ist diese Konfigurationseigenschaft deaktiviert, da diese API als erste für die API Authentifizierung aufgerufen wird.

Standardwert

(Aktiviert)

Authentifizierungsmodus

Beschreibung

Wählen Sie diese Option aus, wenn Sie die API mit Standardauthentifizierung oder Bearer-Token Authentifizierung authentifizieren möchten. Wird die Option Basisauthentifizierung oder Bearer-Token ausgewählt, müssen die entsprechende Benutzer-ID und Passwort in der Datenquelle des Benutzers verwaltet werden. Für den Authentifizierungsmodus Manager verhält es sich genauso, wenn der Parameter `api_auth_mode = Manager` im Anforderungsheader verwendet wird. Diese Dropdown-Auswahl ist gültig nur wenn 'Authentifizierung für API Zugriff erforderlich' ausgewählt wird.

Standardwert

Manager

Berechtigungsinhaber der Datenquelle

Beschreibung

Geben Sie den Benutzernamen an, der die Datenquelle mit den erforderlichen Authentifizierungsdaten enthält. Die Datenquelle enthält die Benutzer ID und das Passwort bei der Auswahl von Standardauthentifizierung in der Dropdown-Liste vom Authentifizierungsmodus. Die Datenquelle enthält Bearer-Token bei der Auswahl von Bearer-Token in der Dropdown-Liste vom Authentifizierungsmodus.

Standardwert

asm_admin

Datenquelle

Beschreibung

Geben Sie den Namen der Datenquelle an, der unter dem in dem Feld 'Berechtigungsinhaber der Datenquelle' angegebenen Benutzer erstellt wird.

Standardwert

API_SECRET_DS

Related information

Sicherheitsframework für Unica-APIs *(on page 265)*

Unica Platform | Sicherheit | API management | [Product] | Unica Platform | Richtlinie

(Affinium|suite|security|apiSecurity|manager|managerPolicy) Verwenden Sie die Vorlagen in dieser Kategorie, um die Authentifizierung für Unica APIs zu konfigurieren. Sie können den Zugriff blockieren oder HTTPS oder die Authentifizierung für APIs als erforderlich festlegen.

API-URI

Beschreibung

Für jedes Produkt wird der erste Teil des URI durch den Sicherheitsrahmen wie folgt aufgelöst: `http[s]://host:port/context root/api/product`

Deshalb sollten Sie in diesem Feld nur die Ressourcennamen der zu konfigurierenden API eingeben. Die einzugebende Zeichenfolge finden Sie in der API-Dokumentation des Produkts.

Der für diese Eigenschaft verwendete Wert muss mit einem / (Schrägstrich) beginnen, andernfalls wird die Konfiguration vom Sicherheitsframework ignoriert.

Diese Eigenschaft unterstützt sowohl die exakte URL-Übereinstimmung als auch die Musterübereinstimmung für die konfigurierten APIs.

- Für die exakte Übereinstimmung kann die URI mit einem Schrägstrich (/) oder dem Ressourcennamen enden.
- Für die Musterübereinstimmung muss die URI mit einem Stern (*) enden.

Wenn Sie den Wert dieser Eigenschaft auf `/*` festlegen, werden die Einstellungen, die Sie für andere Einstellungen in dieser Kategorie verwenden, auf alle APIs des Produkts angewendet.

Note: Bei der API Unica Platform `login` ist diese Konfigurationseigenschaft schreibgeschützt.

Standardwert

/policy/partitions/*

API-Zugriff blockieren

Beschreibung

Wählen Sie diese Option aus, wenn Sie eine API daran hindern möchten, auf ein Produkt zuzugreifen. Diese Option ist standardmäßig nicht ausgewählt.

Wenn eine API geblockt ist, gibt der Sicherheitsfilter den HTTP-Statuscode 403 (unzulässig) zurück.

Standardwert

(Deaktiviert)

Sicherer API-Zugriff über HTTPS

Beschreibung

Wählen Sie diese Option aus, wenn Sie einer API den Zugriff auf ein Produkt nur über HTTPS ermöglichen möchten. Diese Option ist standardmäßig ausgewählt.

Wenn auf eine API, bei der diese Eigenschaft aktiviert ist, über HTTP statt HTTPS zugegriffen wird, gibt der Sicherheitsfilter den HTTP-Statuscode 403 (unzulässig) zurück.

Standardwert

(Deaktiviert)

Authentifizierung für API-Zugriff erfordern

Beschreibung

Wählen Sie diese Option aus, wenn Sie als erforderlich festlegen möchten, dass eine API authentifiziert wird, bevor sie auf ein Produkt zugreifen kann. Diese Option ist standardmäßig ausgewählt.

Wenn auf eine API, bei der diese Eigenschaft aktiviert ist, mit ungültigen Berechtigungsnachweisen zugegriffen wird, gibt der Sicherheitsfilter den HTTP-Statuscode 401 (nicht berechtigt) zurück.

Note: Bei der API Unica Platform `login` ist diese Konfigurationseigenschaft deaktiviert, da diese API als erste für die API Authentifizierung aufgerufen wird.

Standardwert

(Aktiviert)

Authentifizierungsmodus

Beschreibung

Wählen Sie diese Option aus, wenn Sie die API mit Standardauthentifizierung oder Bearer-Token Authentifizierung authentifizieren möchten. Wird die Option Basisauthentifizierung oder Bearer-Token ausgewählt, müssen die entsprechende Benutzer-ID und Passwort in der Datenquelle des Benutzers verwaltet werden. Für den Authentifizierungsmodus Manager verhält es sich genauso, wenn der Parameter `api_auth_mode = Manager` im Anforderungsheader verwendet wird. Diese Dropdown-Auswahl ist gültig nur wenn 'Authentifizierung für API Zugriff erforderlich' ausgewählt wird.

Standardwert

Manager

Berechtigungsinhaber der Datenquelle

Beschreibung

Geben Sie den Benutzernamen an, der die Datenquelle mit den erforderlichen Authentifizierungsdaten enthält. Die Datenquelle enthält die Benutzer ID und das Passwort bei der Auswahl von Standardauthentifizierung in der Dropdown-Liste vom Authentifizierungsmodus. Die Datenquelle enthält Bearer-Token bei der Auswahl von Bearer-Token in der Dropdown-Liste vom Authentifizierungsmodus.

Standardwert

asm_admin

Datenquelle

Beschreibung

Geben Sie den Namen der Datenquelle an, der unter dem in dem Feld 'Berechtigungsinhaber der Datenquelle' angegebenen Benutzer erstellt wird.

Standardwert

API_SECRET_DS

Related information

Sicherheitsframework für Unica-APIs *(on page 265)*

Unica Platform | Sicherheit | API management | [Produkt] | Unica Platform | Konfiguration

(Affinium|suite|security|apiSecurity|manager|managerConfiguration)Verwenden Sie die Vorlagen in dieser Kategorie, um die Authentifizierung für Unica APIs zu konfigurieren. Sie können den Zugriff blockieren oder HTTPS oder die Authentifizierung für APIs als erforderlich festlegen.

API-URI

Beschreibung

Für jedes Produkt wird der erste Teil des URI durch den Sicherheitsrahmen wie folgt aufgelöst: `http[s]://host:port/context root/api/product`

Deshalb sollten Sie in diesem Feld nur die Ressourcennamen der zu konfigurierenden API eingeben. Die einzugebende Zeichenfolge finden Sie in der API-Dokumentation des Produkts.

Der für diese Eigenschaft verwendete Wert muss mit einem / (Schrägstrich) beginnen, andernfalls wird die Konfiguration vom Sicherheitsframework ignoriert.

Diese Eigenschaft unterstützt sowohl die exakte URL-Übereinstimmung als auch die Musterübereinstimmung für die konfigurierten APIs.

- Für die exakte Übereinstimmung kann die URI mit einem Schrägstrich (/) oder dem Ressourcennamen enden.
- Für die Musterübereinstimmung muss die URI mit einem Stern (*) enden.

Wenn Sie den Wert dieser Eigenschaft auf `/*` festlegen, werden die Einstellungen, die Sie für andere Einstellungen in dieser Kategorie verwenden, auf alle APIs des Produkts angewendet.

Note: Bei der API Unica Platform `login` ist diese Konfigurationseigenschaft schreibgeschützt.

Standardwert

/datasource/config

API-Zugriff blockieren

Beschreibung

Wählen Sie diese Option aus, wenn Sie eine API daran hindern möchten, auf ein Produkt zuzugreifen. Diese Option ist standardmäßig nicht ausgewählt.

Wenn eine API geblockt ist, gibt der Sicherheitsfilter den HTTP-Statuscode 403 (unzulässig) zurück.

Standardwert

(Deaktiviert)

Sicherer API-Zugriff über HTTPS

Beschreibung

Wählen Sie diese Option aus, wenn Sie einer API den Zugriff auf ein Produkt nur über HTTPS ermöglichen möchten. Diese Option ist standardmäßig ausgewählt.

Wenn auf eine API, bei der diese Eigenschaft aktiviert ist, über HTTP statt HTTPS zugegriffen wird, gibt der Sicherheitsfilter den HTTP-Statuscode 403 (unzulässig) zurück.

Standardwert

(Deaktiviert)

Authentifizierung für API-Zugriff erfordern

Beschreibung

Wählen Sie diese Option aus, wenn Sie als erforderlich festlegen möchten, dass eine API authentifiziert wird, bevor sie auf ein Produkt zugreifen kann. Diese Option ist standardmäßig ausgewählt.

Wenn auf eine API, bei der diese Eigenschaft aktiviert ist, mit ungültigen Berechtigungsnachweisen zugegriffen wird, gibt der Sicherheitsfilter den HTTP-Statuscode 401 (nicht berechtigt) zurück.

Note: Bei der API Unica Platform `login` ist diese Konfigurationseigenschaft deaktiviert, da diese API als erste für die API Authentifizierung aufgerufen wird.

Standardwert

(Aktiviert)

Authentifizierungsmodus

Beschreibung

Wählen Sie diese Option aus, wenn Sie die API mit Standardauthentifizierung oder Bearer-Token Authentifizierung authentifizieren möchten. Wird die Option Basisauthentifizierung oder Bearer-Token ausgewählt, müssen die entsprechende Benutzer-ID und Passwort in der Datenquelle des Benutzers verwaltet werden. Für den Authentifizierungsmodus Manager verhält es sich genauso, wenn der Parameter `api_auth_mode = Manager` im Anforderungsheader verwendet wird. Diese Dropdown-Auswahl ist gültig nur wenn 'Authentifizierung für API Zugriff erforderlich' ausgewählt wird.

Standardwert

Manager

Berechtigungsinhaber der Datenquelle

Beschreibung

Geben Sie den Benutzernamen an, der die Datenquelle mit den erforderlichen Authentifizierungsdaten enthält. Die Datenquelle enthält die Benutzer ID und das Passwort bei der Auswahl von Standardauthentifizierung in der Dropdown-Liste vom Authentifizierungsmodus. Die Datenquelle enthält Bearer-Token bei der Auswahl von Bearer-Token in der Dropdown-Liste vom Authentifizierungsmodus.

Standardwert

asm_admin

Datenquelle

Beschreibung

Geben Sie den Namen der Datenquelle an, der unter dem in dem Feld 'Berechtigungsinhaber der Datenquelle' angegebenen Benutzer erstellt wird.

Standardwert

API_SECRET_DS

Related information

Sicherheitsframework für Unica-APIs *(on page 265)*

Unica Platform | Sicherheit | API management | [Produkt] | Unica Platform | Datasource

(Affinium|suite|security|apiSecurity|manager|managerDatasource) Verwenden Sie die Vorlagen in dieser Kategorie, um die Authentifizierung für Unica APIs zu konfigurieren. Sie können den Zugriff blockieren oder HTTPS oder die Authentifizierung für APIs als erforderlich festlegen.

API-URI

Beschreibung

Für jedes Produkt wird der erste Teil des URI durch den Sicherheitsrahmen wie folgt aufgelöst: `http[s]://host:port/context root/api/product`

Deshalb sollten Sie in diesem Feld nur die Ressourcennamen der zu konfigurierenden API eingeben. Die einzugebende Zeichenfolge finden Sie in der API-Dokumentation des Produkts.

Der für diese Eigenschaft verwendete Wert muss mit einem / (Schrägstrich) beginnen, andernfalls wird die Konfiguration vom Sicherheitsframework ignoriert.

Diese Eigenschaft unterstützt sowohl die exakte URL-Übereinstimmung als auch die Musterübereinstimmung für die konfigurierten APIs.

- Für die exakte Übereinstimmung kann die URI mit einem Schrägstrich (/) oder dem Ressourcennamen enden.
- Für die Musterübereinstimmung muss die URI mit einem Stern (*) enden.

Wenn Sie den Wert dieser Eigenschaft auf `/*` festlegen, werden die Einstellungen, die Sie für andere Einstellungen in dieser Kategorie verwenden, auf alle APIs des Produkts angewendet.

Note: Bei der API Unica Platform `login` ist diese Konfigurationseigenschaft schreibgeschützt.

Standardwert

/datasource

API-Zugriff blockieren

Beschreibung

Wählen Sie diese Option aus, wenn Sie eine API daran hindern möchten, auf ein Produkt zuzugreifen. Diese Option ist standardmäßig nicht ausgewählt.

Wenn eine API geblockt ist, gibt der Sicherheitsfilter den HTTP-Statuscode 403 (unzulässig) zurück.

Standardwert

(Deaktiviert)

Sicherer API-Zugriff über HTTPS

Beschreibung

Wählen Sie diese Option aus, wenn Sie einer API den Zugriff auf ein Produkt nur über HTTPS ermöglichen möchten. Diese Option ist standardmäßig ausgewählt.

Wenn auf eine API, bei der diese Eigenschaft aktiviert ist, über HTTP statt HTTPS zugegriffen wird, gibt der Sicherheitsfilter den HTTP-Statuscode 403 (unzulässig) zurück.

Standardwert

(Aktiviert)

Authentifizierung für API-Zugriff erfordern

Beschreibung

Wählen Sie diese Option aus, wenn Sie als erforderlich festlegen möchten, dass eine API authentifiziert wird, bevor sie auf ein Produkt zugreifen kann. Diese Option ist standardmäßig ausgewählt.

Wenn auf eine API, bei der diese Eigenschaft aktiviert ist, mit ungültigen Berechtigungsnachweisen zugegriffen wird, gibt der Sicherheitsfilter den HTTP-Statuscode 401 (nicht berechtigt) zurück.

Note: Bei der API Unica Platform `login` ist diese Konfigurationseigenschaft deaktiviert, da diese API als erste für die API Authentifizierung aufgerufen wird.

Standardwert

(Aktiviert)

Authentifizierungsmodus

Beschreibung

Wählen Sie diese Option aus, wenn Sie die API mit Standardauthentifizierung oder Bearer-Token Authentifizierung authentifizieren möchten. Wird die Option Basisauthentifizierung oder Bearer-Token ausgewählt, müssen die entsprechende Benutzer-ID und Passwort in der Datenquelle des Benutzers verwaltet werden. Für den Authentifizierungsmodus Manager verhält es sich genauso, wenn der Parameter `api_auth_mode = Manager` im

Anforderungsheader verwendet wird. Diese Dropdown-Auswahl ist gültig nur wenn 'Authentifizierung für API Zugriff erforderlich' ausgewählt wird.

Standardwert

Manager

Berechtigungsinhaber der Datenquelle

Beschreibung

Geben Sie den Benutzernamen an, der die Datenquelle mit den erforderlichen Authentifizierungsdaten enthält. Die Datenquelle enthält die Benutzer ID und das Passwort bei der Auswahl von Standardauthentifizierung in der Dropdown-Liste vom Authentifizierungsmodus. Die Datenquelle enthält Bearer-Token bei der Auswahl von Bearer-Token in der Dropdown-Liste vom Authentifizierungsmodus.

Standardwert

asm_admin

Datenquelle

Beschreibung

Geben Sie den Namen der Datenquelle an, der unter dem in dem Feld 'Berechtigungsinhaber der Datenquelle' angegebenen Benutzer erstellt wird.

Standardwert

API_SECRET_DS

Related information

Sicherheitsframework für Unica-APIs *(on page 265)*

Unica Platform | Sicherheit | API management | [Produkt] | Unica Platform | Anmeldung

(Affinium|suite|security|apiSecurity|manager|managerLogin) Verwenden Sie die Vorlagen in dieser Kategorie, um die Authentifizierung für Unica APIs zu konfigurieren. Sie können den Zugriff blockieren oder HTTPS oder die Authentifizierung für APIs als erforderlich festlegen.

API-URI

Beschreibung

Für jedes Produkt wird der erste Teil des URI durch den Sicherheitsrahmen wie folgt aufgelöst: `http[s]://host:port/context root/api/product`

Deshalb sollten Sie in diesem Feld nur die Ressourcennamen der zu konfigurierenden API eingeben. Die einzugebende Zeichenfolge finden Sie in der API-Dokumentation des Produkts.

Der für diese Eigenschaft verwendete Wert muss mit einem / (Schrägstrich) beginnen, andernfalls wird die Konfiguration vom Sicherheitsframework ignoriert.

Diese Eigenschaft unterstützt sowohl die exakte URL-Übereinstimmung als auch die Musterübereinstimmung für die konfigurierten APIs.

- Für die exakte Übereinstimmung kann die URI mit einem Schrägstrich (/) oder dem Ressourcennamen enden.
- Für die Musterübereinstimmung muss die URI mit einem Stern (*) enden.

Wenn Sie den Wert dieser Eigenschaft auf `/*` festlegen, werden die Einstellungen, die Sie für andere Einstellungen in dieser Kategorie verwenden, auf alle APIs des Produkts angewendet.

Note: Bei der API Unica Platform `login` ist diese Konfigurationseigenschaft schreibgeschützt.

Standardwert

/authentication/v1/login

API-Zugriff blockieren

Beschreibung

Wählen Sie diese Option aus, wenn Sie eine API daran hindern möchten, auf ein Produkt zuzugreifen. Diese Option ist standardmäßig nicht ausgewählt.

Wenn eine API geblockt ist, gibt der Sicherheitsfilter den HTTP-Statuscode 403 (unzulässig) zurück.

Standardwert

(Deaktiviert)

Sicherer API-Zugriff über HTTPS

Beschreibung

Wählen Sie diese Option aus, wenn Sie einer API den Zugriff auf ein Produkt nur über HTTPS ermöglichen möchten. Diese Option ist standardmäßig ausgewählt.

Wenn auf eine API, bei der diese Eigenschaft aktiviert ist, über HTTP statt HTTPS zugegriffen wird, gibt der Sicherheitsfilter den HTTP-Statuscode 403 (unzulässig) zurück.

Standardwert

(Deaktiviert)

Authentifizierung für API-Zugriff erfordern

Beschreibung

Wählen Sie diese Option aus, wenn Sie als erforderlich festlegen möchten, dass eine API authentifiziert wird, bevor sie auf ein Produkt zugreifen kann. Diese Option ist standardmäßig ausgewählt.

Wenn auf eine API, bei der diese Eigenschaft aktiviert ist, mit ungültigen Berechtigungsnachweisen zugegriffen wird, gibt der Sicherheitsfilter den HTTP-Statuscode 401 (nicht berechtigt) zurück.

Note: Bei der API Unica Platform `login` ist diese Konfigurationseigenschaft deaktiviert, da diese API als erste für die API Authentifizierung aufgerufen wird.

Standardwert

(Deaktiviert)

Authentifizierungsmodus

Beschreibung

Wählen Sie diese Option aus, wenn Sie die API mit Standardauthentifizierung oder Bearer-Token Authentifizierung authentifizieren möchten. Wird die Option Basisauthentifizierung oder Bearer-Token ausgewählt, müssen die entsprechende Benutzer-ID und Passwort in der Datenquelle des Benutzers verwaltet werden. Für den Authentifizierungsmodus Manager verhält es sich genauso, wenn der Parameter `api_auth_mode = Manager` im Anforderungsheader verwendet wird. Diese Dropdown-Auswahl ist gültig nur wenn 'Authentifizierung für API Zugriff erforderlich' ausgewählt wird.

Standardwert

Manager

Berechtigungsinhaber der Datenquelle

Beschreibung

Geben Sie den Benutzernamen an, der die Datenquelle mit den erforderlichen Authentifizierungsdaten enthält. Die Datenquelle enthält die Benutzer ID und das Passwort bei der Auswahl von Standardauthentifizierung in der Dropdown-Liste vom Authentifizierungsmodus. Die Datenquelle enthält

Bearer-Token bei der Auswahl von Bearer-Token in der Dropdown-Liste vom Authentifizierungsmodus.

Standardwert

asm_admin

Datenquelle

Beschreibung

Geben Sie den Namen der Datenquelle an, der unter dem in dem Feld 'Berechtigungsinhaber der Datenquelle' angegebenen Benutzer erstellt wird.

Standardwert

API_SECRET_DS

Related information

Sicherheitsframework für Unica-APIs *(on page 265)*

Unica Platform | Sicherheit | API management | [Produkt] | Unica Marketing Campaign | Interact Collection

(Affinium|suite|security|apiSecurity|campaign|Interact Collection) Verwenden Sie die Vorlagen in dieser Kategorie, um die Authentifizierung für Unica APIs zu konfigurieren. Sie können den Zugriff blockieren oder HTTPS oder die Authentifizierung für APIs als erforderlich festlegen.

API-URI

Beschreibung

Für jedes Produkt wird der erste Teil des URI durch den Sicherheitsrahmen wie folgt aufgelöst: `http[s]://host:port/context root/api/product`

Deshalb sollten Sie in diesem Feld nur die Ressourcennamen der zu konfigurierenden API eingeben. Die einzugebende Zeichenfolge finden Sie in der API-Dokumentation des Produkts.

Der für diese Eigenschaft verwendete Wert muss mit einem / (Schrägstrich) beginnen, andernfalls wird die Konfiguration vom Sicherheitsframework ignoriert.

Diese Eigenschaft unterstützt sowohl die exakte URL-Übereinstimmung als auch die Musterübereinstimmung für die konfigurierten APIs.

- Für die exakte Übereinstimmung kann die URI mit einem Schrägstrich (/) oder dem Ressourcennamen enden.
- Für die Musterübereinstimmung muss die URI mit einem Stern (*) enden.

Wenn Sie den Wert dieser Eigenschaft auf `/*` festlegen, werden die Einstellungen, die Sie für andere Einstellungen in dieser Kategorie verwenden, auf alle APIs des Produkts angewendet.

Note: Bei der API Unica Platform `login` ist diese Konfigurationseigenschaft schreibgeschützt.

Standardwert

/rest/v1/interactCollection/*

API-Zugriff blockieren

Beschreibung

Wählen Sie diese Option aus, wenn Sie eine API daran hindern möchten, auf ein Produkt zuzugreifen. Diese Option ist standardmäßig nicht ausgewählt.

Wenn eine API geblockt ist, gibt der Sicherheitsfilter den HTTP-Statuscode 403 (unzulässig) zurück.

Standardwert

(Deaktiviert)

Sicherer API-Zugriff über HTTPS

Beschreibung

Wählen Sie diese Option aus, wenn Sie einer API den Zugriff auf ein Produkt nur über HTTPS ermöglichen möchten. Diese Option ist standardmäßig ausgewählt.

Wenn auf eine API, bei der diese Eigenschaft aktiviert ist, über HTTP statt HTTPS zugegriffen wird, gibt der Sicherheitsfilter den HTTP-Statuscode 403 (unzulässig) zurück.

Standardwert

(Deaktiviert)

Authentifizierung für API-Zugriff erfordern

Beschreibung

Wählen Sie diese Option aus, wenn Sie als erforderlich festlegen möchten, dass eine API authentifiziert wird, bevor sie auf ein Produkt zugreifen kann. Diese Option ist standardmäßig ausgewählt.

Wenn auf eine API, bei der diese Eigenschaft aktiviert ist, mit ungültigen Berechtigungsnachweisen zugegriffen wird, gibt der Sicherheitsfilter den HTTP-Statuscode 401 (nicht berechtigt) zurück.

Note: Bei der API Unica Platform `login` ist diese Konfigurationseigenschaft deaktiviert, da diese API als erste für die API Authentifizierung aufgerufen wird.

Standardwert

(Deaktiviert)

Authentifizierungsmodus

Beschreibung

Wählen Sie diese Option aus, wenn Sie die API mit Standardauthentifizierung oder Bearer-Token Authentifizierung authentifizieren möchten. Wird die Option Basisauthentifizierung oder Bearer-Token ausgewählt, müssen die entsprechende Benutzer-ID und Passwort in der Datenquelle des Benutzers verwaltet werden. Für den Authentifizierungsmodus Manager verhält es sich genauso, wenn der Parameter `api_auth_mode = Manager` im Anforderungsheader verwendet wird. Diese Dropdown-Auswahl ist gültig nur wenn 'Authentifizierung für API Zugriff erforderlich' ausgewählt wird.

Standardwert

Manager

Berechtigungsinhaber der Datenquelle

Beschreibung

Geben Sie den Benutzernamen an, der die Datenquelle mit den erforderlichen Authentifizierungsdaten enthält. Die Datenquelle enthält die Benutzer ID und das Passwort bei der Auswahl von Standardauthentifizierung in der Dropdown-Liste vom Authentifizierungsmodus. Die Datenquelle enthält Bearer-Token bei der Auswahl von Bearer-Token in der Dropdown-Liste vom Authentifizierungsmodus.

Standardwert

asm_admin

Datenquelle

Beschreibung

Geben Sie den Namen der Datenquelle an, der unter dem in dem Feld 'Berechtigungsinhaber der Datenquelle' angegebenen Benutzer erstellt wird.

Standardwert

API_SECRET_DS

Related information

Sicherheitsframework für Unica-APIs *(on page 265)*

Unica Platform | Sicherheit | API management | [Produkt] | Unica Marketing Campaign | Ausgelöste Nachrichten

(Affinium|suite|security|apiSecurity|campaign|Interact Collection) Verwenden Sie die Vorlagen in dieser Kategorie, um die Authentifizierung für Unica APIs zu konfigurieren. Sie können den Zugriff blockieren oder HTTPS oder die Authentifizierung für APIs als erforderlich festlegen.

API-URI

Beschreibung

Für jedes Produkt wird der erste Teil des URI durch den Sicherheitsrahmen wie folgt aufgelöst: `http[s]://host:port/context root/api/product`

Deshalb sollten Sie in diesem Feld nur die Ressourcennamen der zu konfigurierenden API eingeben. Die einzugebende Zeichenfolge finden Sie in der API-Dokumentation des Produkts.

Der für diese Eigenschaft verwendete Wert muss mit einem / (Schrägstrich) beginnen, andernfalls wird die Konfiguration vom Sicherheitsframework ignoriert.

Diese Eigenschaft unterstützt sowohl die exakte URL-Übereinstimmung als auch die Musterübereinstimmung für die konfigurierten APIs.

- Für die exakte Übereinstimmung kann die URI mit einem Schrägstrich (/) oder dem Ressourcennamen enden.
- Für die Musterübereinstimmung muss die URI mit einem Stern (*) enden.

Wenn Sie den Wert dieser Eigenschaft auf `/*` festlegen, werden die Einstellungen, die Sie für andere Einstellungen in dieser Kategorie verwenden, auf alle APIs des Produkts angewendet.

Note: Bei der API Unica Platform `login` ist diese Konfigurationseigenschaft schreibgeschützt.

Standardwert

/rest/v1/triggeredMessages/*

API-Zugriff blockieren

Beschreibung

Wählen Sie diese Option aus, wenn Sie eine API daran hindern möchten, auf ein Produkt zuzugreifen. Diese Option ist standardmäßig nicht ausgewählt.

Wenn eine API geblockt ist, gibt der Sicherheitsfilter den HTTP-Statuscode 403 (unzulässig) zurück.

Standardwert

(Deaktiviert)

Sicherer API-Zugriff über HTTPS

Beschreibung

Wählen Sie diese Option aus, wenn Sie einer API den Zugriff auf ein Produkt nur über HTTPS ermöglichen möchten. Diese Option ist standardmäßig ausgewählt.

Wenn auf eine API, bei der diese Eigenschaft aktiviert ist, über HTTP statt HTTPS zugegriffen wird, gibt der Sicherheitsfilter den HTTP-Statuscode 403 (unzulässig) zurück.

Standardwert

(Deaktiviert)

Authentifizierung für API-Zugriff erfordern

Beschreibung

Wählen Sie diese Option aus, wenn Sie als erforderlich festlegen möchten, dass eine API authentifiziert wird, bevor sie auf ein Produkt zugreifen kann. Diese Option ist standardmäßig ausgewählt.

Wenn auf eine API, bei der diese Eigenschaft aktiviert ist, mit ungültigen Berechtigungsnachweisen zugegriffen wird, gibt der Sicherheitsfilter den HTTP-Statuscode 401 (nicht berechtigt) zurück.

Note: Bei der API Unica Platform `login` ist diese Konfigurationseigenschaft deaktiviert, da diese API als erste für die API Authentifizierung aufgerufen wird.

Standardwert

(Deaktiviert)

Authentifizierungsmodus

Beschreibung

Wählen Sie diese Option aus, wenn Sie die API mit Standardauthentifizierung oder Bearer-Token Authentifizierung authentifizieren möchten. Wird die Option Basisauthentifizierung oder Bearer-Token ausgewählt, müssen die entsprechende Benutzer-ID und Passwort in der Datenquelle des Benutzers verwaltet werden. Für den Authentifizierungsmodus Manager verhält es sich genauso, wenn der Parameter `api_auth_mode = Manager` im Anforderungsheader verwendet wird. Diese Dropdown-Auswahl ist gültig nur wenn 'Authentifizierung für API Zugriff erforderlich' ausgewählt wird.

Standardwert

Manager

Berechtigungsinhaber der Datenquelle

Beschreibung

Geben Sie den Benutzernamen an, der die Datenquelle mit den erforderlichen Authentifizierungsdaten enthält. Die Datenquelle enthält die Benutzer ID und das Passwort bei der Auswahl von Standardauthentifizierung in der Dropdown-Liste vom Authentifizierungsmodus. Die Datenquelle enthält Bearer-Token bei der Auswahl von Bearer-Token in der Dropdown-Liste vom Authentifizierungsmodus.

Standardwert

asm_admin

Datenquelle

Beschreibung

Geben Sie den Namen der Datenquelle an, der unter dem in dem Feld 'Berechtigungsinhaber der Datenquelle' angegebenen Benutzer erstellt wird.

Standardwert

API_SECRET_DS

Related information

Sicherheitsframework für Unica-APIs *(on page 265)*

Unica Platform | Sicherheit | API management | [Produkt] | Unica Marketing Campaign | Campaign REST API Filter

(Affinium|suite|security|apiSecurity|campaign|Campaign REST API Filter) Verwenden Sie die Vorlagen in dieser Kategorie, um die Authentifizierung für Unica APIs zu konfigurieren. Sie können den Zugriff blockieren oder HTTPS oder die Authentifizierung für APIs als erforderlich festlegen.

API-URI

Beschreibung

Für jedes Produkt wird der erste Teil des URI durch den Sicherheitsrahmen wie folgt aufgelöst: `http[s]://host:port/context root/api/product`

Deshalb sollten Sie in diesem Feld nur die Ressourcennamen der zu konfigurierenden API eingeben. Die einzugebende Zeichenfolge finden Sie in der API-Dokumentation des Produkts.

Der für diese Eigenschaft verwendete Wert muss mit einem / (Schrägstrich) beginnen, andernfalls wird die Konfiguration vom Sicherheitsframework ignoriert.

Diese Eigenschaft unterstützt sowohl die exakte URL-Übereinstimmung als auch die Musterübereinstimmung für die konfigurierten APIs.

- Für die exakte Übereinstimmung kann die URI mit einem Schrägstrich (/) oder dem Ressourcennamen enden.
- Für die Musterübereinstimmung muss die URI mit einem Stern (*) enden.

Wenn Sie den Wert dieser Eigenschaft auf `/*` festlegen, werden die Einstellungen, die Sie für andere Einstellungen in dieser Kategorie verwenden, auf alle APIs des Produkts angewendet.

Note: Bei der API Unica Platform `login` ist diese Konfigurationseigenschaft schreibgeschützt.

Standardwert

/rest/v1/*

API-Zugriff blockieren

Beschreibung

Wählen Sie diese Option aus, wenn Sie eine API daran hindern möchten, auf ein Produkt zuzugreifen. Diese Option ist standardmäßig nicht ausgewählt.

Wenn eine API geblockt ist, gibt der Sicherheitsfilter den HTTP-Statuscode 403 (unzulässig) zurück.

Standardwert

(Deaktiviert)

Sicherer API-Zugriff über HTTPS

Beschreibung

Wählen Sie diese Option aus, wenn Sie einer API den Zugriff auf ein Produkt nur über HTTPS ermöglichen möchten. Diese Option ist standardmäßig ausgewählt.

Wenn auf eine API, bei der diese Eigenschaft aktiviert ist, über HTTP statt HTTPS zugegriffen wird, gibt der Sicherheitsfilter den HTTP-Statuscode 403 (unzulässig) zurück.

Standardwert

(Deaktiviert)

Authentifizierung für API-Zugriff erfordern

Beschreibung

Wählen Sie diese Option aus, wenn Sie als erforderlich festlegen möchten, dass eine API authentifiziert wird, bevor sie auf ein Produkt zugreifen kann. Diese Option ist standardmäßig ausgewählt.

Wenn auf eine API, bei der diese Eigenschaft aktiviert ist, mit ungültigen Berechtigungsnachweisen zugegriffen wird, gibt der Sicherheitsfilter den HTTP-Statuscode 401 (nicht berechtigt) zurück.

Note: Bei der API Unica Platform `login` ist diese Konfigurationseigenschaft deaktiviert, da diese API als erste für die API Authentifizierung aufgerufen wird.

Standardwert

(Aktiviert)

Authentifizierungsmodus

Beschreibung

Wählen Sie diese Option aus, wenn Sie die API mit Standardauthentifizierung oder Bearer-Token Authentifizierung authentifizieren möchten. Wird die Option Basisauthentifizierung oder Bearer-Token ausgewählt, müssen die entsprechende Benutzer-ID und Passwort in der Datenquelle des Benutzers verwaltet werden. Für den Authentifizierungsmodus Manager verhält es sich genauso, wenn der Parameter `api_auth_mode = Manager` im Anforderungsheader verwendet wird. Diese Dropdown-Auswahl ist gültig nur wenn 'Authentifizierung für API Zugriff erforderlich' ausgewählt wird.

Standardwert

Manager

Berechtigungsinhaber der Datenquelle

Beschreibung

Geben Sie den Benutzernamen an, der die Datenquelle mit den erforderlichen Authentifizierungsdaten enthält. Die Datenquelle enthält die Benutzer ID und das Passwort bei der Auswahl von Standardauthentifizierung in der Dropdown-Liste vom Authentifizierungsmodus. Die Datenquelle enthält Bearer-Token bei der Auswahl von Bearer-Token in der Dropdown-Liste vom Authentifizierungsmodus.

Standardwert

asm_admin

Datenquelle

Beschreibung

Geben Sie den Namen der Datenquelle an, der unter dem in dem Feld 'Berechtigungsinhaber der Datenquelle' angegebenen Benutzer erstellt wird.

Standardwert

API_SECRET_DS

Related information

Sicherheitsframework für Unica-APIs *(on page 265)*

Unica Platform | Sicherheit | API management | [Produkt] | Unica Marketing Campaign | Engage REST API Filter

(Affinium|suite|security|apiSecurity|campaign|Engage REST API Filter) Verwenden Sie die Vorlagen in dieser Kategorie, um die Authentifizierung für Unica APIs zu konfigurieren. Sie können den Zugriff blockieren oder HTTPS oder die Authentifizierung für APIs als erforderlich festlegen.

API-URI

Beschreibung

Für jedes Produkt wird der erste Teil des URI durch den Sicherheitsrahmen wie folgt aufgelöst: `http[s]://host:port/context root/api/product`

Deshalb sollten Sie in diesem Feld nur die Ressourcennamen der zu konfigurierenden API eingeben. Die einzugebende Zeichenfolge finden Sie in der API-Dokumentation des Produkts.

Der für diese Eigenschaft verwendete Wert muss mit einem / (Schrägstrich) beginnen, andernfalls wird die Konfiguration vom Sicherheitsframework ignoriert.

Diese Eigenschaft unterstützt sowohl die exakte URL-Übereinstimmung als auch die Musterübereinstimmung für die konfigurierten APIs.

- Für die exakte Übereinstimmung kann die URI mit einem Schrägstrich (/) oder dem Ressourcennamen enden.
- Für die Musterübereinstimmung muss die URI mit einem Stern (*) enden.

Wenn Sie den Wert dieser Eigenschaft auf `/*` festlegen, werden die Einstellungen, die Sie für andere Einstellungen in dieser Kategorie verwenden, auf alle APIs des Produkts angewendet.

Note: Bei der API Unica Platform `login` ist diese Konfigurationseigenschaft schreibgeschützt.

Standardwert

/rest/engage/*

API-Zugriff blockieren

Beschreibung

Wählen Sie diese Option aus, wenn Sie eine API daran hindern möchten, auf ein Produkt zuzugreifen. Diese Option ist standardmäßig nicht ausgewählt.

Wenn eine API geblockt ist, gibt der Sicherheitsfilter den HTTP-Statuscode 403 (unzulässig) zurück.

Standardwert

(Deaktiviert)

Sicherer API-Zugriff über HTTPS

Beschreibung

Wählen Sie diese Option aus, wenn Sie einer API den Zugriff auf ein Produkt nur über HTTPS ermöglichen möchten. Diese Option ist standardmäßig ausgewählt.

Wenn auf eine API, bei der diese Eigenschaft aktiviert ist, über HTTP statt HTTPS zugegriffen wird, gibt der Sicherheitsfilter den HTTP-Statuscode 403 (unzulässig) zurück.

Standardwert

(Deaktiviert)

Authentifizierung für API-Zugriff erfordern

Beschreibung

Wählen Sie diese Option aus, wenn Sie als erforderlich festlegen möchten, dass eine API authentifiziert wird, bevor sie auf ein Produkt zugreifen kann. Diese Option ist standardmäßig ausgewählt.

Wenn auf eine API, bei der diese Eigenschaft aktiviert ist, mit ungültigen Berechtigungsnachweisen zugegriffen wird, gibt der Sicherheitsfilter den HTTP-Statuscode 401 (nicht berechtigt) zurück.

Note: Bei der API Unica Platform `login` ist diese Konfigurationseigenschaft deaktiviert, da diese API als erste für die API Authentifizierung aufgerufen wird.

Standardwert

(Deaktiviert)

Authentifizierungsmodus

Beschreibung

Wählen Sie diese Option aus, wenn Sie die API mit Standardauthentifizierung oder Bearer-Token Authentifizierung authentifizieren möchten. Wird die Option Basisauthentifizierung oder Bearer-Token ausgewählt, müssen die entsprechende Benutzer-ID und Passwort in der Datenquelle des Benutzers verwaltet werden. Für den Authentifizierungsmodus Manager verhält es sich genauso, wenn der Parameter `api_auth_mode = Manager` im

Anforderungsheader verwendet wird. Diese Dropdown-Auswahl ist gültig nur wenn 'Authentifizierung für API Zugriff erforderlich' ausgewählt wird.

Standardwert

Manager

Berechtigungsinhaber der Datenquelle

Beschreibung

Geben Sie den Benutzernamen an, der die Datenquelle mit den erforderlichen Authentifizierungsdaten enthält. Die Datenquelle enthält die Benutzer ID und das Passwort bei der Auswahl von Standardauthentifizierung in der Dropdown-Liste vom Authentifizierungsmodus. Die Datenquelle enthält Bearer-Token bei der Auswahl von Bearer-Token in der Dropdown-Liste vom Authentifizierungsmodus.

Standardwert

asm_admin

Datenquelle

Beschreibung

Geben Sie den Namen der Datenquelle an, der unter dem in dem Feld 'Berechtigungsinhaber der Datenquelle' angegebenen Benutzer erstellt wird.

Standardwert

API_SECRET_DS

Related information

Sicherheitsframework für Unica-APIs *(on page 265)*

Unica Platform | Sicherheit | API management | [Produkt] | Unica Marketing Campaign | Campaign REST API V2 Filter

(Affinium|suite|security|apiSecurity|campaign|Campaign REST API V2 Filter) Verwenden Sie die Vorlagen in dieser Kategorie, um die Authentifizierung für Unica APIs zu konfigurieren. Sie können den Zugriff blockieren oder HTTPS oder die Authentifizierung für APIs als erforderlich festlegen.

API-URI

Beschreibung

Für jedes Produkt wird der erste Teil des URI durch den Sicherheitsrahmen wie folgt aufgelöst: `http[s]://host:port/context root/api/product`

Deshalb sollten Sie in diesem Feld nur die Ressourcennamen der zu konfigurierenden API eingeben. Die einzugebende Zeichenfolge finden Sie in der API-Dokumentation des Produkts.

Der für diese Eigenschaft verwendete Wert muss mit einem / (Schrägstrich) beginnen, andernfalls wird die Konfiguration vom Sicherheitsframework ignoriert.

Diese Eigenschaft unterstützt sowohl die exakte URL-Übereinstimmung als auch die Musterübereinstimmung für die konfigurierten APIs.

- Für die exakte Übereinstimmung kann die URI mit einem Schrägstrich (/) oder dem Ressourcennamen enden.
- Für die Musterübereinstimmung muss die URI mit einem Stern (*) enden.

Wenn Sie den Wert dieser Eigenschaft auf `/*` festlegen, werden die Einstellungen, die Sie für andere Einstellungen in dieser Kategorie verwenden, auf alle APIs des Produkts angewendet.

Note: Bei der API Unica Platform `login` ist diese Konfigurationseigenschaft schreibgeschützt.

Standardwert

/rest/v2/*

API-Zugriff blockieren

Beschreibung

Wählen Sie diese Option aus, wenn Sie eine API daran hindern möchten, auf ein Produkt zuzugreifen. Diese Option ist standardmäßig nicht ausgewählt.

Wenn eine API geblockt ist, gibt der Sicherheitsfilter den HTTP-Statuscode 403 (unzulässig) zurück.

Standardwert

(Deaktiviert)

Sicherer API-Zugriff über HTTPS

Beschreibung

Wählen Sie diese Option aus, wenn Sie einer API den Zugriff auf ein Produkt nur über HTTPS ermöglichen möchten. Diese Option ist standardmäßig ausgewählt.

Wenn auf eine API, bei der diese Eigenschaft aktiviert ist, über HTTP statt HTTPS zugegriffen wird, gibt der Sicherheitsfilter den HTTP-Statuscode 403 (unzulässig) zurück.

Standardwert

(Deaktiviert)

Authentifizierung für API-Zugriff erfordern

Beschreibung

Wählen Sie diese Option aus, wenn Sie als erforderlich festlegen möchten, dass eine API authentifiziert wird, bevor sie auf ein Produkt zugreifen kann. Diese Option ist standardmäßig ausgewählt.

Wenn auf eine API, bei der diese Eigenschaft aktiviert ist, mit ungültigen Berechtigungsnachweisen zugegriffen wird, gibt der Sicherheitsfilter den HTTP-Statuscode 401 (nicht berechtigt) zurück.

Note: Bei der API Unica Platform `login` ist diese Konfigurationseigenschaft deaktiviert, da diese API als erste für die API Authentifizierung aufgerufen wird.

Standardwert

(Aktiviert)

Authentifizierungsmodus

Beschreibung

Wählen Sie diese Option aus, wenn Sie die API mit Standardauthentifizierung oder Bearer-Token Authentifizierung authentifizieren möchten. Wird die Option Basisauthentifizierung oder Bearer-Token ausgewählt, müssen die entsprechende Benutzer-ID und Passwort in der Datenquelle des Benutzers verwaltet werden. Für den Authentifizierungsmodus Manager verhält es sich genauso, wenn der Parameter `api_auth_mode = Manager` im Anforderungsheader verwendet wird. Diese Dropdown-Auswahl ist gültig nur wenn 'Authentifizierung für API Zugriff erforderlich' ausgewählt wird.

Standardwert

Manager

Berechtigungsinhaber der Datenquelle

Beschreibung

Geben Sie den Benutzernamen an, der die Datenquelle mit den erforderlichen Authentifizierungsdaten enthält. Die Datenquelle enthält die Benutzer ID und das Passwort bei der Auswahl von Standardauthentifizierung in der Dropdown-Liste vom Authentifizierungsmodus. Die Datenquelle enthält

Bearer-Token bei der Auswahl von Bearer-Token in der Dropdown-Liste vom Authentifizierungsmodus.

Standardwert

asm_admin

Datenquelle

Beschreibung

Geben Sie den Namen der Datenquelle an, der unter dem in dem Feld 'Berechtigungsinhaber der Datenquelle' angegebenen Benutzer erstellt wird.

Standardwert

API_SECRET_DS

Related information

Sicherheitsframework für Unica-APIs *(on page 265)*

Platform | Sicherheit | JWT Authentifizierung

Die JWT-Authentifizierung wird für Journey Designer und Unica Campaign verwendet. Die JWT-Authentifizierung ermöglicht ein Single Sign-on zwischen Anwendungen.

JWT-Authentifizierung aktivieren

Beschreibung

Wenn das Kontrollkästchen für diese Eigenschaft ausgewählt wurde, dann wird die JWT-Authentifizierung aktiviert.

Diese Eigenschaft gilt nur in Umgebungen, bei denen Journey Designer in Unica Campaign integriert ist.

Standardwert

`inaktiviert`

JWT-Service-URL

Beschreibung

Die URL für den JWT-Service. Dieser Wert unterscheidet sich je nachdem, ob Sie Unica Platform FixPack 10.0.0.1 angewendet haben. Beachten Sie dazu die folgenden Beispiele.

- Wenn Sie FixPack 10.0.0.1 **nicht** angewendet haben:

  `http://IP_ADDRESS/jwt/api/v1/tokens`
- Wenn Sie FixPack 10.0.0.1 angewendet haben:

  `http://IP_ADDRESS/api/v1/keys`

Diese Eigenschaft gilt nur in Umgebungen, bei denen Journey Designer in Unica Campaign integriert ist.

Geheimer Schlüssel für JWT

Beschreibung

Der geheime Schlüssel für die gemeinsame Nutzung wird von Unica Platform zur Authentifizierung an den JWT-Service gesendet. Dieser Schlüssel wird von Unica Platform und Journey Designer gemeinsam genutzt. Der JWT-Aussteller wird dem geheimen JWT-Schlüssel für die gemeinsame Nutzung im JWT-Service zugeordnet.

Diese Eigenschaft gilt nur in Umgebungen, bei denen Journey Designer mit Unica Campaign integriert ist und bei denen Unica Platform Version 10.0.0.0 installiert ist (dort wird Unica Platform FixPack 10.0.0.1 **nicht** angewendet).

JWT-Aussteller

Beschreibung

Der Name des Ausstellers und die Version, die von Unica Platform zur Authentifizierung an den JWT-Service gesendet wird.

Diese Eigenschaft gilt nur in Umgebungen, bei denen Journey Designer in Unica Campaign integriert ist.

Platform | Benachrichtigungen

Eigenschaften in dieser Kategorie steuern das Verhalten des Systems für Benachrichtigungen, die Unica-Produkte an Benutzer senden können.

Aufbewahrungszeitraum für Benachrichtigungen (in Tagen)

Beschreibung

Gibt die Zeitspanne in Tagen an, die ein Systemalert zu Archivierungszwecken nach seinem Ablaufdatum, das von der Anwendung bereitgestellt wird, die den Alert gesendet hat, aufbewahrt wird. Alerts, die älter sind als die vorgegebene Anzahl von Tagen, werden aus dem System gelöscht.

Standardwert

`90`

Sendeintervall für E-Mails (in Minuten)

Beschreibung

Gibt an, wie viele Minuten das System wartet, bis neue Benachrichtigungs-E-Mails gesendet werden.

Standardwert

`30`

Max. Sendeversuche für E-Mail

Beschreibung

Gibt an, wie oft das System versucht, Benachrichtigungs-E-Mails zu senden, wenn der erste Sendeversuch fehlschlägt.

Standardwert

`1`

Platform | Prüfereignisse

Die Eigenschaft auf dieser Seite legt fest, ob Prüfereignisse verfolgt werden.

Ist Ereignisprüfung aktiviert?

Beschreibung

Gibt an, ob Prüfereignisse aktiviert sind.

Standardwert

`Falsch`

Gültige Werte

`True | False`

Platform | Prüfereignisse | Konfiguration der Prüfereignisse

Die auf dieser Seite ausgewählten Ereignisse sind in den Sicherheitsprüfungsberichten verfügbar.

An- und Abmeldeereignisse für alle Konten erfassen

Beschreibung

Gibt an, ob der Benutzername und das Datum und die Uhrzeit für An- und Abmeldeereignisse für alle Benutzerkonten verfolgt werden.

Überschreiten des Zeitlimits von Benutzersitzungen bei allen Konten erfassen

Beschreibung

Gibt an, ob der Kontobenutzername und das Datum und die Uhrzeit von Sitzungen überwacht werden, bei denen automatisch das zulässige Zeitlimit überschritten wurde.

An- und Abmeldeereignisse für Mitglieder der Gruppe "HighSeverityAccounts" erfassen

Beschreibung

Gibt an, ob der Benutzername und das Datum und die Uhrzeit für An- und Abmeldeereignisse für Konten überwacht werden, die in Unica Platform Mitglieder der Gruppe **highSeverityAccounts** sind. Um dieses

Feature zu aktivieren, müssen Sie eine Bewertungsebene für diese Konfigurationseigenschaft festlegen und der Gruppe highSeverityAccounts Benutzer hinzufügen.

Änderungen bei der Zugehörigkeit zur LDAP-Gruppe erfassen

Beschreibung

Gibt an, ob das Hinzufügen oder Löschen von Konten zusammen mit den Benutzernamen und dem Datum und der Uhrzeit dieser Aktionen für Benutzerkonten aufgezeichnet werden, die von einem LDAP-Server synchronisiert werden. Diese Eigenschaft ist nur gültig, wenn Unica Platform mit einem unterstützten LDAP-Server wie beispielsweise einem HCL Security Directory-Server oder Windows™ Active Directory integriert ist.

Aktivieren und Inaktivieren von Konten erfassen

Beschreibung

Gibt an, ob der Kontobenutzername und das Datum und die Uhrzeit des Aktivierens oder Inaktivierens von Benutzerkonten aufgezeichnet werden sollen.

Änderungen der Kontokennwörter erfassen

Beschreibung

Gibt an, ob der Kontobenutzername und das Datum und die Uhrzeit des Änderns von Kennwörtern aufgezeichnet werden sollen.

Sperrung der Kontokennwörter erfassen

Beschreibung

Gibt an, ob der Kontobenutzername und das Datum und die Uhrzeit des Sperrens eines Kennworts aufgrund von zu vielen Anmeldeversuchen aufgezeichnet werden sollen.

Erstellen und Löschen von Gruppen in Platform erfassen

Beschreibung

Gibt an, ob aufgezeichnet werden soll, wenn Gruppen hinzugefügt oder gelöscht werden.

Änderungen bei der Gruppenzugehörigkeit in Platform erfassen

Beschreibung

Gibt an, ob aufgezeichnet werden soll, wenn Benutzerkonten einer Gruppe hinzugefügt oder aus einer Gruppe entfernt werden.

Änderungen bei der Gruppenzugehörigkeit in Platform erfassen

Beschreibung

Gibt an, ob Änderungen an den Gruppenberechtigungen aufgezeichnet werden sollen.

Erstellen oder Löschen von Rollen erfassen

Beschreibung

Gibt an, ob aufgezeichnet werden soll, wenn Rollen hinzugefügt oder gelöscht werden. Es werden nur Rollen überwacht, die auf der Seite **Einstellungen > Benutzerrollen und Berechtigungen** gezeigt werden.

Änderungen der Rollenzugehörigkeit erfassen

Beschreibung

Gibt an, ob Änderungen an Rollenzugehörigkeiten aufgezeichnet werden sollen. Es werden nur Rollen überwacht, die auf der Seite **Einstellungen > Benutzerrollen und Berechtigungen** gezeigt werden.

Änderungen der Rollenberechtigungen erfassen

Beschreibung

Gibt an, ob Änderungen an Rollenberechtigungen aufgezeichnet werden sollen. Es werden nur Rollen überwacht, die auf der Seite **Einstellungen > Benutzerrollen und Berechtigungen** gezeigt werden.

Änderungen der Eigenschaften auf der Konfigurationsseite erfassen

Beschreibung

Gibt an, ob Änderungen an Konfigurationseigenschaften auf der Seite **Einstellungen > Konfiguration** aufgezeichnet werden sollen. Es werden Änderungen durch Benutzer auf der Seite "Konfiguration" und Ausführungen des Tools `configTool` überwacht. Bei einer Installation oder einem Upgrade von Installationsprogrammen vorgenommene Konfigurationsänderungen werden nicht überwacht.

Sicherung der Prüfung aktivieren

Beschreibung

Gibt an, ob Prüfdaten in der Tabelle `USM_AUDIT_BACKUP` gesichert werden sollen.

Wichtig: Da dies eine Bootstrap-Eigenschaft ist, die beim Starten der Unica Platform-Webanwendung gelesen wird, müssen Sie die Unica Platform-Webanwendung stoppen und neu starten, wenn Sie diesen Eigenschaftswert ändern.

Standardwert

`Falsch`

Gültige Werte

`True | False`

Archivieren der Daten nach der hier angegebenen Anzahl an Tagen

Beschreibung

Gibt das Intervall in Tagen zwischen Sicherungen der Prüfung an. Die archivierten Daten werden in der Tabelle `USM_AUDIT_BACKUP` gespeichert Tabelle und können in den Prüfereignisbericht aufgenommen werden, wenn Sie einen benutzerdefinierten Datumsbereich mit Daten aus dem Archiv festlegen.

Wichtig: Da dies eine Bootstrap-Eigenschaft ist, die beim Starten der Unica Platform-Webanwendung gelesen wird, müssen Sie die Unica Platform-Webanwendung stoppen und neu starten, wenn Sie diesen Eigenschaftswert ändern.

Prüfdatensätze für die hier angegebene Anzahl an Tagen im primären Bereich behalten

Beschreibung

Gibt an, wie viele Tage mit Daten in der Tabelle `USM_AUDIT` für den Prüfereignisbericht aufbewahrt werden sollen. Wenn die Standardeinstellungen für den Prüfereignisbericht wirksam sind, werden nur die Daten in der Tabelle `USM_AUDIT` im Bericht gezeigt.

Wichtig: Da dies eine Bootstrap-Eigenschaft ist, die beim Starten der Unica Platform-Webanwendung gelesen wird, müssen Sie die Unica Platform-Webanwendung stoppen und neu starten, wenn Sie diesen Eigenschaftswert ändern.

Archivstartzeit

Beschreibung

Gibt die Uhrzeit an, zu der das System Prüfdaten in ein Archiv verschiebt. Verwenden Sie das 24-Stunden-Format für diesen Wert.

Wichtig: Da dies eine Bootstrap-Eigenschaft ist, die beim Starten der Unica Platform-Webanwendung gelesen wird, müssen Sie die Unica

Platform-Webanwendung stoppen und neu starten, wenn Sie diesen Eigenschaftswert ändern.

Name der die Benachrichtigungen über die Prüfung der Sicherung erhaltenden Gruppe

Beschreibung

Gibt die Unica-Gruppe an, deren Mitglieder eine Benachrichtigung über den Empfang von Archivierungssicherung erhalten müssen. Für diese Eigenschaft kann nur eine einzige Gruppe angegeben werden. Benutzer in dieser Gruppe können ihr Abonnement an dieser Benachrichtigung einrichten, indem Sie auf der Seite **Einstellungen > Benutzer** auf **Benachrichtigungsabonnement** klicken.

Platform | Prüfereignisse | Konfiguration der Priorität von Prüfereignissen

Der Schweregrad, den Sie auf dieser Seite für jedes Ereignis angeben, erscheint im Prüfereignisbericht. Sie können den Schweregrad zum Sortieren und Filtern der Berichtsdaten verwenden. Die Ereignisse sind mit denen in der Kategorie **Platform | Prüfereignisse | Konfiguration der Prüfereignisse** identisch.

Digital Analytics-Konfigurationseigenschaften

Dieser Abschnitt beschreibt die Digital Analytics-Konfigurationseigenschaften, die auf der Seite "Konfiguration" zur Verfügung stehen.

Diese Konfigurationseigenschaften werden zum Konfigurieren einer einmaligen Anmeldung (Single Sign-on; SSO) zwischen Digital Analytics und Unica verwendet. Ausführliche Informationen zu dieser Integration finden Sie im Unica Platform Administratorhandbuch.

Digital Analytics®

Die Eigenschaft in dieser Kategorie ist Teil der Konfiguration zum Aktivieren der einmaligen Anmeldung (Single Sign-on, SSO) zwischen Digital Analytics und Unica.

Coremetrics® Analytics aktivieren

Beschreibung

Dies ist Teil der Konfiguration zum Aktivieren der einmaligen Anmeldung (Single Sign-on; SSO) zwischen Digital Analytics und Unica.

Legen Sie den Wert `true` fest. Dies ist einer der Schritte zum Aktivieren der einmaligen Anmeldung (Single Sign-on, SSO).

Ausführliche Informationen zu dieser Integration finden Sie im Unica Platform Administratorhandbuch.

Standardwert

`false`

Digital Analytics® | Integration | Partitionen | Partition[n]

Eigenschaften in dieser Kategorie sind Teil der Konfiguration zum Aktivieren der einmaligen Anmeldung (Single Sign-on, SSO) zwischen Digital Analytics und Unica.

Platform-Benutzer für Coremetrics®-Konto

Beschreibung

Gibt den Anmeldenamen des Unica-Benutzerkontos an, das den geheimen Digital Analytics-Schlüssel für gemeinsame Nutzung in einer Datenquelle enthält.

Dies ist Teil der Konfiguration zum Aktivieren der einmaligen Anmeldung (Single Sign-on; SSO) zwischen Digital Analytics und Unica. Ausführliche Informationen zu dieser Integration finden Sie im Unica Platform Administratorhandbuch.

Standardwert

`asm_admin`

Datenquelle für Coremetrics®-Konto

Beschreibung

Gibt den Namen der Datenquelle an, die zum Speichern des geheimen Digital Analytics-Schlüssels für gemeinsame Nutzung erstellt wurde.

Dies ist Teil der Konfiguration zum Aktivieren der einmaligen Anmeldung (Single Sign-on; SSO) zwischen Digital Analytics und Unica. Ausführliche Informationen zu dieser Integration finden Sie im Unica Platform Administratorhandbuch.

Standardwert

`CoremetricsDS`

Berichtskonfigurationseigenschaften

Die Berichtskonfigurationseigenschaften für Unica befinden sich unter **Einstellungen > Konfiguration > Berichte**.

Zum Generieren von Berichten wird die Unica-Suite mit Cognos® einer Business-Intelligence-Anwendung, integriert. Verwenden Sie die Eigenschaften **Integrationen > Cognos** zum Ermitteln Ihres Cognos®-Systems. Anschließend müssen Sie für Unica Campaign, Unica Deliver und Unica Interact zusätzliche Eigenschaften konfigurieren, um die Berichtsschemas einzurichten und anzupassen. Weitere Informationen zu den Konfigurationseigenschaften finden Sie im Installations- und Konfigurationshandbuch für Cognos-Berichte.

Unica Plan Konfigurationseinstellungen

Die Konfigurationseigenschaften von Unica Plan sind auf der Seite **Einstellungen > Konfiguration** verfügbar. Für weitere Einzelheiten zu den Konfigurationseigenschaften, siehe Plan Administratorhandbuch.

Unica Campaign Konfigurationseigenschaften

Die Konfigurationseigenschaften für Unica Campaign sind unter **Einstellungen Konfiguration** zu finden. Weitere Details zu den Konfigurationseigenschaften finden Sie im Campaign-Administratorhandbuch.

Unica Deliver Konfigurationseigenschaften

Die Unica Deliver Konfigurationseigenschaften sind auf der Seite "Konfiguration" verfügbar. Weitere Informationen zu den Konfigurationseigenschaften finden Sie im Bereitstellungs- und Administratorhandbuch.

Unica Interact Konfigurationseigenschaften

Die Unica Interact Konfigurationseigenschaften sind auf der Seite "Konfiguration" verfügbar. Weitere Informationen zu den Konfigurationseigenschaften finden Sie im Interact-Administratorhandbuch.

Konfigurationseigenschaften von Unica Journey

Die Unica Journeyintegrations-Konfigurationseigenschaften sind auf der Seite **Einstellungen > Konfiguration** verfügbar. Weitere Informationen zu den Konfigurationseigenschaften finden Sie im Unica Journey-Administratorhandbuch.

Konfigurationseigenschaften von Unica Content Integration

Die Unica Inhaltsteintegrations-Konfigurationseigenschaften sind auf der Seite **Einstellungen > Konfiguration** verfügbar. Einzelheiten zu den Eigenschaften auf der Konfiguration finden Sie im Content Integration-Administratorhandbuch.

Unica Collaborate Konfigurationseigenschaften

Die Unica Collaborateintegrations-Konfigurationseigenschaften sind auf der Seite **Einstellungen > Konfiguration** verfügbar. Weitere Informationen zu den Konfigurationseigenschaften finden Sie im Unica Collaborate-Administratorhandbuch.

Weitere Konfigurationseigenschaften befinden sich in XML-Dateien im Unica Collaborate-Installationsverzeichnis.

IBM SPSS Modeler Advantage Enterprise Marketing Management Edition-Konfigurationseigenschaften

Eigenschaften in dieser Kategorie geben Werte an, die zum Konfigurieren von Unica für die einmalige Anmeldung (Single Sign-on) mit IBM SPSS Modeler Advantage Enterprise Marketing Management Edition verwendet werden.

Vollständige Anweisungen zur Konfiguration der einmaligen Anmeldung mit IBM SPSS Modeler Advantage Enterprise Marketing Management Edition finden Sie im Unica Campaign und IBM SPSS Modeler Advantage Enterprise Marketing Management Edition Integrationshandbuch

SPSS® | integration

Eigenschaften in dieser Kategorie werden für die Konfiguration von Unica Platform für Single Sign-on mit IBM SPSS Modeler Advantage Enterprise Marketing Management Edition verwendet.

Platform-Benutzer für IBM® SPSS®-Konto

Beschreibung

Geben Sie den Anmeldenamen für das IBM SPSS Modeler Advantage Enterprise Marketing Management Edition-Konto ein, das Sie für Single Sign-on mit IBM SPSS Modeler Advantage Enterprise Marketing Management Edition erstellt oder ermittelt haben.

Standardwert

`asm_admin`

Verfügbarkeit

Diese Eigenschaft wird nur für die Konfiguration von Unica Platform für Single Sign-on mit IBM SPSS Modeler Advantage Enterprise Marketing Management Edition verwendet.

Datenquelle für IBM® SPSS®-Konto

Beschreibung

Legen Sie diese Eigenschaft auf den Namen der Datenquelle fest, die Sie für den Systembenutzer erstellt haben, als Sie Single Sign-on mit IBM SPSS Modeler Advantage Enterprise Marketing Management Edition konfiguriert haben. Wenn Sie **SPSS_MA_ADMIN_DS** als Datenquellennamen verwendet haben, können Sie den Standardwert dieser Eigenschaft beibehalten.

Standardwert

SPSS_MA_ADMIN_DS

Verfügbarkeit

Diese Eigenschaft wird nur für die Konfiguration von Unica Platform für Single Sign-on mit IBM SPSS Modeler Advantage Enterprise Marketing Management Edition verwendet.

Ist diese Bewertung nur Integration

Beschreibung

Wird nicht unterstützt.

Standardwert

FALSE

Verfügbarkeit

Diese Eigenschaft wird nur für die Konfiguration von Unica Platform für Single Sign-on mit IBM SPSS Modeler Advantage Enterprise Marketing Management Edition verwendet.

SPSS® | integration | Partitionen | Partition [n]

Die Eigenschaft in dieser Kategorie wird für die Konfiguration von Unica Platform für Single Sign-on mit IBM SPSS Modeler Advantage Enterprise Marketing Management Edition verwendet.

Aktivieren IBM® SPSS®

Beschreibung

Legen Sie diese Eigenschaft auf TRUE fest, um Single Sign-on mit IBM SPSS Modeler Advantage Enterprise Marketing Management Edition zu aktivieren.

Bei jeder Partition, bei der es Benutzer mit Single Sign-on geben sollte, müssen Sie **SPSS MA EMM Edition | Integration | Partitionen | partitionTemplate** verwenden, um die Konfigurationseigenschaft **enableSPSS** für diese Partition zu erstellen. Der Name der mit der Vorlage erstellten Kategorie muss genau dem Namen der entsprechenden Campaign-Partition entsprechen. Da die Standardpartition1 bereits über die Konfigurationseigenschaft **IBM SPSS aktivieren** verfügt, müssen Sie sie nicht mit der Vorlage erstellen.

Standardwert

FALSE

Verfügbarkeit

Diese Eigenschaft wird nur für die Konfiguration von Unica Platform für Single Sign-on mit IBM SPSS Modeler Advantage Enterprise Marketing Management Edition verwendet.

SPSS® | Navigation

Eigenschaften in dieser Kategorie haben Auswirkungen auf die Integration von IBM SPSS Modeler Advantage Enterprise Marketing Management Edition in Unica Campaign. Diese Eigenschaften definieren die Speicherposition des Decision Management-Servers und des IBM SPSS Collaboration and Deployment Services-Servers.

IBM® SPSS® Decision Management-Server-URL

Beschreibung

Die URL des SPSS® Decision Management-Servers. Konfigurieren Sie diese URL mit dem Namen oder der IP-Adresse des Servers gefolgt von dem Port, auf dem IBM SPSS Modeler Advantage Enterprise Marketing Management Edition auf dem Server gehostet wird.

Standardwert

Eines der folgenden Formate:

- `http://<server name>:<port>/DM`
- `http://<server IP address>:<port>/DM`

Gültige Werte

Die URL des SPSS® Decision Management-Servers.

C&DS-Server

Beschreibung

Der Name des IBM SPSS Collaboration and Deployment Services-Servers.

Standardwert

Keine

Gültige Werte

Gültiger Name oder gültige IP-Adresse des Servers, auf dem IBM SPSS Collaboration and Deployment Services installiert und konfiguriert wurde.

C&DS-Port

Beschreibung

Der Port, an dem sich der IBM SPSS Collaboration and Deployment Services-Server befindet.

Standardwert

Keine

Gültige Werte

Gültige Nummer des Ports, auf dem IBM SPSS Collaboration and Deployment Services gehostet wird.

Opportunity Detect und Unica Interact Advanced Patterns - Konfigurationseigenschaften

In diesem Abschnitt werden die Konfigurationseigenschaften von Opportunity Detect und Unica Interact Advanced Patterns auf der Seite 'Konfiguration' beschrieben.

Opportunity Detect und Interact Advanced Patterns | Navigation

Eigenschaften in dieser Kategorie geben Werte an, die intern zum Navigieren zwischen Unica-Produkten verwendet werden.

welcomePageURI

Beschreibung

Der Uniform Resource Identifier (URI) der Opportunity Detect-Indexseite. Dieser Wert wird intern von Unica-Anwendungen verwendet. Das Ändern dieses Werts ist nicht zu empfehlen.

Standardwert

`/index.jsp`

seedName

Beschreibung

Wird intern von Unica-Anwendungen verwendet. Das Ändern dieses Werts ist nicht zu empfehlen.

Standardwert

`Detect`

Typ

Beschreibung

Wird intern von Unica-Anwendungen verwendet. Das Ändern dieses Werts ist nicht zu empfehlen.

Standardwert

`Detect`

httpPort

Beschreibung

Die vom Anwendungsserver verwendete Portnummer für Verbindungen zur Opportunity Detect-Anwendung.

Standardwert

`7001`

httpsPort

Beschreibung

Die vom Anwendungsserver für sichere Verbindungen zur Opportunity Detect-Anwendung verwendete Portnummer.

Standardwert

`7001`

serverURL

Beschreibung

Die URL der Opportunity Detect-Installation. Gültig sind sowohl das HTTP- als auch das HTTPS-Protokoll. Wenn Sie sich in einer Clusterumgebung befinden und vom Standardport `80` oder `443` abweichende Ports für Ihre Bereitstellung verwenden möchten, keine Portnummer im Wert dieser Eigenschaft verwenden.

Wenn Benutzer mit dem Chrome-Browser auf Opportunity Detect zugreifen, dann verwenden Sie den vollständig qualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) in der URL. Der Chrome-Browser kann nicht auf die Produkt-URLs zugreifen, wenn der FQDN nicht verwendet wird.

Wichtig: Wenn UnicaProdukte in einer dezentralen Umgebung installiert werden, müssen Sie für alle Anwendungen der Suite den Namen der Maschine anstatt der IP-Adresse in der Navigations-URL verwenden.

Standardwert

[server-url]

logoutURL

Beschreibung

Intern verwendet. Das Ändern dieses Werts ist nicht zu empfehlen.

Unica Platform verwendet diesen Wert, um den Logout-Handler jeder registrierten Anwendung aufzurufen, wenn der Benutzer auf den Abmeldungslink in Unica klickt.

serverURLInternal

Beschreibung

Intern verwendet. Das Ändern dieses Werts ist nicht zu empfehlen.

displayName

Beschreibung

Intern verwendet. Das Ändern dieses Werts ist nicht zu empfehlen.

Standardwert

```
Opportunity Detect
```

Opportunity Detect und Interact Advanced Patterns | System | Fernsteuerungs-Web-Service Streams

Die Eigenschaft in dieser Kategorie gibt die URL für den Fernsteuerungs-Web-Service InfoSphere Streams an. Opportunity Detect Design Time kommuniziert mit Opportunity Detect Run Time über diesen Service.

ServerURL

Beschreibung

Die Person, die das Produkt installiert, legt diesen Eigenschaftswert während der Installation fest. Die Standardportnummer lautet 8080.

Standardwert

```
http://[SRCSHost]:[SRCSPort]/axis2/services/RemoteControl
```

Opportunity Detect und Interact Advanced Patterns | System | Echtzeit-Verbindung

Die Eigenschaft in dieser Kategorie gibt die URL für den Web-Service an, die benutzt wird, wenn Unica Interact mit Unica Interact Advanced Patterns integriert ist oder wenn der Web-Service-Anschluss für Eingabedaten verwendet wird.

ServerURL

Beschreibung

Die Person, die das Produkt installiert, legt diesen Eigenschaftswert während der Installation fest. Die Standardportnummer lautet 8282.

Standardwert

```
http://[RealTimeConnectorHost]:[RealTimeConnectorPort]/servlets/
StreamServlet
```

Opportunity Detect und Interact Advanced Patterns | System | Überwachung

Eigenschaften in dieser Kategorie geben Werte an, die sich auf das Überwachungstool auswirken.

Abfrageintervall (in Sekunden)

Beschreibung

Die Anzahl der Sekunden, die der Überwachungsservice zwischen zwei aufeinanderfolgenden Abfragen des Streams-Servers für die Statistiken wartet. Der Standardwert ist 300 Sekunden bzw. 5 Minuten.

Standardwert

```
300
```

Speicherzeitraum (in Tagen)

Beschreibung

Die Anzahl der Tage, die der Überwachungsservice die abgefragten Daten in der Datenbank aufbewahrt. Der Standardwert sind 10 Tage. Daten, deren Alter den angegebenen Zeitraum überschreitet, werden gelöscht.

Standardwert

`10`

Opportunity Detect und Interact Advanced Patterns | System | Verarbeitungsoptionen

Eigenschaften in dieser Kategorie geben Werte an, die sich auf das Überwachungstool auswirken.

Cacheprofildatensätze

Beschreibung

Opportunity Detect kann Profildaten im Cache zwischenspeichern, wodurch sich eine optimale Leistung erzielen lässt. Legen Sie den Wert dieser Eigenschaft auf `True` fest, um das Zwischenspeichern von Profildaten im Cache zu aktivieren.

Wenn Sie über sehr umfangreiche Profildatensätze verfügen, möchten Sie den Standardwert dieser Eigenschaft, nämlich `False`, möglicherweise beibehalten. Hierdurch wird das Zwischenspeichern von Profildaten im Cache inaktiviert und die Probleme aufgrund von Speicherengpässen, die durch das Zwischenspeichern großer Mengen von Profildaten im Cache verursacht werden können, werden beseitigt.

Wenn Sie diesen Eigenschaftswert ändern, müssen Sie Ihren Webanwendungsserver, die Streams-Instanz sowie den StreamsRCS-Service neu starten und alle betroffenen Bereitstellungen erneut bereitstellen.

Standardwert

`False`

Opportunity Detect und Interact Advanced Patterns | Protokollierung

Die Eigenschaft in dieser Kategorie gibt die Position der Opportunity Detect-Protokolldatei an.

log4jConfig

Beschreibung

Die Position der Konfigurationsdatei, die Opportunity Detect für die Protokollierung verwendet. Dieser Wert wird bei der Installation automatisch festgelegt. Wenn Sie diesen Pfad ändern, müssen Sie den Webanwendungsserver neu starten, damit die Änderung wirksam wird.

Standardwert

```
[absolute-path]/conf/detect_log4j.properties
```

Unica Interact Advanced Patterns | System | Interact Designdienst

Die Eigenschaft in dieser Kategorie gibt die URL für den Web-Service an, der es Interact erlaubt, erweiterte Muster automatisch zu erstellen und bereitzustellen, wenn Unica Interact mit Unica Interact Advanced Patterns integriert wird.

ServerURL

Beschreibung

Dieser Web-Service stellt während der Designzeit den Integrationspunkt zwischen Unica Interact und Unica Interact Advanced Patterns dar. Die Person, die das Produkt installiert, legt diesen Eigenschaftswert während der Installation fest. Die Standardportnummer lautet 8181.

Standardwert

```
http://[InteractServiceHost]:[InteractServicePort]/axis2/services/
InteractDesignService
```

Hier sind die vom Installationsprogramm festgelegten Konfigurationseigenschaften aufgeführt.

Insights | Navigation

Die Unica-Suite wird zum Generieren von Berichten mit Unica Insights integriert.

Diese Seite zeigt Eigenschaften an, die URLs und andere Parameter angeben, die vom Unica Insights System verwendet werden.

Seed-Name

Beschreibung:

Wird intern von HCL Unica-Anwendungen verwendet. Das Ändern dieses Werts ist nicht zu empfehlen.

Standardwert

Insights

httpPort

Beschreibung:

Diese Eigenschaft gibt den vom Unica Insights-Webanwendungsserver verwendeten Port an. Wenn Ihre Unica Insights-Installation einen anderen Port als den Standardport verwendet, müssen Sie den Wert dieser Eigenschaft bearbeiten.

Standardwert

7001

httpsPort

Beschreibung:

Wenn SSL konfiguriert ist, gibt diese Eigenschaft den vom -Webanwendungsserver für sichere Verbindungen verwendeten Port an. Wenn Ihre Unica Insights-Installation einen anderen sicheren Port als den Standardport verwendet, müssen Sie den Wert dieser Eigenschaft bearbeiten.

Standardwert

7001

serverURL

Beschreibung:

Gibt die URL der Unica Insights-Webanwendung an. Verwenden Sie einen vollständig qualifizierten Hostnamen einschließlich des Domänennamens (und den der Unterdomäne, falls zutreffend), der in der Eigenschaft Domäne angegeben ist. Zum Beispiel: http://MyReportServer.MyCompanyDomain.com:7001/ Insights

Standardwert

`http://[CHANGE ME]/hcl-birt`

Gültige Werte

Eine gut zusammengesetzte URL

logoutURL

Beschreibung:

Die Eigenschaft logoutURL wird intern verwendet, um den Logout-Handler der registrierten Anwendung aufzurufen, wenn der Benutzer auf den Abmeldungslink klickt. Ändern Sie diesen Wert nicht.

Standardwert

`/j_spring_security_logout`

Aktiviert

Beschreibung:

Durch Setzen des Werts auf `TRUE` wird sichergestellt, dass Unica Insights als Berichtsmodul verwendet wird.

Anmerkung: Wenn Sie ein Upgrade auf V 12.0 durchführen und das Campaign / Plan / Interact Reports-Paket und die Unica Platform installiert haben, können Sie entweder Cognos-Berichte oder Unica Insights-Berichte anzeigen.

Standardwert

`False`

Gültige Werte

`FALSE | TRUE`

Derzeit werden Unica Insights-Berichte für Oracle-, SQL Server- und DB2-Datenbanken unterstützt.

Anpassung von Style-Sheets und Bildern in Unica-Benutzeroberfläche

Sie können die Darstellung der Benutzeroberfläche anpassen, auf der die meisten Unica-Produktseiten erscheinen. Wenn Sie Cascading Style-Sheets bearbeiten und eigene Diagramme bereitstellen, können Sie viele der Bilder, Schriftarten und Farben in der Benutzeroberfläche ändern.

Dies wird manchmal als Rebranding bezeichnet, da das Logo und Farbschema von HCL mit dem Logo und Farbschema Ihres Unternehmens überschrieben werden kann.

Style-Sheets

Das HTML-Frameset wird durch eine Anzahl von Cascading Style-Sheets formatiert, die sich im Verzeichnis `css` in der Datei `unica.war` befinden. Bei einigen dieser Style-Sheets wird ein Style-Sheet namens `corporatetheme.css` in das Verzeichnis `css\theme` importiert. Standardmäßig ist die Datei `corporatetheme.css` leer. Wenn Sie diese Datei durch eine andere Datei mit Ihren Farben und Bildern ersetzen, können Sie das Aussehen des Framesets ändern.

stellt außerdem im Verzeichnis `css\theme\DEFAULT` in der Datei `unica.war` die Beispieldatei `corporatetheme.css` bereit. Dieses Beispiel-Style-Sheet enthält alle Spezifikationen, die angepasst werden können, sowie Kommentare, in denen erläutert wird, welche Bereiche des Framesets eine einzelne Spezifikation betrifft. Mit dieser Datei als Vorlage können Sie eigene Änderungen gemäß den Anweisungen in diesem Abschnitt vornehmen.

Grafiken

Bilder können im PNG-, GIF- oder JPEG-Format bereitgestellt werden.

verwendet für einige Schaltflächen und Symbole Sprites. Durch die Verwendung von Sprites wird die Anzahl der HTTP-Anforderungen an den Server reduziert und mögliches Flackern reduziert. Wenn Sprites verwendet, enthält der Name des Bilds die Zeichenfolge `_sprites`. Wenn Sie diese Bilder ersetzen möchten, sollten Sie Sprites der gleichen Größe verwenden, da somit die wenigsten Veränderungen am Style-Sheet erforderlich sind. Wenn Sie nicht mit Sprites vertraut sind, erhalten Sie weitere Informationen dazu im Internet.

Vorbereiten des Corporate Theme

Gehen Sie anhand dieser Richtlinien vor, um Ihr Corporate Theme für das Unica-Frameset zu erstellen.

1. Bei der Installation von Unica Platform haben Sie möglicherweise eine EAR-Datei erstellt, die die Datei `unica.war` beinhaltet, oder Sie haben die Datei `unica.war` vielleicht auch normal installiert. Extrahieren Sie in beiden Fällen Ihre installierte Datei, damit Sie auf die Dateien und Verzeichnisse zugreifen können, die in der `Datei unica.war` enthalten sind.
2. Navigieren Sie zu der Datei `corporatetheme.css`, die im Verzeichnis `css\theme \DEFAULT` abgelegt ist.
3. In den Kommentaren in `corporatetheme.css` finden Sie Informationen darüber, welcher Bereich des Frameworks welche Style-Sheet-Spezifikationen betrifft.
4. Anweisungen zur Erstellung Ihrer Bilder finden Sie im Verzeichnis `css\theme\img`.

5. Erstellen Sie Ihr Theme in einem Diagrammprogramm Ihrer Wahl, und notieren Sie sich die Bildernamen, Schriftarten und Hexadezimal-Spezifikationen für die Schriftarten und Hintergrundfarben.
6. Bearbeiten Sie die Datei `corporatetheme.css`, um Ihre Schriftarten, Farben und Bilder verwenden zu können.

Anwenden des Corporate Theme

Mit dieser Prozedur können Sie Ihr Corporate Theme der Unica-Benutzeroberfläche hinzufügen.

1. Platzieren Sie die Bilder, die Sie verwenden möchten (beispielsweise Ihr Logo, Buttons und Symbole) in einem Verzeichnis, auf das von dem Computer aus zugegriffen werden kann, auf dem Unica Platform installiert ist. Sehen Sie sich die geänderte Datei `corporatetheme.css` an, die wie in „Vorbereitung des Corporate Theme“ beschrieben erstellt wurde, um festzulegen, wo die Bilder platziert werden sollen.
2. Ist Unica Platform implementiert, deimplementieren Sie .
3. Bei der Installation von Unica Platform haben Sie möglicherweise eine EAR-Datei erstellt, die die Datei `unica.war` beinhaltet, oder Sie haben die Datei `unica.war` vielleicht auch normal installiert. In beiden Fällen haben Sie folgende Möglichkeiten:
    - Erstellen Sie eine Sicherung Ihrer WAR- oder EAR-Datei, und speichern Sie diese unter einem anderen Namen (z.B. `original_unica.war`). So können Sie Ihre Änderungen falls erforderlich rückgängig machen.
    - Extrahieren Sie Ihre installierte Datei, damit Sie auf die Dateien und Verzeichnisse zugreifen können, die in `unica.war` enthalten sind.
4. Stellen Sie die modifizierte Datei `corporatetheme.css`, die wie in „Vorbereitung des Corporate Theme“ beschrieben erstellt wurde, in das Verzeichnis `css\theme`.

   Dadurch wird die leere Datei `corporatetheme.css`, die dort bereits abgelegt ist, überschrieben.
5. Erstellen Sie die Datei `unica.war` und, falls erforderlich, die darin enthaltene EAR-Datei erneut.
6. Stellen Sie die WAR- oder EAR-Datei bereit.

7. Löschen Sie Ihren Browser-Cache und Melden Sie sich an Unica an.

   Das neue Theme wird angewendet.