LDAP (Active Directory) Systemparameter

Systemparameter für Synchronisierung von Mitarbeiter und Organisationseinheiten von einem LDAP-Server (z.B. Active Directory)

Über das Menü Admin System Parameter müssen für einen LDAP Sync folgende Parameter eingestellt werden.

Key	Default	Erläuterung
LDAP_SYNC_ENABLED	false	Nur wenn dieser Parameter auf true steht, ist eine LDAP Synchronisierung möglich.
LDAP_SERVER		Der Hostname des LDAP Servers.
LDAP_PORT	389	Der Port, auf dem der LDAP Server erreichbar ist.
LDAP_SSL	false	Verbindet via SSL Socket (LDAPS), wenn true.
LDAP_BIND_DN		Der DN bzw. Username, der zur Authentifizierung mit dem LDAP Server verwendet wird. Falls leer, wird die LDAP Verbindung ohne Authentifizierung aufgebaut.
LDAP_BIND_PASSWORD		Das Passwort des Bind DN, das zur Authentifizierung mit dem LDAP Server verwendet wird.
LDAP_EMPLOYEES_BASE_DN		Der Startpunkt, um Mitarbeiter im Directory zu suchen. Beispiel: dc=example,dc=com.
LDAP_EMPLOYEES_FILTER	(objectCategory=user)	Der Suchfilter, um Mitarbeiter im Directory zu finden.
LDAP_EMPLOYEES_ATTRIBUTE_MAPPING	fullString=displayName firstName=givenName location=l email=mail lastName=sn userId=sAMAccountName transientCountryString=c transientDepartmentString=department	Das Mapping von GoCompliant Datenfeldern auf Mitarbeiter LDAP Attributen. Links steht das Datenfeld von GoCompliant, rechts das LDAP Attribut. Zum Beispiel: firstName=givenName Das LDAP Attribut "givenName" wird auf das GoCompliant Datenfeld "firstName" gemappt.
LDAP_EMPLOYEES_OU_MAPPING	false	Wenn false, wird ein neuer Mitarbeiter auf die Root OU gehängt (das ist die einzige initial vorhandene OU: "CEO, Geschäftsleitung"). Wenn true, wird versucht die Mitarbeiter OU automatisch zu setzen. Dazu wird per Default das LDAP Attribut "department" verwendet (Übersteuerung mittels des nächstfolgenden Parameters möglich). Falls eine OU mit dem Wert dieses Attributes entsprechenden OU Code in der GoCompliant Toolsuite gefunden wird, wird diese OU für den Mitarbeiter gesetzt. Beispiel: Es existiert in der GoCompliant Toolsuite eine OU mit OU Code "HR", und das LDAP Attribut eines Mitarbeiterts ist "HR". Dann wird der Mitarbeiter in diese OU eingeordnet.
LDAP_EMPLOYEES_OU_MAPPING_FALLBACK		Wenn der vorige Parameter (LDAP_EMPLOYEES_OU_MAPPING) auf true steht, aber keine OE gefunden werden kann, wird ein neuer Mitarbeiter an diese Fallback OE gehängt.
LDAP_EMPLOYEES_OU_MAPPING_RULES		Gibt Regeln vor (Key-Value Paare), wie von einer LDAP Gruppe oder LDAP OU auf eine im System existierende OE gemappt werden soll. Beispiel: DL_XYZ_00=XYZ DL_AAA_00=AAA

LDAP_EMPLOYEES_OU_MAPPING_VIA_LDAP_GROUP	false	Wenn true, wird nicht das LDAP Attribut department verwendet, sondern das LDAP Attribut "memberOf", um die Mitarbeiter OU zu finden. D.h. wenn der Benutzer Mitglied einer Active Directory Gruppe ist, die exakt mit einem OU Code in der GoCompliant Toolsuite übereinstimmt, wird der Mitarbeiter in diese OU eingeordnet. Es wird die erste passende OE genommen. Gross-/Kleinschreibung wird ignoriert. Falls die Gruppe nicht exakt wie der OU Code lautet, gibt es zwei zusätzliche Möglichkeiten, das Verhalten zu beeinflussen: 1) Via Parameter LDAP_EMPLOYEES_OU_MAPPING_VIA_LDAP_GROUP_PREFIX 2) Falls der OU Code Leerstellen enthält, aber die Gruppe aus Konventionsgründen keine Leerstellen enthalten darf, kann ein Underscore statt Leerstelle verwendet werden. Beispiel: Sowohl die Gruppe "Portfolio Management" als auch die Gruppe "Portfolio_Management" wird auf den OU Code "Portfolio Management" gemappt.
LDAP_EMPLOYEES_OU_MAPPING_VIA_LDAP_GROUP_PREFIX		Nur in Verbindung mit LDAP_EMPLOYEES_OU_MAPPING_VIA_LDAP_GROUP=true: Das angegebene Prefix wird beim Mapping ignoriert. Beispiel: Lautet das Prefix "S-DL_GOCO_" , so wird die Gruppe "S-DL_GOCO_Portfolio_Management" auf den OU Code "Portfolio Management" gemappt.
LDAP_EMPLOYEES_OU_MAPPING_VIA_LDAP_OU	false	Wenn true, wird nicht das LDAP Attribut department verwendet, sondern die im "distinguishedName" enthaltenen OUs verwendet, um die Mitarbeiter OU zu finden; die erste (spezifischste) passende OU wird genommen.
LDAP_EMPLOYEES_OU_MAPPING_CREATE_IF_MISSING		Wenn true, wird bei aktiviertem OU Mapping eine fehlende OU automatisch im System generiert, und eine Ebene unter der Root OE eingehängt.
LDAP_EMPLOYEES_INACTIVATION_PERCENTAGE_THRESHOLD	20	Wird beim Inaktivieren von Mitarbeitern dieser Schwellwert überschritten, so bricht der LDAP Sync ab. Dies fungiert als Sicherheitsnetz und verhindert, dass bei unvorhergesehenen Problemen aus Versehen alle Mitarbeiter inaktiviert werden.
LDAP_SECURITY_GROUPS_ENABLED	false	Wenn true, werden die Benutzerrollen vom LDAP gesteuert. Dazu werden das LDAP Attribut "memberOf" und "primaryGroupID" ausgelesen und mithilfe der Parameter LDAP_SECURITY_GROUPS_MAPPING und LDAP_SECURITY_DOMAINUSER_IS_ENDUSER interpretiert.

LDAP_SECURITY_GROUPS_MAPPING	ENDUSER=GoCompliant Endusers EXPERT=GoCompliant Experts VIEWER=GoCompliant Viewers ADMIN=GoCompliant Admins IT_SUPPORT=GoCompliant IT Support CONTROL_EXPERT=GoCompliant Control Experts CONTROL_VIEWER=GoCompliant Control Viewers CONTROL_COORDINATOR=GoCompliant Control Coordinators ACTION_EXPERT=GoCompliant Action Experts ACTION_VIEWER=GoCompliant Action Viewers ACTION_COORDINATOR=GoCompliant Action Coordinators RISK_EXPERT=GoCompliant Risk Experts RISK_VIEWER=GoCompliant Risk Viewers SYSTEM_ADMIN=GoCompliant System Admins USER_ADMIN=GoCompliant User Admins	Das Mapping von GoCompliant Rollen (siehe Rollen und Rechte) auf das LDAP "memberOf" Attribute (für Active Directory: auf lokale Domänengruppen). Bitte beachten: nach dem letzten Eintrag darf keine Leerzeile stehen. Spezielle Behandlung für die Rolle Enduser: 1) Das Mapping für ENDUSER ist nicht nötig, wenn die GoCompliant Benutzer Domänenbenutzer sind und Parameter LDAP_SECURITY_GROUPS_DOMAINUSER_IS_ENDUSER auf true steht (default). 2) Die Rolle Enduser wird immer automatisch bei allen anderen hinzugefügt (wenn z.B. ein Benutzer Member von "GoCompliant Experts" ist, bekommt er neben der Expert-Rolle automatisch auch die Enduser-Rolle).
LDAP_SECURITY_GROUPS_DOMAINUSER_IS_ENDUSER	true	Wird nur beachtet, wenn LDAP_SECURITY_GROUPS_ENABLED auf true steht. In diesem Fall bekommen Domänenbenutzer (d.h. Benutzer, die als primaryGroupId=513 haben), automatisch die GoCompliant Enduser Rolle.
LDAP_SECURITY_GROUPS_DEFAULT_AREA_KEY		Wenn gesetzt, wird bei Rollen dieser Bereich als Default-Wert gesetzt (statt maximaler Bereich-Reichweite).

Manueller Test

Um Ihre Einstellungen zu prüfen, verwenden Sie im Menü Admin Mitarbeiter den Button "Simulate Sync From Directory". Hier sehen Sie, ob die Verbindung zum LDAP Server hergestellt werden kann, und welche Mitarbeiter-Information geladen werden.

Wenn Sie Ihre Einstellungen erfolgreich getestet haben, können Sie die tatsächliche Synchronisation durchführen über den Button "Sync From Directory". Dadurch werden die Mitarbeiterdaten geladen. Achtung: wenn Sie die Benutzerrollen vom LDAP laden (Parameter LDAP_SECURITY_GROUPS_ENABLED = true), kann es sein, dass Sie Ihre Rolle (z.B. IT-Support) verlieren. Stellen Sie daher zunächst in der Simulation sicher, dass Sie auch nach der Synchronisation noch Ihre Rollen besitzen.

Nächtlicher Batch-Job

Wenn Sie Ihre Einstellungen manuell erfolgreich getestet haben, können Sie die Synchronisation auch nächtlich via Batch-Job durchführen. Dazu entfernen Sie "DirectorySyncJob" aus dem System-Parameter VETOED_JOBS.

Verwandte Seiten

- Systemvoraussetzungen
- Systemparameter
- Wie kann ich vom Tomcat 7 auf Tomcat 9 upgraden?
- Installation eines Updates
- Erstinstallation