LANCOM Management Cloud

Sicherheitsrelevante Einstellungen

02/2026

LANCOM SYSTEMS

Inhalt

1 LANCOM Management Cloud....3
2 Konten- und Rollenkonzept....4
2.1 Konzept von Prinzipalen, Mitgliedschaften und Konten....4
2.1.1 Terminologie....4
2.1.2 Konzept der Rechtevergabe....4
2.1.3 Kontostruktur und Mandantentrennung....5
2.1.4 Prinzip der geringsten Rechte für Mitgliedschaften....5
2.2 Administratoren-Vererbung....6
3 Kontosicherheit....7
3.1 Passwortsicherheit....7
3.1.1 Allgemeine Empfehlungen....7
3.1.2 Passwörter für Prinzipale....7
3.1.3 Passwörter für Geräte, WLAN-SSIDs und VPNs....8
3.2 2FA....8
3.3 Alternative Authentifizierungsmethoden....9
3.3.1 API-Schlüssel....9
3.3.2 IdP-Prinzipalverwaltung....10
3.4 Sitzungssicherheit....12
4 Protokollierung....13
4.1 Audit-Protokollierung....13
4.2 Geräteprotokollierung....14
5 Offboarding....15
5.1 Manuelles Offboarding....15
5.2 Offboarding für über IdP verwaltete Prinzipale....15

1 LANCOM Management Cloud

Dieses Dokument beschreibt die sicherheitsrelevanten Einstellungen der LANCOM Management Cloud (LMC). Es dient als Referenz für den sicheren Betrieb der LMC.

2 Konten- und Rollenkonzept

2.1 Konzept von Prinzipalen, Mitgliedschaften und Konten

2.1.1 Terminologie

Prinzipal

Eine technische Repräsentation einer Person, die auf die LMC zugreifen kann. Ein Prinzipal wird bei der Anmeldung durch eine E-Mail-Adresse identifiziert und besitzt eine technische Referenz (UUID), die für die interne Datenverarbeitung in der LMC verwendet wird.

Konto

Eine Entität, auf die authentifizierte und autorisierte Prinzipale zugreifen können. Ein Konto wird durch eine UUID identifiziert und enthält menschenlesbare Metadaten.

Berechtigung

Eine Menge von Berechtigungen (ACL), die dem Konzept von Rollen entspricht.

Mitgliedschaft

Eine Zuordnung, die einen Prinzipal mit einer Berechtigung für ein bestimmtes Konto verknüpft.

2.1.2 Konzept der Rechtevergabe

1. Als erster Schritt werden von der LMC verwaltete Prinzipale von Kontoadministratoren zu einem Konto eingeladen und erhalten eine bestimmte Berechtigungsstufe. Über einen IdP verwaltete Prinzipale können sich ohne vorherige Einladung registrieren. Beide Arten von Prinzipalen müssen ein Formular ausfüllen und eine E-Mail-Adresse, ein Passwort, eine Anrede sowie einen Vor- und Nachnamen angeben, wobei die letzten drei Angaben auch fiktiv sein dürfen. Beide Arten von Prinzipalen müssen außerdem das jeweils aktuelle Dokument „Principal Terms of Use" akzeptieren.
2. Bei der Anmeldung wird der Prinzipal über die zuvor für diesen Prinzipal registrierte E-Mail-Adresse identifiziert, die innerhalb einer LMC-Installation eindeutig ist.
3. Jede Kontoeinladung muss vom eingeladenen Prinzipal akzeptiert werden, bevor sie wirksam wird.
   a. Es ist möglich, einen Prinzipal einzuladen und die Mitgliedschaft wieder zu entfernen, bevor der Prinzipal sie akzeptiert hat. Das Ergebnis ist ein Prinzipalprofil ohne Mitgliedschaften. Dies ist zwar nutzlos, stellt jedoch einen gültigen Zustand dar (der Prinzipal kann sich anmelden, hat jedoch nur Zugriff auf das Prinzipalprofil).
   b. Die Einladung ist zudem zeitlich begrenzt und läuft ab. Der Prinzipal kann sich jedoch auch nach Ablauf der Einladung noch registrieren (sein Prinzipalprofil erstellen), was zu einem ähnlichen Zustand führt (keine gültige Mitgliedschaft).
   c. Sowohl für von der LMC verwaltete als auch für über IdP authentifizierte Prinzipale kann eine Mitgliedschaft später hinzugefügt werden, indem eine weitere Einladung zu einem Konto gesendet wird.
   d. Für über IdP autorisierte Prinzipale müssen die entsprechenden Zugriffsrechte im IdP vergeben werden (siehe auch *Alternative Authentifizierungsmethoden*).
4. Die Kombination aus einem Prinzipal, einer bestimmten Konto-ID und einer bestimmten Berechtigung, die diesem Prinzipal für dieses Konto erteilt wurde, ergibt eine Mitgliedschaft, die den Zugriff auf das Konto ermöglicht.
5. Ein Prinzipal ohne direkte Mitgliedschaft und ohne über eine IdP-Autorisierung gewährte Berechtigung hat keinen Zugriff auf ein Konto und kann lediglich die Details in seinem Bereich des Prinzipalprofils anzeigen und bearbeiten.

2.1.3 Kontostruktur und Mandantentrennung

In der LMC wird zwischen drei verschiedenen Kontotypen unterschieden:

- Eine Distribution mit klar definierten Berechtigungen und Verantwortlichkeiten auf Distributionsebene (übergreifendes Kundenmanagement; mehrere pro LMC-Instanz sowie mehrere pro großem Partnerkunden möglich).
- Eine Organisation mit klar definierten Berechtigungen und Verantwortlichkeiten auf Organisationsebene (übergreifendes Kundenmanagement; mehrere pro LMC-Instanz, in der Regel eine pro Partnerkunden).
- Ein Projekt mit klar definierten Berechtigungen für Geräte-, Netzwerk-, Netzwerksicherheits-, Lizenzverwaltung usw. (mehrere pro LMC-Instanz, mehrere pro Partnerkunden, in der Regel eines pro Endkunden).

Daten sind strikt pro Konto getrennt und können nur dann abgerufen werden, wenn einem einzelnen Prinzipal eine Mitgliedschaft für den Zugriff auf dieses spezifische Konto erteilt wurde.

Konten sind hierarchisch angeordnet: Ein Projekt muss innerhalb einer Organisation erstellt werden, und Organisationen werden unter Distributions angelegt. Einige Funktionen erlauben die Verwaltung von Projekten aus der übergeordneten Organisation heraus (z. B. Administratoren-Vererbung und Geräte-Pools, die zur Zuweisung von Geräten zu Projekten verwendet werden können), was weiter unten näher beschrieben wird.

2.1.4 Prinzip der geringsten Rechte für Mitgliedschaften

Als Best Practice sollten einem Prinzipal nur die minimal erforderlichen Rechte gewährt werden, damit der Prinzipal eine bestimmte Aufgabe in der Anwendung ausführen kann. Im Kontext der LMC bedeutet dies, Projektadministratorrechte nur mit großer Sorgfalt zu vergeben und nach Möglichkeit eine Berechtigung mit weniger Rechten zu verwenden. Die folgenden Berechtigungen können auf jeder Kontoebene vergeben werden:

- Standardberechtigungen auf Distributionsebene:
  - Distributionsadministrator: Berechtigt zur Verwaltung von Organisationen, Administratoren und Geräten. Hat uneingeschränkten Zugriff auf Distributionsinformationen.
- Standardberechtigungen auf Organisationsebene:
  - Organisationsadministrator: Berechtigt zur Verwaltung von Projekten, Prinzipalen und Geräten. Hat uneingeschränkten Zugriff auf Organisationsinformationen.
  - Organisationsbetrachter: Berechtigt, organisationsbezogene Informationen anzuzeigen, jedoch nicht zu bearbeiten.
- Standardberechtigungen auf Projektebene:
  - Projektadministrator: Berechtigt zur Verwaltung des Projekts, der Prinzipale und der Geräte. Hat uneingeschränkten Zugriff auf Projektinformationen.
  - Technischer Administrator: Berechtigt zur Verwaltung von Standorten, Netzwerken und Geräten. Projektinformationen sind schreibgeschützt, und die Verwaltung von Prinzipalen ist nicht erlaubt.
  - Projektmitglied: Berechtigt zur Verwaltung und Überwachung der Geräte des Projekts. Hat schreibgeschützten Zugriff auf Projektinformationen.
  - Rollout-Assistent: Wird von der LMC Rollout Assistant App verwendet, um das Claiming von Geräten in diesem Projekt zu vereinfachen. Berechtigt zum Hinzufügen von Geräten und zum Lesen von Geräteinformationen.
  - Hotspot-Betreiber: Ausschließlich zur Verwaltung des Hotspots berechtigt.
  - Projektbeobachter: Ausschließlich berechtigt, geräte- und projektbezogene Informationen anzuzeigen, jedoch nicht zu bearbeiten.

Für von der LMC verwaltete Prinzipale kann in jedem Konto, auf das der Prinzipal zugreifen kann, eine unterschiedliche Berechtigung vergeben werden. Dies gilt auch für über IdP authentifizierte Prinzipale.

Wenn die IdP-Autorisierung für ein Konto konfiguriert und aktiviert ist, werden die Berechtigungen eines Prinzipals und die daraus resultierenden Rechte aus den im IdP zugewiesenen Rollen abgeleitet (siehe auch *IdP-Prinzipalverwaltung*). Dies führt dazu, dass pro Prinzipal und pro Kontoebene jeweils dieselbe Berechtigung vergeben wird – oder gar keine –, es ist jedoch beispielsweise nicht möglich, dass ein Prinzipal in einem Projekt Projektadministrator und in einem zweiten Projekt innerhalb derselben Organisation Hotspot-Betreiber ist. Bei Verwendung der IdP-basierten

Prinzipalverwaltung wird empfohlen, den Einladungsmechanismus nicht zu verwenden, um Berechtigungen an Prinzipale zu vergeben, die für dieses Konto über den IdP autorisiert sind. Durch das explizite Einladen von Benutzern entstehen sogenannte „direkte Mitgliedschaften", die die IdP-basierte Zugriffskontrolle außer Kraft setzen.

2.2 Administratoren-Vererbung

Die Administratoren-Vererbung kann genutzt werden, um die Sicherheit zu erhöhen und die Verwaltung für Managed Service Provider (MSPs) zu vereinfachen, die typischerweise über eine Organisation verfügen und separate untergeordnete Projekte für ihre Kunden verwenden. Anstatt Prinzipale einzeln zu jedem Projekt einzuladen und separat zu verwalten, ermöglicht die Administratoren-Vererbung Mitgliedern der Organisation, auf untergeordnete Projekte zuzugreifen, ohne explizit zu jedem einzelnen Projekt eingeladen zu werden. Dies vereinfacht die Zugriffskontrolle, da diese Prinzipale zentral innerhalb der Organisation verwaltet werden können (z. B. wenn ein Prinzipal das Unternehmen verlässt und keinen Zugriff mehr auf LMC-Konten haben soll). Dadurch entfällt die Notwendigkeit, für alle betroffenen Prinzipale direkte Mitgliedschaften in jedem Projekt anzulegen, und der Aufwand zur Durchsetzung von Zugriffsbeschränkungen auf Projektebene wird reduziert.

Direkte Mitgliedschaften (die über explizite Einladungen erstellt werden) und Administratoren-Vererbung können in gemischten Szenarien pro Prinzipal und Konto kombiniert werden. Infolgedessen kann einem einzelnen Prinzipal über die Administratoren-Vererbung ein Projektzugriff mit anderen Rechten gewährt werden als über die Annahme einer Einladung und den Erhalt einer direkten Mitgliedschaft. In solchen Fällen haben über direkte Mitgliedschaften gewährte Rechte Vorrang vor vererbten Rechten, was zu einem höheren Rechteumfang führen kann, als durch die Administratoren-Vererbung beabsichtigt. Aus diesem Grund empfehlen wir, direkte Mitgliedschaften in Szenarien mit Administratoren-Vererbung nur mit großer Sorgfalt zu verwenden. Als sichere Voreinstellung ist die LMC-Administratoren-Vererbung in Organisationen deaktiviert und muss von Organisationsadministratoren aktiviert werden. Beim Aktivieren der LMC-Administratoren-Vererbung muss eine Berechtigung auf Projektebene ausgewählt werden; diese Berechtigung wird auf alle vererbten Prinzipale in sämtlichen Projekten innerhalb der Organisation angewendet.

Die IdP-Administratoren-Vererbung kann unabhängig von der LMC-Administratoren-Vererbung auf Organisationsebene aktiviert werden. Im Kontext der IdP-Authentifizierung funktioniert sie wie die oben beschriebene LMC-Administratoren-Vererbung, ist jedoch auf die Prinzipale beschränkt, die über die IdP-Konfiguration für diese spezifische Organisation verwaltet werden. Wenn die IdP-Autorisierung in der LMC ebenfalls aktiviert ist, werden Berechtigungen und die daraus resultierenden Rechte aus den vom IdP zurückgegebenen Werten sowie aus den bei der IdP-Einrichtung konfigurierten Gruppenzuordnungen abgeleitet (siehe auch *Offboarding für über IdP verwaltete Prinzipale*).

Projektadministratoren können sowohl die LMC-Administratoren-Vererbung als auch die IdP-Administratoren-Vererbung separat deaktivieren, indem sie die entsprechende Einstellung in den Projekteinstellungen aktivieren. Jede Änderung des Vererbungsstatus wird im Organisationsprotokoll erfasst. Beide Opt-out-Optionen sind in der Telekom Schwestercloud vertraglich bedingt nicht verfügbar.

3 Kontosicherheit

3.1 Passwortsicherheit

3.1.1 Allgemeine Empfehlungen

Für die LMC befolgen wir allgemeine Empfehlungen zur Auswahl sicherer und gut merkbarer Passwörter sowie dazu, was vermieden werden sollte, wie beispielsweise die Empfehlungen vom *Bundesamt für Sicherheit in der Informationstechnik (BSI)*. .

- Kreativität kennt keine Grenzen, das Passwort muss jedoch leicht zu merken sein. Hilfreiche Strategien sind unter anderem:
  - Verwendung eines Satzes und Nutzung nur des ersten (oder zweiten oder letzten) Buchstabens jedes Wortes
  - Ersetzen einiger Buchstaben durch Zahlen oder Sonderzeichen
- Verwendung eines vollständigen Satzes als Passwort
  - Aneinanderreihen mehrerer Wörter, getrennt durch Sonderzeichen
  - Zufällige Auswahl von 5–6 Wörtern aus einem Wörterbuch und Trennung durch Leerzeichen, was das Passwort leicht merkbar und gut einzugeben, aber schwer zu knacken macht
- Grundsätzlich gilt: Je länger, desto besser. Für ein gutes Passwort sind Länge und Komplexität entscheidend.
  - Ein kurzes, komplexes Passwort sollte mindestens 8 Zeichen lang sein und vier Zeichentypen enthalten: Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.
  - Ein langes, weniger komplexes Passwort sollte mindestens 25 Zeichen lang sein.
  - Für WLAN-Verschlüsselungsverfahren wie WPA2 oder WPA3 sollte das Passwort mindestens 20 Zeichen lang sein, da Offline-Angriffe möglich sind.
- Grundsätzlich können alle verfügbaren Zeichen verwendet werden (Groß- und Kleinbuchstaben, Ziffern sowie Sonderzeichen wie Leerzeichen, ?!%+…).
- Ungeeignete Passwörter sind unter anderem Namen von Familienmitgliedern, Haustieren, besten Freunden, Lieblingsprominenten, Geburtsdaten und ähnliche persönliche Informationen. Passwörter sollten außerdem nicht aus gängigen Variationen, Wiederholungen oder Tastaturmustern wie „asdfgh" oder „1234abcd" bestehen.
- Vermeiden Sie es, einem Passwort lediglich einige Ziffern anzuhängen oder gängige Sonderzeichen (z. B. „$", „!", „?", „#") an den Anfang oder das Ende eines ansonsten einfachen Passworts zu setzen.
- Die Verwendung eines Passwortmanagers wird empfohlen, um verschiedene Passwörter zu verwalten und den Manager mit einem starken Master-Passwort zu schützen. Auf diese Weise muss sich ein Prinzipal nur ein einziges starkes Passwort merken und kann dennoch überall sehr starke, eindeutige Passwörter verwenden.
- Sprachspezifische Zeichen und Umlaute wie „ä, ö, ü, ß, €, ¢" sollten vermieden werden, da sie bei nicht-deutschen Diensten und Tastaturen möglicherweise nicht verfügbar sind oder unterschiedlich codiert werden.

3.1.2 Passwörter für Prinzipale

In der Standardkonfiguration erfordert die LMC eine Passwortlänge von mindestens acht Zeichen, darunter mindestens eine Zahl und ein Sonderzeichen. Es wird dringend empfohlen, ein Passwort zu erstellen, das den oben genannten Richtlinien entspricht. Zusätzlich kann die entsprechende Umgebungsvariable angepasst werden, um strengere Passwortrichtlinien für Prinzipale durchzusetzen. Dies wird für jede private LMC-Installation empfohlen. Außerdem gilt es als bewährte Praxis, für jeden Prinzipal in jeder LMC-Instanz unterschiedliche Passwörter zu verwenden und dabei den in *Allgemeine Empfehlungen* genannten Empfehlungen zu folgen.

3.1.3 Passwörter für Geräte, WLAN-SSIDs und VPNs

Grundsätzlich wird dringend empfohlen, keine fernverwaltete Ressource ungeschützt zu lassen, also nach Möglichkeit immer einen Passwortschutz zu verwenden. Dabei sind die allgemeinen Richtlinien zur Passwortsicherheit zu beachten. In einigen Fällen kann für die Gerätekonfiguration ein projektweites Passwort festgelegt werden. Wir empfehlen diese Option nicht und sie sollte nur dann verwendet werden, wenn dies wirklich erforderlich ist. Die Verwendung eines unterschiedlichen Passworts für jedes einzelne Gerät ist deutlich sicherer. Wenn sich ein gemeinsames Passwort für die Gerätekonfiguration pro Konto nicht vermeiden lässt, wird dringend empfohlen, hierfür ein besonders sicheres Passwort zu wählen.

3.2 2FA

Um eine zusätzliche Ebene der Zugriffskontrolle und Sicherheit hinzuzufügen, können von der LMC verwaltete Prinzipale die Zwei-Faktor-Authentifizierung (2FA) für ihren Prinzipal aktivieren. Das zusätzliche Geheimnis wird verwendet, um ein zeitbasiertes Einmalpasswort (TOTP) zu erzeugen. Das gemeinsam genutzte Geheimnis, das von der Authenticator-App zur Generierung von TOTPs verwendet wird, wird von der LMC erstellt. Dieses gemeinsame Geheimnis kann entweder in einer Authenticator-App auf einem mobilen Gerät oder in einer browserbasierten Passwortmanager-Erweiterung auf einem beliebigen Computer gespeichert werden. Die zweite Option wird nur empfohlen, wenn der LMC-Prinzipal sicherstellen kann, dass er die einzige Person mit Zugriff auf die Passwortmanager-Erweiterung dieses Browsers ist. Sicherheitsmaßnahmen zum Schutz von browserbasierten Passwortmanager-Erweiterungen oder mobilen Geräten liegen außerhalb des Umfangs dieser Dokumentation.

Sicherheitskritische Kunden können eine Projektoption aktivieren, die vor dem Betreten des Projekts eine 2FA erfordert. Das Aktivieren oder Deaktivieren von 2FA-Beschränkungen für ein Projekt wird im Projektprotokoll erfasst. Von der LMC verwaltete Prinzipale, die keinen zweiten Faktor bereitstellen können oder deren gemeinsames Geheimnis von anderer Software erzeugt wurde, können diese Projekte nicht betreten. Prinzipale müssen für jede LMC-Instanz, auf die sie zugreifen können, einen separaten TOTP-Generator einrichten, da jede LMC-Instanz für jeden Prinzipal unterschiedliche gemeinsame Geheimnisse erzeugt.

Für über einen IdP verwaltete Prinzipale muss der IdP gemäß den unternehmensinternen Sicherheitsrichtlinien konfiguriert werden. Richtlinien zur sicheren IdP-Konfiguration liegen außerhalb des Umfangs dieser Dokumentation. Die LMC überprüft keine MFA-bezogenen Claims im bereitgestellten ID-Token, da die branchenübliche Best Practice davon ausgeht, dass über den IdP verwaltete Prinzipale ausreichend geschützt sind, um auf die meisten durch 2FA eingeschränkten Ressourcen zuzugreifen.

Für durch LMC-2FA eingeschränkte Ressourcen können Projektadministratoren festlegen, ob (a) keine Zugriffsbeschränkungen für ein Projekt gelten, (b) nur von der LMC verwalteten Prinzipalen der Zutritt zum Projekt nach Bereitstellung ihres persönlichen zweiten Faktors erlaubt wird oder (c) entweder eine IdP-Anmeldung oder der persönliche zweite Faktor des Prinzipals erforderlich ist, um auf das Konto zuzugreifen. Die dritte Option ermöglicht es Prinzipalen aus jedem in der LMC-Instanz konfigurierten IdP, das Projekt zu betreten, sofern sie zusätzlich über Zugriffsberechtigungen entweder durch eine direkte Mitgliedschaft oder durch eine IdP-Autorisierung verfügen. Weitere Details zur IdP-Benutzerverwaltung finden Sie in *Alternative Authentifizierungsmethoden*.

Um für besonders kritische Ressourcen eine weitere Ebene der Zugriffskontrolle hinzuzufügen, sollten zusätzlich auch Sicherheitsmaßnahmen außerhalb der LMC in Betracht gezogen werden. Diese Maßnahmen sind nicht Gegenstand dieser Dokumentation.

3.3 Alternative Authentifizierungsmethoden

3.3.1 API-Schlüssel

In der LMC stehen mehrere Arten von API-Schlüsseln zur Verfügung. Jeder Typ hat einen unterschiedlichen Geltungsbereich und Zweck.

	SIEM-API-Schlüssel	Prinzipalgebundene Einzelkonto-Schlüssel	Prinzipalgebundene kontoübergreifende Schlüssel
Konto-Geltungsbereich	Einzelnes Konto	Ein Konto, einschließlich direkter untergeordneter Konten.	Auswahl eines, mehrerer oder aller Konten eines Prinzipals, auch für Geschwisterkonten möglich.
Berechtigungen	SIEM-relevante APIs	Alle APIs gemäß der pro Konto vergebenen Mitgliedschaft, einschließlich Schreiboperationen.	Alle APIs gemäß der pro Konto vergebenen Mitgliedschaft, einschließlich Schreiboperationen.
Maximale Gültigkeitsdauer	Unbegrenzt, regelmäßige Rotation empfohlen	1–3650 Tage, kurzlebige Schlüssel und regelmäßige Rotation empfohlen.	1–365 Tage, kurzlebige Schlüssel und regelmäßige Rotation empfohlen.
Maximale Anzahl	Einer pro Projekt	Fünf pro Konto und Prinzipal, insgesamt 100 pro Prinzipal.	Fünf pro Konto und Prinzipal, insgesamt 100 pro Prinzipal.
Anwendungsfälle	Abruf von Geräte-Logs eines einzelnen Kontos zur Überwachung der Nutzung, Abfrage eines bestimmten Satzes SIEM-relevanter APIs.	Z. B. Abruf von Monitoring-Daten mehrerer untergeordneter Konten; Zuweisung von Netzwerken zu mehreren Standorten per API-Skript; Claiming, Lizenzierung und Zuweisung von Geräten zu Standorten per API-Skript; Massenkonfiguration von Geräten per API-Skript.	Z. B. Abruf von Monitoring-Daten mehrerer untergeordneter Konten; Zuweisung von Netzwerken zu mehreren Standorten per API-Skript; Claiming, Lizenzierung und Zuweisung von Geräten zu Standorten per API-Skript; Massenkonfiguration von Geräten per API-Skript.

SIEM-API-Schlüssel (Security Information and Event Management) können für bestimmte Endpunkte in der LMC ausgestellt werden und dienen ausschließlich dazu, Informationen über bestimmte Ereignisse innerhalb eines einzelnen Kontos zu sammeln. Jeder andere Endpunkt gibt bei Zugriff mit einem SIEM-API-Schlüssel einen beschreibenden HTTP-Fehler zurück, und diese Schlüssel können nicht für Schreib- oder Löschoperationen verwendet werden.

Nur Projektadministratoren können SIEM-API-Schlüssel erstellen oder widerrufen. Projektadministratoren müssen sicherstellen, dass die SIEM-API-Schlüssel eines Projekts rotiert werden, sobald ein Prinzipal, der Zugriff auf diese Schlüssel hatte, keinen Zugriff mehr auf das Projekt besitzt (siehe *Offboarding*).

Prinzipalgebundene API-Schlüssel sind an einen einzelnen Prinzipal gebunden und übernehmen (spiegeln) dessen Berechtigungen innerhalb des LMC-Kontos, auf das der Prinzipal mit dem API-Schlüssel zugreift. Sie eignen sich besonders, wenn Aktionen einer bestimmten Person zugeordnet werden müssen (z. B. für Audits, prinzipalspezifische Limits oder fein granulare Autorisierung) oder für persönliche Automatisierungen wie Skripte, die die API mit den Rechten des LMC-Kontos des Prinzipals aufrufen. Jeder Prinzipal verfügt in der Regel über eigene Schlüssel, die nur für diesen Prinzipal sichtbar und verwaltbar sind. Dies unterstützt prinzipalspezifische Audit-Trails und ermöglicht eine einfachere Incident Response durch das Widerrufen einzelner Schlüssel anstelle der Rotation eines gemeinsam genutzten SIEM-API-Schlüssels.

Der Geltungsbereich eines prinzipalgebundenen API-Schlüssels wird bei der Erstellung ausgewählt und kann entweder auf ein einzelnes Konto (Organisation oder Projekt; „Einzelkonto-API-Schlüssel“) beschränkt sein oder kontoübergreifenden Zugriff erlauben. Einzelkonto-Schlüssel können jeweils nur ein Projekt oder eine Organisation umfassen. Jeder prinzipalgebundene API-Schlüssel mit Zugriff auf eine Organisation, in der die LMC-Administratoren-Vererbung aktiviert

ist, erlaubt zudem den Zugriff – über den API-Schlüssel – auf alle untergeordneten Projekte für aus dieser Organisation vererbte Prinzipale, sofern Projektadministratoren die Administratoren-Vererbung nicht deaktiviert haben.

Kontoübergreifende Zugriffsschlüssel können eine Auswahl von Geschwisterkonten oder alle Konten umfassen, in denen der Prinzipal Mitglied ist, unabhängig von deren Beziehung zu einem bestimmten übergeordneten Konto. Aufgrund ihres potenziell sehr großen Geltungsbereichs müssen kontoübergreifende Schlüssel mit großer Sorgfalt erstellt und sicher gespeichert werden.

Standardmäßig ist die Anzahl der prinzipalgebundenen API-Schlüssel auf 100 Schlüssel pro Prinzipal begrenzt. Zusätzlich ist die Anzahl der prinzipalgebundenen API-Schlüssel pro Prinzipal und Projekt auf fünf begrenzt.

Jede Erstellung oder jeder Widerruf eines prinzipalgebundenen oder SIEM-API-Schlüssels wird in den Konten protokolliert, auf die der Schlüssel zugreifen kann. Im Fall der Administratoren-Vererbung erfolgt die Protokollierung nur in der Organisation, in der der Schlüssel erstellt oder widerrufen wird, nicht jedoch in den untergeordneten Konten. Bei der Erstellung eines API-Schlüssels wird der Schlüsselwert selbst nur einmal angezeigt, sodass Prinzipale ihn sofort kopieren müssen. Wird dies versäumt, muss der Schlüssel widerrufen und ein neuer erstellt werden.

Für jeden API-Schlüssel müssen Prinzipale basierend auf Geltungsbereich und Nutzung eine Ablaufoption wählen:

- Da SIEM-API-Schlüssel nur einen begrenzten Satz von Rechten für diesen Zweck gewähren, sind sie nicht für ein automatisches Ablaufen vorgesehen. Sie können jederzeit von einem Projektadministrator widerrufen werden. Dennoch empfehlen wir dringend, SIEM-API-Schlüssel regelmäßig zu widerrufen, neu zu erstellen und erneut bereitzustellen, um potenzielle Sicherheitsrisiken zu reduzieren.
- Prinzipalgebundene API-Schlüssel mit Einzelkonto-Geltungsbereich auf Projektebene können eine Gültigkeit von 1 bis 365 Tagen haben oder auf „unbegrenzt" gesetzt werden. Die Option „unbegrenzt" ist jedoch durch das LMC-Backend auf eine maximale Laufzeit von 3650 Tagen beschränkt. Wir empfehlen dringend, für alle Einzelkonto-API-Schlüssel eine zeitbasierte Ablaufdauer zu verwenden. Kurzlebige Schlüssel und regelmäßige Rotation gelten als Best Practice.
- Prinzipalgebundene API-Schlüssel mit kontoübergreifendem Geltungsbereich werden immer mit einer zeitbasierten, automatischen Ablaufdauer erstellt. Die Ablaufdauer muss bei jeder Erstellung eines API-Schlüssels ausgewählt werden und kann zwischen 1 und 365 Tagen liegen. Kurzlebige Schlüssel und regelmäßige Rotation gelten als Best Practice.

Projektadministratoren können festlegen, die Nutzung von API-Schlüsseln für das von ihnen verantwortete Konto vollständig zu untersagen. Für Konten, deren Administratoren den Zugriff per API-Schlüssel deaktiviert haben, können keine neuen API-Schlüssel erstellt werden. Der Versuch, mit einem vor der Einschränkung erstellten Schlüssel auf solche Konten zuzugreifen, führt zu einem HTTP-403-Fehler (Forbidden).

Jeder Kontozugriff mit einem beliebigen API-Schlüssel wird im entsprechenden Kontoprotokoll erfasst. Jede Verwaltungsaktion, die üblicherweise im Kontokontext protokolliert wird, ist als mit einem API-Schlüssel ausgeführt gekennzeichnet.

Seit Dezember 2025 können API-Schlüssel in der LMC weder von über einen IdP verwalteten Prinzipalen erstellt noch verwendet werden. Sofern nicht durch Compliance-Anforderungen untersagt, erlaubt die LMC eine Mischung aus über IdP verwalteten und von der LMC verwalteten Prinzipalen innerhalb eines Kontos. In diesem Szenario können von der LMC verwaltete Prinzipale mit persönlichen API-Schlüsseln für Automatisierungen verwendet werden. Die Nutzung von API-Schlüsseln muss dann von Kontoadministratoren eng überwacht werden, zusammen mit gegebenenfalls erforderlichen manuellen Offboarding-Maßnahmen für Prinzipale (siehe auch *Manuelles Offboarding*). Weitere Sicherheitsverbesserungen für die Nutzung von API-Schlüsseln in Szenarien mit IdP-Benutzerverwaltung in der LMC werden derzeit untersucht.

3.3.2 IdP-Prinzipalverwaltung

Die auf einem Identity Provider (IdP) basierende Prinzipalverwaltung wurde in der LMC eingeführt, um rechtliche Anforderungen der EU zu erfüllen und die Verwaltung von Prinzipalen in der LMC zu vereinfachen. Um strenge Zugriffskontrollanforderungen zu erfüllen, delegiert die LMC den Identitätsnachweis vollständig an den IdP über den OpenID-Connect-(OIDC-)Authorization-Code-Flow mit PKCE. Der IdP überprüft die Anmeldedaten des Prinzipals (E-Mail-Adresse und im IdP gespeichertes Passwort) und stellt anschließend ein signiertes ID-Token aus, das von der LMC validiert und zur Herstellung einer lokalen Sitzung für die Prinzipalidentität verwendet wird. Nachdem die Identität des Prinzipals verifiziert wurde, kommt die integrierte Sitzungsverwaltung der LMC zum Einsatz.

Derzeit haben sich Microsoft Entra ID (OIDC-v2-Endpunkte), Keycloak, Okta/Auth0, OpenText Access und Ping Identity als kompatibel erwiesen. Wir gehen davon aus, dass auch andere IdPs funktionieren, sofern sie den OIDC-Standard korrekt implementieren. In diesem Szenario gilt:

1. Die Anmeldung an der LMC erfolgt über den IdP des Kunden.
2. Die LMC vertraut ausschließlich signierten und validierten Antworten und sieht oder speichert niemals die primären Anmeldedaten des Prinzipals.
3. Passwörter, persönliche 2FA-Geheimnisse und persönliche API-Schlüssel für Prinzipale mit einer bestimmten E-Mail-Domäne werden entfernt, sobald eine IdP-Konfiguration für diese Domäne aktiviert wird, um die Sicherheit zu erhöhen.
4. Ist der IdP nicht erreichbar, treten typische HTTP-Fehler auf. Nur wenn die entsprechende IdP-Konfiguration von einem Kontoadministrator deaktiviert wird, können Prinzipale der betroffenen Domäne die Funktion „Passwort vergessen" auf der LMC-Anmeldeseite nutzen, um wieder Zugriff zu erhalten. Dies funktioniert nur so lange, wie die IdP-Konfiguration für diese Domäne deaktiviert bleibt. Wird sie erneut aktiviert, entfernt die LMC erneut alle Passwörter, zweiten Faktoren und prinzipalgebundenen API-Schlüssel, die diese Prinzipale in der Zwischenzeit eingerichtet oder erstellt haben.

Um die IdP-Authentifizierung für Prinzipale einer bestimmten Domäne zu aktivieren, kann die entsprechende IdP-Konfiguration in einem beliebigen LMC-Konto erstellt werden. Jede Änderung an der Konfiguration wird im Protokoll dieses Kontos erfasst.

Ist die IdP-Prinzipalverwaltung und -Authentifizierung für eine Domäne aktiviert, können Prinzipale dieser Domäne selbstständig LMC-Prinzipale anlegen, indem sie:

1. die LMC-Anmeldeseite aufrufen
2. die IdP-Authentifizierung durchführen
3. erstmals zur LMC zurückkehren und das bereitgestellte Dokument „Principal Terms of Use" akzeptieren
4. falls die IdP-Konfiguration für die Domäne nur für die Authentifizierung eingerichtet ist, müssen Kontoadministratoren diesen Prinzipalen Kontoeinladungen senden, damit sie mit der durch die Einladung gewährten Rolle auf das Konto zugreifen können.

Darüber hinaus kann die LMC so konfiguriert werden, dass die einem Prinzipal gewährte Berechtigung auf Grundlage von Autorisierungsdaten bestimmt wird, die vom IdP bereitgestellt werden, sowie von in der LMC konfigurierten Zuordnungen. In diesem Fall liefert der IdP die Identität sowie grob granulare Signale (Gruppen/Rollen), die einer LMC-Berechtigung zugeordnet werden. Feingranulare Prüfungen werden von den eigenen RBAC-Regeln der LMC bei jeder UI- oder API-Operation durchgesetzt, basierend auf der etablierten Prinzipalidentität und dem Kontokontext. Für diese Prinzipale kommen LMC-Mitgliedschaften nicht zur Anwendung, und es werden keine Mitgliedschaften für den Prinzipal gespeichert. Dadurch wird sichergestellt, dass einem Prinzipal ausschließlich die aus dem ID-Token der aktuellen Sitzung abgeleiteten Rechte gewährt werden. Es wird nicht empfohlen, diesen Prinzipalen zusätzliche direkte Mitgliedschaften im IdP-autorisierten Konto (oder dessen Kontohierarchie) zuzuweisen, da direkte Mitgliedschaften die vom IdP gewährten Rechte überschreiben würden. Direkte Mitgliedschaften für IdP-autorisierte Prinzipale können jedoch jederzeit in Geschwisterkonten erstellt werden, um Zugriff außerhalb des IdP-autorisierten Kontos (oder der Kontohierarchie) zu gewähren.

Stand Dezember 2025:

- Über IdP-Gruppen-/App-Rollen-Zuordnungen kann pro Prinzipal nur eine LMC-Berechtigung vergeben werden, was zu einer einzelnen Rolle (z. B. einer Projektrolle) über alle Projekte hinweg führt, auf die der Prinzipal zugreifen kann.
- Mehrere IdP-Gruppen können derselben LMC-Berechtigung zugeordnet werden.
- Eine IdP-Gruppe/App-Rolle kann entweder für die Organisations- oder die Projektzuordnung leer gelassen werden. In diesem Fall haben Prinzipale mit dieser IdP-Gruppe/App-Rolle keinen Zugriff auf die Kontoebene, auf der die LMC-Berechtigungszuordnung leer ist.

Wann immer ein IdP-Benutzerkonto deaktiviert wird oder sich die entsprechende Gruppenmitgliedschaft bzw. App-Rolle im IdP ändert, führt die nächste Anmeldung an der LMC (oder die Sitzungsvalidierung) zu aktualisierten Berechtigungen – oder zum Entzug des Zugriffs – in der LMC.

3.4 Sitzungssicherheit

Authentifizierung und Autorisierung in der LMC basieren auf signierten JSON Web Tokens (JWTs). Mithilfe des Signaturmechanismus können andere Microservices die Integrität der in einem Token enthaltenen Informationen validieren. Von Prinzipalen verwendete Browser-Instanzen (Clients) können einen dedizierten Endpunkt aufrufen, um neue Access-Tokens zu erhalten, entweder durch Verwendung von Benutzername und Passwort oder unter Nutzung bestehender Tokens. Nach der Ausstellung kann der Client das Token (innerhalb des vordefinierten Zeitrahmens) verwenden, um nachzuweisen, dass er authentifiziert und autorisiert ist, auf die angeforderte Geschäftslogik zuzugreifen. Dies geschieht durch das Einfügen des Tokens in den Header jeder Anfrage.

Dieser Ansatz hat mehrere Auswirkungen auf die Benutzererfahrung:

- Um eine nahtlose Benutzererfahrung zu ermöglichen, kann eine einzelne LMC-UI-Sitzung über mehrere Tabs innerhalb derselben Browser-Instanz hinweg genutzt werden.
- Das Schließen des Browsers beendet die LMC-Sitzung nicht, sofern sie in der Zwischenzeit nicht abläuft.
- Das Öffnen eines zweiten Fensters desselben Browsers erfordert keine erneute Anmeldung des Prinzipals.
- Das Öffnen eines anderen Browsers (z. B. Firefox zusätzlich zu Chrome/Edge) oder des ersten Inkognito-/Privat-Tabs in einer Browser-Instanz erfordert, dass der Prinzipal durch Anmeldung an der LMC eine neue LMC-Sitzung erstellt.
- Aktive LMC-Sitzungen werden auch über Inkognito-/Privat-Tabs innerhalb derselben Inkognito-/Privat-Browser-Instanz hinweg geteilt.
- Alle oben genannten Punkte gelten ebenfalls für über einen IdP verwaltete Prinzipale.
- In Umgebungen mit gemeinsam genutzten Geräten wird dringend empfohlen, sich von der LMC abzumelden und alle LMC-Browser-Tabs zu schließen, bevor ein Gerät unbeaufsichtigt gelassen wird. Sicherheitsmaßnahmen zum Schutz des Geräts oder des Betriebssystems selbst liegen außerhalb des Umfangs dieser Dokumentation.
- Um zu verhindern, dass LMC-Sitzungen unbegrenzt verlängert werden, können Prinzipale in ihrem Profil konfigurieren, wie lange eine aktive Sitzung von der LMC-UI aufrechterhalten werden soll. Der Standardwert beträgt 30 Minuten, kann jedoch beispielsweise auf 5 Minuten reduziert oder auf maximal 12 Stunden erhöht werden. Für typische geschäftliche Anwendungsfälle empfehlen wir, den Standardwert von 30 Minuten beizubehalten.

Die Sitzungsverwaltung des IdP folgt denselben Prinzipien wie oben beschrieben.

4 Protokollierung

Die Protokollierung in der LMC ist an mehreren Stellen verfügbar, und der Zugriff auf Protokolle ist auf bestimmte Prinzipalrollen beschränkt (Organisationsadministrator auf Organisationsebene; Projektadministrator und technischer Administrator auf Projektebene). Jeder Protokolleintrag wird während der Verarbeitung der entsprechenden Aktion im LMC-Backend erstellt. Protokollmeldungen verwenden je nach Ereignistyp und Sprache (Englisch oder Deutsch) unterschiedliche Vorlagen. Jeder Service stellt eigene Übersetzungsvorlagen für die jeweils anwendbaren Meldungstypen bereit. Protokolleinträge selbst können weder von einem LMC-Prinzipal noch von einem Automatisierungsprinzipal oder von dem Service, der den Eintrag erstellt hat, verändert werden. Der Schutz von Protokolleinträgen auf Datenbankebene liegt außerhalb des Umfangs dieser Dokumentation.

4.1 Audit-Protokollierung

Audit-Protokolle auf Kontoebene für Distributionen, Organisationen und Projekte werden für 365 Tage gespeichert. Danach werden die entsprechenden Datenbankeinträge durch automatisierte Datenbank-Jobs gelöscht. Nur Kontoadministratoren oder technische Projektadministratoren können auf Audit-Protokolle zugreifen.

Typischerweise werden Aktionen, die in den Projekteinstellungen oder auf Verwaltungsseiten durchgeführt werden, audit-protokolliert, zum Beispiel:

- Erstellung oder Löschung von Prinzipalkonten
- Erstellung oder Widerruf von API-Schlüsseln
- Anmeldungen von Prinzipalen am Konto (einschließlich über IdP verwalteter Prinzipale)
- Änderungen an den Mitgliedschaften eines Prinzipals innerhalb eines Kontos
- Aktivieren oder Entfernen einer 2FA-Beschränkung für ein Konto oder jede andere kontosicherheitsrelevante Änderung
- Erstellung oder Änderung von Netzwerken
- Claiming von Geräten, deren Entfernung oder Änderungen des Lizenzstatus

Jeder Audit-Protokolleintrag enthält mindestens einen Übersichtsbereich, der ohne weitere Interaktion auf einen Blick lesbar ist:

- Protokollebene und Zeitstempel der Aktion
- Einen menschenlesbaren Aktionstyp
- Die E-Mail-Adresse des Prinzipals, der die Aktion ausgeführt hat, die zum Protokolleintrag geführt hat

Beim Erweitern eines Protokolleintrags werden zusätzliche Informationen angezeigt:

- Der Service, der den Eintrag erstellt hat
- Eine Kennung der betroffenen Entität (in der Regel der vom Prinzipal vergebene Name) sowie die Quelle der Aktion. Die Quelle kann der Browser sein, der für den Zugriff auf die LMC-UI verwendet wurde; in diesem Fall werden Browsertyp, Betriebssystem und die aktuelle Version der LMC-UI protokolliert.
- Wird eine Aktion durch Automatisierung durchgeführt, werden die IP-Adresse, von der die Anfrage ausgegangen ist, sowie – sofern bekannt – das zur Auslösung der Aktion verwendete Tool protokolliert.

Der Zugriff auf Audit-Protokolle über API-Schlüssel ist auf prinzipalgebundene API-Schlüssel von von der LMC verwalteten Kontoadministratoren und technischen Projektadministratoren beschränkt (siehe auch *Alternative Authentifizierungsmethoden*).

4.2 Geräteprotokollierung

Geräteprotokolle können auf Projektebene nur von Projektadministratoren, technischen Administratoren und Projektmitgliedern eingesehen werden. Um ein Geräteprotokoll anzuzeigen, muss das entsprechende Gerät ausgewählt und die Konfigurationsseiten geöffnet werden. Jeder Geräteprotokolleintrag enthält mindestens einen Übersichtsbereich, der ohne weitere Interaktion auf einen Blick lesbar ist:

- Protokollebene und Zeitstempel der Aktion
- Einen menschenlesbaren Aktionstyp
- Die E-Mail-Adresse des Prinzipals, der die Aktion ausgeführt hat, die zum Protokolleintrag geführt hat. Wurde eine Aktion über die lokale Konfigurationsoberfläche des Geräts durchgeführt, wird statt der E-Mail-Adresse des LMC-Prinzipals der Wert „system“ angezeigt.

Beim Erweitern eines Protokolleintrags werden zusätzliche Informationen angezeigt:

- Der Service, der den Eintrag erstellt hat
- Die Geräte-ID
- Der Gerätename sowie gegebenenfalls geänderte Gerätekonfigurationswerte

Geräteprotokolle können außerdem automatisiert entweder über SIEM-API-Schlüssel oder über prinzipalgebundene API-Schlüssel abgerufen werden (siehe auch *Alternative Authentifizierungsmethoden*).

5 Offboarding

Um sicherzustellen, dass ein LMC-Prinzipal nach dem Ausscheiden eines Mitarbeiters aus dem Unternehmen keinen Zugriff mehr auf Ressourcen eines bestimmten Kunden hat, gibt es grundsätzlich zwei Möglichkeiten, in diesem Fall die Zuständigkeiten zu trennen.

5.1 Manuelles Offboarding

Das Offboarding von von der LMC verwalteten Prinzipalen erfordert manuelle Schritte, die von einem Kontoadministrator durchgeführt werden müssen (je nach Anwendbarkeit auf Distributions-, Organisations- und Projektebene). Diese Maßnahmen müssen für jeden Prinzipal abgeschlossen werden, der keinen Zugriff mehr auf die LMC haben soll, und umfassen die folgenden Schritte:

1. Entfernen aller Mitgliedschaften aus allen Konten, auf die der Prinzipal zugreifen kann.
2. Entfernen direkter Mitgliedschaften aus allen untergeordneten Konten von Organisationen mit aktivierter Administratoren-Vererbung, auf die der Prinzipal aufgrund der Administratoren-Vererbung Zugriff hat und für die der Prinzipal zusätzlich eine Einladung angenommen hat.
3. Widerrufen der persönlichen API-Schlüssel des Prinzipals.
4. Rotation der SIEM-API-Schlüssel für Projekte, auf die der Prinzipal Zugriff hat.
5. Ändern der Geräte- und Hotspot-Passwörter für Konten, auf die der Prinzipal Zugriff hat.
6. Zusätzlich wird empfohlen, den LMC-Prinzipal selbst zu löschen. Dies kann nur durch die Person erfolgen, der der Prinzipal gehört, über den Bereich des Prinzipalprofils oder durch das Einreichen einer speziellen, dokumentierten Anfrage des Unternehmens, dem das Konto gehört, an das LMC-Support-Kompetenzteam (erfordert eine Anfrage und entsprechende Dokumentation in Support Jira).

5.2 Offboarding für über IdP verwaltete Prinzipale

Das Offboarding von über einen IdP verwalteten Prinzipalen erfordert weniger manuellen Aufwand als das Offboarding von von der LMC verwalteten Prinzipalen, muss jedoch mit derselben Sorgfalt durchgeführt werden.

1. Für jede Person mit LMC-Zugriff, die (a) nicht mehr für ein Unternehmen arbeitet oder (b) innerhalb dieses Unternehmens die Zuständigkeiten ändert, müssen die IdP-Administratoren des Unternehmens die IdP-Konfiguration des Prinzipals so anpassen, dass die LMC beim Anmeldevorgang kein positives Ergebnis mehr erhält.
2. Bei jedem Anmeldeversuch überprüft die LMC den für die E-Mail-Domäne des Prinzipals konfigurierten IdP, um zu verifizieren, ob der Prinzipal weiterhin aktiv, gültig und in diesem IdP vorhanden ist.
   a. Solange diese Prüfung erfolgreich ist, darf sich der Prinzipal an der LMC anmelden.
   b. Schlägt diese Prüfung fehl, wird der Zugriff auf die LMC verweigert.
3. Darüber hinaus empfehlen wir dringend, regelmäßig zu überprüfen und anzupassen:
   a. Den LMC-Zugriff und die gewährten Rechte aller Prinzipale, unabhängig davon, ob diese in der LMC selbst oder im IdP verwaltet werden.
   b. Ob die Administratoren-Vererbung für eine Organisation oder einen bestimmten Prinzipal noch erforderlich ist und ob direkte Projektmitgliedschaften für ursprünglich vererbte Administratoren weiterhin benötigt werden (falls zutreffend).

Für über IdP authentifizierte Prinzipale speichert die LMC direkte Mitgliedschaften. Bitte beachten Sie daher unbedingt Folgendes: **Auch wenn die IdP-Prinzipalauthentifizierung aktiviert ist, müssen die Mitgliedschaften eines Prinzipals immer manuell entfernt werden, um Passwort-Reset-Umgehungen zu verhindern, falls eine IdP-Konfiguration von einem Kontoadministrator deaktiviert wird.**

Für über IdP autorisierte Prinzipale werden Zugriffsrechte zusätzlich auf Basis der vom IdP zurückgegebenen Werte vergeben. In diesem Fall speichert die LMC keine Mitgliedschaften, sodass das Deaktivieren des Prinzipals – oder das Entziehen seiner Rechte – im zuständigen IdP ausreicht, um den Zugriff des Prinzipals auf die LMC effektiv zu unterbinden. **Dennoch müssen alle direkten Mitgliedschaften für IdP-autorisierte Prinzipale ebenfalls manuell entfernt werden.** Das Löschen des LMC-Prinzipals selbst ist optional und muss wie oben beschrieben erfolgen.