Gerätestatus

- Geräteübersicht
- Standortkarte
- SIM-Verwaltung
- Befehle

Geräteübersicht

Öffnen Sie ein Gerät über **Dashboard → Geräte**, indem Sie auf die Gerätezeile klicken. Der Seitentitel zeigt das **Modell** (sofern verfügbar) und die interne **Id** des Geräts.

Historische Daten im Vergleich zur aktuellen Registrierung

Wenn ein Gerät mehrere Registrierungen hat, kann Cerberus Enterprise einen schreibgeschützten historischen Datensatz anzeigen. In diesem Fall zeigt die Seite ein Banner **Historische Daten** und eine Schaltfläche zum Zurückkehren zu den aktuellen Registrierungsdaten an.

Oberste Felder

Der obere Bereich fasst die Geräteidentität, die Zuweisung und den Verwaltungsstatus zusammen. Einige Felder sind plattformspezifisch und erscheinen nur bei Android- oder Apple-Geräten.

- **Id** und **Modell**: schreibgeschützte Kennungen.
- **Benutzer**: zeigt den aktuell zugewiesenen Benutzer (sofern vorhanden). Über das Benutzermenü können Sie **Benutzer öffnen** oder **Benutzer ändern** oder einen Benutzer zuweisen, wenn keiner festgelegt ist.
- **Verwaltungsmodus** und **Eigentum**: werden in der Benutzeroberfläche mit Tooltips angezeigt.
- **Status**: aktueller Gerätestatus (mit Symbol und Details im Tooltip). Ein Gerät im Verloren-Modus zeigt **Verloren** sowohl auf Android als auch auf Apple, und ein Banner oben auf der Seite erklärt, was als Nächstes zu tun ist.
- **ADE-Profil** (nur Apple): zeigt das zugewiesene Automated Device Enrollment-Profil (sofern vorhanden) und ermöglicht das Öffnen oder Ändern.
- **Richtlinie**: zeigt die zugewiesene Richtlinie und ermöglicht das Öffnen oder Ändern oder das Zuweisen einer Richtlinie, wenn keine festgelegt ist.
- **Compliance-Status der Richtlinie** (wenn eine Richtlinie zugewiesen ist): gibt an, ob das Gerät compliant ist.
- **Richtlinienversion** (wenn eine Richtlinie zugewiesen ist): gibt an, ob auf dem Gerät die neueste Richtlinienversion angewendet wurde.
- **Cerberus Enterprise-App** (nur iPhone und iPad): der Status der Cerberus Enterprise-App, die Cerberus auf dem Gerät installiert. **Nicht verfügbar** (iOS oder iPadOS älter als

18.4, keine Seriennummer auf einem Firmengerät oder kein Managed Apple Account auf einem privaten Gerät); **Auf privaten Geräten noch nicht verfügbar**; **Warten auf Geräteinformationen**; **Warten auf die Benutzerlizenz des Managed Apple Account** (private Geräte, während Apple die Lizenz bestätigt); **Nicht installiert** (die App ist nicht in Ihrer Apple Business-Mediathek oder Apps and Books ist nicht eingerichtet, mit einem Link zu **Kontoeinstellungen**); **Installiert · Apps and Books erfordert Aufmerksamkeit** (das Token ist abgelaufen oder die App hat Ihre Mediathek verlassen: die App bleibt installiert); **Konfiguration nicht verfügbar**; **Wird installiert…** (wenn das Gerät 30 Minuten lang keinen Statusbericht sendet, empfiehlt der Tooltip zu prüfen, ob es online ist, und es neu zu starten, was die Installation normalerweise erneut startet); **Warten auf die Genehmigung durch den Benutzer**; **Der Benutzer hat abgelehnt** und **Installation fehlgeschlagen** (beide mit **Erneut versuchen**, das das Gerät erneut auffordert); **Installiert · warten auf den Start der App** (die App wurde noch nicht geöffnet); **Installiert · Konfiguration nicht akzeptiert**; und, sobald die App registriert ist, ihre Version, ihr letzter Kontakt und ob Benachrichtigungen aktiviert sind.
- **Registriert am** und **Letzter Statusbericht**: Zeitstempel für die Registrierung und den zuletzt gemeldeten Status.
- **Registrierung aufgehoben am**: wird angezeigt, wenn die Registrierung des Geräts aufgehoben wurde.

> Einige Daten und Bereiche sind nur verfügbar, wenn die entsprechende Kategorie in der Geräterichtlinie aktiviert ist. Weitere Informationen finden Sie auf den Seiten **Statusberichte** und **Standort und Geofences**.

Panels

Die Geräteseite ist in ausklappbare Bereiche gegliedert. Je nach Plattform und Status sehen Sie möglicherweise einen oder mehrere der folgenden Bereiche:

- **Standortkarte**: ein Panel mit Registerkarten mit der **Standort**-Historie für das aktuelle Gerät und, auf Android-Geräten, iPhones und iPads, einer Registerkarte **Geofence** für Geofence-Übergänge.
- **SIM-Verwaltung**: Geräte-EID sowie installierte SIMs und eSIMs. Auf Android außerdem die eSIM-Befehle und deren Verlauf; auf unternehmenseigenen iPhones und iPads mit Mobilfunk außerdem Datenroaming, Persönlicher Hotspot und **Mobilfunktarife aktualisieren**. Siehe die spezielle Seite **SIM-Verwaltung**.
- **Befehle**: Senden Sie Befehle an das Gerät und rufen Sie den Befehlsverlauf auf (plattformspezifisch).
- **Sicherheitszustand**: der Sicherheitszustand des Geräts und seine Risiken. Auf Android auch das Play Integrity-Urteil. Bis das Gerät dies meldet, steht **Nicht angegeben** oder **Noch nicht gemeldet** auf einem Android-Gerät, das noch keine Sicherheitsdaten

gesendet hat.

- **Warum das Gerät nicht konform ist**: wird nur angezeigt, wenn das Gerät nicht konform ist, mit einem roten Warnsymbol; öffnen Sie den Bereich, um die Gründe zu sehen. Auf Android werden die Richtlinieneinstellungen aufgeführt, die nicht eingehalten werden; auf Apple wird außerdem angegeben, ob eine Compliance-Regel das Gerät blockiert hat.
- **Gerätestatus** (nur Apple): vom Gerät gemeldete Betriebssystemversion, Fortschritt der Softwareaktualisierung, Sperrcode, FileVault, Batterie und Konten sowie die dafür verfügbaren Betriebssystemupdates. Siehe die Seite **Befehle**.
- **Anwendungen** (Android): installierte Apps und ihre Rückmeldungen und Fehlerberichte.
- **Anwendungen** (nur Apple): die von der Richtlinie installierten Apps, die mit Befehlen installierten Apps und die vom Benutzer installierten Apps, mit ihrem Installationsstatus, Fehlern und Aktionen (Wiederholen, Entfernen). Auf Macs werden außerdem die von der Richtlinie installierten Pakete mit ihrem Status und **Erneut installieren** aufgelistet; als verwaltete Apps installierte Pakete haben ein **Verwaltet**-Chip, und ein Hinweis erläutert, wann ein Paket unverwaltet installiert wurde und warum oder wann seine App eine Stunde nach dem Download nicht gefunden wurde. Auf iPhones und iPads hat die App Cerberus Enterprise das Chip **Von Cerberus installiert**; sie wird nicht unter dem Filter **Richtlinie** aufgeführt. Eine App, deren verwaltete Konfiguration das Gerät nicht akzeptiert hat, hat das Chip **Konfiguration nicht akzeptiert**. Auf privaten iPhones und iPads (Benutzerregistrierung) zeigt eine Zeile das Verwaltete Apple Account, dessen Benutzerlizenzen die App Store-Apps verwenden; Apps, die auf ihre Lizenz warten, zeigen **Warten auf Benutzerlizenz** oder **Benutzerlizenz fehlgeschlagen**, eine App, deren Installationsaufforderung der Benutzer abgebrochen hat, zeigt **Warten auf Genehmigung der Installation durch den Benutzer**, und **Erneut anfordern** fordert die Lizenz erneut bei Apple an oder zeigt die Aufforderung erneut an. Siehe die Seite **Befehle**.
- **Profile, Zertifikate und Sicherheit** (nur Apple): vom Gerät gemeldete Konfigurationsprofile, Zertifikate und Sicherheitsstatus.
- **Inventaränderungen** (nur Apple): eine Zeitleiste der auf dem Gerät installierten, entfernten oder aktualisierten Apps, Profile und Zertifikate, durchsuchbar und nach Art und Änderung filterbar. Siehe die Seite **Befehle**.
- **Shared iPad-Benutzer** und **Mac-Benutzer** (nur Apple): die Benutzer eines Shared iPad und die Benutzer eines Mac. Siehe die Seite **Befehle**.
- **Statusberichte**: zusätzliche vom Gerät gemeldete Daten, dargestellt als Baum aus Kategorien und Werten.
- **Registrierungsverlauf**: frühere Registrierungen für dasselbe physische Gerät, dargestellt als Liste.

Registerkarten des Standortbereichs

Der Bereich **Standortkarte** verwendet Registerkarten, um den Standortverlauf und Geofence-Übergänge getrennt zu halten.

- **Standort**: zeigt Verlaufsfilter, eine Datumsbereichssuche, Standortmarkierungen, den Genauigkeitskreis und Steuerelemente für das Live-Tracking des aktuellen Geräts.
- **Geofence** (Android, iPhone und iPad): zeigt den Verlauf der Geofence-Übergänge auf einer eigenen Karte, mit Zeitraumfiltern, einem optionalen Schalter für archivierte Geofences und einer seitlichen Liste der Übergänge. Auf iPhones und iPads informiert zudem eine Statuszeile, wenn Geofencing auf dem Gerät nicht funktionieren kann.

Das vollständige Verhalten dieser Registerkarten finden Sie unter **Standortkarte**.

Aktionen

Unten auf der Seite können Sie Daten aktualisieren und je nach Plattform, Gerätestatus und Lizenzstatus Aktionen ausführen.

- **Daten aktualisieren**: lädt den Gerätedatensatz neu.
- **Gerät deaktivieren** / **Gerät aktivieren** (nur Android): in unterstützten Zuständen verfügbar.
- **Geräteregistrierung aufheben**: entfernt die Verwaltung vom Gerät. Das genaue Verhalten hängt von Plattform und Eigentum ab (zum Beispiel kann Android ein Arbeitsprofil löschen oder auf die Werkseinstellungen zurücksetzen).
- **Gerät löschen**: verfügbar, wenn die Registrierung des Geräts bereits aufgehoben wurde und sein Datensatz entfernt werden kann.

Standortkarte

Diese Seite dokumentiert die gerätespezifischen Standortwerkzeuge, die in **Geräteübersicht** verfügbar sind. Der Bereich enthält einen Tab **Standort** für den Positionsverlauf und auf Android-Geräten, iPhones und iPads einen Tab **Geofence** für Geofence-Übergänge.

Voraussetzungen

Auf Android werden Gerätestandortdaten nur angezeigt, wenn die Standortmeldung in der Geräterichtlinie aktiviert ist. Um sie zu aktivieren, öffnen Sie die Richtlinie und schalten Sie **Standort und Geofences → Standort melden** ein. Weitere Informationen finden Sie unter **Standort und Geofences**.

Auf iPhones und iPads stammt der Standort von der Cerberus Enterprise-App, sobald der Benutzer ihn zulässt, oder vom Befehl **Gerät orten**, während sich das Gerät im Verloren-Modus befindet. Macs und andere Apple-Geräte melden ihren Standort nicht.

> Bei Geräten, die nicht vollständig verwaltet werden, können Standortdaten weiterhin davon abhängen, dass die Cerberus Enterprise App über die erforderlichen Standortberechtigungen verfügt und die Standortdienste auf dem Gerät aktiviert sind.

> Auf persönlichen Geräten (User Enrollment) sind Standort und Geofences nur verfügbar, wenn in der Apple-Richtlinie **Standort und Geofences auf persönlichen Geräten** aktiviert ist und der Benutzer den Standort für die Cerberus Enterprise App erlaubt. Andernfalls zeigt die Geräteseite ihres Geräts die Standortaktionen oder die Live-Verfolgung nicht an. Der Verloren-Modus ist auf persönlichen Geräten nie verfügbar.

> Die globale Karte für mehrere Geräte, die über das Dashboard verfügbar ist, finden Sie unter **Standortkarte des Dashboards**.

Ladezustand und Zustand ohne Daten

- Während die Standortdaten geladen werden, zeigt der Bereich eine Ladeüberlagerung auf der Karte an.
- Wenn für das Gerät keine Standortdaten verfügbar sind, zeigt der Bereich die Meldung **Keine Standortdaten verfügbar** an. Auf Android wird ein Hinweis ergänzt, die Standortmeldung in der zugewiesenen Richtlinie zu aktivieren, wenn sie deaktiviert ist. Auf Apple wird angegeben, woher der Standort stammt oder dass dieser Gerätetyp ihn nicht meldet.
- Wenn ein Datumsfilter aktiv ist und keine Beispiele dazu passen, zeigt der Bereich **Im ausgewählten Datumsbereich sind keine Daten verfügbar**.

Standort-Tab

Öffnen Sie den Tab **Standort**, um den Verlauf für ein einzelnes Gerät zu prüfen. Zu den verfügbaren Filtern gehören der letzte bekannte Standort, aktuelle Verlaufszeiträume, ein benutzerdefinierter Datumsbereich und die Live-Verfolgung.

- **Zuletzt**: zeigt den letzten bekannten Standort.
- **Heute**, **Letzte 7 Tage** und **Letzte 30 Tage**: zeigen aufgezeichnete Standorte für den ausgewählten Zeitraum.
- **Suchen**: ermöglicht die Auswahl eines benutzerdefinierten Datumsbereichs.
- **Live**: startet oder beendet die Live-Verfolgung für das aktuelle Gerät.

> Standorte werden **90 Tage** lang aufbewahrt: Ältere werden jede Nacht automatisch gelöscht. Der letzte Standort jedes registrierten Geräts bleibt immer erhalten, sodass das Gerät auch dann auf den Karten bleibt, wenn es sich lange nicht gemeldet hat. Bei entfernten Geräten und früheren Registrierungen werden alle Standorte gelöscht, die älter als 90 Tage sind. Deshalb kann der Datumsbereich von **Suchen** nicht mehr als 90 Tage in der Vergangenheit beginnen.

Markerdetails

Wenn Sie auf einen Standortmarker klicken, wird ein Informationsfenster geöffnet mit:

- Der Zeitstempel des Standortdatensatzes.
- Die gemeldete **Genauigkeit** (in Metern).
- Die gemeldete **Geschwindigkeit**, wenn das Gerät sie bereitstellt.
- Die gemeldete **Richtung** bzw. der Kurswinkel, wenn das Gerät sie bereitstellt.

Genauigkeitskreis

Wenn das Informationsfenster geöffnet ist, wird um die Markierung ein Genauigkeitskreis angezeigt. Der Radius des Kreises entspricht der gemeldeten Genauigkeit (in Metern). Beim Schließen des Informationsfensters wird der Kreis ausgeblendet.

Live-Tracking

In der Geräteverlaufsansicht startet die Auswahl des Filters **Live** eine Echtzeit-Verfolgungsanfrage für genau dieses Gerät. Cerberus Enterprise fordert vor dem Start der Anfrage eine Bestätigung an.

- Live-Tracking läuft bis zu **15 Minuten**.
- Während Live-Tracking aktiv ist, zeigen Android-Geräte eine Benachrichtigung und iPhones und iPads den Standortindikator.
- Während Live-Tracking aktiv ist, aktualisiert das Panel fortlaufend den neuesten Standort und der Live-Indikator bleibt sichtbar.
- Wenn Sie den Filter Live erneut auswählen, können Sie das Live-Tracking vor Ablauf des Zeitlimits beenden.
- Auf **iPhone und iPad** läuft das Live-Tracking über die App Cerberus Enterprise, wobei der Standortzugriff auf **Immer** gesetzt sein muss. Die Anfrage weckt die App normalerweise auch dann, wenn sie nicht geöffnet ist, und die App sendet anschließend für die gesamte Sitzung Standorte. iOS garantiert diese Anfragen nicht: Das System kann sie verzögern oder nicht zustellen, etwa im Energiesparmodus oder ohne Netzwerkverbindung. Wenn innerhalb von 2 Minuten kein Standort eintrifft, bricht das Dashboard die Anfrage ab: Bitten Sie den Benutzer, die App einmal zu öffnen, und versuchen Sie es dann erneut.

Geofence-Tab

Auf Android-Geräten, iPhones und iPads zeigt die zweite Registerkarte Geofence-Übergänge an, die aus den in der zugewiesenen Richtlinie definierten Geofences erzeugt wurden.

- Die Karte zeigt die aktuellen Geofence-Bereiche zusammen mit den aufgezeichneten Übergangspunkten.
- In der Übergangsliste rechts können Sie Ereignisse zum **Betreten** und **Verlassen** prüfen.
- Verfügbar sind die Filter **Heute**, **Letzte 7 Tage**, **Letzte 30 Tage** und eine benutzerdefinierte Datumsbereichssuche.
- **Archivierte einschließen** zeigt auch Übergänge zu alten Geofence-Definitionen an, die in der aktuellen Richtlinie nicht mehr vorhanden sind.
- Geofence-Übergänge werden **90 Tage** lang aufbewahrt, ältere werden jede Nacht automatisch gelöscht. Daher kann die Suche mit benutzerdefiniertem Datumsbereich

nicht mehr als 90 Tage in der Vergangenheit beginnen.

Auf iPhones und iPads zeigt eine Statuszeile oben auf der Registerkarte, wenn die Richtlinie aktive Geofences enthält, ob Geofencing auf dem Gerät funktioniert. Sie informiert Sie, wenn es nicht funktionieren kann: Die App Cerberus Enterprise hat den Server nicht kontaktiert oder muss aktualisiert werden, der Standortzugriff ist nicht auf **Immer** gesetzt, **Präziser Standort** oder **Hintergrundaktualisierung** ist deaktiviert, der **Energiesparmodus** war aktiviert, als die App zuletzt ihre Einstellungen gemeldet hat (Geofence-Ereignisse und -Änderungen können sich dann um Stunden verzögern), oder die App hat die neuesten Geofences noch nicht übernommen. Wenn alles funktioniert, zeigt sie an, wie viele Geofences die App überwacht.

Details zu Geofence-Übergängen

Wenn Sie einen Übergang auswählen, werden seine Details auf der Karte geöffnet und der entsprechende Listeneintrag hervorgehoben. Sofern verfügbar, zeigt Cerberus Enterprise für diesen Übergang auch die Gerätekoordinaten und die gemeldete Genauigkeit an.

SIM-Verwaltung

Die Geräteseite bietet einen Bereich **SIM-Verwaltung**. Auf Android-Geräten verwaltet er die auf dem Gerät installierten SIMs und eSIM-Profile, fügt eSIM-Profile hinzu oder entfernt sie und zeigt den Verlauf der an das Gerät gesendeten eSIM-Befehle. Auf unternehmenseigenen iPhones und Mobilfunk-iPads zeigt er die vom Gerät gemeldeten SIMs und eSIM-Tarife und ermöglicht dem Gerät, die vom Mobilfunkanbieter vorbereiteten eSIM-Tarife herunterzuladen: siehe **iPhone und iPad** unten.

> Vollständig verwaltete Geräte melden SIM-Informationen, wenn die Berichterstattung **Netzwerkinformationen** in der Geräterichtlinie aktiviert ist (diese Option ist von Cerberus Enterprise immer aktiviert). Siehe die Seite **Statusberichterstattung**.

Geräte-EID

Die EID (eUICC Identifier) identifiziert die eSIM-Hardware des Geräts. Mobilfunkanbieter verwenden sie, um eSIM-Profile an das Gerät zu binden. Daher ist das Abrufen der EID in der Regel der erste Schritt eines eSIM-Bereitstellungsablaufs.

- **Unternehmenseigene Geräte** (Android 13 und höher): Die EID wird automatisch mit dem Gerätestatus gemeldet, und es ist keine Interaktion durch den Benutzer erforderlich.
- **Privat genutzte Geräte** (Android 13 und höher): Verwenden Sie die Schaltfläche **EID anfordern**. Der Benutzer erhält auf dem Gerät eine Benachrichtigung mit der Aufforderung, die EID freizugeben, und kann die Anfrage genehmigen oder ablehnen. Die EID wird nur angezeigt, wenn der Benutzer zustimmt. Solange die Anfrage aussteht, bleibt die Schaltfläche deaktiviert.

> Bevor eine EID-Anfrage gesendet wird, erscheint ein Bestätigungsdialog, da der Benutzer auf dem Gerät eine Benachrichtigung erhält.

Installierte SIMs

Die Tabelle **Installierte SIMs** listet die aktuell für das Gerät bekannten SIMs auf, einschließlich physischer SIMs und eSIM-Profile. Auf privat genutzten Geräten werden mit dem Befehl **eSIM hinzufügen** installierte eSIM-Profile auch dann angezeigt, wenn das Gerät keine SIM-Informationen

meldet.

- **Mobilfunkanbieter**: der mit der SIM verknüpfte Name des Mobilfunkanbieters (sofern gemeldet).
- **Telefonnummer**: die mit der SIM verknüpfte Telefonnummer (sofern gemeldet).
- **ICCID**: der Integrated Circuit Card Identifier der SIM.
- **Aktivierungsstatus**: ob die eSIM aktiviert ist oder nicht. Wird nur für eSIMs auf Android 15 und höher gemeldet.
- **Konfigurationsmodus**: ob die eSIM von einem Administrator oder vom Benutzer konfiguriert wurde. Wird nur für eSIMs auf Android 15 und höher gemeldet.
- **SIM-Typ**: zeigt an, ob das Gerät den Eintrag als eSIM meldet.

> eSIMs mit einem laufenden oder ausgeführten (nicht fehlgeschlagenen) Entfernungsbefehl zeigen vorübergehend den Aktivierungsstatus **Wird entfernt** an. Der Eintrag verschwindet aus der Liste, wenn das Gerät die aktualisierte SIM-Liste meldet. Während eine Entfernung läuft, ist die Schaltfläche zum Entfernen nicht verfügbar, damit derselbe Befehl nicht zweimal gesendet wird.

eSIM entfernen

Verwenden Sie die Schaltfläche zum Entfernen neben einer installierten eSIM, um ihr Profil vom Gerät zu entfernen. Ein Bestätigungsdialog fordert Sie auf, die ICCID der zu entfernenden eSIM zu bestätigen, bevor der Befehl gesendet wird. Das Entfernen einer eSIM wird auf Android 15 und höher unterstützt.

eSIM hinzufügen

Der Abschnitt **eSIM hinzufügen** installiert ein neues eSIM-Profil auf dem Gerät (unterstützt auf Android 15 und höher). Er erfordert:

- **Gültigkeit**: wie lange der Befehl gültig ist, wenn er nicht sofort ausgeführt werden kann.
- **Aktivierungscode**: der vom Mobilfunkanbieter bereitgestellte Aktivierungscode für das eSIM-Profil. Sie können den vollständigen Code eingeben oder nur die SM-DP+-Adresse, damit das Gerät ein Profil findet, das der Mobilfunkanbieter bereits mit seiner EID verknüpft hat.
- **Aktivierungsstatus**: ob das eSIM-Profil nach dem Herunterladen automatisch aktiviert oder unaktiviert gelassen werden soll, damit der Benutzer es manuell aktiviert.

Befehlsverlauf

Unterhalb des Abschnitts eSIM hinzufügen zeigt das Panel den Verlauf der an das Gerät gesendeten eSIM-Befehle: **eSIM hinzufügen**, **eSIM entfernen** und **EID anfordern**. Die Tabelle ist sortierbar und unterstützt die Seitenaufteilung. Einige Zeilen können erweitert werden, um die Befehlsparameter (zum Beispiel den Aktivierungscode oder die ICCID) und den Ausführungsstatus anzuzeigen, einschließlich der eSIM-Fehlerdetails, wenn ein Vorgang auf dem Gerät fehlschlägt.

- **Erstellungsdatum**
- **Befehl**
- **Gültigkeit**
- **Status**
- **Fehler**: zeigt den eSIM-Fehlerstatus an (zum Beispiel *Benutzer hat abgelehnt*, *Ungültiger Aktivierungscode* oder *ICCID nicht gefunden*), wenn die Befehlsausführung ihn meldet.
- **Ausführungsdatum**

eSIMs beim Zurücksetzen und Aufheben der Registrierung löschen

Wenn Sie das Gerät über den Befehlsbereich zurücksetzen, steuert die Option **eSIMs löschen**, ob eSIM-Profile beim Zurücksetzen entfernt werden. Auf privat genutzten Geräten mit Arbeitsprofil ist diese Option standardmäßig aktiviert (verwaltete eSIMs werden entfernt, private eSIMs bleiben unberührt). Dieselbe Option ist im Bestätigungsdialog **Geräteregistrierung aufheben** verfügbar.

iPhone und iPad

Das Panel wird für iPhones und für iPads angezeigt, die Mobilfunkdaten gemeldet haben (ein iPad ohne Mobilfunk hat keine), und nur, wenn das Gerät unternehmenseigen ist und keine Benutzerregistrierung darstellt. Die Mobilfunkinformationen des Geräts werden zusammen mit den Geräteinformationen abgefragt: bei der Registrierung, täglich, mit **Geräteinformationen aktualisieren**, wenn der Besitz auf unternehmenseigen wechselt, und einige Minuten nach **Mobilfunktarife aktualisieren**.

- **Geräte-EID**: die zusammen mit den SIMs gemeldete EID, mit einer Schaltfläche zum Kopieren für den Mobilfunkanbieter. Wenn das Gerät sie nicht meldet, findet der Benutzer sie unter Einstellungen > Allgemein > Info.
- **Gemeldet**, **Datenroaming**, **Persönlicher Hotspot** und **Modem-Firmware**: wann das Gerät geantwortet hat und welchen Zustand es gemeldet hat. Datenroaming und Persönlicher Hotspot können mit **Geräteeinstellungen** im Befehlsbereich geändert

werden, der auch den aktuellen Zustand anzeigt.
- **SIMs**: eine Zeile pro SIM oder eSIM-Tarif (Dual-SIM-Geräte haben zwei), mit dem vom Gerät gemeldeten Steckplatz, seiner Bezeichnung und seinem Typ (**eSIM**, wenn das Gerät die EID damit meldet, andernfalls **SIM-Karte**), dem Mobilfunkanbieter (der Heimatanbieter in einem Tooltip, wenn das Gerät in einem anderen Netz roamt), der Telefonnummer, ICCID, EID, IMEI, der für Daten und für Anrufe verwendeten SIM sowie dem Roaming. Ein eSIM-Steckplatz ohne Tarif wird ausgegraut als **Kein Tarif** angezeigt.
- **Dieses Gerät hat keine SIM gemeldet** bedeutet, dass das Gerät ohne SIM geantwortet hat; **Noch keine Mobilfunkinformationen** bedeutet, dass es noch nicht geantwortet hat: Verwenden Sie **Geräteinformationen aktualisieren**.

> Telefonnummern, ICCID, IMEI und EID identifizieren die Person und die Leitung: Sie werden niemals bei privat genutzten Geräten oder Benutzerregistrierungen abgefragt. Wenn ein Gerät privat genutzt wird, werden die Informationen sofort entfernt und in den Ergebnissen der alten Geräteinformationsbefehle im Befehlsverlauf ausgeblendet. Sie werden nicht exportiert und nicht in den Systemprotokollen geschrieben.

Mobilfunktarife aktualisieren

iPhone und iPad können eine eSIM nicht über einen Aktivierungscode installieren. Der Mobilfunkanbieter bindet (reserviert) den eSIM-Tarif auf seinem eSIM-Server (SM-DP+) an die EID des Geräts und teilt Ihnen die Adresse dieses Servers mit; **Mobilfunktarife aktualisieren** fordert das Gerät dann auf, die für es bereitstehenden Tarife herunterzuladen. Die Schaltfläche **Mobilfunktarife aktualisieren** im Panel wählt den Befehl im Befehlsbereich aus, in dem Sie die **URL des eSIM-Servers des Mobilfunkanbieters** eingeben:

- **Eine https://-Adresse**, die unverändert gesendet wird. Adressen mit http://, einem Benutzernamen oder Passwort oder einem #-Teil werden nicht akzeptiert.
- **Ein Hostname**, zum Beispiel *smdp.carrier.example*, der als https://smdp.carrier.example gesendet wird.
- **Ein LPA-Aktivierungscode** (LPA:1$server$code, der Text eines eSIM-QR-Codes): Es wird nur der Server verwendet, da der Befehl den Code nicht übertragen kann. Der Tarif muss vom Mobilfunkanbieter an die Geräte-EID gebunden sein, andernfalls findet das Gerät nichts zum Herunterladen.

Das Gerät installiert und aktiviert den Tarif, ohne den Benutzer zu fragen, auch wenn es nicht überwacht wird. Erfolg im Befehlsverlauf bedeutet, dass das Gerät die Anfrage akzeptiert hat, nicht dass ein Tarif installiert wurde: Die Installation kann bis zu drei Minuten dauern, und Cerberus Enterprise fragt das Gerät etwa drei Minuten später erneut nach seinen SIMs, sodass der neue Tarif im Panel erscheint. Die Fehler 36001 (das Gerät konnte sein Mobilfunksystem nicht erreichen), 36002 (keine eSIM-Unterstützung) und 36003 (Mobilfunksystem ausgelastet, versuchen Sie es später erneut) werden in den Systemprotokollen erläutert. Ein einmal heruntergeladener Tarif kann nicht erneut heruntergeladen werden: Wenn die Installation fehlschlägt, wenden Sie sich an den

Mobilfunkanbieter. Der Befehl ist auch für mehrere Geräte gleichzeitig im Menü **Apple-Geräteaktionen** der Seite Geräte verfügbar.

Was Apple nicht erlaubt

- **eSIM hinzufügen** über einen Aktivierungscode: nicht möglich, verwenden Sie **Mobilfunktarife aktualisieren** mit einem an die EID gebundenen Tarif.
- **eSIM entfernen**: Eine eSIM kann nicht einzeln aus der Ferne entfernt werden. Das Löschen des Geräts mit deaktivierter Option **eSIM-Datentarif behalten** entfernt alle eSIMs. Um einen einzelnen Tarif zu beenden, bitten Sie den Mobilfunkanbieter, ihn zu deaktivieren: Der Tarif bleibt auf dem Gerät, kann aber keine Verbindung herstellen.
- **EID anfordern**: nicht erforderlich, die EID wird mit den SIMs unternehmenseigener Geräte übermittelt.
- **Macs** haben keine Mobilfunk- oder eSIM-Verwaltung.

Befehle

Die Geräteseite bietet einen Bereich **Befehle**, um Fernbefehle an ein verwaltetes Gerät zu senden. Die verfügbaren Befehle hängen von der Plattform (Android oder Apple) und dem Gerätestatus ab.

Befehle können nur an ein derzeit registriertes Gerät gesendet werden. Bei einem Gerät mit aufgehobener Registrierung, bei einem ADE-Gerät, das noch nicht registriert ist, und beim historischen Datensatz einer früheren Registrierung zeigt der Bereich nur den Befehlsverlauf.

> Wenn das Gerät derzeit nicht online ist, wird der Befehl zugestellt und ausgeführt, sobald das Gerät eine Verbindung zum Internet herstellt. Für Android-Befehle können Sie den Parameter **Gültigkeit** festlegen, um zu bestimmen, wie lange ein nicht zugestellter Befehl gültig bleibt.

Android-Befehle (AMAPI)

Für Android-Geräte enthält der Bereich Befehle ein Feld **Gültigkeit** (Wert + Einheit) und eine Auswahl **Befehl**. Einige Befehle erfordern zusätzliche Parameter, die dynamisch angezeigt werden, wenn Sie den Befehl auswählen.

Allgemeine Parameter

- **Gültigkeit**: wie lange der Befehl gültig ist, wenn er nicht sofort ausgeführt werden kann.
- **Befehl**: wählen Sie aus, welche Aktion an das Gerät gesendet werden soll.

Befehle ohne zusätzliche Felder

- **Gerät sperren**: sperrt das Gerät.
- **Gerät neu starten**: startet das Gerät neu. Erfordert Android 7.0 oder neuer.
- **Verloren-Modus deaktivieren**: nimmt das Gerät aus dem Verloren-Modus.
- **Eigentum abgeben**: entfernt das Arbeitsprofil und alle Richtlinien von einem unternehmenseigenen Gerät mit Android 8.0 oder neuer und überlässt es der privaten Nutzung. Apps und Daten des persönlichen Profils bleiben erhalten. Das Gerät wird vom Server gelöscht, nachdem es den Befehl bestätigt hat. Dies kann nicht rückgängig gemacht werden.

Befehle mit zusätzlichen Feldern

- **Passwort zurücksetzen**: erfordert **Neues Passwort** und **Neues Passwort bestätigen** . Zu den optionalen Umschaltern gehören **Jetzt sperren**, **Eingabe erforderlich** und **Beim Start keine Anmeldeinformationen abfragen**.
- **App-Daten löschen**: erfordert den Ziel-**Paketnamen**.
- **Verloren-Modus aktivieren**: erfordert eine **Nachricht für den Verloren-Modus** und unterstützt optionale Kontaktfelder (Straßenadresse, Organisation, Telefonnummer, E-Mail). Wenn das Gerät dies meldet, wird sein Status **Verloren**, die Geräteseite zeigt ein Banner und dieser Befehl wird ausgeblendet, bis der Verloren-Modus deaktiviert wird.
- **Gerät löschen**: unterstützt eine **Nachricht mit Löschgrund** (wird Benutzern auf privaten Geräten angezeigt) und optionale Löschoptionen, einschließlich **eSIMs löschen**.

> Die eSIM-Befehle (**eSIM hinzufügen**, **eSIM entfernen**, **EID anfordern**) sind im dedizierten Bereich **SIM-Verwaltung** verfügbar.

Befehlsverlauf

Unterhalb der Sendesteuerelemente zeigt das Dashboard eine Tabelle mit dem Befehlsverlauf. Die Tabelle ist sortierbar und unterstützt Seitenumbruch. Einige Zeilen können erweitert werden, um zusätzliche Parameter oder Ausführungsdetails anzuzeigen.

Android-Verlaufsspalten

- **Erstellungsdatum**
- **Befehl**
- **Gültigkeit**
- **Status**
- **Fehler**
- **Ausführungsdatum**

Apple-Befehle (MDM)

Für Apple-Geräte bietet der Bereich Befehle eine Auswahl **Befehl**. Einige Befehle erfordern zusätzliche Eingaben. Wie bei Android wird unten eine Tabelle mit dem Befehlsverlauf angezeigt.

Befehle mit zusätzlichen Feldern

- **App installieren**: erfordert die **Bundle-ID** der Anwendung.

- **Benachrichtigung senden**: erfordert eine **Benachrichtigungsnachricht** (maximale Länge 200 Zeichen).

Auf iPhones und iPads erreichen **Benachrichtigung senden** und die Live-Ortung das Gerät über die **Cerberus Enterprise**-App: Sie sind deaktiviert, bis die App installiert ist und Benachrichtigungen registriert hat (siehe Feld **Cerberus Enterprise-App**). Beim Start der Live-Ortung wird „Live-Ortungsanforderung an das Gerät gesendet“ angezeigt: Die Ortung beginnt, wenn das Gerät seinen ersten Standort sendet. iOS kann die Anforderung verzögern oder nicht zustellen, zum Beispiel im Stromsparmodus oder ohne Netzwerkverbindung: Wenn innerhalb von 2 Minuten kein Standort eintrifft, bitten Sie den Benutzer, die App einmal zu öffnen. Wenn eine Anforderung fehlschlägt, gibt die Meldung den Grund an, zum Beispiel dass die App noch nicht registriert ist, der Benachrichtigungsschlüssel des Servers fehlt oder das Benachrichtigungs-Token des Geräts nicht mehr gültig ist.

Geräteaktionen

Nur die vom Gerät unterstützten Befehle werden aufgelistet: Einige erfordern ein überwachtes iPhone oder iPad, andere sind auf einem Mac nicht verfügbar. Bei störenden Aktionen wird eine Bestätigung angefordert.

- **Gerät sperren**: sperrt den Bildschirm, optional mit Nachricht und Telefonnummer. Ein Mac wird neu gestartet und mit einer sechsstelligen PIN gesperrt, die einmal nach dem Senden des Befehls und in den Befehlsdetails angezeigt wird. Das iPhone zeigt den Titel „iPhone verloren“ über Ihrer Nachricht an, obwohl dieser Befehl den Verloren-Modus nicht aktiviert.
- **Verloren-Modus aktivieren** (überwachtes iPhone und iPad): sperrt das Gerät und zeigt Ihre Nachricht, Telefonnummer und Fußnote auf dem Sperrbildschirm an. Während der Verloren-Modus aktiv ist, zeigt die Seite ein Banner und die Befehle **Gerät orten** (der Standort erscheint auf der Standortkarte), **Ton abspielen** und **Verloren-Modus deaktivieren**.
- Das Gerät teilt demjenigen, der es hält, mit, dass es geortet wurde: Nach **Gerät orten** zeigt der Sperrbildschirm **iPhone geortet** mit der Uhrzeit und dem Namen des Servers, der den Standort empfangen hat, sowie eine Schaltfläche **Weiter**. iOS zeigt diesen Hinweis an, und er kann nicht deaktiviert werden.
- **Code löschen**: entfernt den Code eines iPhone oder iPad, zum Beispiel wenn der Benutzer ihn vergessen hat. Wenn die Richtlinie einen Code erfordert, wird der Benutzer aufgefordert, einen neuen festzulegen.
- **Geräteinformationen aktualisieren**: fragt das Gerät nach seinen Informationen (Überwachung, OS-Version, Sicherheitsstatus, MDM-Zertifikat) und seinem Inventar.
- **Geräteeinstellungen**: öffnet ein Fenster zum Ändern des Gerätenamens, des Hostnamens eines Mac, von Bluetooth, Datenroaming, Persönlichem Hotspot, Zeitzone, Hintergrundbild, ob die Aktivierungssperre zulässig ist, und bei einem Shared iPad seiner Einstellungen (siehe unten). Nur die geänderten Einstellungen werden gesendet; die vom Gerät nicht unterstützten sind mit dem Grund deaktiviert. Ein Gerät kann Datenroaming

oder Persönlichen Hotspot bestätigen, ohne sie anzuwenden (zum Beispiel wenn der SIM-Tarif keinen Persönlichen Hotspot enthält), daher liest Cerberus Enterprise sie etwa 30 Sekunden später erneut aus und schreibt eine Warnung in die Systemprotokolle, wenn sie sich nicht geändert haben.
- **Gerät neu starten** und **Gerät ausschalten**: startet das Gerät nach einer Bestätigung sofort neu oder schaltet es aus.
- **Gerät löschen**: löscht alle Inhalte und Einstellungen und entfernt das Gerät aus der Verwaltung. Auf iPhone und iPad können Sie den eSIM-Datentarif behalten und die Näheinrichtung überspringen; ein Mac erhält eine sechsstellige PIN.
- **Return to Service** (Option von **Gerät löschen**, iPhone und iPad mit iOS 17 oder neuer): Nach dem Löschen richtet sich das Gerät ohne Eingreifen von selbst wieder ein und registriert sich erneut mit seiner aktuellen Richtlinie, seinem Benutzer und seinem Eigentum. Wählen Sie für die Einrichtung ein Wi-Fi-Netzwerk der Geräterichtlinie aus, es sei denn, das Gerät verfügt über Ethernet oder mobile Daten: Es können nur persönliche Netzwerke (mit Passwort, ohne Zertifikate) verwendet werden, da das Gerät noch keinen Benutzer und kein Zertifikat hat. Die Aktivierungssperre muss deaktiviert sein.
- **Mobilfunkpläne aktualisieren** (iPhone und iPad mit Mobilfunk, iOS 13 oder neuer, nicht User Enrollment): Geben Sie die vom Mobilfunkanbieter bereitgestellte **Carrier eSIM Server-URL** ein (eine https://-Adresse, einen Hostnamen oder einen LPA-Aktivierungscode, von dem nur der Server verwendet wird), und das Gerät lädt die eSIM-Pläne herunter, die der Anbieter an seine EID gebunden hat. Die EID des Geräts wird unter dem Feld angezeigt, damit Sie sie an den Anbieter senden können. Siehe die Seite **SIM-Verwaltung**.
- Wenn Sie **eSIM-Datentarif behalten** deaktivieren, werden beim Löschen alle eSIMs entfernt. Die Richtlinienbeschränkung **eSIM behalten, wenn das Gerät gelöscht wird** (überwachte Geräte, iOS 17.2 oder neuer) gilt für Löschvorgänge, die auf dem Gerät gestartet wurden (zu viele fehlgeschlagene Codeeingaben, Alle Inhalte und Einstellungen löschen): Apple dokumentiert ihre Auswirkung auf diesen Befehl nicht.
- **Benutzer abmelden** (Shared iPad): meldet den aktuellen Benutzer ab und kehrt zum Anmeldebildschirm zurück. Daten, die noch nicht mit iCloud synchronisiert wurden, bleiben auf dem iPad.

Shared iPad

Ein Shared iPad wird von mehreren Personen genutzt, jede mit ihrem eigenen Managed Apple Account, oder von Gästen mit temporären Sitzungen. Es wird mit einem ADE-Profil eingerichtet, das Shared iPad aktiviert (siehe die Seite **Apple Automated Device Enrollment**), und sein Feld **Registrierungstyp** zeigt **Shared iPad** an.

- **Shared iPad-Benutzer**: die Benutzer des iPad, mit dem angemeldeten Benutzer, dem von ihnen belegten Speicher und ob einige Daten noch nicht mit iCloud synchronisiert wurden. Verwenden Sie **Aktualisieren**, um die Liste erneut vom iPad anzufordern. Ein Benutzer kann mit seinen Daten gelöscht werden, außer dem angemeldeten Benutzer

(melden Sie ihn zuerst ab); **Alle Benutzer löschen** erfordert iPadOS 14 oder neuer. Wenn die Daten noch nicht synchronisiert wurden, warnt die Bestätigung, dass sie verloren gehen.
- **Geräteeinstellungen**: der Speicher für jeden Benutzer, die erwartete Anzahl an Benutzern, die Inaktivitätszeit, nach der Benutzer und Gastsitzungen abgemeldet werden, nur Gastsitzungen, die auf dem Anmeldebildschirm vorgeschlagenen Domains für Managed Apple Accounts, wie viele Tage sich ein Benutzer anmelden kann, ohne das Passwort online zu prüfen, und das Überspringen der Sprach- und Regionseinrichtung für neue Benutzer. Leere Felder behalten ihren aktuellen Wert; Einstellungen, die ein neueres iPadOS erfordern, sind deaktiviert.

Mac-Benutzer

Auf einem Mac listet der Bereich **Mac-Benutzer** die Benutzer auf, die in der Verwaltung registriert sind, normalerweise der Benutzer, der den Mac registriert hat. Die Konten der Richtlinie werden in ihren Sitzungen installiert. Für jeden Benutzer wird angezeigt, wann er registriert wurde, der letzte Bericht seiner Sitzung und der Status der Konten: **Aktuell**, **Warten auf den Benutzer** (der Mac installiert sie, wenn der Benutzer angemeldet ist), **Nicht angewendet** mit den vom Mac gemeldeten Gründen oder **Keine Konten**, wenn die Richtlinie keine enthält. Verwenden Sie **Neu laden**, um die Liste erneut zu lesen.

Aktivierungssperre

Das Feld **Aktivierungssperre** zeigt, ob die Aktivierungssperre aktiviert ist. Wenn sie aktiviert ist, kann ein gelöschtes Gerät nur mit dem Apple Account des Benutzers oder mit dem Umgehungscode des Geräts erneut eingerichtet werden. Überwachte Geräte aktivieren die Aktivierungssperre nur, wenn sie in **Geräteeinstellungen** zulässig ist. Cerberus Enterprise fordert von überwachten Geräten ihren Umgehungscode an und speichert ihn: Verwenden Sie **Umgehungscode anzeigen** im Feldmenü, um ihn anzuzeigen (nur Administratoren können das, und jede Anzeige wird im Systemprotokoll aufgezeichnet), und geben Sie ihn dann als Passwort auf dem Aktivierungssperrbildschirm des Geräts ein, wobei der Apple Account leer bleibt.

Recovery Lock und Firmware-Passwort (Mac)

Ein Mac mit Apple Silicon zeigt das Feld **Recovery Lock**, ein Mac mit Intel-Prozessor das Feld **Firmware-Passwort**. Beide schützen den Mac beim Start: Mit Recovery Lock fragt recoveryOS nach dem Passwort; mit einem Firmware-Passwort fragt der Mac danach, um von einem anderen Datenträger oder aus der Wiederherstellung zu starten. Das Feld zeigt, ob der Mac ein Passwort meldet, und in seinem Tooltip, wann Cerberus Enterprise es gespeichert und wann es zuletzt überprüft wurde.

- **Passwort festlegen oder ändern**: Cerberus Enterprise generiert ein Passwort aus 20 Buchstaben, die bei jeder Tastaturbelegung auf denselben Tasten liegen, oder ein Administrator gibt eines ein (8 bis 64 Zeichen ohne Akzente; andere Rollen können nur eines generieren, da sie gespeicherte Passwörter nicht sehen können). Das Passwort wird verschlüsselt gespeichert, bevor es gesendet wird, und ersetzt das gespeicherte Passwort erst, wenn der Mac es bestätigt. Wenn auf dem Mac bereits ein Passwort außerhalb von Cerberus Enterprise festgelegt ist, geben Sie es als aktuelles Passwort ein: Es wird einmalig verwendet und nicht gespeichert.
- **Passwort überprüfen**: fragt den Mac, ob das gespeicherte Passwort korrekt ist. Das Ergebnis steht im Tooltip und im Systemprotokoll.
- **Passwort anzeigen**: Nur Administratoren können das gespeicherte Passwort sehen, und jede Anzeige wird im Systemprotokoll aufgezeichnet. Generierte Passwörter werden in Vierergruppen von Buchstaben angezeigt: Geben Sie sie ohne Leerzeichen ein.
- **Passwort löschen**: entfernt das Passwort vom Mac.

Ein Mac mit Intel-Prozessor startet neu, um eine Änderung des Firmware-Passworts anzuwenden: Bis dahin wird weiterhin das vorherige Passwort benötigt („Passwort anzeigen“ listet es auf), und eine weitere Änderung kann nicht gesendet werden. Apple akzeptiert außerdem nur einen Firmware-Passwort-Befehl alle 30 Sekunden. Die Passwörter werden im Befehlsverlauf ausgeblendet.

Wenn ein Mac die Verwaltung verlässt (Registrierung aufgehoben, vom Benutzer entfernt oder gelöscht), entfernt macOS Recovery Lock von selbst, und Cerberus Enterprise verwirft das gespeicherte Recovery Lock-Passwort; dasselbe geschieht, wenn der Mac meldet, dass er kein Recovery Lock hat, zum Beispiel nachdem er sich erneut registriert. Wenn Sie die Registrierung eines Mac aufheben (oder seine Richtlinie löschen), wird ein gespeichertes Firmware-Passwort zuerst gelöscht, der Mac startet neu und verlässt dann die Verwaltung. Wenn das Löschen fehlschlägt, verlässt der Mac die Verwaltung trotzdem, und das Passwort bleibt gespeichert, sodass Sie es weiterhin anzeigen können. Ein Mac, der vom Benutzer aus der Verwaltung entfernt oder gelöscht wurde, behält sein Firmware-Passwort: Cerberus Enterprise behält es ebenfalls. Durch Löschen des Geräteeintrags wird das gespeicherte Passwort gelöscht. Sie werden daher zuerst um Bestätigung gebeten: Notieren Sie das Passwort, denn ohne es kann nur Apple es entfernen.

FileVault (Mac)

Das Feld **FileVault** zeigt, ob die Festplatte des Mac verschlüsselt ist, und in seinem Tooltip, ob Cerberus Enterprise seinen persönlichen Wiederherstellungsschlüssel speichert. Ein Mac sendet den Schlüssel, wenn FileVault aktiviert wird, nachdem er die FileVault-Einstellung seiner Richtlinie erhalten hat (siehe die Seite **macOS** der Apple-Richtlinien).

- **Wiederherstellungsschlüssel anzeigen**: Nur Administratoren können den Schlüssel sehen, und jede Anzeige wird im Systemprotokoll aufgezeichnet. Verwenden Sie ihn am Anmeldefenster des Mac, um das Passwort des Benutzers zurückzusetzen, oder in der Wiederherstellung, um die Festplatte zu entsperren. Er bleibt verfügbar, nachdem der Mac

die Verwaltung verlassen hat; durch Löschen des Geräteeintrags wird er gelöscht.
- **Wiederherstellungsschlüssel ändern**: Der Mac ersetzt seinen persönlichen Wiederherstellungsschlüssel und sendet den neuen verschlüsselt; der alte Schlüssel funktioniert nicht mehr. Dies ist nur möglich, wenn der gespeicherte Schlüssel gelesen werden kann: Der Mac wird damit entsperrt, und es ist kein Benutzerpasswort erforderlich. Der gespeicherte Schlüssel wird im Befehlsverlauf ausgeblendet und vom Server entfernt, sobald der Mac antwortet (oder nach 7 Tagen ohne Antwort).

Bootstrap Token (Mac)

Ein Mac mit macOS 10.15 oder neuer sendet seinen **Bootstrap Token** an den Verwaltungsserver, wenn sich ein Benutzer mit einem sicheren Token anmeldet. Der Server behält ihn und gibt ihn nur an diesen Mac zurück, der ihn verwendet, um neuen Benutzern ein sicheres Token zu geben und auf einem Mac mit Apple Silicon Softwareupdates zu installieren und Kernel-Erweiterungen zu genehmigen, ohne ein Administratorpasswort anzufordern. Niemand kann den Token sehen, weder im Dashboard noch anderswo. Das Feld **Bootstrap Token** zeigt seinen Status:

- **Hinterlegt**: Der Server hat den Token; der Tooltip zeigt, wann der Mac ihn gesendet hat.
- **Früher hinterlegt**: Das gespeicherte Token wurde vor der letzten Registrierung oder MDM-Zertifikaterneuerung des Mac gesendet. Nach einer Erneuerung ist das zu erwarten: Das Token bleibt erhalten, und der Mac sendet es nicht erneut. Nach einer neuen Registrierung ist es möglicherweise nicht mehr gültig: Führen Sie `sudo profiles install -type bootstraptoken` im Terminal auf dem Mac aus.
- **Nicht hinterlegt**: Der Mac hat noch keinen Token gesendet. Um ihn jetzt zu senden, führt ein Administrator des Mac im Terminal `sudo profiles install -type bootstraptoken` aus (`sudo profiles status -type bootstraptoken` zeigt, ob er hinterlegt ist).

Der Tooltip gibt auch an, ob der Mac den Token zur Authentifizierung zulässt. Macs, die mit Automated Device Enrollment eingerichtet wurden, lassen ihn automatisch zu; auf anderen Macs mit Apple Silicon kann ein Benutzer ihn in Startup Security Utility in recoveryOS zulassen. Intel-Macs können den Token nicht zur Authentifizierung verwenden (**Nicht unterstützt**), aber ein hinterlegter Token gibt neuen Benutzern weiterhin ein sicheres Token. Jedes Mal, wenn ein Mac seinen Token sendet, entfernt oder anfordert, wird dies im Systemprotokoll aufgezeichnet.

Gerätestatus und OS-Updates

Der Bereich **Gerätestatus** zeigt, was das Gerät über sich selbst meldet: die OS-Version und den Build, den Fortschritt eines Softwareupdates (ausstehende Version, Frist, was es ausgelöst hat, Fehler), ob ein Code festgelegt ist und der Richtlinie entspricht, FileVault auf einem Mac, den Batteriezustand und die auf dem Gerät konfigurierten Konten.

Die Liste **Verfügbare Updates** zeigt die OS-Updates, die das Gerät installieren kann, erfasst bei der Registrierung und wöchentlich. Verwenden Sie **Nach Updates suchen**, um sie jetzt anzufordern, und **Installieren**, um ein Update sofort zu installieren (das Gerät startet nach einer

Bestätigung neu) oder nur herunterzuladen und den Benutzer installieren zu lassen. Dies funktioniert auf überwachten iPhones und iPads sowie auf Macs bis iOS, iPadOS und macOS 26: Bei späteren Versionen und zum Aktualisieren vieler Geräte verwenden Sie die erforderlichen Updates der Richtlinie (siehe die Seite **Softwareupdates** der Apple-Richtlinien).

Ein Mac mit Apple Silicon installiert ein Update nur dann ohne Eingabe eines Administratorpassworts, wenn er sein Bootstrap Token zur Authentifizierung zulässt und der Token hinterlegt ist (siehe Bootstrap Token oben). Andernfalls weist die Bestätigung darauf hin, dass ein Benutzer möglicherweise ein Administratorpasswort eingeben muss, bevor das Update installiert wird.

Anwendungen und Inventar

Der Bereich **Anwendungen** listet alle Apps des Geräts in einer Tabelle auf. Der Installationsstatus der von der Richtlinie oder mit einem Befehl installierten Apps wird vom Gerät live gemeldet; Versionen, Größen und die vom Benutzer installierten Apps stammen aus der letzten App-Liste, die bei der Registrierung und wöchentlich erfasst wird. Verwenden Sie **Gerät abfragen**, um sie jetzt anzufordern.

- **Verwaltung**: **Richtlinie** für Apps, die durch die Geräterichtlinie installiert wurden, **Verwaltet** für Apps, die mit einem Befehl wie **App installieren** installiert wurden, **Nicht verwaltet** für die vom Benutzer installierten. Die Cerberus Enterprise-App hat den Chip **Von Cerberus installiert**.
- **Handlungsbedarf**: Apps, deren Installation fehlgeschlagen ist, die vom Benutzer abgelehnt oder entfernt wurden oder auf den Benutzer warten. Öffnen Sie eine Zeile, um den Fehler anzuzeigen; fehlgeschlagene Richtlinien-Apps können mit der Wiederholen-Schaltfläche erneut installiert werden. Integrierte Apps und App Store-Apps, die das Gerät als nicht validiert meldet, werden nicht gezählt.
- **App entfernen**: verwaltete Apps können mit ihren Daten entfernt werden. Um eine von der Richtlinie installierte App zu entfernen, entfernen Sie sie aus der Richtlinie. Die Richtlinie sendet diesen Befehl auch selbst, wenn ein als verwaltete App installiertes Mac-Paket aus der Richtlinie entfernt wird.

Der Bereich **Profile, Zertifikate und Sicherheit** zeigt die vom Gerät gemeldeten Konfigurationsprofile, Zertifikate und den Sicherheitsstatus (Code, Verschlüsselung, FileVault und Firewall auf einem Mac).

> Auf persönlichen Geräten werden die vom Benutzer installierten Apps nicht erfasst, und es werden nur die von Cerberus Enterprise verwalteten Profile und Zertifikate aufgelistet.

Der Bereich **Inventaränderungen** zeigt, was sich zwischen zwei vom Gerät gesendeten Listen geändert hat: installierte, entfernte oder aktualisierte Apps (mit alter und neuer Version), installierte, entfernte oder aktualisierte Profile sowie hinzugefügte oder entfernte Zertifikate. Eine Änderung wird erkannt, wenn das Gerät eine neue Liste sendet – wöchentlich für Apps und Profile,

täglich für Zertifikate – oder wenn Sie **Gerät abfragen** verwenden: Das angezeigte Datum ist das Erkennungsdatum, die Änderung fand zwischen der vorherigen Liste und dieser statt. Die erste Liste eines Geräts und die erste nach einer neuen Registrierung oder einer Eigentumsänderung wird nur als Ausgangspunkt erfasst. Suchen Sie nach Name oder Kennung, und filtern Sie nach Art und Änderung. Änderungen werden 365 Tage lang aufbewahrt.

> Wenn ein OS-Update viele Apple-Apps auf einmal ersetzt, werden sie als eine Zeile angezeigt (zum Beispiel "23 Apple-Apps aktualisiert"), die Sie erweitern können. Eine Erneuerung des MDM-Zertifikats wird als **MDM-Zertifikat erneuert** angezeigt. Auf persönlichen Geräten werden nur die Änderungen der von Cerberus Enterprise verwalteten Elemente angezeigt.

Apple-Verlaufsspalten

- **Erstellungsdatum**
- **Befehl**
- **Status**: **Gesendet** (wartet auf das Gerät, wird zugestellt, sobald es sich verbindet), **Erfolgreich**, **Beantwortet** (öffnen Sie die Zeile, um das Ergebnis zu sehen), **Warten auf das Gerät** (das Gerät kann den Befehl derzeit nicht ausführen), **Fehlgeschlagen** (öffnen Sie die Zeile, um den Grund zu sehen) oder **Abgebrochen** (die Befehlswarteschlange des Geräts wurde geleert, zum Beispiel als es sich erneut registriert hat).
- **Ausführungsdatum**

Aktualisieren

Verwenden Sie die Aktualisierungsaktion im Bereich Befehle, um den Befehlsverlauf neu zu laden.