jamf | SCHOOL

Sicherheitsübersicht

2. März 2021

jamf

Jamf
100 Washington Ave S Suite 1100
Minneapolis, MN 55401-2155
(612) 605-6625

Inhalt

Jamf School

Übersicht

In diesem Leitfaden erfahren Sie mehr über die Funktionen und das Framework für Sicherheit und Geräteverwaltung von Jamf School. Jamf School ist eine Lösung zur Endpunktverwaltung für Mac Computer in institutionellem Besitz, iPhone und iPad Geräte in institutionellem und persönlichem Besitz sowie Apple TV Geräte in institutionellem Besitz. Jamf School umfasst die folgenden Komponenten:

- Den Jamf School Server
- Framework zur Geräteverwaltung
- Verteilung von Inhalten
- Jamf School Anwendungen:
  - Jamf Teacher
  - Jamf School Student
  - Jamf Parent

Jamf School ist ein gehosteter Dienst in Jamf Cloud. Weitere Informationen zu Jamf Cloud finden Sie unter Cloud MDM auf der Jamf Website.

Datenerfassung

Bei Jamf müssen Sie keine vertraulichen oder sensiblen persönlichen Daten angeben, um Jamf School zu verwenden. Bei Jamf School werden nur Daten erfasst, die für den Betrieb der Software zwingend erforderlich sind, sowie alle Daten, die Sie in den gehosteten Diensten zur Verwaltung Ihrer Geräte eingeben. Bei Jamf werden zusätzliche Daten, die Kunden in den gehosteten Diensten eingeben, weder kontrolliert noch Regelungen unterworfen.

Für Computer und Mobilgeräte erfasste Informationen

Computer und Mobilgeräte können viele Arten von Bestandsinformationen an Jamf School übermitteln. Grundlegende Bestandsinformationen, z. B. Informationen zu Hardware, Betriebssystem, Benutzer, Standort, Sicherheitsberichten, Speicher und Anwendungen, werden automatisch erfasst.

Weitere Informationen zu den in Jamf School erfassten Daten finden Sie unter Anzeigen und Bearbeiten von Geräteinformationen in Jamf School in der *Jamf School Dokumentation mit Bereitstellungsleitfaden*.

Mit Apple School Manager geteilte Informationen

Wenn die Verbindung zwischen Jamf School und Apple School Manager erfolgreich hergestellt wurde, können Sie wählen, ob die an Apple School Manager gesendeten Benutzerdaten anonymisiert werden sollen. Weitere Informationen finden Sie unter Integration von Jamf School in Apple School Manager in der *Jamf School Dokumentation mit Bereitstellungsleitfaden*.

Mit Microsoft Intune geteilte Informationen

Wenn die Verbindung zwischen Jamf School und Microsoft Intune erfolgreich hergestellt wurde, werden von Jamf School zu jedem bei Azure AD registrierten Computer Bestandsinformationen an Microsoft Intune gesendet.

Notiz: Es werden keine Bestandsinformationen mit Microsoft Intune geteilt, es sei denn, die Azure Active Directory Einstellungen sind in Jamf School aktiviert. Weitere Informationen finden Sie unter Integration in Microsoft Azure in der *Jamf School Dokumentation mit Bereitstellungsleitfaden*.

Von Jamf School verwendete Netzwerkports

Die vollständige Liste der erforderlichen Ports hängt von den spezifischen Diensten und Funktionen ab, die in einer bestimmten Umgebung aktiviert sind.

Um sicherzustellen, dass Jamf School korrekt mit verwalteten Geräten und Apple kommunizieren kann, müssen die folgenden Ports in allen Umgebungen grundlegende Funktionen erfüllen:

Port	Protokoll	Beschreibung	Verbindungen
5223 /443	TCP	Hiermit wird die ordnungsgemäße Kommunikation zwischen Jamf School und den verwalteten Geräten sichergestellt. Vergewissern Sie sich, dass in allen Client-Netzwerken ausgehende Verbindungen zu und Weiterleitungen von dem **IP-Adressblock 17.0.0.0/8 von Apple** über diese Ports erlaubt sind. Dadurch wird die ordnungsgemäße Funktionsweise des Apple Push Notification service (APNs) in Ihrem Netzwerk gewährleistet.	Zu Jamf School und APNs

Port	Protokoll	Beschreibung	Verbindungen
389 /636	LDAP oder LDAPS	Eine Integration von **Verzeichnisdiensten** via LDAP (Port 389) oder LDAPS (LDAP über SSL, Port 636) kann zur Benutzerauthentifizierung, Gerätezuweisung und zum Abrufen von Informationen über Benutzer und Gruppenmitgliedschaften genutzt werden.	Jamf School Server zu LDAP- /Domänencontroller **Hinweis:** Alle LDAP-Verbindungen des Jamf School Servers gehen von Jamf Pro Server aus.

Neben den in der Tabelle aufgeführten Ports finden Sie in diesen Apple Dokumentationen weitere Ports, die der Positivliste hinzugefügt werden müssen:

- Von Apple-Softwareprodukten verwendete TCP- und UDP-Ports
  Hier erfahren Sie mehr über die von Apple Produkten verwendeten TCP- und UDP-Ports.
- Apple-Produkte in Unternehmensnetzwerken verwenden
  Hier erfahren Sie, welche Hosts und Ports für die Verwendung von Apple Produkten in Unternehmensnetzwerken benötigt werden.

Verschlüsselung der Kommunikation

Die Kommunikation zwischen Jamf School und den verwalteten Computern und Mobilgeräten wird nach dem Standard „Transmission Layer Security“ (TLS) verschlüsselt.

Computer können so konfiguriert werden, dass sie eine zertifikatbasierte Kommunikation mit Jamf School nutzen und für die Jamf School Web-App eine SSL-Zertifikatüberprüfung anfordern. Wenn die zertifikatbasierte Kommunikation aktiviert ist, prüft Jamf School einen Gerätesignatur-Header bei jeglicher sensibler Kommunikation und antwortet nur, wenn die Signatur mit dem Gerät übereinstimmt, für das Ressourcen angefordert werden. Wenn die SSL-Zertifikatüberprüfung aktiviert ist, müssen Computer eine Überprüfung des SSL-Zertifikats für die Jamf School Web-App durchführen. Alle Antworten, die ein ungültiges SSL-Zertifikat enthalten, werden zurückgewiesen.

Für die Verwaltung von MDM-kompatiblen Computern und Mobilgeräten wird eine Standard-Kommunikationsverschlüsselung genutzt, wie sie der Apple Push-Benachrichtigungsdienst (APNs) bietet.

Datenbankverschlüsselung

Die gesamte Jamf School Datenbank wird im Ruhezustand verschlüsselt, einschließlich aller Protokolle, Backups und Snapshots.

Passwörter für Jamf School Administratoraccounts werden mit der passwortbasierten Schlüsselableitungsfunktion bcrypt gehasht. Zertifikatpasswörter werden ebenfalls verschlüsselt und gespeichert, um sie bei der Benutzerauthentifizierung zu verwenden.

Die individuellen FileVault Wiederherstellungsschlüssel werden mit einem Standard-AES-256-Algorithmus mit einem eindeutigen Schlüssel für jede Jamf School Instanz verschlüsselt, der in der Datenbank gespeichert wird.

Schwachstellenbewertungen

Vor jeder Veröffentlichung werden automatisierte Penetrationstests und Prüfungen auf Schwachstellen für Jamf School durchgeführt. Darüber hinaus werden jährlich codegestützte Penetrationstests und Schwachstellenbewertungen durch einen externen Sicherheitsberater durchgeführt.

Audits anderer Anbieter

Jamf ist dabei, ein Service Organization Control 2 (SOC 2) Type 2 Audit für die von Jamf School gehosteten Dienste abzuschließen. Wenden Sie sich für weitere Informationen an Ihren Vertriebs- oder Supportmitarbeiter.

Der Jamf School Server

Übersicht

Jamf School ist eine Web-App mit einem MySQL Backend, das als administrativer Kern von Jamf School genutzt wird. Mit Jamf School können Sie Bestandsmanagement- und Fernverwaltungsfunktionen sowie Konfigurationsaufgaben auf verwalteten Computern und Mobilgeräten durchführen. Alle sonstigen Administrationsanwendungen von Jamf School kommunizieren mit dem Jamf School Server.

Der Server, auf dem Jamf School gehostet ist, muss die Mindestanforderungen des Betriebssystems und der Datenbankkonfiguration erfüllen. Detaillierte Informationen zu diesen Anforderungen finden Sie im Abschnitt Systemanforderungen von Jamf School in der *Jamf School Dokumentation mit Bereitstellungsleitfaden*.

Verteilte Server und Jamf School Web-App-Clustering

Die Jamf School Web-App- und Datenbankserver sind auf separate Server verteilt, und es kann derselbe Datenbankserver mit mehreren Web-App-Servern verwendet werden.

Jamf School Administratoraccounts

Die Anmeldedaten für den lokalen Jamf School Administratoraccount werden in der Datenbank gespeichert und vom Jamf School Server authentifiziert. Zwei-Faktor-Authentifizierung und die Funktion zum Zurücksetzen eines verlorenen Passworts sind für lokale Jamf School Administratoraccounts verfügbar.

Die Jamf School Web-App kann so konfiguriert werden, dass sie den Zugriff auf die Administratorbenutzeroberfläche einschränkt, aber trotzdem Geräteverwaltungsfunktionen nur für Computer, nur für Mobilgeräte oder für beides erlaubt. Rollenbasierter Zugriff mit feinstufigen Rechten für Erstellen, Lesen, Aktualisieren und Löschen ist für Jamf School Objekte verfügbar.

Integration von Verzeichnisdiensten

Jamf School unterstützt die Integration der folgenden Verzeichnisdienste:

- Open Directory von Apple
- Active Directory von Microsoft
- NetIQ eDirectory

Durch die Integration eines LDAP-Verzeichnisdienstes können Sie:

- Benutzerinformationen aus dem Verzeichnisdienst zum Zweck der Bestandserfassung abrufen und automatisch einfügen
- Benutzeraccounts oder Gruppen in Jamf School anhand des Verzeichnisdienstes erstellen
- Dafür sorgen, dass sich Benutzer mit ihren Anmeldedaten für den LDAP-Verzeichnisdienst bei Jamf Teacher, Jamf School Student oder dem Registrierungsportal anmelden
- Dafür sorgen, dass sich die Benutzer während der Einrichtung ihres Mobilgeräts mit ihren Anmeldedaten für den LDAP-Verzeichnisdienst anmelden
- Benutzer oder Gruppen aus dem Verzeichnisdienst zum Anwendungsbereich für Fernverwaltungsaufgaben hinzufügen

Weiterführende Informationen finden Sie im Abschnitt Konfigurieren der Authentifizierung über LDAP in Jamf School in der *Jamf School Dokumentation mit Bereitstellungsleitfaden*.

Multi-Faktor- oder Single Sign-On Authentifizierung

Single Sign-On mit SAML 2.0 Authentifizierung wird in Jamf School unterstützt. Die Single Sign-On (SSO) Funktion ermöglicht die Integration in einen externen Identitätsdienst und die Aktivierung von SSO für den Jamf School Server und die gerätebasierte Registrierung (macOS und iOS). Jamf School unterstützt die Anmeldung via Google und Microsoft Azure zur Authentifizierung. Weitere Informationen finden Sie in den Abschnitten Einrichten der Anmeldung via Google in Jamf School und Integration in Microsoft Azure in der *Jamf School Dokumentation mit Bereitstellungsleitfaden*.

Prüfprotokolle

Jamf School erfasst Prüfprotokolle für Ereignisse in Jamf School sowie für Ereignisse in der Jamf School Zwei-Faktor-Authentifizierung. Administratoren können in Jamf School die Prüfprotokolle für Jamf School Ereignisse anzeigen, indem sie zu **Organisation > Audit Log** navigieren, und die Prüfprotokolle zu Jamf School Zwei-Faktor-Authentifizierungsereignissen, indem sie zu **Mein Account > Letztes Ereignis** navigieren.

Framework zur Geräteverwaltung

Registrierung von Computern

Als Registrierung wird das Hinzufügen von Mac Computern zu Jamf School bezeichnet. Während der Registrierung werden von den Computern Bestandsinformationen an Jamf School übermittelt. Weitere Informationen zu den verschiedenen Möglichkeiten, Computer bei Jamf School zu registrieren, finden Sie unter Registrierungsmethoden in der *Jamf School Dokumentation mit Bereitstellungsleitfaden*.

Auf verwalteten Computern installierte Komponenten

Die folgenden Komponenten können auf verwalteten Computern installiert werden:

- **MDM-Profil –** Dieses Profil enthält eine SCEP-Registrierungsanfrage und eine MDM-Registrierungsanfrage. Das MDM-Profil muss zur Installation vom Benutzer akzeptiert werden.
- **Vertrauensprofil –** Dieses Profil enthält das CA-Zertifikat. Mit dem CA-Zertifikat werden die Zertifizierungsstelle (CA) und die Mobilgeräte als vertrauenswürdig eingestuft. Wenn Sie Mobilgeräte per automatischer Geräteregistrierung oder per Apple Configurator und per Registrierungs-URL registriert haben, ist das Vertrauensprofil kein separates Profil, sondern im MDM-Profil enthalten.
- **Jamf Teacher für macOS –** Mit Jamf Teacher können Sie macOS Profile, Apps und Bücher an Mobilgeräte verteilen, damit sie von den Benutzern installiert werden. Jamf Teacher ermöglicht Lehrern auch eine begrenzte Verwaltung von Schülergeräten.
- **Jamf School Student für macOS –** Mit Jamf School Student können Sie macOS Profile, Apps und Bücher an Mobilgeräte verteilen, damit sie von den Benutzern installiert werden. Jamf School Student ermöglicht Lehrern in Verbindung mit Jamf Teacher auch eine begrenzte Verwaltung von Schülergeräten.
- **Jamf School Self Service für macOS –** Mit Jamf School Self Service können Sie macOS Profile, Apps und Bücher an Mobilgeräte verteilen, damit sie von den Benutzern installiert werden.
- **Skripterstellungs-Daemon –** Wenn das Skripterstellungsmodul aktiviert ist, können Sie mit diesem Daemon Skripts auf verwalteten Computern ausführen.

Registrierung von Mobilgeräten

Bei der Registrierung werden Mobilgeräte zu Jamf School hinzugefügt, um eine Verbindung zwischen den Geräten und Jamf School herzustellen. Dadurch können Sie für diese Geräte Aufgaben im Zusammenhang mit der Erfassung von Bestandsinformationen, der Konfiguration von Einstellungen und Sicherheitsfeatures sowie der Verteilung von Inhalten ausführen. Weitere Informationen zu den verschiedenen Möglichkeiten, Mobilgeräte bei Jamf School zu registrieren, finden Sie unter Registrierungsmethoden in der *Jamf School Dokumentation mit Bereitstellungsleitfaden*.

Auf Mobilgeräten installierte Komponenten

Die folgenden Komponenten werden auf verwalteten Mobilgeräten installiert:

- **MDM-Profil –** Dieses Profil enthält eine SCEP-Registrierungsanfrage und eine MDM-Registrierungsanfrage. Das MDM-Profil muss zur Installation vom Benutzer akzeptiert werden.
- **Vertrauensprofil –** Dieses Profil enthält das CA-Zertifikat. Mit dem CA-Zertifikat werden die Zertifizierungsstelle (CA) und die Mobilgeräte als vertrauenswürdig eingestuft. Wenn Sie Mobilgeräte per automatischer Geräteregistrierung oder per Apple Configurator und per Registrierungs-URL registriert haben, ist das Vertrauensprofil kein separates Profil, sondern im MDM-Profil enthalten.
- **Gerätezertifikat –** Dieses Zertifikat überprüft die Identität verwalteter Mobilgeräte jedes Mal, wenn diese Geräte mit Jamf School kommunizieren.
- **Jamf Teacher für iOS –** Mit Jamf Teacher können Sie iOS Profile, Apps und Bücher an Mobilgeräte verteilen, damit sie von den Benutzern installiert werden. Jamf Teacher ermöglicht Lehrern auch eine begrenzte Verwaltung von Schülergeräten.
- **Jamf School Student für iOS –** Mit Jamf School Student können Sie iOS Profile, Apps und Bücher an Mobilgeräte verteilen, damit sie von den Benutzern installiert werden. Jamf School Student ermöglicht Lehrern in Verbindung mit Jamf Teacher auch eine begrenzte Verwaltung von Schülergeräten.

Protokolle von Computern und Mobilgeräten

Jamf School ermöglicht es Administratoren, Prüfprotokolle für die 500 letzten Schnellaktionsbefehle anzuzeigen, die an Computer und Mobilgeräte gesendet wurden. Administratoren können Prüfprotokolle in Jamf School anzeigen, indem sie zu **Geräte > Übersicht** navigieren und auf einen Gerätedatensatz und dann auf **Prüfprotokoll** klicken.

Auf verwalteten Computern und Mobilgeräten verfügbare Befehle zur Fernverwaltung

Eine Liste der verfügbaren Fernbefehle, mit denen Sie Aufgaben aus der Ferne ausführen können, finden Sie im Abschnitt Befehle für Schnellaktionen im Zusammenhang mit der Geräteverwaltung in der *Jamf School Dokumentation mit Bereitstellungsleitfaden*.

Jamf School Anwendungen

Jamf Teacher

Jamf Teacher ist als kostenlose App verfügbar und ermöglicht Lehrern in Kombination mit der Jamf School Student App die Verwaltung von Schülergeräten im Unterricht. Die Verwaltungsfunktionen von Jamf Teacher werden in Jamf School unter **Organisation > Einstellungen > Jamf School Teacher** konfiguriert. Weitere Informationen zur Konfiguration dieser Funktionen finden Sie unter Konfigurieren der Jamf Teacher App in Jamf School in der *Jamf School Dokumentation mit Bereitstellungsleitfaden*.

Abhängig von den Einstellungen, die von Ihrer Schule aktiviert werden, können Lehrer mit Jamf Teacher Folgendes durchführen:

- Klassen erstellen und verwalten
- Unterrichtseinheiten erstellen und starten
- Eine Unterrichtseinheit freigeben
- Schüler zu einer Fernunterrichtsklasse einladen
- Nachrichten an Schüler senden
- Apps für Schüler anfordern
- Ihre Geräte verwalten

Lehrer können mit Jamf Teacher weder Jamf School Daten auf ihrem Gerät noch den Bildschirm eines Schülers anzeigen.

Authentifizierung bei Jamf Teacher

Um dafür zu sorgen, dass Benutzer sich mit einem LDAP-Account anmelden können bzw. müssen, muss in Jamf School zunächst ein LDAP-Server eingerichtet werden. Weitere Informationen finden Sie unter Konfigurieren der Authentifizierung über LDAP in Jamf School in der *Jamf School Dokumentation mit Bereitstellungsleitfaden*.

Um dafür zu sorgen, dass Benutzer sich mit einem Jamf School Benutzeraccount anmelden können bzw. müssen, muss zunächst ein Account für den jeweiligen Benutzer erstellt werden. Weitere Informationen finden Sie unter Erstellen von Benutzeraccounts in der *Jamf School Dokumentation mit Bereitstellungsleitfaden*.

Jamf School Student

Jamf School Student ist eine kostenlose App, in der Schüler auf Apps, Profile und Dokumente zugreifen können, die ihnen zugewiesen wurden. In Kombination mit der Jamf Teacher App ermöglicht sie Lehrern darüber hinaus die Verwaltung der Schülergeräte in ihren Klassen. Die Verwaltungsfunktionen von Jamf School Student werden in Jamf School unter **Organisation > Einstellungen > Jamf School Student** konfiguriert. Weitere Informationen zur Konfiguration dieser Funktionen finden Sie unter Konfigurieren der Jamf School Student App in Jamf School in der *Jamf School Dokumentation mit Bereitstellungsleitfaden*.

Abhängig von den Einstellungen, die von Ihrer Schule aktiviert werden, können Schüler mit Jamf School Student Folgendes durchführen:

- Apps, Dokumente und Profile anzeigen, die ihnen zugewiesen sind
- Nachrichten an ihren Lehrer senden und Nachrichten von ihrem Lehrer empfangen
- Die Hand heben, um dem Lehrer eine Frage zu stellen
- Auf ihren Geräten verfügbare Betriebssystem-Updates anzeigen und ausführen, die Gerätedetails aktualisieren, den Code löschen, die Aktivierungssperre aufheben und die auf dem Gerät gespeicherten Daten löschen

Authentifizierung bei Jamf School Student

Um dafür zu sorgen, dass Benutzer sich mit einem LDAP-Account anmelden können bzw. müssen, muss in Jamf School zunächst ein LDAP-Server eingerichtet werden. Weitere Informationen finden Sie unter Konfigurieren der Authentifizierung über LDAP in Jamf School in der *Jamf School Dokumentation mit Bereitstellungsleitfaden*.

Um dafür zu sorgen, dass Benutzer sich mit einem Jamf School Benutzeraccount anmelden können bzw. müssen, muss zunächst ein Account für den jeweiligen Benutzer erstellt werden. Weitere Informationen finden Sie unter Erstellen von Benutzeraccounts in der *Jamf School Dokumentation mit Bereitstellungsleitfaden*.

Jamf Parent

Die kostenlose Jamf Parent App ermöglicht die Verwaltung von an Schüler ausgegebenen Geräten, indem die Nutzung von Apps und Funktionen der Geräte erlaubt oder eingeschränkt wird. Eltern können die Geräte ihrer Kindern auf zweierlei Weise zu Jamf Parent hinzufügen: Sie scannen entweder auf dem Schülergerät einen QR-Code oder melden sich mit ihren in Jamf School erstellten Anmeldeinformationen an. Wenn die Schülergeräte durch Scannen eines QR-Codes zu Jamf Parent hinzugefügt werden, erübrigt sich die Erstellung einer Benutzergruppe mit den zugehörigen Accounts für die Eltern in Jamf School. Sie können mit Jamf School Benutzeraccounts und -gruppen

für Eltern erstellen. Weitere Informationen finden Sie unter Erstellen von Benutzeraccounts und Erstellen von Anmeldeinformationen für Benutzeraccounts in der *Jamf School Dokumentation mit Bereitstellungsleitfaden*.

Weitere Informationen zur Konfiguration dieser Funktionen finden Sie unter Konfigurieren der Jamf Parent App in Jamf School in der *Jamf School Dokumentation mit Bereitstellungsleitfaden*.

Verwalten von Apps auf Mobilgeräten

Mit verwalteten Apps kann der Administrator verhindern, dass ein Backup von Daten erstellt wird, und verlangen, dass die App und die zugehörigen Daten vom Gerät entfernt werden, wenn das MDM-Profil entfernt wird.

Weiterführende Informationen finden Sie unter Verwaltete Apps in Jamf School in der *Jamf School Dokumentation mit Bereitstellungsleitfaden*.

Sicherheitseinstellungen auf verwalteten Computern

Verwalten von FileVault auf Computern

Die folgenden Optionen sind für die Verwaltung von FileVault auf verwalteten Computern verfügbar:

Konfiguration:

- Konfigurationen für die Festplattenverschlüsselung
- macOS Profil mit einer Payload für Sicherheit und Datenschutz

Bericht:

- Erweiterte Suchvorgänge nach Computern
- Dynamische Computergruppe, bei der das Kriterium „FileVault aktiviert“ verwendet wird
- Dynamische Computergruppe, bei der das Kriterium „Hat institutionellen Wiederherstellungsschlüssel“ verwendet wird
- Dynamische Computergruppe, bei der das Kriterium „Hat persönlichen Wiederherstellungsschlüssel “ verwendet wird
- Dynamische Computergruppe, bei der das Kriterium „Persönlicher Schlüssel in Escrow“ verwendet wird

Optionen für Systemintegritätsschutz

Für Computer, die von Jamf School verwaltet werden, sind die folgenden Optionen zum Schutz der Systemintegrität verfügbar:

Bericht:

- Status für Systemintegritätsschutz beim Anzeigen von Bestandsinformationen
- Erweiterte Suchvorgänge nach Computern
- Dynamische Gruppe, bei der das Kriterium „Hat Systemintegritätsschutz aktiviert“ verwendet wird

Gatekeeper Optionen

Für Computer, die von Jamf School verwaltet werden, ist die folgende Gatekeeper Option verfügbar:

Konfiguration:

Computerprofil mit einer Payload für Sicherheit und Datenschutz

Optionen für die Verwaltung von Einstellungen

Jamf School ermöglicht die Bereitstellung von Profilen, die von Apple bereitgestellte Standard-Payloads enthalten, um Einstellungen auf Computern und Mobilgeräten zu verwalten.

Anwenden randomisierter Passwörter auf Verwaltungsaccounts

Gerätebasierte Einladungen zur Registrierung von Computern sind standardmäßig so konfiguriert, dass für den Verwaltungsaccount zufällige Passwörter generiert werden, wodurch der Registrierungseinladung ein zufälliges Passwort mit der angegebenen Anzahl alphanumerischer Zeichen zugewiesen wird. Der Verwaltungsaccount erhält das zufällige Passwort beim Einlösen der Einladung, wenn die folgenden Voraussetzungen erfüllt sind:

- Der Computer ist in Jamf School noch nicht vorhanden oder, falls doch, gibt es dafür keinen bestehenden Verwaltungsaccount.
- Der angegebene Verwaltungsaccount ist auf dem Computer noch nicht vorhanden.

Wenn der Computer bereits vorhanden ist und bereits verwaltet wird (erneute Registrierung), wird das vorhandene Passwort für den Verwaltungsaccount anstelle des randomisierten Passworts aus der Registrierungseinladung verwendet. Ist der Account bereits auf dem Computer vorhanden, wird das Passwort im Jamf School Bestand gespeichert. Das Passwort wird auf dem Computer nicht aktualisiert, sodass bestimmte Funktionen beeinträchtigt sein können.

Gerätemanagement-Funktionen

Je nach Eigentümerschaft, Gerätetyp und installierter Betriebssystemversion können unterschiedliche Funktionen zur Verwaltung eines Geräts verfügbar sein. Eine Übersicht über die mit Jamf School verfügbaren Verwaltungsfunktionen finden Sie in folgenden Abschnitten in der *Jamf School Dokumentation mit Bereitstellungsleitfaden*:

- Anzeigen und Bearbeiten von Geräteinformationen in Jamf School
- Befehle für Schnellaktionen im Zusammenhang mit der Geräteverwaltung

Verteilung von Inhalten an verwaltete Computer und Mobilgeräte

Jamf School unterstützt einen Cloud-Verteilungspunkt, der die Amazon S3 oder Amazon CloudFront Content Delivery Networks (CDNs) zum Hosten von Dateien nutzt.

Jamf Cloud Hosting

Übersicht

Jamf verwaltet Ihre Jamf School Serverinfrastruktur über den Jamf Cloud Hosting-Dienst. Jamf Cloud Instanzen können die folgenden Komponenten umfassen:

- Eine gehostete Jamf School Umgebung
- Flexible Lastverteiler
- HAProxy Lastverteiler
- NGINX Lastverteiler
- Amazon Aurora
- Java Development Kit (kompatibel zu OpenJDK)
- Linux basiertes Hostbetriebssystem

Geografische Regionen

Für Jamf Cloud werden Server in Deutschland, Japan und den USA genutzt. Ruhende Daten für europäische Kunden bleiben in Deutschland.

Dienstverfügbarkeit

Bei Jamf Cloud wird eine geclusterte Jamf School Konfiguration mit mehreren Web-Apps mit Lastverteilung genutzt.

Es werden regelmäßige Wartungsarbeiten durchgeführt, die Upgrades der Jamf School Version, Infrastruktur- und Sicherheitsverbesserungen beinhalten können. Kunden werden vor dem Beginn von Wartungsarbeiten, die einen Dienstausfall unumgänglich machen, benachrichtigt.

Datenbank-Backups

Datenbanken werden kontinuierlich auf einen anderen Server in einem anderen Rechenzentrum repliziert. Alle 24 Stunden wird ein Snapshot von jeder Datenbank erstellt, der im Falle eines kritischen Ereignisses zur Wiederherstellung der Daten verwendet werden kann.

Wiederherstellung

Für Jamf Cloud werden Anwendungs- und Datenbankserver in mehreren Rechenzentren genutzt, um eine hohe Verfügbarkeit und Wiederherstellung im Fall eines Dienstausfalls bereitzustellen.

Verschlüsselung der Kommunikation

Für Jamf Cloud wird ein externes SSL-Zertifikat eines anderen Anbieters für die Jamf School Web-App verwendet. Darüber hinaus wird bei Jamf Cloud für Daten, die zwischen einem verwalteten Endpunkt und dem Jamf School Server übertragen werden, TLS genutzt.

Logische Datentrennung

Daten werden in der Jamf Cloud Infrastruktur auf verschiedenen Ebenen logisch getrennt. Nur Prozesse und Threads wie z. B. Abfragen innerhalb des Kontexts einer authentifizierten Organisation dürfen auf die Daten dieser Organisation zugreifen. Diese Einschränkung gilt für alle Daten und Prozesse/Threads, sowohl im Speicher als auch auf Laufwerken.

Zugriff für Mitarbeiter

Jamf Support Mitarbeiter können sich bei den Servern, auf denen Jamf School gehostet wird, anmelden und auf Einstellungen zugreifen, die mit dem Supportproblem eines Kunden zusammenhängen. In seltenen Fällen kann es vorkommen, dass Mitarbeiter von Jamf Cloud Operations auf Ihre Datenbank zugreifen müssen, um ein Supportproblem zu lösen. Hierbei unternehmen die Mitarbeiter alle Anstrengungen, um Ihre Privatsphäre zu respektieren, und greifen nur auf die Dateien und Einstellungen zu, die zur Durchführung der erforderlichen Aufgaben benötigt werden.

Gemeinsames Sicherheitsmodell

Jeder Anbieter, der zur Unterstützung von Jamf Cloud eingesetzt wird, muss sich an die gleichen Sicherheitsmaßnahmen halten, die auch von Jamf angewendet werden. Anbieter müssen eine Anbieterbewertung bestehen, bevor ihre Produkte oder Dienste in der Jamf Cloud Umgebung bereitgestellt werden. Jeder Anbieter ist für die Sicherheit der von ihm angebotenen Produkte oder Dienste verantwortlich. Jamf ist für die sichere Nutzung der Produkte oder Dienste verantwortlich.

Physische Sicherheit

Alle für Jamf Cloud verwendeten physischen Rechenzentren werden von Amazon Web Services verwaltet. Zusätzlich werden physische Sicherheitsmaßnahmen wie biometrische Zugangskontrollen, rund um die Uhr anwesendes bewaffnetes Wachpersonal und Videoüberwachung eingesetzt, um sicherzustellen, dass kein unbefugter Zugang möglich ist. Weitere Informationen finden Sie in der Dokumentation Amazon Web Services: Übersicht über die Sicherheitsprozesse von Amazon.

Schwachstellenbewertungen

Jamf Cloud wird Penetrationstests und Schwachstellenbewertungen unterzogen. Darüber hinaus kommen in Jamf Cloud Tools für kontinuierliche Schwachstellenüberwachung und Intrusion Detection zum Einsatz.