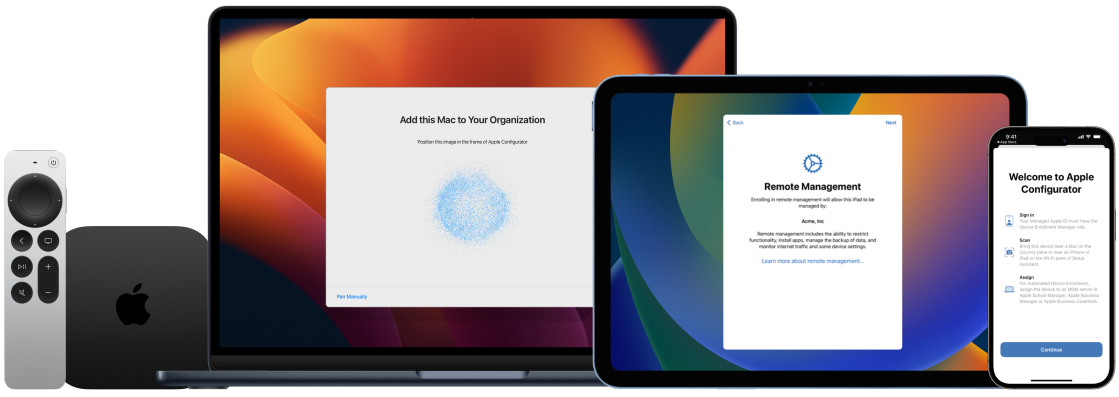
Training

Apple Deployment und Verwaltung

Leitfaden zur Prüfungsvorbereitung



Inhalt

Über die Prüfung

Die Prüfung „Apple Deployment and Verwaltung“ testet dein Verständnis der Tools, Dienste und bewährten Vorgehensweisen, die du für die Bereitstellung, Sicherung und Verwaltung von Apple-Geräten in großem Maßstab in großen Organisationen benötigst. Wenn du die Prüfung bestehst, erhältst du das Zertifikat „Apple Certified IT Professional“. Weitere Informationen findest du auf Apple Training.

Diese Prüfung basiert auf iOS 17, iPadOS 17 und macOS Sonoma.

Auf die Prüfung vorbereiten

Die Prüfung deckt nicht nur die Themen des Kurses „Apple Deployment and Management“, sondern alle in diesem Leitfaden aufgeführten Lernziele ab. Um die Prüfung zu bestehen, musst du mehrere Apple-Ressourcen studieren und praktische Erfahrungen bei der Bereitstellung und Verwaltung von Apple-Geräten sammeln. Abhängig von deinem Hintergrund, deinem technischen Fachwissen und deiner Erfahrung mit der Bereitstellung und Verwaltung von Apple-Geräten kann die Vorbereitung auf diese Prüfung 30 bis 60 Stunden dauern.

Um dich auf die Prüfung vorzubereiten, gehe wie folgt vor:

- Mache dich mit der Unterstützung von iPhone-, iPad- und Mac-Benutzern in einem Unternehmen vertraut.
- Sammle praktische Erfahrungen mit dem Deployment und der Verwaltung von Apple-Geräten in einer Organisation.
- Lies die Lernziele in diesem Leitfaden und identifiziere die Ressourcen, die du zum Lernen benötigst.
- Absolviere den Onlinekurs Apple Deployment and Management. Studiere den Inhalt und die verlinkten Ressourcen, führe die Übungen durch, und nutze die Fragen zur Überprüfung deines Verständnisses in jedem Artikel oder Lernprogramm, um dein Wissen zu festigen.
- Übe anhand der Beispielfragen in diesem Leitfaden.

Lernziele

Bereitstellung

Erläutern, inwiefern sich Eigentumsmodelle für Geräte auf die Bereitstellungsstrategie eines Unternehmens auswirken.

- Benutzereigene Geräte registrieren (Englisch)
- Organisations-Apps und Daten verwalten (Englisch)
- Trennung von Benutzer- und Organisationsdaten durch Apple
- Registrieren persönlicher Geräte durch Benutzer

Dienste für die Identitäts- und Authentifizierungsverwaltung wie Gesamtauthentifizierung (SSO) und Entra ID (früher Azure AD) evaluieren, um den sicheren Zugriff auf die Ressourcen Ihrer Organisation mit Apple-Geräten zu verwalten.

- Bewertung von Authentifizierung und Benutzerdiensten (Englisch)
- Platform Single Sign-on für macOS

Die Netzwerkinfrastruktur einer Organisation im Hinblick auf Profile und Payloads für Apple-Geräte bewerten.

- Netzwerkverkehr verwalten
- Einstellungen der MDM-Payload „Regeln für Netzwerkbenutzung“ für Apple-Geräte

Anforderungen der accountgesteuerten Geräteregistrierung mit der profilbasierten Geräteregistrierung vergleichen.

- Accountgesteuerte Geräteregistrierung

Die wichtigsten Überlegungen für die Bereitstellung von Apple-Geräten in Szenarien mit Geräten im Besitz einer Organisation identifizieren.

- Registrierungs- und Systemassistent verwalten (Englisch)
- Grundlegendes zur Geräteregistrierung (Englisch)
- Geräteregistrierung und MDM
- Automatisierte Geräteregistrierung und MDM

In einem gegebenen Szenario eine Bereitstellungsstrategie für verschiedene Eigentumsmodelle und Quellen für den Gerätekauf entwickeln.

- Gerätezuweisungen verwalten (Englisch)
- Gerätezulieferer in Apple Business Manager verwalten
- Gerätezulieferer in Apple School Manager verwalten

Merkmale und Funktionen verwalteter Geräte zwischen Apple Configurator und MDM miteinander vergleichen.

- Die Funktionen des Apple Configurators entdecken (Englisch)
- Geräte für die Wiederinbetriebnahme vorbereiten (Englisch)
- Reparieren und Wiederherstellen von Apple-Geräten
- iPhone, iPad oder Apple TV-Geräte aktualisieren oder wiederherstellen

Erklären, wie sich die mobile Geräteverwaltung auf die Fähigkeit der Benutzer:innen auswirkt, Einstellungen auf Apple-Geräten zu konfigurieren.

- Optionen für Bildschirmbereiche des Systemassistenten
- Einstellungen der MDM-Payload „Firewall“ für Apple-Geräte

Deklarative Geräteverwaltung erklären.

- Verstehen, wie MDM funktioniert (Englisch)
- Das MDM-Framework von Apple entdecken (Englisch)
- Geräte abfragen (Englisch)
- Einführung in die deklarative Geräteverwaltung für Apple-Geräte
- Deklarationen

Hauptzweck und -funktion der Apple-Verwaltungsarchitektur verstehen.

- Das MDM-Framework von Apple entdecken (Englisch)
- Eine Sicherheitsstrategie entwerfen (Englisch)
- Softwareupdates verwalten (Englisch)
- Einführung in MDM-Profile (Mobile Device Management)
- Über Softwareupdates für Apple-Geräte
- Verwenden der MDM zum Anwenden von Softwareupdates auf Apple-Geräte
- Löschen von Apple-Geräten

Eigentums- und Registrierungsoptionen für alle Registrierungsarten erklären.

- Geräteeigentum und Registrierung planen (Englisch)
- Eine Sicherheitsstrategie entwerfen (Englisch)
- Einführung in die Registrierungsarten für Apple-Geräte
- Geräteregistrierung und MDM
- Automatisierte Geräteregistrierung und MDM
- Apple Gerätebetreuung

Apple Business Manager und Apple School Manager

Apple Business Manager oder Apple School Manager mit der MDM-Lösung der Organisation verknüpfen.

- Hinzufügen eines MDM-Servers (Englisch)
- Einen MDM-Server von Drittanbietern in Apple Business Manager verknüpfen
- Einen MDM-Server von Drittanbietern in Apple School Manager verknüpfen

Voraussetzungen für die Verzeichnissynchronisierung für Apple Business Manager oder Apple School Manager erläutern.

- Bewertung von Authentifizierung und Benutzerdiensten (Englisch)
- Apple Business Manager oder Apple School Manager verwenden (Englisch)
- Die verknüpfte Authentifizierung mit Google Workspace in Apple Business Manager verwenden

Integrationsstandards für öffentliche oder interne Identitätsanbieter zur Integration mit Apple Business Manager oder Apple School Manager herausfinden.

- Apple Business Manager oder Apple School Manager verwenden (Englisch)
- Hier erfährst du, welche Studierendeninformationssysteme (SIS) von Apple School Manager unterstützt werden

Erläutern, warum eine Organisation Apple Business Manager oder Apple School Manager verwendet.

- Geräteeigentum und Registrierung planen (Englisch)
- Apple Business Manager oder Apple School Manager verwenden (Englisch)
- Auswahl einer Verteilungsmethode (Englisch)
- Organisations-Apps und Daten verwalten (Englisch)
- Einen Benutzer-Account in Apple School Manager kontrollieren
- Apple School Manager mit deinem Studierendeninformationssystem (SIS) integrieren
- Von Einlösecodes zur verwalteten Verteilung migrieren
- Inhalts-Token in Apple School Manager übertragen
- Inhalts-Token in Apple Business Manager übertragen
- Einführung in die Inhaltsverteilung für Apple-Geräte
- Einführung in die Registrierungsarten für Apple-Geräte
- Automatisierte Geräteregistrierung und MDM

Den Zweck von Rollen und Standorten in Apple Business Manager oder Apple School Manager herausfinden.

- Apple Business Manager oder Apple School Manager verwenden (Englisch)
- Einführung in Rollen und Berechtigungen in Apple School Manager

Erläutern, wer nach der Verteilung gekaufter Volumenlizenzen für Apps und Bücher deren Eigentümer:in ist.

- Inhalte über Apps und Bücher kaufen (Englisch)
- Auswahl einer Verteilungsmethode (Englisch)
- Organisations-Apps und Daten verwalten (Englisch)
- Einführung in die Inhaltsverteilung für Apple-Geräte

Geräte aus Apple Configurator zu Apple Business Manager oder Apple School Manager hinzufügen.

- Geräte manuell zu Ihrer Organisation hinzufügen (Englisch)
- Geräte aus Apple Configurator in Apple Business Manager hinzufügen
- Geräte aus Apple Configurator in Apple Business Manager hinzufügen

Inhalte als Volumenlizenzen in Apple Business Manager oder Apple School Manager kaufen.

- Inhalte über Apps und Bücher kaufen (Englisch)
- Inhalts-Token in Apple Business Manager verwalten
- Inhalts-Token in Apple School Manager verwalten

Inhalts-Token in Apple Business Manager oder Apple School Manager verwalten.

- Inhalte über Apps und Bücher kaufen (Englisch)
- Inhalts-Token in Apple Business Manager verwalten
- Inhalts-Token in Apple School Manager verwalten

Lizenzen an einen anderen Standort in Apple Business Manager oder Apple School Manager übertragen.

- Inhalte über Apps und Bücher kaufen (Englisch)
- Lizenzen in Apple Business Manager übertragen
- Lizenzen in Apple School Manager übertragen

Netzwerk

Die Infrastruktur der Organisation – d. h. WLAN-Abdeckung und -Kapazität, Proxys, Firewalls, VPN und Bonjour – für die Verwendung durch Apple-Geräte konfigurieren.

- Vorbereiten Ihres Netzwerks (Englisch)
- Die richtige WLAN-Kapazität erzielen
- Apple Produkte in Unternehmensnetzwerken verwenden
- Von Apple Softwareprodukten verwendete TCP- und UDP-Ports
- Infrastrukturelle Voraussetzungen

Voraussetzungen und technische Überlegungen zur Integration von Apple-Geräten in ein bestehendes Netzwerk zusammenfassen.

- Vorbereiten Ihres Netzwerks (Englisch)
- Apple Produkte in Unternehmensnetzwerken verwenden

Erläutern, wie das Inhaltscaching in macOS geladene Apple-Inhalte im Netzwerk zwischenspeichert und optimiert.

- Inhaltscaching verstehen (Englisch)
- Planen und Konfigurieren von Inhaltscaching

Herausfinden, wie Inhaltscaching über Subnetze hinweg funktioniert.

- Inhaltscaching verstehen (Englisch)
- So funktioniert das Inhaltscaching

Die wichtigsten Überlegungen zur Verbindung von verwalteten Apple-Geräten mit WLAN-Netzwerken kennenlernen.

- Vorbereiten Ihres Netzwerks (Englisch)
- WLAN-Netzwerken beitreten (Englisch)
- Wie iOS, iPadOS und macOS entscheiden, mit welchem WLAN-Netzwerk sie sich automatisch verbinden

Drahtlose Authentifizierungsmethoden konfigurieren, mit der die Organisation Apple-Geräte mit dem Netzwerk verbinden kann.

- WLAN-Netzwerken beitreten (Englisch)
- MDM-Einstellungen für WEP-, WPA-, WPA2-, WPA2/WPA3 für Apple-Geräte
- Sicherer Zugriff auf drahtlose Netzwerke
- Verbinden von Apple-Geräten mit WLANs

Apple-Geräte für die Verbindung mit drahtlosen 802.1X-Netzwerken konfigurieren.

- Vorbereiten Ihres Netzwerks (Englisch)
- WLAN-Netzwerken beitreten (Englisch)
- Verbinden von Apple-Geräten mit 802.1X-Netzwerken

Die wichtigsten Payloads und Einstellungen identifizieren, mit denen MDM ein verwaltetes Apple-Gerät so konfiguriert, dass es sich automatisch mit einem unterstützten WLAN-Netzwerk und einem unterstützten Authentifizierungsprotokoll verbindet.

- WLAN-Netzwerken beitreten (Englisch)
- MDM-Einstellungen für EAP (Extensible Authentication Protocol) für Apple-Geräte

Geräte für die automatische Verwendung von Always-On-VPN mit MDM konfigurieren.

- VPN auf Apple-Geräten verwenden (Englisch)
- VPN-Übersicht für die Implementierung von Apple-Geräten

Eine Relay-Netzwerkerweiterung für verwaltete Apps, Domains oder das gesamte Gerät in einer MDM-Lösung konfigurieren.

- Organisations-Apps und Daten verwalten (Englisch)
- Einstellungen der MDM-Payload „Relay“ für Apple-Geräte

Netzwerkprioritäten für WLAN und Mobilfunknetze für Apple-Geräte konfigurieren.

- WLAN-Netzwerken beitreten (Englisch)
- Netzwerkverkehr verwalten (Englisch)
- App-Prioritäten konfigurieren (Englisch)
- Cisco Fastlane-MDM-Einstellungen für Apple-Geräte

Globale HTTP-Proxy-Payload-Einstellungen für Apple-Geräte konfigurieren.

- Netzwerkverkehr verwalten (Englisch)
- Einstellungen der MDM-Payload „Globaler HTTP-Proxy“ für Apple-Geräte
- DNS der MDM-Payload „Globaler HTTP-Proxy“ für Apple-Geräte

Die wichtigsten Ports und Protokolle ermitteln, die von MDM für die Kommunikation mit APNs verwendet werden.

- Vorbereiten Ihres Netzwerks (Englisch)
- Konfigurieren von Geräten für die Zusammenarbeit mit APNS

Verstehen, dass Relays auf verwaltete Apps, Domains oder das gesamte Gerät angewendet werden können.

- Einstellungen der MDM-Payload „Relay“ für Apple-Geräte
- Verwenden von Netzwerkrelays auf Apple-Geräten
- Netzwerkrelays
- Netzwerkrelays in iOS, iPadOS, macOS und tvOS

Strategien zur Optimierung der Netzwerkkonfiguration für den Zugriff von Geräten auf Apple-spezifische Dienste in der Organisation evaluieren und empfehlen.

- macOS-WLAN-Roaming für Unternehmenskunden
- Wie iOS, iPadOS und macOS entscheiden, mit welchem WLAN-Netzwerk sie sich automatisch verbinden
- Unterstützung für WLAN-Roaming auf Apple-Geräten

Das Netzwerk für die Bildschirmüberwachung mit Classroom und Apple Remote Desktop konfigurieren.

- Von Apple Softwareprodukten verwendete TCP- und UDP-Ports
- Infrastrukturelle Voraussetzungen

Sicherheit

Konfigurationsoptionen für Apple-Gerätecodes ermitteln.

- Verwenden von Code-Payloads (Englisch)
- Einstellungen der MDM-Payload „Code“ für Apple-Geräte

Die wichtigsten Einschränkungen für betreute Apple-Geräte kennenlernen.

- Nutzung von Einschränkungs-Payloads (Englisch)
- Apple Gerätebetreuung
- MDM-Einschränkungen für betreute Apple-Geräte

Die wichtigsten Einschränkungen für nicht betreute Apple-Geräte kennenlernen.

- Nutzung von Einschränkungs-Payloads (Englisch)
- Überprüfen von MDM-Einschränkungen für Apple-Geräte

Beschreiben, was in macOS, iOS und iPadOS verschlüsselt ist, einschließlich wo Schlüssel für FileVault gespeichert werden können.

- Daten mit FileVault schützen (Englisch)
- Institutionelle oder persönliche Wiederherstellungsschlüssel

Hauptzweck und -funktion des Modus „Verloren“ in Bezug auf verwaltete Apple-Geräte verstehen.

- Mit MDM den Modus „Verloren“ verwalten (Englisch)
- Verlorene Geräte verwalten (Englisch)
- Verlorene oder gestohlene betreute Geräte orten
- Sperren und Orten von Apple-Geräten

Hauptzweck und -funktion der Aktivierungssperre in Bezug auf verwaltete Apple-Geräte definieren.

- Aktivierungssperre verwalten (Englisch)
- recoveryOS-Passwort
- Aktivierungssperre auf Apple-Geräten
- Organisationsverlinkte Aktivierungssperre für iPhone und iPad

Verschiedene Arten biometrischer Funktionen auf Apple-Geräten beschreiben.

- Sicherheit bei Touch ID
- Informationen zur fortschrittlichen Sicherheitstechnologie von Touch ID
- Verwendung von Face ID und Touch ID
- Verwenden von Touch ID auf dem Mac
- Einrichten von Face ID auf dem iPhone

Die wichtigsten Komponenten des Apple-Sicherheitsmodells beschreiben.

- Grundlegendes zur Geräteregistrierung (Englisch)
- Secure Enclave
- Sicherheit von Face ID und Touch ID
- Hardwaresicherheit – Übersicht
- Sicherheit der Apple Plattformen

Organisationseigene Sicherheitsrichtlinien auf MDM-Einstellungen anwenden, mit denen sich Apps, die sicher und ohne Beeinträchtigung der Plattformintegrität ausgeführt werden, auf einem verwalteten Apple-Gerät installieren und verwalten lassen.

- Organisations-Apps und Daten verwalten (Englisch)
- Verteilen von Apps an Geräte
- Verteilen von verwalteten Apps an Apple-Geräte

Support

Definieren, was ein Schlüsselbund ist, und erklären, was Benutzer:innen mit Schlüsselbundverwaltung in macOS tun können.

- Sicherheit von Schlüsselbunddaten
- Ändern der Passwörter-Einstellungen auf dem Mac

Die macOS-Wiederherstellung beschreiben und erläutern, was Benutzer:innen damit tun können.

- Tastenkombinationen beim Startvorgang des Mac
- Verfügbare Apps in macOS-Wiederherstellung auf einem Mac mit Apple Chips
- Computer mit macOS-Wiederherstellung starten

Erklären, was die Konsole ist und wie sie zur Analyse oder Behebung von Benutzerproblemen verwendet wird.

- Konsole – Benutzerhandbuch für Mac
- Teilen von Protokollmeldungen, Aktivitäten oder Berichten in der App „Konsole“ auf dem Mac

Die wichtigsten Komponenten eines digitalen Zertifikats erkennen und klassifizieren.

- Zertifikate verwalten (Englisch)
- Einführung in die Zertifikatsverwaltung für Apple-Geräte

Tethered Caching einrichten.

- Einführung in das Inhaltscaching
- Konfigurieren des Inhaltscaching auf dem Mac
- MDM-Abfragen zu Netzwerkinformationen für Apple-Geräte
- So funktioniert die Option „Inhaltscaching“ > „Internetverbindung teilen“ zusammen mit einer MDM-Lösung

Erklären, was Terminal ist und wie es zur Analyse oder Behebung von Benutzerproblemen verwendet wird.

- Konsole – Benutzerhandbuch für Mac
- Terminal – Benutzerhandbuch für Mac
- WLAN-Netzwerke mit Apple Network Responsiveness testen

Vom Caching-Dienst unterstützte Inhaltstypen beschreiben.

- Inhaltscaching verstehen (Englisch)
- Von Inhaltscaching in macOS unterstützte Inhaltsarten

Beschreiben, welche Änderungen FileVault am macOS-Startvorgang vornimmt.

- Daten mit FileVault schützen (Englisch)
- Einführung zu macOS-Wiederherstellung
- Verwenden von macOS-Wiederherstellung auf einem Mac mit Apple Chips
- Verwenden von macOS-Wiederherstellung auf einem Intel-basierten Mac
- Funktionsweise der FileVault auf dem Mac
- Daten auf deinem Mac mit FileVault schützen
- Volumeverschlüsselung mit FileVault bei macOS
- Verwenden von Secure Token, Bootstrap Token und Volume-Eigentum in Implementierungen
- Verwalten von FileVault mit der MDM

Die Bedeutung von Wiederherstellungsschlüsseln, persönlichen Wiederherstellungsschlüsseln und der MDM-Hinterlegung erklären.

- Daten mit FileVault schützen (Englisch)
- Funktionsweise der FileVault auf dem Mac
- Daten auf deinem Mac mit FileVault schützen
- Tastenkombinationen beim Startvorgang des Mac
- Verfügbare Apps in macOS-Wiederherstellung auf einem Mac mit Apple Chips
- Computer mit macOS-Wiederherstellung starten
- Institutionelle oder persönliche Wiederherstellungsschlüssel
- Einstellungen der MDM-Payload „FileVault“ für Apple-Geräte

Inhaltscaching auf dem Mac konfigurieren.

- Inhaltscaching verstehen (Englisch)
- Inhaltscaching aktivieren (Englisch)
- Erweiterte Einstellungen für das Inhaltscaching konfigurieren (Englisch)
- Inhaltscaching optimieren (Englisch)
- Konfigurieren des Inhaltscaching auf dem Mac
- Ändern der Einstellungen „Inhaltscaching“ auf dem Mac
- Vornehmen von Änderungen an den Inhaltscaching-Optionen für Clients auf dem Mac
- Ändern der Inhaltscaching-Optionen für übergeordnete Elemente auf dem Mac
- Ändern der Inhaltscaching-Optionen für Peers auf dem Mac
- Ändern der Speicheroptionen fürs Inhaltscaching auf dem Mac
- Einführung in das Inhaltscaching
- Konfigurieren des Inhaltscaching auf dem Mac
- MDM-Abfragen zu Geräteinformationen für Apple-Geräte
- So funktioniert die Option „Inhaltscaching“ > „Internetverbindung teilen“ zusammen mit einer MDM-Lösung
- Von Inhaltscaching in macOS unterstützte Inhaltsarten

Mobile Geräteverwaltung (MDM)

Beschreiben, was MDM ist und wie es funktioniert.

- Grundlegendes zur Geräteregistrierung (Englisch)
- Registrierungsprofile

MDM-Migration planen.

- Einführung in die Planung der MDM-Migration
- Konfigurieren deiner neuen MDM-Lösung
- Neuregistrieren der Geräte in der MDM-Lösung

Benutzereigene Geräte manuell bei einer MDM-Lösung registrieren.

- Grundlegendes zur Geräteregistrierung (Englisch)
- Benutzereigene Geräte registrieren (Englisch)
- Benutzerregistrierung und MDM
- Benutzerregistrierung und verwaltete Apple-IDs
- Informationen zum Blockierungsmodus

Die Aktionen vergleichen, die MDM-Admins auf einem verwalteten, benutzereigenen Apple-Gerät und einem Apple-Gerät im Besitz der Organisation durchführen können.

- Verstehen, wie MDM funktioniert (Englisch)
- Eine Sicherheitsstrategie entwerfen (Englisch)
- Registrierungs- und Systemassistent verwalten (Englisch)
- Benutzereigene Geräte registrieren (Englisch)
- VPN auf Apple-Geräten verwenden (Englisch)
- Mit MDM den Modus „Verloren“ verwalten (Englisch)
- Auto Advance und automatische Geräteregistrierung (macOS)
- MDM-Befehle für Apple-Geräte
- Sperren und Orten von Apple-Geräten
- Geräte und Unternehmensdaten verwalten (Englisch)
- MDM-Befehle für Apple-Geräte
- VPN pro App
- Übersicht der VPN-Einstellungen für Apple-Geräte
- Benutzerregistrierung und Pro-App-Netzwerk
- MDM-Befehle für die Benutzerregistrierung

Ein Registrierungsprofil erstellen und in einer MDM-Lösung zuweisen.

- MDM-Payload-Liste für die automatische Geräteregistrierung
- Einstellungen der MDM-Payload „Home-Bildschirmlayout“ für Apple-Geräte

Mit Apple Configurator ein iPhone, iPad oder Apple TV bei einer MDM-Lösung registrieren.

- Die Funktionen des Apple Configurators entdecken (Englisch)

Herausfinden, welche Systemassistent-Optionen auf Apple-Geräten konfiguriert werden können.

- Einstellungen der MDM-Payload „Systemassistent“ für Apple-Geräte
- Verwalten des Systemassistenten für Apple-Geräte

Die accountgesteuerte Geräteregistrierung auf iPhone, iPad und Mac verwenden, um das Gerät bei einer MDM-Lösung zu registrieren.

- Organisations-Apps und Daten verwalten (Englisch)
- Accountgesteuerte Geräteregistrierung
- Trennung von Benutzer- und Organisationsdaten durch Apple
- Geräteregistrierung und MDM

Einschränkungen identifizieren, die nur für betreute Apple-Geräte gelten.

- Eine Sicherheitsstrategie entwerfen (Englisch)
- Nutzung von Einschränkungs-Payloads (Englisch)
- MDM-Einschränkungen für betreute Apple-Geräte
- Apple-Gerätebetreuung
- MDM-Einschränkungen für iPhone- und iPad-Geräte
- Überprüfen von MDM-Einschränkungen für Apple-Geräte

Das Installieren oder Entfernen von Apps durch Benutzer:innen verhindern.

- Eine Sicherheitsstrategie entwerfen (Englisch)
- Organisations-Apps und Daten verwalten (Englisch)
- Die Entfernung oder Installation von Apps verhindern (Englisch)
- Überprüfen von MDM-Einschränkungen für Apple-Geräte
- MDM-Einschränkungen für iPhone- und iPad-Geräte
- Einstellungen der MDM-Payload „Mitteilungen“ für Apple-Geräte
- Verteilen von verwalteten Apps an Apple-Geräte

Schnelle Sicherheitsmaßnahmen auf Apple-Geräten verwalten.

- Softwareupdates verwalten (Englisch)
- Nutzung von Einschränkungs-Payloads (Englisch)
- Schnelle Sicherheitsmaßnahmen und MDM

Die Einschränkung „In verwalteter Umgebung öffnen“ auf einem verwalteten iPhone oder iPad konfigurieren.

- Organisations-Apps und Daten verwalten (Englisch)
- Einschränkungen und Funktionen für verwaltete Apps

Die Verwendung von Passwörtern während der Registrierung erzwingen.

- Eine Sicherheitsstrategie entwerfen (Englisch)
- Registrierungs- und Systemassistent verwalten (Englisch)
- Verwenden von Code-Payloads (Englisch)
- Einstellungen der MDM-Payload „Code“ für Apple-Geräte
- Optionen für Bildschirmbereiche des Systemassistenten
- Auto Advance und automatische Geräteregistrierung (macOS)
- MDM-Payload-Liste für die automatische Geräteregistrierung

Eine MDM-Lösung verwenden, um Code-Anforderungen für Apple-Geräte zu konfigurieren.

- Verwenden von Code-Payloads (Englisch)
- Einstellungen der MDM-Payload „Code“ für Apple-Geräte

Eine MDM-Lösung verwenden, um FileVault auf verwalteten Mac-Computern vorauszusetzen.

- Daten mit FileVault schützen (Englisch)
- Bootstrap Token

Den Modus „Verloren“ und die Aktivierungssperre auf verwaltete Geräte anwenden.

- Eine Sicherheitsstrategie entwerfen (Englisch)
- Mit MDM den Modus „Verloren“ verwalten (Englisch)
- Aktivierungssperre verwalten (Englisch)
- Verlorene Geräte verwalten (Englisch)
- Organisationsbezogene Aktivierungssperre für iPhone und iPad
- Verlorene oder gestohlene betreute Geräte orten

Demonstrieren, wie Geräte mit einer MDM-Lösung sicher gelöscht werden.

- Verlorene Geräte verwalten (Englisch)
- Löschen von Apple-Geräten

Die Arten von Abfragen identifizieren, die auf einem verwalteten Apple-Gerät von MDM unterstützt werden.

- Geräte abfragen (Englisch)
- MDM-Abfrage zu Sicherheitsaspekten für Apple-Geräte

Softwareupdates auf verwalteten iPhone-, iPad- und Apple TV-Geräten verschieben.

- Softwareupdates verwalten (Englisch)
- Softwareupdates und -upgrades verschieben

Aufführen, was mit einer MDM-Lösung auf einem Gerät verwaltet werden kann und welche Maßnahmen durchgeführt werden können.

- Eine Sicherheitsstrategie entwerfen (Englisch)
- Nutzung von Einschränkungs-Payloads (Englisch)
- MDM-Einschränkungen für überwachte Apple-Geräte
- Apple-Gerätebetreuung
- MDM-Einschränkungen für iPhone- und iPad-Geräte
- Überprüfen von MDM-Einschränkungen für Apple-Geräte
- MDM-Befehle für Apple-Geräte

`cfgutil`-Scripting verwenden, um sich wiederholende Aufgaben zu automatisieren, die in Apple Configurator nicht vorhanden sind.

- Die Funktionen des Apple Configurators entdecken (Englisch)
- Verwenden des Befehlszeilenprogramms von Apple Configurator

Den EraseDevice-Befehl für iPhone und iPad verwenden, um Geräte zur Wiederinbetriebnahme in einer MDM-Lösung schnell zurückzusetzen.

- Geräte für die Wiederinbetriebnahme vorbereiten (Englisch)
- Wiederinbetriebnahme von iPhone- und iPad-Geräten
- Löschen von Apple-Geräten
- Details zum Löschbefehl des Geräts

Den Systemassistenten für Apple-Geräte im Besitz der Organisation in einer MDM-Lösung konfigurieren.

- Registrierungs- und Systemassistent verwalten (Englisch)
- Optionen für Bildschirmbereiche des Systemassistenten

MDM verwenden, um detaillierte Informationen über ein verwaltetes Apple-Gerät anzuzeigen.

- Geräte abfragen (Englisch)
- MDM-Anfragen für die Benutzerregistrierung
- MDM-Abfragen zu Geräteinformationen für Apple-Geräte
- MDM-Abfragen zu Netzwerkinformationen für Apple-Geräte
- MDM-Abfragen zum Betriebssystem für Apple-Geräte

- MDM-Abfragen zu installierten Apps für Apple-Geräte
- MDM-Abfrage zu Sicherheitsaspekten für Apple-Geräte

Den Zweck bzw. die Funktion der Verwendung von Einschränkungen auf verwalteten Apple-Geräten ermitteln.

- Eine Sicherheitsstrategie entwerfen (Englisch)
- Inhaltscaching verstehen (Englisch)
- Nutzung von Einschränkungs-Payloads (Englisch)
- Inhaltscache konfigurieren
- MDM-Einschränkungen für überwachte Apple-Geräte
- MDM-Einschränkungen für iPhone- und iPad-Geräte
- Überprüfen von MDM-Einschränkungen für Apple-Geräte

Zubehörbeschränkungen für iPhone, iPad und Mac verwalten.

- Thunderbolt- und USB-Kopplung verwalten (Englisch)
- MDM-Verwaltung von Hostkoppelungen

Apple-Geräte mit Mobilfunkverbindung implementieren.

- Implementieren von Geräten mit Mobilfunkverbindungen über die MDM-Lösung
- Informationen zur Einschränkung von Änderungen an den eSIMs

Beispielfragen

Um für die Prüfung zu üben, versuche jede dieser Beispielfragen zu beantworten. Verwende dann den Lösungsschlüssel, um deine Antworten zu überprüfen. Diese Beispielfragen beziehen sich nicht auf die eigentliche Prüfung, sondern repräsentieren die Arten von Fragen, die enthalten sind.

Frage 1

Wer behält die Lizenz einer verwalteten App im Apple Business Manager oder Apple School Manager, wenn die App widerrufen wird?

A. Der:die Gerätebenutzer:in

B. Die Organisation

C. Der:die Benutzer:in der verwalteten Apple-ID

D. Der:die Inhaber:in der persönlichen Apple-ID

Frage 2

Mit welcher Sicherheits-MDM-Abfrage kannst du prüfen, ob das Startvolume auf einem Mac geschützt ist?

A. „Wo ist?“ aktiviert

B. Code vorhanden

C. Sicherer Startstatus

D. Verschlüsselungstyp der Hardware

Frage 3

Das Inhaltscaching ist auf einem verwalteten Mac mini mit einer Cachegröße von 300 GB konfiguriert, um Benutzer:innen von geteilten iPad-Geräten zu unterstützen. Benutzer:innen sagen, dass das Laden großer, in iCloud gespeicherter Dateien länger dauert als zuvor.

Wie kannst du das Laden von iCloud-Benutzerdaten beschleunigen?

A. Erhöhe die Cachegröße.

B. Verwende den MDM-Befehl `PurgeCache`, um den Cache zu leeren.

C. Tue nichts. Beim Inhaltscaching werden keine iCloud-Benutzerdaten gespeichert.

D. Lösche den Ordner `/Library/Application Support/Apple/AssetCache`.

Frage 4

Welche Sicherheits-MDM-Abfrage solltest du verwenden, um zu überprüfen, ob Mac-Computer Zugriff auf Websites haben, während gleichzeitig der unbefugte Zugriff auf Benutzerdateien verhindert wird?

A. Firewall-Einstellungen

B. „Wo ist?“ aktiviert

C. Code vorhanden

D. Verschlüsselungstyp der Hardware

Frage 5

Das Informationssicherheitsteam von BetterBag möchte verhindern, dass Benutzer:innen Konfigurationsprofile manuell in den Systemeinstellungen auf ihren per Geräteregistrierung verwalteten Mac-Computern installieren.

Was ist auf den verwalteten Mac-Computern erforderlich, um diese Strategie umzusetzen?

A. Sie müssen betreut werden.

B. Sie müssen macOS 13 oder höher verwenden.

C. Sie müssen in Apple Business Manager zugewiesen werden.

D. Sie müssen mit der automatischen Geräteregistrierung registriert werden.

Frage 6

BetterBag IT möchte sicherstellen, dass Mac-Benutzer:innen nicht von einem anderen Volume als dem vorgesehenen Startvolume starten können.

Welche Sicherheits-MDM-Abfrage kannst du verwenden?

A. „Wo ist?“ aktiviert

B. Code vorhanden

C. Status des Firmware-Passworts

D. Verschlüsselungstyp der Hardware

Frage 7

Eine benutzerdefinierte BetterBag-App wird unerwartet beendet. Der App-Entwickler bittet um den Protokollbericht.

Wie findest und sendest du das richtige Protokoll?

A. Öffne den Aktivitätsmonitor, klicke auf „Ansicht“ und wähle „Systemdiagnose ausführen“.

B. Gib im Terminal `tail -f /Applications/BetterBag.app/Contents/MacOS/BetterBag` ein.

C. Öffne die Konsole, klicke in der Seitenleiste auf „Protokollberichte“, suche nach BetterBag, wähle das Protokoll aus und klicke auf die Taste „Teilen“.

D. Öffne die Konsole, klicke in der Seitenleiste auf „Diagnoseberichte“, suche nach BetterBag, wähle das Protokoll aus und klicke auf die Taste „Teilen“.

Frage 8

Mit welchen beiden Zertifikatskomponenten kannst du einen Client oder Server sicher identifizieren und die Kommunikation zwischen ihnen verschlüsseln?

A. Öffentlicher Schlüssel und privater Schlüssel

B. Vertrauensschlüssel und Vertrauenszertifikat

C. Zwischenzertifikat und Vertrauensschlüssel

D. Vertrauenszertifikat und Zwischenzertifikat

Frage 9

Kristin muss überprüfen, ob eine Gruppe neuer Mitarbeiter:innen ihre verwalteten iPad-Geräte eingerichtet hat, um zu verhindern, dass unbefugte Benutzer:innen auf Dateien zugreifen.

Welche Sicherheits-MDM-Abfrage kann sie verwenden?

A. Code vorhanden

B. Sicherer Startstatus

C. Status des Firmware-Passworts

D. Verwalten der Aktivierungssperre

Frage 10

BetterBag erfordert, dass die FileVault-Verschlüsselung alle verwalteten Mac-Computer schützt.

Was muss die MDM-Lösung von BetterBag hinterlegen, um mobilen Konten einen sicheren Token zu gewähren?

A. Ein Inhaltstoken

B. Einen Bootstrap-Token

C. Einen persönlichen Wiederherstellungsschlüssel

D. Einen institutionellen Wiederherstellungsschlüssel

Frage 11

Das Sicherheitsteam von BetterBag möchte verwaltete iPhone-Geräte wiederbeschaffen, die gestohlen wurden.

Welche MDM-Einstellung musst du aktivieren, um ein gestohlenes iPhone zu orten?

A. Apple Karten

B. „Wo ist?“

C. Ortungsdienste

D. Verwalteter Modus „Verloren“

Frage 12

BetterBag verwendet die automatische Geräteregistrierung für alle verwalteten Apple-Geräte. Du musst alle Daten vom Mac eines:einer vorherigen Benutzer:in entfernen, bevor du sie dem:der nächsten Benutzer:in bereitstellen kannst.

Mit welchem MDM-Befehl kannst du Geräte erneut bereitstellen?

A. Verwaltete Apps deinstallieren

B. Bereitstellungsprofil löschen

C. Das Bereitstellungsprofil installieren

D. Inhalte und Einstellungen löschen

Frage 13

Die Buchhaltungsabteilung von BetterBag möchte sicherstellen, dass die auf ihren iPad-Geräten enthaltenen Finanzdaten sicher sind.

Mit welcher Sicherheits-MDM-Abfrage kannst du bestätigen, dass sensible Daten sicher sind?

A. Sicherer Startstatus

B. Verschlüsselungstyp der Hardware

C. Status des Firmware-Passworts

D. Verwalten der Aktivierungssperre

Frage 14

BetterBag möchte sicherstellen, dass sich Kund:innen nicht auf iPad-Geräten im Einzelhandelskiosk anmelden können.

Welche Sicherheits-MDM-Abfrage kannst du verwenden?

A. Sicherer Startstatus

B. Status des Firmware-Passworts

C. Verwalten der Aktivierungssperre

D. Code kompatibel mit Profilen

Frage 15

Welcher MDM-Befehl verhindert, dass Unbefugte auf Daten auf einem verlorenen oder gestohlenen iPhone oder iPad zugreifen können?

A. `ActivationLockRequest`

B. `DeviceLock`

C. `EraseDevice`

D. `SetAutoAdminPassword`

Frage 16

Das Sicherheitsteam von BetterBag möchte überprüfen, ob Mitarbeiter:innen die Anforderungen zum Schutz ihrer iPad-Geräte vor Verlust und Diebstahl erfüllen.

Welche Sicherheits-MDM-Abfrage sollten sie verwenden?

A. „Wo ist?“ aktiviert

B. Sicherer Startstatus

C. Status des Firmware-Passworts

D. Verwalten der Aktivierungssperre

Frage 17

Das verwaltete iPhone eines ehemaligen Mitarbeiters muss wieder in Betrieb genommen werden. Ihre MDM-Lösung kann die Aktivierungssperre nicht entfernen.

Wie kannst du die organisationsverlinkte Aktivierungssperre deaktivieren?

A. Gib die persönlichen Anmeldeinformationen der Apple-ID in den iCloud-Einstellungen auf dem Bildschirm „Aktivierungssperre“ ein.

B. Gib im Aktivierungssperrbildschirm die Anmeldedaten der verwalteten Apple-ID ein, mit denen das Geräteregistrierungstoken erstellt wurde.

C. Suche im Apple Business Manager oder Apple School Manager das Gerät und sende den Befehl `Aktivierungssperre löschen`.

D. Verwende die MDM-Lösung, um den Befehl `Code löschen` an das Gerät zu senden. Die gerätebasierte Aktivierungssperre wird automatisch deaktiviert.

Frage 18

BetterBag IT möchte die iPad-Geräte seiner Führungskräfte so konfigurieren, dass sie mit der sichersten verfügbaren Verschlüsselung auf das WLAN-Netzwerk des Unternehmens zugreifen. Die IT benötigt das WLAN-Netzwerk von BetterBag, um auch die Kompatibilität mit anderen Geräten aufrechtzuerhalten, die möglicherweise nicht den neuesten Standard unterstützen.

Welche Authentifizierungsmethode erfüllt diese Anforderungen am ehesten?

A. Persönlicher WPA2

B. WPA3 Enterprise

C. WLAN-geschützter Zugriff

D. Verkabelter gleichwertiger Datenschutz

Frage 19

Du hast gespendete Mac-Computer manuell zu Apple School Manager hinzugefügt und sie in der MDM-Lösung registriert.

Wie ist der Verwaltungsstatus der Mac-Computer, nachdem du sie manuell hinzugefügt und bei der MDM-Lösung registriert hast?

A. Sie werden betreut und ein:e Benutzer:in kann sie jederzeit abmelden.

B. Sie werden nicht betreut und ein:e Benutzer:in kann sie jederzeit abmelden.

C. Ein:e Benutzer:in kann sie für bis zu 30 Tage aus der Geräteverwaltung entbinden.

D. Ein:e Benutzer:in kann sie für bis zu 60 Tage aus der Geräteverwaltung entbinden.

Frage 20

Welche Sicherheits-MDM-Abfrage solltest du verwenden, um zu überprüfen, ob die kritischen Dateispeicherorte eines Mac-Computers gesichert sind?

A. „Wo ist?“ aktiviert

B. Code vorhanden

C. Verschlüsselungstyp der Hardware

D. Systemintegritätsschutz aktiviert

Frage 21

Welchen Terminalbefehl solltest du verwenden, wenn du Shell-Skripte schreiben und bestimmte Prozesse mit Apple Configurator für Mac automatisieren möchtest?

A. `Automator`

B. `cfgenrollment`

C. `cfgutil`

D. `startosinstall`

Frage 22

Welcher Bildschirm des Systemassistenten kann auf einem betreuten iPhone, das bei Apple Business Manager registriert ist, nicht so konfiguriert werden, dass er übersprungen wird?

A. Apple-ID

B. Sprache

C. Ortungsdienste

D. Allgemeine Geschäftsbedingungen

Frage 23

Ein:e BetterBag-Benutzer:in erhält in den Einstellungen auf seinem verwalteten iPhone die Benachrichtigung „Der Mobilfunktarif kann installiert werden“. Auf dem verwalteten iPhone kann kein Mobilfunktarif installiert werden, obwohl der:die Benutzer:in Anrufe tätigen kann.

Was ist der wahrscheinlichste Grund dafür, dass ein Mobilfunktarif nicht installiert werden kann?

A. Die eSIM wurde bereits verwendet.

B. Das iPhone kann den Apple Lookup Service nicht erreichen.

C. Die Einschränkung `AllowESIMModification` ist aktiviert.

D. Die Einschränkung `AllowESIMModification` ist deaktiviert.

Frage 24

Welcher MDM-Befehl kann ein iPhone veranlassen, ein eSIM-Profil vom (SM-DP+)-Server eines Mobilfunkanbieters herunterzuladen?

A. InstallESIM

B. CarrierActivation

C. Mobilfunktarife bereitstellen

D. eSIM vom Netzbetreiber abfragen

Frage 25

Welche Einstellung konfiguriert die automatische Proxy-Einrichtung in der globalen HTTP-Proxy-MDM-Payload?

A. Authentifizierungsart

B. Passwort

C. Proxy-PAC-URL

D. Sicherheitstyp

Frage 26

Welche Rolle in Apple Business Manager oder Apple School Manager verfügt über Standardberechtigungen zum Hinzufügen, Zuweisen, Aufheben der Zuweisung und Freigeben von Geräten?

A. Administrator:in

B. Inhaltsmanager:in

C. Mangager:in

D. Mitarbeiter:in

Frage 27

BetterBag erfordert auf allen iPhone und iPad-Geräten ein maximales Code-Alter.

Wie hoch ist das maximale Code-Alter, das du mit einer MDM-Lösung festlegen kannst?

A. 90 Tage

B. 180 Tage

C. 365 Tage

D. 730 Tage

Frage 28

Wie viele Tage kann eine MDM-Lösung maximal die Umgehungscodes für die Aktivierungssperre von neu betreuten iPad-Geräten abrufen?

A. 7 Tage

B. 15 Tage

C. 21 Tage

D. 90 Tage

Frage 29

Welcher Deklarationstyp wird verwendet, um dem Gerät den Gesamtverwaltungsstatus zu übermitteln und Details zur Organisation und den Funktionen der MDM-Lösung zu beschreiben?

A. Geräte

B. Registrierungen

C. Verwaltung

D. Sicherheit

Frage 30

Eva bereitet den Einsatz einer Flotte von Mac-Computern vor. Sie möchte sicherstellen, dass nur zugelassene Mac-Computer auf das Inhaltscaching zugreifen können.

In welchem Payload sollte sie diese Einstellung konfigurieren?

A. Inhaltscaching

B. Datenschutz und Sicherheit

C. Einschränkungen

D. Systemeinstellungen

Lösungsschlüssel

Frage 1: B

Frage 2: C

Frage 3: A

Frage 4: A

Frage 5: B

Frage 6: C

Frage 7: C

Frage 8: A

Frage 9: A

Frage 10: B

Frage 11: D

Frage 12: D

Frage 13: B

Frage 14: D

Frage 15: C

Frage 16: A

Frage 17: B

Frage 18: A

Frage 19: C

Frage 20: D

Frage 21: C

Frage 22: B

Frage 23: D

Frage 24: D

Frage 25: C

Frage 26: A

Frage 27: D

Frage 28: B

Frage 29: C

Frage 30: C

Prüfungsdetails

- Der Name der Prüfung lautet „Apple Deployment und Verwaltung Prüfung (DEP-2024-DEU)“.
- Die Prüfung umfasst etwa 90 bewertete technische Fragen, für deren Beantwortung du 120 Minuten Zeit hast.
- Du musst mindestens 75 Prozent aller Fragen korrekt beantworten, um zu bestehen. Die Ergebnisse werden nicht auf- oder abgerundet.
- Bei der Prüfung werden Multiple-Choice-Fragen mit Einzelauswahl und Multiple-Choice-Fragen mit Mehrfachauswahl verwendet.
- Während der Prüfung darfst du keine Hilfsmittel oder Referenzen verwenden.

Prüfung ablegen

Die „Apple Deployment und Verwaltung Prüfung“ wird online über das Pearson OnVUE-System abgelegt. Plane deinen Prüfungstermin im Voraus, um die Prüfung in einer einzigen Sitzung abzuschließen. Für die Prüfung ist ein ungestörter Raum und ein aktueller Personalausweis erforderlich.

Mehr über das Ablegen einer Pearson OnVUE-Onlineprüfung erfährst du in diesem kurzen Video.

Führe folgende Schritte aus, um die Prüfung zu planen und abzulegen:

1. Melde dich mit deiner Apple-ID und deinem Passwort bei ACRS (Apple Certification Records System) an.
2. Klicke auf „Verfügbare Prüfungen“. Klicke dann auf Prüfung „Apple Deployment und Verwaltung“, um den Anmeldeprozess für die Prüfung zu starten.
3. Aktualisiere deine Daten im Bereich „Kontaktdaten für Prüfung und Zertifizierung“. Beantworte die Fragen zu den zusätzlichen Informationen. Wenn du spezielle Anforderungen für die Teilnahme an der Prüfung hast, fülle bitte die entsprechenden Felder aus. Klicke dann auf die Senden-Taste.
4. Achte auf der Benachrichtigungsseite auf folgenden Text: „Du kannst mit dem Prüfungsprozess für die Prüfung „Apple Deployment und Verwaltung“ fortfahren.“ Klicke unter „Pearson VUE“ auf „Weiter“.
5. Folge den Anweisungen, um deine Prüfung zu planen und zu bezahlen.

Führe am Tag deiner geplanten Prüfung die folgenden Schritte aus:

1. Melde dich 30 Minuten vor deiner geplanten Prüfungszeit bei ACRS mit deiner Apple-ID und deinem Passwort an.
2. Klicke auf der Startseite auf „Apple Deployment und Verwaltung Prüfung“.
3. Klicke auf „Prüfung beginnen“ und folge dann den Anweisungen.

Nachdem du die Prüfung abgelegt hast, erhältst du von Pearson eine E-Mail mit deinem Ergebnis. Wenn du die Prüfung beim ersten Versuch nicht bestehst, kannst du eine weitere Zulassung kaufen und die Prüfung nach 14 Tagen wiederholen. Du hast vier Versuche, die Prüfung zu bestehen.

Über die Zertifizierung

Das digitale Badge „Apple Certified IT Professional“ zeichnet dich als qualifizierte Fachkraft aus, verschafft dir einen Wettbewerbsvorteil auf dem sich ständig weiterentwickelnden Arbeitsmarkt sowie eine Assoziation mit der leistungsstarken Marke Apple.

Wenn du die Prüfung bestanden hast, erhältst du von Credly per E-Mail die Anweisungen dafür, dein digitales Badge abzuholen.

Digitale Badges sind ab dem Datum, an dem sie gesammelt wurden, zwei Jahre lang gültig, aber bestimmte Ablaufdaten variieren. Du hältst dein Badge auf dem neuesten Stand, indem du die Rezertifizierungsprüfung bei der Veröffentlichung und vor dem Ablaufdatum des Badges ablegst. Gehe regelmäßig zur Apple-Training Website und melde dich bei ACRS an, um sicherzustellen, dass du informiert bist, sobald eine Rezertifizierungsprüfung verfügbar ist.