3. Klicken Sie unter *Konten* auf die Registerkarte *Auf Arbeits- oder Schulkonto zugreifen*.
4. Wählen Sie das Einbindungskonto aus und klicken Sie auf *Info*.
5. Klicken Sie im Abschnitt *Erweiterter Diagnosebericht* auf *Bericht erstellen*.
6. Öffnen Sie die Berichtsdatei MDMDiagReport in einem Webbrowser und blättern Sie zum Abschnitt *Enrolled configuration sources and target resources* (registrierte Konfigurationsquellen und Zielressourcen).
7. Falls Sie die Eigenschaft *MDMDeviceWithAAD* nicht finden, wurde das Gerät nicht automatisch registriert und muss registriert werden, damit es die Richtlinien erhält.

Prüfungsziel 2.4: Benutzerprofile verwalten

Sofern Sie ein Gerät nicht ausschließlich als Kioskgerät oder interaktive Anzeige ohne Benutzeranmeldung einsetzen, müssen Sie die verschiedenen Benutzerprofiltypen kennen, die auf Windows 10-Geräten verwendet werden. Benutzerprofile enthalten Informationen und Einstellungen für den Gerätebenutzer und ermöglichen es, ihm eine einheitliche und an seine Vorlieben angepasste Bedienoberfläche anzuzeigen.

Es können unterschiedliche Profiltypen konfiguriert werden, und Sie müssen wissen, für welche Situationen sich jeder Typ eignet. Außerdem sollten Sie wissen, wie Daten im Profil gespeichert werden. Moderne Geräte sind in zunehmendem Maß mit Microsoft-Clouddiensten verbunden und in Azure Active Directory registriert. Die Cloud-Anbindung ermöglicht es Geräten, ihre Profildaten zwischen mehreren Geräten zu übertragen und somit die Benutzer- und App-Einstellungen zwischen allen Geräten zu synchronisieren, an denen der Benutzer arbeitet. Dieses Feature wird als *Enterprise State Roaming* bezeichnet. Sie müssen wissen, wie Sie Enterprise State Roaming konfigurieren und wann der Einsatz dieses Features in einer Organisation sinnvoll ist.

Weil die Internetkonnektivität am modernen Arbeitsplatz allgegenwärtig ist, wollen immer mehr Unternehmen verhindern, dass Mitarbeiter Daten lokal auf den Geräten speichern. Sie müssen wissen, wie Sie Daten von den Geräten verlagern und auf Cloud-Speicher wie OneDrive for Business umleiten.

Dieses Prüfungsziel behandelt folgende Themen:

- Benutzerprofile konfigurieren
- Synchronisierungseinstellungen konfigurieren
- Ordnerumleitung implementieren
- Umleitung bekannter Ordner für OneDrive implementieren
- Enterprise State Roaming in Azure AD konfigurieren

Benutzerprofile konfigurieren

Die Benutzerprofiltypen, die in älteren Windows-Versionen verfügbar waren, sind auch in Windows 10 noch vorhanden. Wenn ein Benutzer sich zum ersten Mal an einem Gerät anmeldet, wird ein Benutzerprofil erstellt, das auf dem Standardprofil im Ordner *Benutzer* basiert.

Bei künftigen Anmeldungen des Benutzers lädt das System dieses Benutzerprofil, damit die Umgebung und die Systemkomponenten so konfiguriert sind, wie es im Profil eingestellt ist.

Ein Benutzerprofil umfasst zwei Elemente.

- **Registrierungsstruktur** Jedes Benutzerprofil enthält die Datei *Ntuser.dat*. Wenn ein Benutzer sich an Windows anmeldet, lädt das System diese Datei in die Registrierung und weist sie der Registrierungsunterstruktur HKEY_CURRENT_USER zu. Die USER-Abschnitte der Registrierung enthalten Benutzereinstellungen, zum Beispiel Desktophintergrund und Bildschirmschoner.
- **Ein Satz von Profilordnern, die im Dateisystem gespeichert sind** Jedes von Windows erstellte Benutzerprofil hat einen eigenen Unterordner mit dem Namen des Benutzers. Dieser Benutzerordner enthält einen Satz von Benutzereinstellungen, Anwendungseinstellungen und Benutzerdaten in verschiedenen Unterordnern, zum Beispiel *AppData*, *Desktop*, *Downloads* und *Documents*.

Es gibt mehrere Benutzerprofiltypen: lokale, servergespeicherte, verbindliche, superverbindliche und temporäre Benutzerprofile:

- **Lokale Benutzerprofile** Ein lokales Benutzerprofil (engl. local user profile) wird auf der lokalen Festplatte des Computers gespeichert. Alle Änderungen am lokalen Benutzerprofil betreffen den Benutzer und den Computer, auf dem die Änderungen vorgenommen werden.
- **Servergespeicherte Benutzerprofile** Ein servergespeichertes Benutzerprofil (engl. roaming user profile) ist eine Kopie des lokalen Profils, die im Netzwerk gespeichert wurde, zum Beispiel in einer Serverfreigabe. Jedes Mal, wenn sich der Benutzer an einem Gerät im Netzwerk anmeldet, wird dieses Profil verwendet. Falls sich das Profil seit der letzten Anmeldung auf dem aktuellen Gerät verändert hat, lädt Windows das neueste Profil aus dem Netzwerkspeicherort herunter. Änderungen am servergespeicherten Benutzerprofil werden mit der Netzwerkkopie des Profils synchronisiert, sobald sich der Benutzer abmeldet. Mit servergespeicherten Benutzerprofilen erhält der Benutzer auf jedem Computer, an dem er in einem Netzwerk arbeitet, seine individuell angepassten Umgebungs- und Systemeinstellungen. Einer der Nachteile bei diesem Profiltyp ist, dass die Anmeldung des Benutzers an seinem Computer sehr lange dauern kann, wenn er ein umfangreiches Profil hat, weil er zum Beispiel viele große Dateien auf dem Desktop speichert. Wenn servergespeicherte Benutzerprofile verwendet werden, werden Ordner wie *Temporary Internet Files* oder *AppData\Local* nicht synchronisiert.

- **Verbindliche Benutzerprofile** Ein verbindliches Benutzerprofil (engl. mandatory user profile) ist ein unveränderliches Profil. Alle Änderungen, die der Benutzer an den Desktopeinstellungen durchführt, gehen verloren, sobald er sich abmeldet. Dieser Profiltyp wird normalerweise schnell geladen. Administratoren können den Benutzern damit eine einheitliche, wenn auch unflexible Umgebung zur Verfügung stellen. Andere Szenarien, in denen verbindliche Benutzerprofile eingesetzt werden, sind Kioskgeräte oder Bildungseinrichtungen. Nur Systemadministratoren können verbindliche Benutzerprofile ändern. Um ein verbindliches Benutzerprofil zu erstellen, sollte ein Administrator erst ein servergespeichertes Benutzerprofil konfigurieren, dann die Profileinstellungen nach Bedarf anpassen und schließlich die Datei *NTuser.dat* (die Registrierungsstruktur) in *Ntuser.man* umbenennen. Die Dateierweiterung *.man* kennzeichnet ein schreibgeschütztes verbindliches Profil; Änderungen, die der Benutzer am Profil vornimmt, werden grundsätzlich nicht gespeichert.
- **Superverbindliche Benutzerprofile** Ein superverbindliches Profil (engl. super-mandatory profile) entsteht, wenn ein Administrator die Erweiterung *.man* an den Ordnernamen des servergespeicherten Benutzerprofils anhängt. Verbindliche und superverbindliche Benutzerprofile verhalten sich ähnlich, beide verwerfen Änderungen des Benutzers. Der Vorteil eines superverbindlichen Profils ist, dass ein Benutzer kein temporäres Profil erhält. Falls die Netzwerkkopie eines servergespeicherten verbindlichen Profils nicht verfügbar ist, bekommt der Benutzer ein temporäres Profil. Wenn ein Benutzer mit einem temporären Profil Zugriff auf ein Gerät erhält, verstößt das möglicherweise gegen die Sicherheitsrichtlinie der Organisation. Um ein superverbindliches Benutzerprofil für den Benutzer *User1* zu erstellen, sollte ein Administrator zuerst ein verbindliches Benutzerprofil konfigurieren, das im Ordner *\\Server\Profiles\User1.V6* gespeichert wird, dann die Erweiterung *.man* an den Ordnernamen anhängen und das Profil unter *\\Server\Profiles\User1.man.V6* speichern.
- **Temporäre Benutzerprofile** Wenn ein Fehler verhindert, dass das normale Profil eines Benutzers geladen wird, wird ein temporäres Profil erstellt. Dieses Profil wird am Ende jeder Sitzung gelöscht, somit gehen bei der Abmeldung des Benutzers alle Änderungen verloren, die er vorgenommen hat.

WEITERE INFORMATIONEN **Verbindliche Benutzerprofile**

Wie Sie verbindliche Benutzerprofile erstellen, erklärt die Microsoft-Website unter:

https://docs.microsoft.com/Windows/client-management/mandatory-user-profile

Windows 10-Profile werden in einem freigegebenen Ordner auf einem Netzwerkserver gespeichert, jeweils ein Ordner pro Benutzer. Der Benutzerprofilordner enthält Anwendungseinstellungen und Einstellungen für andere Systemkomponenten. Sofern der Profilordner nicht umgeleitet wird, enthält das Profil auch benutzerspezifische Daten, zum Beispiel die Desktop-, Startmenü- und Dokumentordner des Benutzers.

Die Einstellungen im Benutzerprofil werden für jeden Benutzer und jede Windows-Version separat verwaltet. Wenn Sie ein servergespeichertes oder verbindliches Profil erstellen, muss die Datei in einem freigegebenen Ordner mit der richtigen Erweiterung für das Betriebssystem gespeichert werden, auf das die Einstellungen angewendet werden. Zum Beispiel liegt das Profil von *User1* für die Arbeit unter Windows 10, Version 1809, in einem Ordner namens *\\Server\Profiles\User1.v6*. Tabelle 2–12 listet die Erweiterungen für die letzten Betriebssystemversionen auf.

Betriebssystemversion	Profilerweiterung
Windows 7	v2
Windows 8.1	v4
Windows 10, Versionen 1507 und 1511	v5
Windows 10, Versionen 1607, 1703, 1709, 1803 und 1809	v6

Tab. 2–12 Erweiterungen für verbindliche Profile

In manchen Szenarien sind verbindliche Profile sehr nützlich. Allerdings verwenden viele Organisationen servergespeicherte Benutzerprofile für all ihre Benutzer. Benutzerprofile ermöglichen es, Benutzern dieselben Einstellungen bereitzustellen, die sie bei der letzten Abmeldung konfiguriert hatten. In einer Umgebung mit gemeinsam genutzten Computern erhält jeder Benutzer nach der Anmeldung seinen angepassten Desktop.

Daten und Einstellungen, die in den Profilordnern eines Benutzers gespeichert wurden, stehen nur dem Benutzer selbst zur Verfügung, andere Benutzer können nicht darauf zugreifen oder etwas ändern. Änderungen, die auf einem gemeinsam genutzten Computer vorgenommen werden, werden im Profil des Benutzers gespeichert; sie haben keine Auswirkung auf die Computereinstellungen, die für andere Benutzer gelten. Ändert zum Beispiel ein Benutzer die Standardschriftgröße in Word, hat das keine Auswirkung auf andere Benutzer, die sich später am selben Computer anmelden.

Größe des Benutzerprofils minimieren

Ein Nachteil bei der Verwendung von servergespeicherten Benutzerprofilen, die den Benutzerzustand (mit Ordnern, Anwendungseinstellungen und Einstellungen für andere Systemkomponenten) enthalten, besteht darin, dass Profile sehr groß werden und dass sich der Anmeldeprozess für die Benutzer deswegen eine Weile hinzieht.

Benutzer haben Schreibberechtigungen für die Dateien und Ordner im Benutzerprofil. Daher kann das Profil in der Standardeinstellung recht groß werden, besonders wenn Benutzer umfangreiche CAD- oder Mediendateien in ihrem Profilordner speichern. Sie haben bereits erfahren, dass Administratoren verbindliche Benutzerprofile implementieren können, bei denen die Benutzer ihr Benutzerprofil nicht verändern können. Dieser Ansatz eignet sich allerdings nur für wenige Umgebungen.

Administratoren haben folgende Methoden zur Auswahl, wenn sie die Größe eines Profils beschränken wollen. Dazu wird der physische Speicherplatz für die Benutzerprofile begrenzt.

- **Kontingente** Sie können Dateikontingente anwenden, um den Platz zu begrenzen, der einem Benutzer auf einem Volume oder in einem freigegebenen Ordner, in dem ein servergespeichertes Benutzerprofil liegt, zur Verfügung steht. Auf dem lokalen Computer können Sie das Datenträgerkontingent in den Volumeeigenschaften konfigurieren. Werden Profile auf einem Dateiserver gespeichert, können Sie in Windows Server 2019 den Knoten *Kontingentverwaltung* im Ressourcen-Manager für Dateiserver verwenden, um den Platz für Ordner zu begrenzen, die servergespeicherte Benutzerprofile oder umgeleitete Ordner enthalten. Im Ressourcen-Manager für Dateiserver können Sie die auf Dateiservern gespeicherten Daten verwalten und klassifizieren, Sie können hier unter anderem Kontingente für Ordner festlegen. Außerdem können Sie im Ressourcen-Manager für Dateiserver Berichte erstellen, mit denen Sie die Speichernutzung überwachen.
- **Umleitung der Profilordner** Sie können bestimmte Ordner, zum Beispiel den Ordner *Dokumente*, so umleiten, dass sie außerhalb des Benutzerprofils gespeichert werden. Das Ziel kann ein freigegebener Ordner auf einem Dateiserver oder OneDrive for Business sein. Für Domänenbenutzer können Sie über Gruppenrichtlinien die Ordnerumleitung mit verschiedenen Einstellungen (zum Beispiel durch Festlegen von Kontingenten) konfigurieren, um die Größe der umgeleiteten Ordner zu begrenzen.
- **Größe des Benutzerprofils mit Gruppenrichtlinien begrenzen** Sie können die Größe von lokalen oder servergespeicherten Benutzerprofilen einschränken, indem Sie die Gruppenrichtlinie *Profilgröße beschränken* aktivieren (Abbildung 2–15). In dieser Richtlinie legen Sie die maximale Profilgröße sowie eine Nachricht fest, die den Benutzern angezeigt wird, falls ihr Profil das Kontingent überschreitet.

WEITERE INFORMATIONEN **Kontingentverwaltung**

Wie Sie mit dem Ressourcen-Manager für Dateiserver Kontingente verwalten, erklärt die Microsoft-Website unter:

https://docs.microsoft.com/Windows-server/storage/fsrm/quota-management

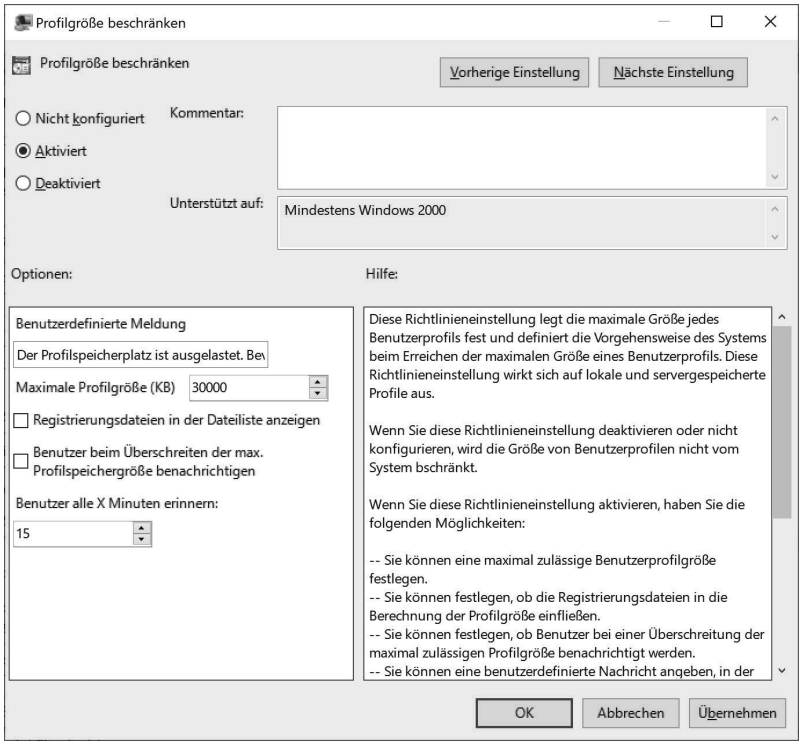

Abb. 2–15 Profilgröße beschränken

Synchronisierungseinstellungen konfigurieren

Ein Feature von Windows 10 ermöglicht Ihnen, eine Kopie Ihrer Geräteeinstellungen geschützt in Ihrem Microsoft-Konto zu speichern. Dieses Feature wurde erstmals in Windows 8 eingeführt. Wenn sich ein Benutzer mit seinem Microsoft-Konto an einem Gerät anmeldet, werden die Einstellungen aus dem Cloud-Konto heruntergeladen und auf das Gerät angewendet. Die Einstellungen bleiben synchronisiert und alle Änderungen am Profil, zum Beispiel ein neues Design oder ein anderer Desktophintergrund, werden auf anderen Geräten sichtbar, sobald sich der Benutzer dort anmeldet.

Benutzer schätzen die einheitliche Benutzeroberfläche auf all ihren Windows-Geräten, sie brauchen nicht auf jedem Gerät ihre bevorzugten Einstellungen zu konfigurieren. Das spart eine Menge Zeit und Aufwand und steigert die Produktivität der Mitarbeiter; trotzdem verursacht diese Lösung nur minimalen Verwaltungsaufwand.

Auf einem neu installierten Gerät (oder nachdem Sie zum ersten Mal Ihr Microsoft-Konto zum Gerät hinzufügen) bekommen Sie in der Einstellungen-App unter Umständen eine Warnmeldung wie die folgende angezeigt, wenn Sie versuchen, die Synchronisierungseinstellungen zu aktivieren:

```
Ihre Kennwörter werden erst synchronisiert, nachdem Sie Ihre Identität auf diesem
Gerät bestätigt haben.
```

Um Kennwörter zu synchronisieren, müssen Sie Ihre Identität mit einem alternativen E-Mail-Konto bestätigen, das Sie vorher eingerichtet haben; das ist ein Schutzmechanismus für Ihr Microsoft-Konto.

Wenn Sie die Synchronisierung aktiviert haben, synchronisiert Windows die von Ihnen vorgenommenen Einstellungen über alle Windows 10-Geräte hinweg, an denen Sie sich mit Ihrem Microsoft-Konto anmelden.

> ***HINWEIS*** **Enterprise State Roaming**
>
> **Über ein Feature namens Enterprise State Roaming können Sie Benutzer- und App-Einstellungen auch für ein Arbeits- oder Schulkonto synchronisieren. Diese Möglichkeit muss von einem Administrator aktiviert werden, und die Benutzer müssen sich dabei mit einem Azure AD-Konto statt mit einem Microsoft-Konto anmelden. Enterprise State Roaming wird weiter hinten in diesem Kapitel im Abschnitt »Enterprise State Roaming in Azure AD konfigurieren« (Seite 162) behandelt.**

So aktivieren Sie die Gerätesynchronisierungseinstellungen:

1. Öffnen Sie die Einstellungen-App.
2. Wählen Sie *Konten*.
3. Stellen Sie im Abschnitt *Ihre Infos* sicher, dass Sie sich mit einem Microsoft-Konto angemeldet haben. Ist das nicht der Fall, können Sie auf den Link klicken und sich mit Ihrem Microsoft-Konto anmelden.
4. Wählen Sie unter *Konten* den Abschnitt *Einstellungen synchronisieren*.
5. Schalten Sie die Option *Synchronisierungseinstellungen* ein (Abbildung 2–16).
6. Im Abschnitt *Einzelne Synchronisierungseinstellungen* können Sie folgende Einstellungen ein- oder ausschalten:
   - Design
   - Kennwörter
   - Spracheinstellungen
   - Erleichterte Bedienung
   - Weitere Windows-Einstellungen

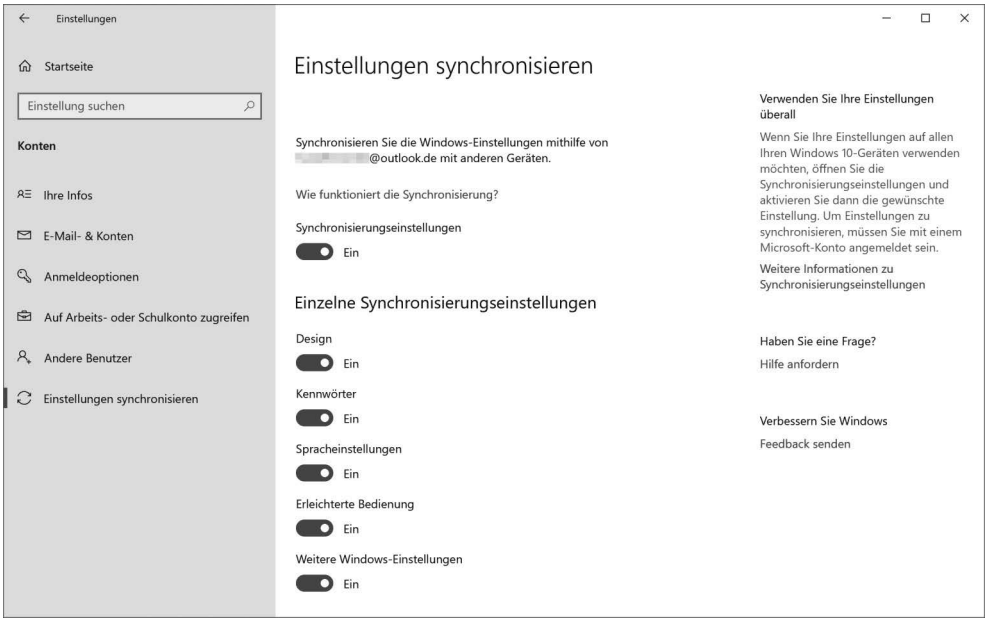

Abb. 2–16 Windows-Einstellungen synchronisieren

Die synchronisierten Einstellungen sind umfangreich und können den Aufwand zum Konfigurieren weiterer Geräte deutlich verringern. Tabelle 2–13 listet einige der Kategorien und wichtige Einstellungen auf, die auf einem Windows 10-Desktopgerät synchronisiert werden.

Gruppe von Einstellungen	Einstellung
Weitere Windows-Einstellungen	**Maus:** ■ Größe des Mauszeigers ändern ■ Farbe des Mauszeigers ändern
Design	**Konten:** Kontobild **Desktoppersonalisierung:** ■ Desktopdesign (Hintergrund, Systemfarbe, Standardsystemsounds und Bildschirmschoner) ■ Diashow-Hintergrund ■ Taskleisteneinstellungen (Position, automatisch ausblenden und so weiter)
Kennwörter	**Anmeldeinformationen:** Anmeldeinformationstresor **WLAN:** WLAN-Profile (nur WPA)
App-spezifisch	**App-Daten:** Einzelne Apps können Daten synchronisieren **Eingabeaufforderung:** Standardeinstellungen für Eingabeaufforderung

→

Gruppe von Einstellungen	Einstellung
Microsoft Edge-Browser	■ Leseliste ■ Favoriten ■ Top-Websites ■ Eingetippte URLs ■ Favoritenleisteneinstellungen ■ Startschaltfläche anzeigen ■ Pop-ups blockieren ■ Bei jedem Download nach dem Speicherort fragen ■ Speichern der Kennwörter anbieten ■ »Do Not Track«-Anforderungen senden ■ Formulareinträge speichern ■ Such- und Websitevorschläge während der Eingabe anzeigen ■ Cookie-Einstellungen ■ Websites das Speichern geschützter Medienlizenzen auf meinem Gerät erlauben ■ Einstellungen für Sprachausgabe
Internet Explorer-Browser	■ Offene Registerkarten (URL und Titel) ■ Leseliste ■ Eingetippte URLs ■ Browserverlauf ■ Favoriten ■ Ausgeschlossene URLs ■ Startseiten ■ Domänenvorschläge
Erleichterte Bedienung	**Hoher Kontrast:** Ein oder Aus, Designeinstellungen **Tastatur:** Benutzer können: ■ Bildschirmtastatur ein-/ausschalten ■ Einrastfunktion aktivieren (standardmäßig aus) ■ Anschlagverzögerung aktivieren (standardmäßig aus) ■ Umschalttasten aktivieren (standardmäßig aus) **Bildschirmlupe:** ■ Farbinvertierung ein- oder ausschalten (standardmäßig aus) ■ Lupe folgt dem Tastaturfokus ■ Lupe folgt dem Mauszeiger ■ Nach der Anmeldung des Benutzers starten (standardmäßig aus) **Sprachausgabe:** ■ Schnellstartleiste ■ Tonhöhe der Stimme ändern ■ Tipps zum Interagieren mit Steuerelementen und Schaltfläche hören (standardmäßig an) ■ Zeichen bei der Eingabe hören (standardmäßig an) ■ Wörter bei der Eingabe hören (standardmäßig an)

→

Gruppe von Einstellungen	Einstellung
	■ Texteinfügemarke soll dem Sprachausgabecursor folgen (standardmäßig an) ■ Sprachausgabecursor auf dem Bildschirm anzeigen (standardmäßig an) ■ Audiohinweise ausgeben (standardmäßig an) ■ Tasten auf der Bildschirmtastatur aktivieren, wenn ich meinen Finger von der Tastatur nehme (standardmäßig aus) **Erleichterte Bedienung:** ■ Cursorbreite ändern ■ Desktophintergrundbild nicht anzeigen (standardmäßig aus)
Sprache	**Datum, Uhrzeit und Region:** ■ Uhrzeit automatisch festlegen (Internet-Zeitsynchronisierung) ■ 24-Stunden-Uhr ■ Datum und Uhrzeit ■ Sommer-/Winterzeit ■ Land/Region ■ Erster Tag der Woche ■ Regionale Formatierung ■ Kurzes Datum ■ Langes Datum ■ Kurze Uhrzeit ■ Lange Uhrzeit **Sprache:** ■ Sprachprofil ■ Rechtschreibprüfung (automatische Korrektur und Hervorheben von Fehlern) ■ Liste der Tastaturen **Eingabe:** ■ Rechtschreibwörterbuch ■ Rechtschreibfehler automatisch korrigieren ■ Rechtschreibfehler hervorheben ■ Wortvorschläge bei der Eingabe anzeigen ■ Nach Auswahl eines Textvorschlags Leerzeichen einfügen ■ Nach Doppeltippen auf die Leertaste Punkt einfügen ■ Ersten Buchstaben in jedem Satz zum Großbuchstaben machen ■ Bei Doppeltipp auf die Umschalttaste nur Großbuchstaben verwenden ■ Beim Tippen Tastensounds ausgeben ■ Personalisierungsdaten für Bildschirmtastatur

Tab. 2–13 Synchronisierte Windows-Einstellungen

Folgende Geräteeinstellungen werden nicht geräteübergreifend synchronisiert:

- Konten: weitere Kontoeinstellungen
- Alle Bluetooth-Einstellungen
- Desktoppersonalisierung: Startseitenlayout
- Alle Sperrbildschirmeinstellungen
- Maus: alle anderen Einstellungen
- Alle Energie- und Stromspareinstellungen

Im Microsoft Edge-Browser können Benutzer die Synchronisierungseinstellungen direkt in der App anpassen. So aktivieren oder deaktivieren Sie die Synchronisierung der Microsoft Edge-Einstellungen:

1. Klicken Sie in Microsoft Edge auf *Einstellungen und mehr* (das Symbol mit den drei Punkten).
2. Wählen Sie *Einstellungen* (mit dem Zahnradsymbol).
3. Schalten Sie auf der Registerkarte *Allgemein* im Abschnitt *Konto* die Option *Synchronisieren Sie Ihre Microsoft Edge-Favoriten, die Leseliste, häufig besuchte Websites und weitere Einstellungen auf allen Geräten* ein oder aus.
4. Klicken Sie irgendwo auf die Webseite, um das Flyout-Menü *Einstellungen* auszublenden.

In Windows 10, Version 1803 und neuer, können die Benutzer die Synchronisierung von Internet Explorer-Einstellungen direkt im Internet Explorer folgendermaßen aktivieren oder deaktivieren:

1. Klicken Sie im Internet Explorer-Menü auf *Extras* (Zahnradsymbol).
2. Klicken Sie auf *Internetoptionen*.
3. Wählen Sie die Registerkarte *Erweitert*.
4. Aktivieren oder deaktivieren Sie in der Liste *Einstellungen* unter der Rubrik *Browsen* das Kontrollkästchen *Synchronisierung von Internet Explorer-Einstellungen und -Daten aktivieren*.
5. Klicken Sie auf *OK*.

Mit den folgenden Schritten beenden Sie die Synchronisierung Ihrer Einstellungen zwischen allen Ihren Geräten und löschen das Cloud-Backup Ihrer persönlichen Einstellungen:

1. Schalten Sie auf allen Geräten, die mit Ihrem Microsoft-Konto verknüpft sind, die Synchronisierung der Einstellungen in der Einstellungen-App aus.
2. Öffnen Sie einen Webbrowser und melden Sie sich mit Ihrem Microsoft-Konto bei *https://account.microsoft.com/devices* an.
3. Wählen Sie das Gerät aus, das Sie verwalten wollen, und klicken Sie auf *Verwalten*.
4. Klicken Sie oben auf der Geräteseite auf *Weitere Aktionen* und dann auf *Entfernen der Cloudsicherung für persönliche Einstellungen*.

5. Falls der Befehl *Entfernen der Cloudsicherung für persönliche Einstellungen* nicht sichtbar ist, müssen Sie sicherstellen, dass die Synchronisierung für alle aufgelisteten Geräte ausgeschaltet ist.

So löschen Sie ein Gerät aus Ihrer Geräteliste:

1. Öffnen Sie einen Webbrowser und melden Sie sich mit Ihrem Microsoft-Konto bei *https://account.microsoft.com/devices* an.
2. Gehen Sie zu *Gerätelimits verwalten* und suchen Sie das Gerät, das Sie entfernen wollen.
3. Wählen Sie *Entfernen*, um das Gerät zu löschen.

Ordnerumleitung implementieren

Damit keine zu großen Datenmengen auf einem Gerät gespeichert werden (oft im Profil eines Benutzers), können Administratoren Gruppenrichtlinien konfigurieren, die einzelne Profilordner an einen anderen Speicherort umleiten. Dieser Speicherort ist üblicherweise ein Ordner, der auf einem Dateiserver im Netzwerk liegt.

Nach der Konfiguration wird der Inhalt des umgeleiteten Ordners vom lokalen Gerät auf den neuen Speicherort verschoben, wo die Dateien für die Benutzer verfügbar sind. Falls die Ordnerumleitung für ein servergespeichertes Benutzerprofil eingerichtet wird, kann der Benutzer von jedem Gerät aus, an dem er sich anmeldet, auf seine Dateien und Ordner zugreifen. Die Benutzer bemerken gar nicht, dass die Umleitung aktiv ist, weil es keine sichtbaren Änderungen an der Benutzeroberfläche des Windows-Explorers gibt.

Dateien und Ordner bleiben in der Netzwerkdateifreigabe und stehen standardmäßig als Offlinedateien zur Verfügung, damit ein Benutzer auch dann auf seine Dateien Zugriff hat, wenn das Gerät vom Netzwerk getrennt ist. Dabei werden Dateien, an denen der Benutzer arbeitet, auf dem Gerät zwischengespeichert und mit der Netzwerkdateifreigabe synchronisiert.

Sie konfigurieren die Ordnerumleitung, indem Sie die entsprechenden Gruppenrichtlinieneinstellungen aktivieren:

1. Starten Sie den Gruppenrichtlinienobjekt-Editor, öffnen Sie das gewünschte Gruppenrichtlinienobjekt und wechseln Sie zum Knoten *Benutzerkonfiguration* > *Richtlinien* > *Windows-Einstellungen* > *Ordnerumleitung*.
2. Klicken Sie mit der rechten Maustaste auf einen Ordner, den Sie umleiten wollen (zum Beispiel *Dokumente*), und wählen Sie den Befehl *Eigenschaften*.
3. Wählen Sie im Eigenschaftendialogfeld in der Dropdownliste *Einstellung* den Eintrag *Standard - Leitet alle Ordner auf den gleichen Pfad um* (Abbildung 2–17).

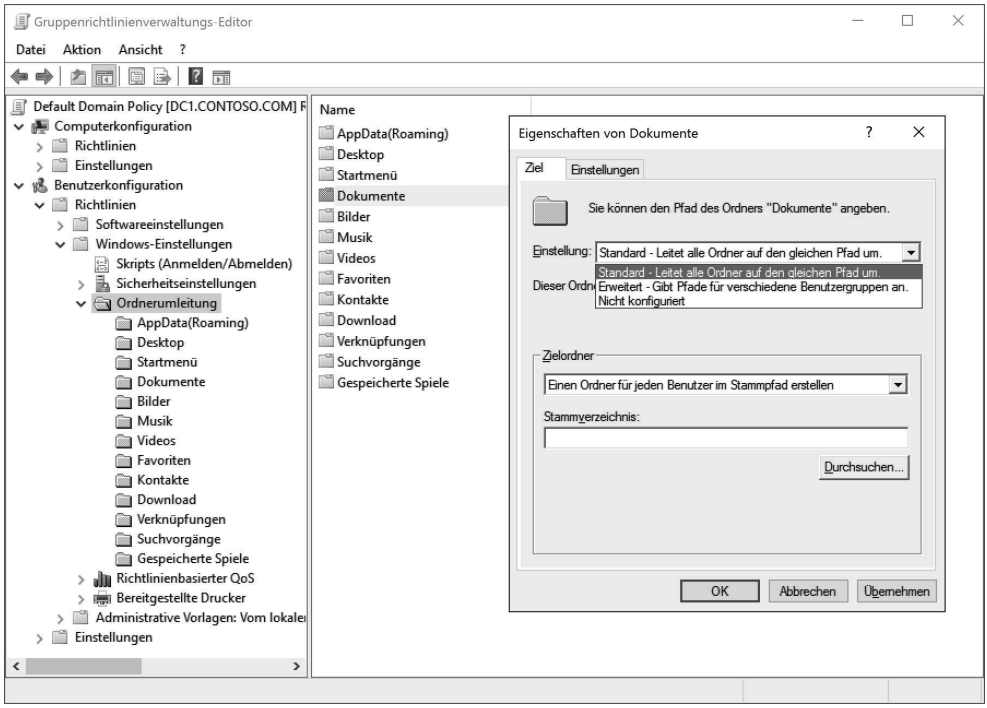

Abb. 2–17 Ordnerumleitung

4. Wählen Sie in der Dropdownliste *Zielordner* den Eintrag *Einen Ordner für jeden Benutzer im Stammpfad erstellen*.
5. Tippen Sie den Pfad der Dateifreigabe, in der die umgeleiteten Ordner gespeichert werden sollen, in das Feld *Stammverzeichnis* ein; zum Beispiel könnte der Pfad **\\LON-DC1.adatum.com\Users$** lauten.
6. Wählen Sie die Registerkarte *Einstellungen* und sehen Sie sich die verfügbaren Einstellungen an.
7. Optional können Sie auf der Registerkarte *Einstellungen* im Abschnitt *Entfernen der Richtlinie* die Option *Ordner nach Entfernen der Richtlinie zurück an den Speicherort des lokalen Benutzerprofils umleiten* auswählen.
8. Klicken Sie auf *OK*.
9. Bestätigen Sie die Warnmeldung, sofern eine erscheint, indem Sie auf *Ja* klicken.

Die Ordnerumleitung bietet einer Organisation drei Vorteile:

- **Geringere Gefahr von Datenverlust** Die Daten sind nicht mehr auf einem lokalen Gerät gespeichert.
- **Zentral gesicherte Daten** Ein Backup der Daten lässt sich zentral auf dem vernetzten Dateiserver anfertigen.

- **Festgelegte Kontingente** Administratoren können ganz einfach den Festplattenplatz begrenzen, der zum Speichern von umgeleiteten Dateien und Ordnern verwendet wird. Optional können Administratoren außerdem einschränken, welche Dateitypen in Benutzerprofilen gespeichert werden dürfen.

> ***WEITERE INFORMATIONEN*** **Ordnerumleitung bereitstellen**
>
> **Wie Sie die Ordnerumleitung bereitstellen, erklärt der folgende Artikel auf der Microsoft-Website:**
>
> ***https://docs.microsoft.com/Windows-server/storage/folder-redirection/deploy-folder-redirection***

Umleitung bekannter Ordner für OneDrive implementieren

OneDrive for Business stellt Ihren Mitarbeitern persönlichen Onlinespeicherplatz zur Verfügung. Sie können dort Arbeitsdateien speichern und schützen, und mit ihren Azure AD-Anmeldeinformationen können sie von mehreren Geräten aus darauf zugreifen. Die Umleitung bekannter Windows-Ordner (Windows Known Folder Move, KFM) für OneDrive ist ein Feature, das die persönlichen Ordner und wichtige Dateien der Benutzer automatisch auf ihr OneDrive for Business-Konto umleitet, das in der Microsoft Cloud gespeichert wird. Dank dieser Umleitung können die Benutzer von unterschiedlichen Geräten und Anwendungen aus auf ihre Dateien zugreifen.

Während immer mehr Organisationen auf die Cloud umsteigen, sinkt wahrscheinlich die Verfügbarkeit lokaler, netzwerkbasierter Dateispeicher. Wird vor einem Migrationsprojekt KFM auf den Geräten aktiviert, erhalten die Benutzer auf dem neuen oder aktualisierten Windows 10-PC sofort einen sicheren Zugang zu ihren Dateien. Alle in OneDrive for Business gespeicherten Daten sind während der Speicherung und während der Übertragung verschlüsselt. Mit Gruppenrichtlinien können Sie festlegen, dass die Synchronisierung fast unmerklich im Hintergrund abläuft.

Folgende Windows-Ordner werden häufig mit KFM umgeleitet:

- Desktop
- Dokumente
- Bilder
- Bildschirmfotos
- Eigene Aufnahmen

Die Benutzer brauchen ihre Arbeitsabläufe nicht zu verändern, wenn die Organisation bekannte Windows-Ordner auf OneDrive umleitet; auf ihren Computern sieht vor, während und nach der Synchronisierung alles gleich aus.

Alle in OneDrive gespeicherten Dateien können für Kollegen freigegeben werden, und die Angestellten können in Echtzeit mit Office-Desktop, Web und mobilen Apps an Office-Dokumenten zusammenarbeiten.

Folgende Lizenzpläne für OneDrive for Business-Abonnements umfassen persönlichen Cloud-Speicher (für Abonnements ab fünf Benutzern):

- SharePoint Online Plan 2
- OneDrive for Business Plan 2
- Office 365 A1, A3, A5, E3, E5, G3 und G5
- Microsoft 365 A3, A5, E3, E5, G3 und G5

HINWEIS **Speicherplatz in OneDrive for Business vergrößern**

In der Standardeinstellung erhält jeder OneDrive for Business-Kunde 1 TB Cloud-Speicher. Hat ein Benutzer 90 Prozent seines 1 TB großen Speichers gefüllt, kann ein Administrator den Platz für diesen Benutzer auf 5 TB erhöhen. Füllt ein Benutzer 90 Prozent seines erweiterten, 5 TB großen Speichers, kann ein Administrator sich an den technischen Support von Microsoft wenden, der den Speicherplatz daraufhin auf 25 TB pro Benutzer vergrößert. Weiterer Speicherplatz jenseits von 25 TB wird einzelnen Benutzern bei Bedarf in Form von SharePoint-Teamsites zur Verfügung gestellt.

Damit Sie die Umleitung bekannter Ordner für OneDrive einrichten können, müssen folgende Voraussetzungen erfüllt sein:

- Auf den Clientgeräten muss mindestens Build 18.111.0603.0004 des OneDrive-Synchronisierungsclients installiert sein.
- Alle vorhandenen Gruppenrichtlinieneinstellungen für eine Windows-Ordnerumleitung in der Domäne müssen gelöscht werden.
- Sie haben die OneNote-Notizbücher der Benutzer aus den bekannten Ordnern heraus verschoben, weil bekannte Ordner, zu denen OneNote-Notizbücher gehören, nicht verschoben werden.

Tabelle 2–14 beschreibt die Gruppenrichtlinien, mit denen Unternehmen die Umleitung bekannter Ordner für OneDrive in einer Umgebung konfigurieren können, die Active Directory-Domänendienste einsetzt.

Gruppenrichtlinieneinstellung	Beschreibung
Benutzer zum Verschieben bekannter Windows-Ordner auf OneDrive auffordern	Diese Richtlinie legt fest, dass Benutzer eine Benachrichtigung angezeigt bekommen (Abbildung 2–18), die erklärt, dass sie ihre Dateien schützen sollen, indem sie ihre bekannten Windows-Ordner automatisch auf OneDrive verschieben lassen. Falls Benutzer den Hinweis ignorieren, erscheint eine Erinnerung im Info-Center, bis die Umleitung abgeschlossen ist. Falls ein Benutzer seine Ordner bereits auf ein anderes OneDrive-Konto umgeleitet hat, wird er aufgefordert, die Ordner auf das OneDrive-Konto der Organisation umzuleiten.
Bekannte Windows-Ordner automatisch auf OneDrive verschieben	Leitet bekannte Ordner ohne irgendeine Benutzerinteraktion auf OneDrive um. Sobald diese Richtlinie konfiguriert ist, werden die Inhalte bekannter Ordner auf OneDrive umgeleitet.
Benutzer am Umleiten ihrer bekannten Windows-Ordner auf ihren PC hindern	Diese Richtlinie hindert Benutzer daran, die Einstellung zu verändern. Somit werden die Benutzer gezwungen, ihre bekannten Ordner auf OneDrive umzuleiten. Wenn diese Richtlinie aktiviert ist, legt sie den folgenden Registrierungsschlüssel fest: `[HKLM\SOFTWARE\Policies\Microsoft\OneDrive]"KFMBlockOptOut"="dword:00000001"`
Benutzer am Verschieben ihrer bekannten Windows-Ordner auf OneDrive hindern	Hindert Benutzer daran, ihre bekannten Windows-Ordner auf OneDrive zu verschieben.

Tab. 2–14 Gruppenrichtlinien für das Umleiten bekannter Windows-Ordner

Die *.adml*- und *.admx*-Dateien mit den Gruppenrichtlinieneinstellungen für die Umleitung bekannter Windows-Ordner finden Sie auf einem Windows 10-Client, der mindestens den Build 18.111.0603.0004 des OneDrive-Synchronisierungsclients installiert hat, im Pfad *%localappdata%\Microsoft\OneDrive\<OneDrive-Version>\adm*.

Um die OneDrive-Gruppenrichtlinien zu verwenden, müssen Sie die *.adml*- und *.admx*-Dateien von einem Client importieren und zum zentralen Gruppenrichtliniespeicher Ihrer Domäne im Pfad *\SYSVOL\domain\Policies\PolicyDefinitions* hinzufügen.

Sobald Sie die *.admx*- und *.adml*-Dateien importiert haben, können Sie sich diese Richtlinien im Gruppenrichtlinien-Editor im Knoten *Computerkonfiguration* > *Richtlinien* > *Administrative Vorlagen* > *OneDrive* ansehen.

WEITERE INFORMATIONEN **Gruppenrichtlinieneinstellungen für den OneDrive-Synchronisierungsclient**

Wie Sie den OneDrive-Synchronisierungsclient in einer Windows Server-Unternehmensumgebung verwalten, beschreibt die Microsoft-Website unter:

https://docs.microsoft.com/onedrive/use-group-policy

Abb. 2–18 Aufforderung an den Benutzer, seine Ordner auf OneDrive umzuleiten

Enterprise State Roaming in Azure AD konfigurieren

Windows 10-Benutzer, die ein Microsoft-Konto verwenden, können ihre Benutzereinstellungen, Edge Browser-Kennwörter und Anwendungseinstellungen zwischen allen Geräten synchronisieren, auf denen sie mit demselben Microsoft-Konto angemeldet sind.

Für Unternehmensbenutzer stellt Azure Active Directory eine Roaming-Funktion zur Verfügung. Administratoren können ein Unternehmensfeature namens *Enterprise State Roaming* aktivieren, damit Azure AD die Windows-Einstellungen, Kennwörter und UWP-App-Einstellungen (Universal Windows Platform) und -Daten der Benutzer über alle Windows-Geräte hinweg synchronisiert. Sind die Profileinstellungen in der Cloud gespeichert, werden die Einstellungen sofort nach der Anmeldung automatisch auf ein neues Gerät angewendet.

Neben den Einstellungen, die als Element der Benutzereinstellungen synchronisiert werden, bietet Enterprise State Roaming folgende Features:

- **Trennung von Unternehmens- und privaten Daten** Die Unternehmensdaten werden nicht mit privaten Daten vermischt. Jedes Cloud-Konto speichert die Daten separat.
- **Verbesserte Sicherheit** Weil Azure Rights Management zum Einsatz kommt, sind die Daten stets verschlüsselt, sowohl während der Übertragung als auch während der Speicherung.
- **Bessere Verwaltung und Überwachung** Im Azure AD-Portal konfigurieren und überwachen Sie, welche Benutzer und Geräte ihre Einstellungen synchronisiert haben.
- **Datenaufbewahrung** Enterprise State Roaming-Daten, die mit Azure synchronisiert wurden, werden für eine Frist zwischen 90 und 180 Tagen nach dem letzten Zugriff aufbewahrt.

Wenn eine Organisation Enterprise State Roaming nutzen will, müssen folgende Voraussetzungen erfüllt sein:

- Windows 10, Version 1511 oder neuer, ist mit den neuesten Updates auf dem Gerät installiert.
- Geräte müssen in Azure AD oder Hybrid-Azure AD eingebunden sein.
- Enterprise State Roaming muss für den Mandanten in Azure AD aktiviert sein.
- Den Benutzern muss bereits eine Azure AD Premium- oder EMS-Lizenz (Enterprise Mobility + Security) zugewiesen sein.
- Geräte müssen neu gestartet werden, nachdem Enterprise State Roaming aktiviert wurde.
- Benutzer müssen sich mit einer Azure AD-Identität anmelden.

Wenn das Enterprise State Roaming aktiviert ist, erhält die Organisation eine kostenlose Lizenz für die eingeschränkte Nutzung von Azure Rights Management innerhalb von Azure Information Protection. Diese Lizenz beschränkt sich auf die Verschlüsselung und Entschlüsselung der Unternehmenseinstellungen und Anwendungsdaten, die über Enterprise State Roaming synchronisiert werden.

So aktivieren Sie Enterprise State Roaming in Azure:

1. Melden Sie sich mit einem globalen Administratorkonto im Azure Admin Center an.
2. Klicken Sie auf *Azure Active Directory* und dann unter *Verwalten* auf *Geräte*.
3. Klicken Sie auf dem Blatt *Geräte - Alle Geräte* unter *Verwalten* auf *Enterprise State Roaming*.
4. Konfigurieren Sie auf dem Blatt *Geräte - Enterprise State Roaming* die Option *Benutzer können Einstellungen und App-Daten geräteübergreifend synchronisieren*; Sie können das Roaming für alle Benutzer oder lediglich für eine ausgewählte Gruppe von Benutzern aktivieren (Abbildung 2–19). Klicken Sie auf *Speichern*.

Abb. 2–19 Enterprise State Roaming konfigurieren

Sobald die Azure AD-Einstellungen konfiguriert sind, müssen Ihre Windows 10-Geräte neu gestartet werden und die Benutzer müssen sich mit ihrer primären Anmeldeidentität authentifizieren.

WEITERE INFORMATIONEN **In Hybrid-Azure AD eingebundene Geräte**

Wie Sie in Hybrid-Azure AD eingebundene Geräte konfigurieren, beschreibt die Microsoft-Website unter:

https://docs.microsoft.com/azure/active-directory/devices/hybrid-azuread-join-manual-steps

Tabelle 2–15 beschreibt, wie lange die Benutzereinstellungen und Anwendungseinstellungen, die über Enterprise State Roaming mit der Microsoft-Cloud synchronisiert werden, aufbewahrt werden.

Aktion	Aufbewahrungsdauer
Explizite Löschung	■ **Gelöschter Benutzer** Wenn ein Azure AD-Benutzerkonto gelöscht wird, werden die zugehörigen Roaming-Daten nach 90 bis 180 Tagen gelöscht. ■ **Gelöschtes Verzeichnis** Wird ein gesamtes Verzeichnis in Azure AD gelöscht, werden alle Einstellungsdaten, die mit diesem Verzeichnis verknüpft sind, nach 90 bis 180 Tagen gelöscht. ■ **Löschungsanforderung** Ein Azure AD-Administrator kann sich an den Azure-Support wenden, um die Daten eines bestimmten Benutzers oder bestimmte Einstellungsdaten löschen zu lassen.
Löschen veralteter Daten	■ Roaming-Daten für ein Benutzerkonto, auf das seit einem Jahr nicht zugegriffen wurde, werden als veraltet (engl. stale) eingestuft und werden unter Umständen aus der Microsoft-Cloud gelöscht. Die Aufbewahrungsdauer kann sich ändern, sie fällt aber nie unter 90 Tage. Ob Daten als veraltet eingestuft werden, hängt von folgenden Kriterien ab: • Falls kein Gerät auf eine Einstellungssammlung zugreift, zum Beispiel die Einstellungen einer bestimmten App oder das Windows 10-Design, wird diese Sammlung veraltet, sobald die Aufbewahrungsdauer abgelaufen ist, und wird möglicherweise gelöscht. • Falls ein Benutzer die Synchronisierung von Einstellungen auf seinem Gerät deaktiviert, werden alle Einstellungsdaten dieses Benutzers veraltet und werden möglicherweise gelöscht, sobald die Aufbewahrungsdauer abgelaufen ist. • Falls das Enterprise State Roaming für das gesamte Verzeichnis deaktiviert wird, endet die Synchronisierung der Einstellungen. Alle Einstellungsdaten für alle Benutzer werden veraltet und werden möglicherweise gelöscht, sobald die Aufbewahrungsdauer abgelaufen ist.
Wiederherstellen gelöschter Daten	Die Aufbewahrungsrichtlinie für Enterprise State Roaming-Daten ist nicht konfigurierbar. Wurden die Synchronisierungsdaten gelöscht, können sie nicht mehr wiederhergestellt werden. Die Daten werden nur in der Microsoft-Cloud gelöscht, nicht auf dem Gerät des Benutzers. Verbindet sich ein Gerät später wieder mit dem Enterprise State Roaming-Dienst, werden die gerätebasierten Einstellungen synchronisiert und in der Microsoft-Cloud gespeichert.

Tab. 2–15 Aufbewahrungsfristen für Enterprise State Roaming-Daten

WEITERE INFORMATIONEN **Enterprise State Roaming in Azure AD**

Wie Sie Enterprise State Roaming in Azure AD aktivieren, beschreibt die Microsoft-Website unter:

https://docs.microsoft.com/azure/active-directory/devices/enterprise-state-roaming-enable

Gedankenexperimente

In diesen Gedankenexperimenten wenden Sie an, was Sie über die in diesem Kapitel behandelten Themen wissen. Die Antworten auf die Fragen der Gedankenexperimente finden Sie im nächsten Abschnitt.

Szenario 1

Contoso hat 2000 Arbeitsstationen, die momentan unter Windows 10 Enterprise laufen und mit Gruppenrichtlinien und SCCM verwaltet werden. Die Firmenleitung hat vor Kurzem Microsoft 365-Lizenzen gekauft und die IT-Abteilung beauftragt, die in Microsoft 365 enthaltene MDM-Funktion zu implementieren. Die meisten Benutzer arbeiten in der Firmenzentrale, etwa 50 Mitarbeiter außerhalb.

Beantworten Sie als Consultant für Contoso folgende Fragen:

1. Welches in Microsoft 365 enthaltene Softwaretool verwenden Sie, um die Co-Verwaltung für die Organisation zu implementieren?
2. Welches Tool stellen Sie auf verwalteten Geräten bereit, um Richtlinien zu bewerten und auf MDM zu migrieren?
3. Die Organisation will ihre lokalen Active Directory-Domänenbenutzer mit Azure AD synchronisieren. Welches Tool muss die Organisation als Vorbereitung installieren, um die Benutzer mit der Cloud zu synchronisieren?
4. Die Firmenleitung möchte so bald wie möglich die Co-Verwaltung für alle Geräte implementieren. Empfehlen Sie eine Strategie, wie die Organisation die Co-Verwaltung einführen sollte.

Szenario 2

Contoso beschäftigt 500 Remotemitarbeiter, die sich über das ganze Land verteilen. Diese Angestellten arbeiten in ihrem Homeoffice und verwenden Surface Book-Geräte. Sie müssen in der Lage sein, eine webbasierte Branchen-App zu nutzen, der Zugriff auf das Unternehmensnetzwerk erfolgt dabei über ein sicheres VPN. Contoso hat vor Kurzem Microsoft 365 angeschafft und will die Sicherheits- und Konformitätsanforderungen des Unternehmens mit MDM bei den Remotearbeitern erzwingen. Das Unternehmens-VPN will Contoso so bald wie möglich außer Betrieb nehmen.

Beantworten Sie Ihrem Manager folgende Fragen:

1. Wenn Mitarbeiter auf die Branchen-App zugreifen, soll das auf sichere Weise geschehen. Welchen Bedingungstyp sollten Sie in eine implementierte Richtlinie für bedingten Zugriff aufnehmen?
2. Welchen Bedingungstyp sollten Sie in eine Richtlinie für bedingten Zugriff aufnehmen, mit der Sie die ausgehende VPN-Verbindung für Remotemitarbeiter ersetzen?
3. Welche Informationen brauchen Sie von den Mitarbeitern, um Ihre Lösung zu implementieren?
4. Ihr Manager hat Sie beauftragt, Ihre Richtlinien für bedingten Zugriff für die Remotemitarbeiter zu implementieren. Was sollten Sie tun, bevor Sie die Richtlinien für die Remotemitarbeiter bereitstellen?

Szenario 3

Ihre Organisation verwendet momentan eine Mischung verschiedener Betriebssysteme auf ihren Geräten, darunter Windows 7 Professional und Windows 10 Pro. Das Unternehmen hat 500 Surface Book-Geräte mit Windows 10 Pro gekauft, die die Hälfte der Windows 7-Geräte ersetzen sollen. Sie haben eine neue Azure AD-Gruppe namens *Surface Book-Geräte* angelegt und eine Regel für dynamische Mitgliedschaft definiert, die alle Surface Book-Geräte zu dieser Gruppe hinzufügt. Das Unternehmen hat vor Kurzem Microsoft 365 Enterprise gekauft und möchte die neuen Geräte ausschließlich mit MDM verwalten.

Beantworten Sie Ihrem Manager folgende Fragen:

1. Sie müssen eine ältere Win32-Anwendung bereitstellen, die für eine bestimmte Abteilung unverzichtbar ist. Wie stellen Sie die Anwendung mit möglichst geringem Verwaltungsaufwand bereit?
2. Die Sicherheitsrichtlinie des Unternehmens verbietet es den Benutzern, Microsoft-Konten auf Unternehmensgeräten zu verwenden. Wie sollten Sie die Unternehmensrichtlinie durchsetzen?
3. Sie haben ein Gerätekonfigurationsprofil bereitgestellt, mit dem Sie das Startmenülayout anpassen. Am nächsten Tag melden Surface Book-Benutzer, dass das einheitliche Startmenülayout auf ihren Geräten nicht implementiert wurde. Sie prüfen, ob die Einstellungen im Konfigurationsprofil und die Bereichsmarkierungen richtig sind. Die entsprechenden Geräte wurden zur dynamischen Gruppe *Surface Book-Geräte* hinzugefügt. Was sollten Sie außerdem prüfen?
4. Sie wollen Gerätekonfigurationsprofile auf den Windows 7 Professional-Geräten bereitstellen. Sie erstellen ein neues Gerätekonfigurationsprofil, aber in der Dropdownliste *Plattform* wird Windows 7 nicht aufgelistet. Warum nicht?
5. Sie sollen alle Geräte über MDM verwalten. Was sollten Sie tun? Ihr Ansatz sollte keine zusätzlichen Kosten verursachen.

Szenario 4

Adatum Corporation verwendet Microsoft 365 Enterprise und hat Windows 10 Enterprise auf allen Geräten implementiert. Die Organisation setzt Co-Verwaltung für die Geräte ein, die in der Firmenzentrale als Domänenmitglieder eingerichtet wurden. Remotemitarbeiter werden über Microsoft Intune verwaltet.

Beantworten Sie Ihrem Manager folgende Fragen:

1. Mitarbeiter der Designabteilung in der Firmenzentrale beschweren sich, dass sie morgens zehn Minuten brauchen, um sich an ihren Geräten anzumelden. Sie untersuchen die Angelegenheit und stellen fest, dass in der Firmenzentrale servergespeicherte Benutzerprofile verwendet werden. Welche zwei Möglichkeiten sollten Sie vorschlagen, um die Anmeldung zu beschleunigen? Ihre Lösungen sollten keine zusätzlichen Kosten verursachen.
2. Sie wollen auf den Geräten mehrerer Remotemitarbeiter die Synchronisierung von Windows-Einstellungen aktivieren, damit Browsereinstellungen wie Kennwörter, Favoriten, Top-Websites und eingetippte URLs zwischen den Geräten der Benutzer synchron gehalten werden. Die Pilotgruppe mit Remotemitarbeitern meldet, dass die Synchronisierung nicht funktioniert. Sie sollen das Problem lediglich für die Pilotgruppe beseitigen. Wie gehen Sie vor?
3. Sie haben Enterprise State Roaming für alle Remotemitarbeiter aktiviert, aber ein Benutzer meldet, dass die Microsoft Edge-Einstellungen nicht zwischen seinen Geräten synchronisiert werden. Sie prüfen, ob Enterprise State Roaming in Azure AD korrekt konfiguriert wurde, und überzeugen sich, dass andere Einstellungen für den Benutzer synchronisiert werden. Wie beseitigen Sie das Problem?
4. Contoso implementiert die Ordnerumleitung für die Profildateien und -ordner der Benutzer. Das Management will den Festplattenplatz nicht einschränken, aber auf dem Dateiserver in der Firmenzentrale wird der freie Speicherplatz knapp. Welche Lösung, die keine zusätzlichen Kosten verursacht, sollten Sie empfehlen?
5. Manche Benutzer haben ein sehr großes Profil und beschweren sich, dass die Anmeldung lange dauert. Contoso verwendet die Ordnerumleitung auf einen Dateiserver in der Firmenzentrale. Als Sie das Problem untersuchen, stellen Sie fest, dass mehrere Benutzer Musik- und Videodateien in ihren Profilen speichern. Wie können Sie den Anmeldeprozess beschleunigen und verhindern, dass Benutzer mehr als 500 MB an Musik- und Videodateien in ihrem Profil speichern?

Antworten zu den Gedankenexperimenten

Dieser Abschnitt enthält die Lösungen zu den Fragen, die in den Gedankenexperimenten gestellt wurden.

Szenario 1

1. Microsoft Intune ist in Microsoft 365 enthalten.
2. Das MDM Migration Analysis Tool (MMAT) wertet aus, welche Gruppenrichtlinien für einen Zielbenutzer beziehungsweise ein Zielgerät konfiguriert wurden, und stellt sie seiner integrierten Liste unterstützter MDM-Richtlinien gegenüber.
3. Azure AD Connect.
4. Die IT-Abteilung sollte Rollout-Gruppen für die phasenweise Einführung der Co-Verwaltung zusammenstellen. Als Gruppen sind eine Pilotgruppe mit wenigen Geräten und eine größere Produktivgruppe sinnvoll. Rollout-Gruppen helfen dabei, Probleme aufzudecken und zu beseitigen, die bei der Implementierung auftreten.

Szenario 2

1. Bei unterstützten Cloud-basierten Apps können Sie Richtlinien für bedingten Zugriff verwenden, die Mehr-Faktoren-Authentifizierung erzwingen.
2. Sie sollten eine Richtlinie für bedingten Zugriff implementieren, die eine standortbasierte Bedingung umfasst.
3. Die Mitarbeiter müssen Ihnen die IP-Adresse ihres Heimnetzwerks mitteilen.
4. Sie sollten einen Testplan für den bedingten Zugriff entwerfen. Dann testen Sie die Richtlinien außerhalb der Produktivumgebung oder bei einer Pilotgruppe der Remotemitarbeiter und stellen sicher, dass die Richtlinien die erwarteten Ergebnisse liefern, wie im Testplan dokumentiert.

Szenario 3

1. Sie können Win32-Anwendungen mit PowerShell auf den Windows 10-Geräten bereitstellen. Das PowerShell-Skript wird von Intune im Remotezugriff ausgeführt, woraufhin die Win32-Anwendung installiert wird.
2. Erstellen Sie ein Windows 10-Gerätekonfigurationsprofil, das Geräteeinschränkungen definiert und die Verwendung von Microsoft-Konten blockiert, und wenden Sie dieses Profil auf alle Geräte an.
3. Sie sollten sicherstellen, dass das Gerätekonfigurationsprofil korrekt an die Sicherheitsgruppe *Surface Book-Geräte* zugewiesen wurde.
4. Gerätekonfigurationsprofile unterstützen nicht die Plattform Windows 7.

5. Mit einem Microsoft 365 Enterprise-Abonnement verfügen Sie über die Lizenz, bei Windows 7-Geräten ein Upgrade auf Windows 10 vorzunehmen; dafür fallen keine zusätzlichen Kosten an.

Szenario 4

1. Es sind mehrere Ansätze möglich. Sie können mit einem Kontingent die Größe der servergespeicherten Benutzerprofile auf dem Dateiserver beschränken, der die Profile hostet. Sie können auch Ordnerumleitung einsetzen, um bestimmte Profilordner auf einen Speicherort im Netzwerk umzuleiten. Die Größe eines servergespeicherten Benutzerprofils sinkt, weil die in umgeleiteten Ordnern gespeicherten Dateien nicht in das servergespeicherte Benutzerprofil aufgenommen werden.
2. Die Synchronisierung von Einstellungen steht für Windows 10-Benutzer zur Verfügung, die Microsoft-Konten verwenden. Es ist unwahrscheinlich, dass Benutzer in einer Unternehmensumgebung sich mit Microsoft-Konten anmelden. Daher sollten Sie Enterprise State Roaming empfehlen. Dazu erstellen Sie eine Azure AD-Sicherheitsgruppe und fügen ihr die Remotemitarbeiter hinzu, die an der Pilotphase teilnehmen. Anschließend aktivieren Sie das Enterprise State Roaming für die Azure AD-Sicherheitsgruppe dieser Remotemitarbeiter.
3. Wahrscheinlich sind in Microsoft Edge die Optionen zum Synchronisieren von Microsoft Edge-Favoriten, Leseliste, Top-Websites und weiteren Einstellungen ausgeschaltet. Schalten Sie diese Optionen ein, um das Problem zu beseitigen.
4. Im Rahmen eines Microsoft 365 Enterprise-Abonnements erhält jeder Benutzer unbegrenzten persönlichen Speicher in OneDrive for Business. Sie sollten dem Unternehmen empfehlen, die Umleitung bekannter Ordner für OneDrive zu konfigurieren und OneDrive for Business-Speicher zu verwenden.
5. Sie können auf einem Windows-Server in der Firmenzentrale den Rollendienst *Ressourcen-Manager für Dateiserver* implementieren, um die Daten, die auf Dateiservern gespeichert sind, zu verwalten und zu klassifizieren. Nach seiner Aktivierung kann der Ressourcen-Manager für Dateiserver die Dateien automatisch klassifizieren und auf Basis dieser Klassifizierungen Aktionen ausführen, zum Beispiel Kontingente für Ordner festlegen und Berichte zur Überwachung der Speichernutzung erstellen. Außerdem sollten Sie die Benutzer darüber informieren, dass die Größe von Dateien im Benutzerprofil künftig eingeschränkt wird.

Zusammenfassung des Kapitels

- Co-Verwaltung bedeutet, dass Sie Geräte sowohl mit System Center Configuration Manager als auch Microsoft Intune verwalten.
- Seit Windows 10, Version 1803, kann Intune den Vorrang für Richtlinien erhalten, wenn sowohl Gruppenrichtlinien als auch entsprechende Intune-Richtlinien auf das Gerät angewendet werden.

- Das MDM Migration Analysis Tool wertet aus, welche Gruppenrichtlinien für einen Zielbenutzer beziehungsweise ein Zielgerät angewendet wurden, und stellt sie seiner integrierten Liste unterstützter MDM-Richtlinien gegenüber.
- Mit Richtlinien für bedingten Zugriff steht Administratoren ein Werkzeug zur Verfügung, über das Azure AD prüfen kann, ob bestimmte Bedingungen erfüllt sind, bevor es den Zugriff auf Unternehmensressourcen gewährt (zum Beispiel auf überwachte Apps).
- Richtlinien für bedingten Zugriff definieren Bedingungen und Steuerelemente, aus denen Regeln zusammengesetzt werden, die Azure AD auswertet.
- Wenn Sie Richtlinien für bedingten Zugriff implementieren, sollten Sie einen Testplan entwickeln.
- Konformitätsrichtlinien stellen sicher, dass Geräte die Konformitätsanforderungen erfüllen, das heißt zum Beispiel, dass sie verschlüsselt sind, dass kein Jailbreak durchgeführt wurde und dass ein Kennwort für den Gerätezugriff eingegeben werden muss.
- Der Zugriff nicht konformer Geräte auf Ressourcen kann blockiert werden oder die Benutzer können Hinweise erhalten, wie sie ihr Gerät richtlinienkonform machen.
- Sind einem Gerät mehrere Gerätekonformitätsrichtlinien zugewiesen, berechnet Intune einen Konformitätsstatus auf Basis des höchsten Schweregrads aller zugewiesenen Richtlinien.
- Geräte prüfen ihren Konformitätsstatus regelmäßig bei Intune; das passiert bei Apple-Geräten alle sechs Stunden, bei Android- und Windows-Geräten alle acht Stunden.
- Intune-Gerätekonfigurationsrichtlinien werden benutzt, um Geräteeinstellungen über MDM zu konfigurieren.
- Intune kann über eine MDM-Erweiterung PowerShell-Skripts auf Windows-Geräte bereitstellen. So können Administratoren bei Bedarf Win32-Anwendungen bereitstellen.
- Bereichsmarkierungen dienen dazu, Intune-Richtlinien für spezifische Azure AD-Gruppen zuzuweisen und zu filtern.
- Sie können mit Intune benutzerdefinierte Richtlinien konfigurieren, indem Sie eine OMA-URI-Richtlinie (Open Mobile Alliance Uniform Resource Identifier) zusammenstellen.
- Ein Benutzerprofil enthält den Benutzerzustand mit Anwendungseinstellungen und Einstellungen anderer Systemkomponenten sowie benutzerspezifische Daten wie Desktop-, Startmenü- und Dokumente-Ordner des Benutzers.
- Es gibt lokale, servergespeicherte, verbindliche, superverbindliche und temporäre Benutzerprofile.
- Falls servergespeicherte Benutzerprofile zu groß werden, kann die Anmeldung der Benutzer sehr lange dauern.

- Ein Benutzer kann wichtige Windows-Einstellungen wie Kennwörter, Designs und Browsereinstellungen mit der Cloud synchronisieren, damit sie auf alle Geräte angewendet werden, bei denen sich der Benutzer unter demselben Microsoft-Konto anmeldet.
- Administratoren können die Ordnerumleitung aktivieren, um einzelne Profilordner in einem Netzwerkordner zu speichern.
- Über die Umleitung bekannter Ordner für OneDrive werden Ordner und wichtige Dateien der Benutzer auf ihre OneDrive for Business-Konten umgeleitet und in der Microsoft-Cloud gespeichert.
- Administratoren können Enterprise State Roaming aktivieren, damit Azure AD die Windows-Einstellungen und UWP-App-Einstellungen (Universal Windows Platform) auf sichere Weise über alle Windows-Geräte der Benutzer hinweg synchronisiert.