

2023-02-17



HORNETSECURITY

365 TOTAL PROTECTION

www.hornetsecurity.com

THE CLOUD SECURITY PIONEER

Inhalt

Sprache und Symbole in der Dokumentation.....	4
Über 365 Total Protection.....	6
Onboarding eines neuen Kunden als Partner.....	8
Onboarding-Link erstellen.....	8
365-Total-Protection-Kunden zum Control Panel hinzufügen.....	9
365 Total Protection einrichten.....	10
365 Total Backup konfigurieren.....	14
Upgrade auf 365 Total Protection als Kunde.....	25
Auf 365 Total Protection upgraden.....	25
Sprache und Symbole in der Dokumentation.....	41
Über die Postfachmigration.....	43
Einschränkungen der Postfachmigration.....	45
Voraussetzungen für die Postfachmigration.....	46
Voraussetzungen für Postfächer.....	47
Rollengruppe auf dem Exchange-Server erstellen.....	48
Rollengruppe in Microsoft 365 erstellen.....	53
Berechtigungen zum Lesen und Verwalten von Postfächern in Microsoft 365 erteilen.....	57
Berechtigungen zum Lesen und Verwalten von Postfächern in Microsoft 365 über PowerShell erteilen.....	60
Zugriff auf Exchange-Webdienste erlauben.....	61
Einschränkung der Exchange-Webdienste deaktivieren.....	63
Migration von Postfachdaten.....	65
Umgebung validieren.....	66
Validierung einer Umgebung zurücksetzen.....	71
Postfächer migrieren.....	73
Postfachmigration abschließen.....	82
365 Total Backup konfigurieren.....	84
Konfiguration der Services von Microsoft.....	95
Grundlegende Einstellungen.....	95

Grundlegende Einstellungen.....	95
Erweiterte Einstellungen.....	109
Erweiterte Einstellungen.....	109
365 Total Protection bestellen.....	111
Anzeige der Anzahl von Postfächern, Lizenzen und Domains.....	112
Verwaltung von Postfächern.....	113
Gruppenverwaltung im Control Panel.....	114
Gruppen aus Microsoft 365 im Control Panel synchronisieren.....	114
Zusammenspiel von 365 Total Protection mit weiteren Services.....	116
Email Encryption.....	116
Continuity Service aktivieren (Nur 365 Total Protection Enterprise).....	117
Synchronisierte Attribute aus dem Azure Active Directory.....	119
Offboarding nach Beenden der Teststellung oder Kündigung.....	121
Connector löschen oder deaktivieren.....	121
Kunden löschen.....	122
Index.....	125



Sprache und Symbole in der Dokumentation

Gender-Erklärung

Aus Gründen der besseren Lesbarkeit wird in dieser Dokumentation die Sprachform des generischen Maskulinums verwendet. Es wird an dieser Stelle darauf hingewiesen, dass die ausschließliche Verwendung der männlichen Form genderunabhängig verstanden werden soll.

Verwendete Symbole

Zur besseren Kenntlichkeit relevanter Schritte innerhalb handlungsanleitender Kapitel werden folgende Symbole verwendet:

Symbol	Bedeutung	Erklärung
	Voraussetzung	Bedingung, die vor dem nächsten Schritt erfüllt sein muss
	Zwischenresultat	Resultat, welches nach einem Schritt zwischenzeitlich erzielt wird
	Endresultat	Resultat, welches nach der Schrittreihenfolge eines handlungsanleitenden Kapitels erzielt wird

Warn- und Sicherheitshinweise

Die Warn- und Sicherheitshinweise werden eingesetzt, um Benutzer über Restrisiken und Gefahren zu informieren und diese mit einer empfohlenen Vorgehensweise zu vermeiden. Folgende Warn- und Sicherheitshinweise werden in dieser Dokumentation verwendet:

Symbol	Bedeutung	Erklärung
	HINWEIS	Weiterführende Informationen innerhalb eines bestimmten Absatzes, die für die Ausführung weiterer Schritte relevant sind.
	TIPP	Hinweis zu Konfigurationsmöglichkeiten.
	WICHTIG	Warnhinweis mit Informationen über Einschränkungen oder wichtige Konfigurationsmöglichkeiten des Services.



Symbol	Bedeutung	Erklärung
	ACHTUNG	Warnhinweis über zusätzliche Kosten, die, abhängig von gebuchten Serviceleistungen, möglicherweise entstehen können.
	WARNUNG	Warnhinweis zum möglichen Verlust von Daten.
	GEFAHR	Sicherheitshinweis zur möglichen System-Infizierung mit einer Malware.



Über 365 Total Protection

Unser Service 365 Total Protection richtet sich an Kunden von Microsoft 365 und schützt deren E-Mails und Daten in Microsoft 365. 365 Total Protection ist speziell für Microsoft 365 entwickelt worden und nahtlos darin integriert.

365 Total Protection ist in den Versionen Business, Enterprise und Enterprise Backup verfügbar. Die Versionen unterscheiden sich in ihrem Funktionsumfang:

- Alle Versionen schützen E-Mails und Daten durch die Filterung von Anhängen (siehe [Über Content Control](#)), selbstdefinierte Regeln zur Filterung von E-Mails (siehe [Über den Compliance Filter](#)) und Einstellungen zur Verschlüsselung von E-Mails (siehe [Email Encryption](#)).
- Die Versionen Enterprise und Enterprise Backup unterstützen zusätzlich die rechtssichere Archivierung von E-Mails (siehe [Archiving](#)), bieten Analysemechanismen zur Erkennung komplexer Bedrohungen (siehe [Aufbau und Funktion von ATP](#)) und halten den E-Mail-Verkehr bei einem Ausfall des E-Mail-Servers aufrecht (siehe [Über den Continuity Service](#)). Zusätzlich haben Administratoren in diesen Versionen die Möglichkeit, bereits zugestellte E-Mails aus den Microsoft-365-Postfächern (siehe [Postfachtypen](#)) ihrer Benutzer zu löschen (siehe [Ex Post Deletion](#)), falls sich beispielsweise eine E-Mail nachträglich als Bedrohung herausgestellt hat.
- Mit der Version Enterprise Backup können zusätzlich die Daten aus dem Microsoft-365-Tenant und Windows-basierten Endpunkten eines Kunden gesichert und wiederhergestellt werden (siehe [Über 365 Total Backup](#)).

Sobald 365 Total Protection für einen Kunden eingerichtet wird, werden die Domains, Gruppen und Benutzer des Kunden im Control Panel mit dessen Microsoft-365-Organisation synchronisiert. Auch nach der Einrichtung werden die Domains, Gruppen und Benutzer im Control Panel regelmäßig mit Microsoft 365 synchronisiert.

Administratoren auf Partnerebene können für einen neuen Kunden 365 Total Protection direkt beim Onboarding einrichten (siehe [Onboarding eines neuen Kunden als Partner](#) auf Seite 8). Bestehende Kunden können jederzeit auf 365 Total Protection upgraden (siehe [Upgrade auf 365 Total Protection als Kunde](#) auf Seite 25).



Hinweis:

Bestehende Kunden, die auf die Version Enterprise oder Enterprise Backup upgraden und bisher einen lokalen Exchange-Server verwendet haben, können während des Upgrades Postfachdaten von ihrem lokalen Exchange-Server zu ihrem Microsoft-365-Tenant migrieren (siehe [Über die Postfachmigration](#) auf Seite 43). Dadurch wird den Kunden der Umstieg auf Microsoft 365 erleichtert.



HORNETSECURITY

Über 365 Total Protection

Nach der Einrichtung von 365 Total Protection startet eine 14-tägige Testphase. Um 365 Total Protection nach der Testphase weiterhin zu nutzen, muss der Kunde den Service erwerben (siehe [365 Total Protection bestellen](#) auf Seite 111).



Onboarding eines neuen Kunden als Partner

Mit 365 Total Protection (siehe [Über 365 Total Protection](#) auf Seite 6) können Partner für Kunden, die ein Konto bei Microsoft 365 haben, die Einrichtung im Control Panel automatisiert durchführen. Alle in Microsoft 365 erstellten Domains und Benutzer des Kunden werden automatisch übernommen und im Control Panel abgebildet.



Hinweis:

Auch Gruppenmitglieder aus Microsoft 365 können im Control Panel synchronisiert werden. Um Gruppenmitglieder zu synchronisieren, müssen Administratoren auf Kundenebene gleichnamige Gruppen im Control Panel erstellen. Für weitere Informationen siehe [Gruppenverwaltung im Control Panel](#) auf Seite 114.

Administratoren auf Partnerebene haben zwei Möglichkeiten, einen Kunden einzurichten: Entweder schickt ein Administrator auf Partnerebene dem Kunden einen Onboarding-Link (siehe [Onboarding-Link erstellen](#) auf Seite 8), mit dem er die Einrichtung selbst vornehmen kann, oder ein Administrator auf Partnerebene meldet sich bei Microsoft mit den administrativen Zugangsdaten des Kunden an und führt den Onboarding-Prozess selbst durch (siehe [365-Total-Protection-Kunden zum Control Panel hinzufügen](#) auf Seite 9). Sobald ein Administrator auf Partnerebene das Onboarding für einen Kunden angestoßen hat, kann der Administrator 365 Total Protection für den Kunden konfigurieren (siehe [365 Total Protection einrichten](#) auf Seite 10). Falls die Version 365 Total Protection Enterprise Backup ausgewählt worden ist, kann der Administrator auf Partnerebene zusätzlich 365 Total Backup für den Kunden konfigurieren, damit die Daten aus dessen Microsoft-365-Tenant gesichert werden.

Im Anschluss müssen noch einige DNS-Einstellungen der Domains durchgeführt werden, um den E-Mail-Verkehr umzuleiten.

Onboarding-Link erstellen

Sie können für Ihre Kunden einen Onboarding-Link erstellen, damit sie die Einrichtung unserer Services selbst durchführen können. Der Link führt zum Onboarding-Formular von 365 Total Protection. Sie können diesen Link an Ihre Kunden weitergeben, damit sie die Einrichtung von 365 Total Protection selbst durchführen können (siehe [365 Total Protection einrichten](#) auf Seite 10). Der Link kann mehrmals verwendet werden.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie den Partner in der Bereichsauswahl aus, unter dem Sie den neuen Kunden erstellen möchten.



3. Navigieren Sie zu **365 Total Protection > 365 Total Protection**.
4. Wählen Sie unter **Ihre Onboarding-Adresse** eine Version von 365 Total Protection für Ihre Kunden aus. Sie haben die folgenden Optionen:

- **Auswahl offen lassen**
- **Business**
- **Enterprise**
- **Enterprise Backup**



Ein eindeutiger Link wird erzeugt.

5. Klicken Sie auf , um den Link in die Zwischenablage zu kopieren.



Ein Onboarding-Link für 365 Total Protection ist erstellt worden.

365-Total-Protection-Kunden zum Control Panel hinzufügen

Sie können einen neuen 365-Total-Protection-Kunden (siehe [Über 365 Total Protection](#) auf Seite 6) zum Control Panel hinzufügen, falls Sie die administrativen Zugangsdaten zur Microsoft-365-Umgebung des neuen Kunden haben.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie in der Bereichsauswahl den Partner aus, unter dem ein neuer 365-Total-Protection-Kunde erstellt werden soll.



Abbildung 1: Partner in der Bereichsauswahl auswählen

3. Navigieren Sie zu **365 Total Protection > 365 Total Protection**.



4. Wählen Sie für den neuen Kunden eine Version von 365 Total Protection aus.



Abbildung 2: Version auswählen



Das Onboarding-Formular wird angezeigt.



Das Onboarding eines neuen 365-Total-Protection-Kunden ist angestoßen worden.

Anschließend können Sie 365 Total Protection für den Kunden einrichten (siehe [365 Total Protection einrichten](#) auf Seite 10).

365 Total Protection einrichten

Sie können 365 Total Protection einrichten.



Sie haben das Onboarding-Formular für 365 Total Protection geöffnet (siehe [365-Total-Protection-Kunden zum Control Panel hinzufügen](#) auf Seite 9).

Sobald Sie das Onboarding-Formular für 365 Total Protection geöffnet haben, können Sie 365 Total Protection (siehe [Über 365 Total Protection](#) auf Seite 6) einrichten.



1.

! Wichtig:

Das Feld **Anzeigename (Domain) im Control Panel** steht für die Hauptdomain des Kunden und nicht für dessen .onmicrosoft-Domain. Die Domain wird im Control Panel angezeigt.

Geben Sie Ihre Kontaktdaten in das Onboarding-Formular ein.

i Hinweis:

Anhand der Kontaktdaten können wir Sie bei Problemen oder Rückfragen kontaktieren.

365 TOTAL PROTECTION ONBOARDING

Anzeigename (Domain) im Control Panel
musterfirma.com

Firma
Musterfirma

Anrede Herr Vorname Max Nachname Mustermann

E-Mail mustermann@musterfirma.com Telefon 123456

Datenschutz
 Ich stimme der Verarbeitung meiner Daten und einer Kontaktaufnahme durch Hornetsecurity oder einen zertifizierten Partner gemäß der [Datenschutzerklärung](#) zu.

IT Security News
 Ich möchte regelmäßig die IT Security News erhalten.

Jetzt starten

Abbildung 3: Kontaktdaten eingeben

2. Setzen Sie ein Häkchen in der Checkbox unter **Datenschutz**.
3. Optional: Falls Sie unsere IT Security News erhalten möchten, setzen Sie ein Häkchen in der Checkbox **Ich möchte regelmäßig die IT Security News erhalten**.



4.

Achtung:

Sobald 365 Total Protection aktiviert wird, startet eine 14-tägige kostenfreie Testphase. Damit ein Kunde den Service nach Ende der Testphase weiterhin verwenden kann, muss der Kunde den Service erwerben (siehe [365 Total Protection bestellen](#) auf Seite 111).

Klicken Sie auf **Jetzt starten**, um den Einrichtungsprozess zu starten.



Die Anmeldeseite von Microsoft wird angezeigt.

5. Melden Sie sich mit Ihren administrativen Zugangsdaten bei Microsoft 365 an.

Microsoft

Anmelden

E-Mail, Telefon oder Skype

Kein Konto? [Erstellen Sie jetzt eins!](#)

[Sie können nicht auf Ihr Konto zugreifen?](#)

Weiter

Abbildung 4: Microsoft-Anmeldedaten eingeben

Hinweis:

Bei der anschließenden Synchronisation werden nur Domains und Postfächer übertragen. Es werden keine Änderungen an den Konfigurationseinstellungen von Microsoft vorgenommen. Auch Gruppen werden mit Microsoft 365 synchronisiert, falls ein Kunde im Control Panel gleichnamige Gruppen manuell erstellt hat (siehe [Gruppenverwaltung im Control Panel](#) auf Seite 114).



- Akzeptieren Sie die angeforderten Berechtigungen, um unsere Services mit Microsoft zu verbinden.



Abbildung 5: Berechtigungen akzeptieren



Die Domains und Postfächer aus Microsoft 365 werden im Control Panel erstellt. Die Domains werden zum Modul **Kundeneinstellungen > Domains** (siehe **Domains**) hinzugefügt. Die Domains erhalten in der Spalte **Verifiziert** zunächst den Status **Nicht verifiziert**. Nach wenigen Minuten wird geprüft, ob die Domains verifiziert werden können (siehe **Verifizierung von Domains**).



Die Domains und Postfächer des Kunden sind im Control Panel erstellt worden. Ab sofort kann sich der Administrator der Microsoft-365-Organisation des Kunden mit seinen Zugangsdaten aus Microsoft 365 im Control Panel anmelden und die Services konfigurieren.

Nach der Synchronisation müssen Sie die Services von Microsoft konfigurieren (siehe **Konfiguration der Services von Microsoft** auf Seite 95), damit Sie unsere Services in vollem Umfang nutzen können.



Falls Sie 365 Total Protection Enterprise Backup ausgewählt haben, müssen Sie zusätzlich 365 Total Backup konfigurieren (siehe [365 Total Backup konfigurieren](#) auf Seite 14), damit die Daten aus dem Microsoft-365-Tenant des Kunden gesichert werden.

365 Total Backup konfigurieren



Sie haben 365 Total Protection Enterprise Backup für einen Kunden eingerichtet (siehe [365 Total Protection einrichten](#) auf Seite 10).

Der Service 365 Total Protection Enterprise Backup kombiniert die Services 365 Total Protection Enterprise und 365 Total Backup miteinander (siehe [Über 365 Total Protection](#) auf Seite 6). Sobald Sie 365 Total Protection Enterprise Backup für einen Kunden eingerichtet haben, können Sie 365 Total Backup für den Kunden konfigurieren. Mit diesem Vorgehen richten Sie 365 Total Backup nach den Standardeinstellungen ein. In dem Fall werden alle Microsoft-365-Postfächer, Dateien in OneDrive-for-Business-Konten und SharePoint-Dokumentbibliotheken sowie Teams-Chats für Benutzer und Gruppen aus dem Tenant des Kunden gesichert.



Hinweis:

Administratoren auf Kundenebene oder Partnerebene können 365 Total Backup mit anderen Einstellungen konfigurieren, indem sie 365 Total Backup über das Modul **Backup > 365 Total Backup** öffnen (siehe [365 Total Backup starten](#)).

Mit 365 Total Backup können auch Daten von Windows-basierten Endpunkten gesichert werden. Endpunkte werden bei der Standardkonfiguration jedoch nicht berücksichtigt. Nur Administratoren auf Partnerebene können Backups von Endpunkten konfigurieren. Dazu können Administratoren auf Partnerebene 365 Total Backup über das Modul **Backup > 365 Total Backup** öffnen.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie in der Bereichsauswahl die Domain des Kunden aus.



3. Navigieren Sie zu **365 Total Protection > 365 Total Protection**.



Der Einrichtungsstatus von 365 Total Protection Enterprise Backup wird angezeigt.

Einrichtungsstatus 365 Total Protection Enterprise Backup

MICROSOFT 365 WURDE VERBUNDEN.

21 Postfächer | 20 Lizenzen | 2 Domains

Konfigurieren Sie die DNS-Einstellungen Ihrer Domains

Die DNS-Einstellungen von mindestens einer synchronisierten Domain wurden noch nicht gesetzt oder sind falsch konfiguriert. Folgen Sie der Anleitung im Handbuch, um die DNS-Einstellungen richtig zu konfigurieren.

Jetzt konfigurieren

365 Total Backup konfigurieren

Klicken Sie auf „Jetzt konfigurieren“, um erforderliche Berechtigungen für die Sicherung Ihres Microsoft-365-Tenants zu gewähren.

Jetzt konfigurieren

Ausgehenden E-Mail-Verkehr konfigurieren

Sie müssen Ihren ausgehenden E-Mail-Verkehr konfigurieren. Eine Anleitung dazu finden Sie in unserem Handbuch.

Automatisch konfigurieren

Abbildung 6: Einrichtungsstatus

4. Klicken Sie unter **365 Total Backup konfigurieren** auf **Jetzt konfigurieren**.



In einem neuen Tab öffnet sich eine Seite zur Konfiguration von 365 Total Backup. Die Daten des Kunden sind voreingestellt.



Hinweis:

Auf der Seite wird die Sprache verwendet, die für den übergeordneten Partner des Kunden im Control Panel eingestellt ist (siehe [Standardwerte für Zeitzone und Sprache einstellen](#)).



5. Klicken Sie auf **Weiter**.

365 Total Backup konfigurieren

Schritt 1
Office-365-Organisation hinzufügen

2 Beenden
Zugang gewähren

Office-365-Organisation hinzufügen

Wählen Sie die Office-365-Organisation aus, die hinzugefügt werden soll.

Kunde auswählen
blueberry.com

Unternehmensname der Office-365-Organisation
onmicrosoft.com

Office-365-Organisation
onmicrosoft.com

Abbrechen Weiter

Abbildung 7: Angaben prüfen



Ein Fenster mit einer Übersicht der Konfigurationsschritte öffnet sich.



6. Klicken Sie auf Schritt 1.

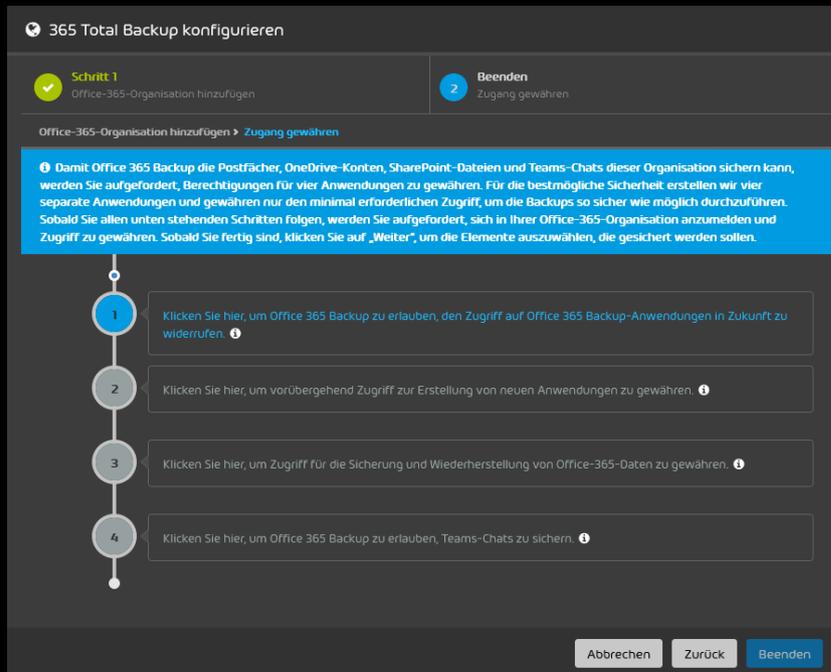


Abbildung 8: Schritt 1 durchführen



Die Anmeldeseite von Microsoft 365 öffnet sich in einem neuen Tab.

7. Melden Sie sich mit den administrativen Zugangsdaten des Kunden bei Microsoft 365 an.



Eine Seite mit angeforderten Berechtigungen wird angezeigt.



8. Gewähren Sie die angeforderten Berechtigungen.

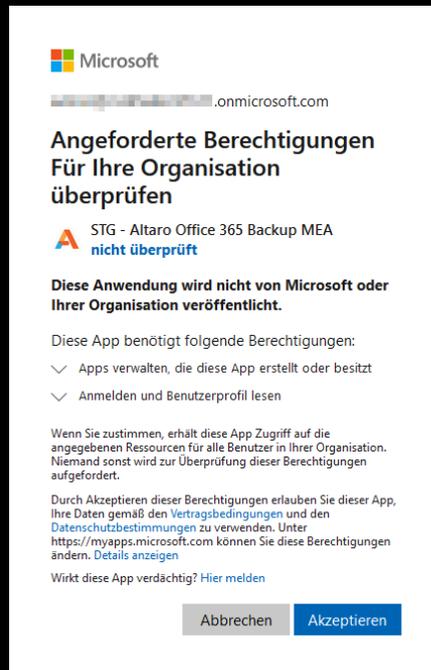


Abbildung 9: Berechtigungen gewähren



Die Berechtigungen werden gewährt. Eine Bestätigungsmeldung wird angezeigt.



Abbildung 10: Bestätigungsfenster

9. Klicken Sie auf **Schließen**.



Der Tab wird geschlossen. Die Übersicht der Konfigurationsschritte wird wieder angezeigt.



10. Klicken Sie auf Schritt 2.

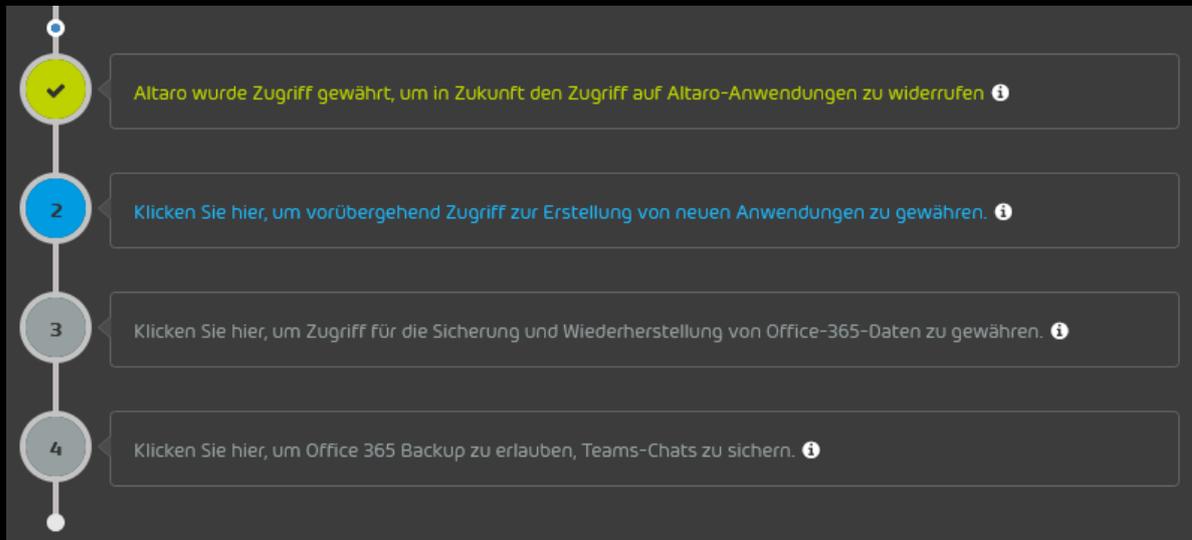


Abbildung 11: Schritt 2 durchführen



Die Anmeldeseite von Microsoft 365 öffnet sich in einem neuen Tab.

11. Melden Sie sich mit den administrativen Zugangsdaten des Kunden bei Microsoft 365 an.



365 Total Backup wird Zugang zum Tenant des Kunden gewährt. Eine Bestätigungsmeldung wird angezeigt.



Abbildung 12: Bestätigungsfenster

12. Klicken Sie auf **Schließen**.



Der Tab wird geschlossen. Die Übersicht der Konfigurationsschritte wird wieder angezeigt.



13. Klicken Sie auf Schritt 3.

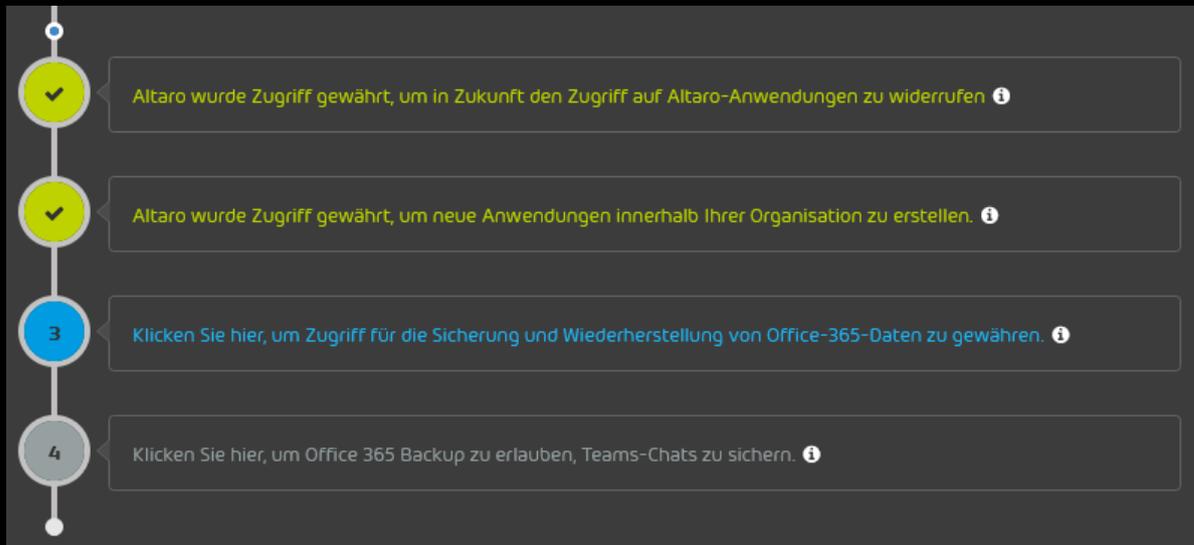


Abbildung 13: Schritt 3 durchführen



Die Anmeldeseite von Microsoft 365 öffnet sich in einem neuen Tab.

14. Melden Sie sich mit den administrativen Zugangsdaten des Kunden bei Microsoft 365 an.



Eine Seite mit angeforderten Berechtigungen wird angezeigt.



15. Gewähren Sie die angeforderten Berechtigungen.

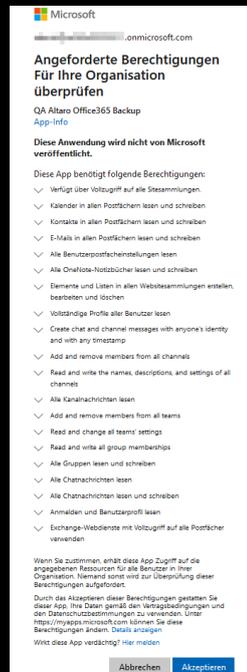


Abbildung 14: Berechtigungen gewähren



Die Berechtigungen werden gewährt. Eine Bestätigungsmeldung wird angezeigt.



Abbildung 15: Bestätigungsfenster



16. Klicken Sie auf Schritt 4.

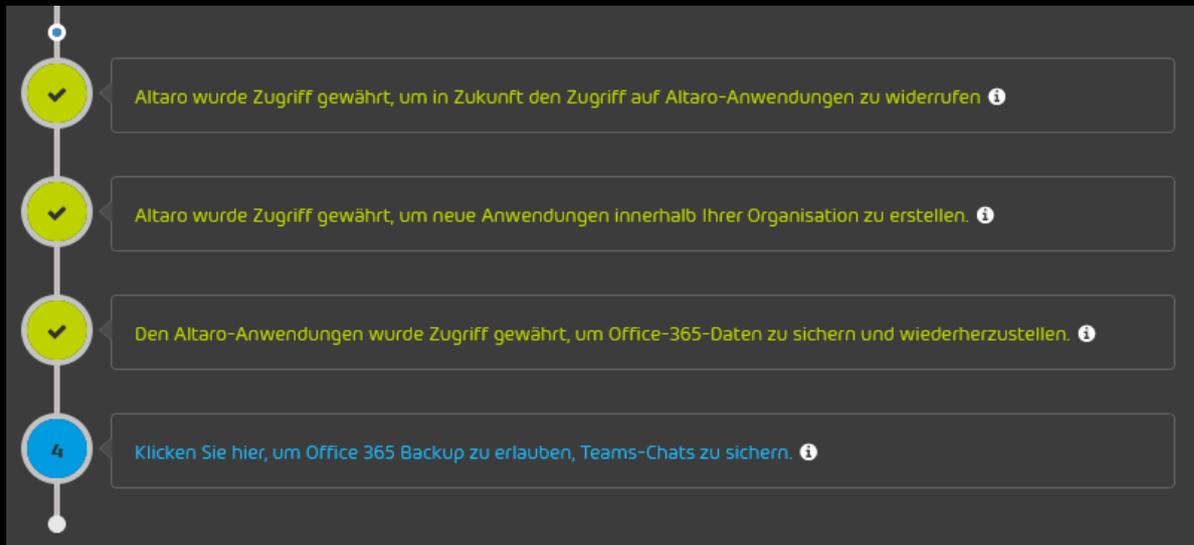


Abbildung 16: Schritt 4 durchführen



Die Anmeldeseite von Microsoft 365 öffnet sich in einem neuen Tab.

17. Melden Sie sich mit den administrativen Zugangsdaten des Kunden bei Microsoft 365 an.



Eine Seite mit angeforderten Berechtigungen wird angezeigt.



18. Gewähren Sie die angeforderten Berechtigungen.

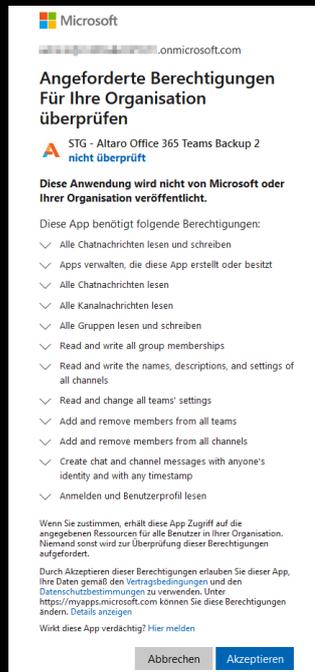


Abbildung 17: Berechtigungen gewähren



Die Berechtigungen werden gewährt. Eine Bestätigungsmeldung wird angezeigt.



Abbildung 18: Bestätigungsfenster

19. Klicken Sie auf **Schließen**.



Der Tab wird geschlossen. Die Übersicht der Konfigurationsschritte wird wieder angezeigt.



20. Klicken Sie auf **Beenden**.

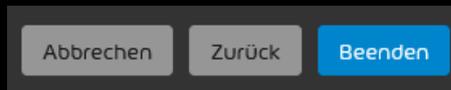


Abbildung 19: Konfiguration beenden



Der Tab wird geschlossen. Im Control Panel wird die Konfiguration von 365 Total Backup im Modul **365 Total Protection** > **365 Total Protection** als abgeschlossen angezeigt.



Abbildung 20: Status der Konfiguration von 365 Total Backup



365 Total Backup ist konfiguriert worden.



Upgrade auf 365 Total Protection als Kunde

Falls ein Kunde einen Microsoft-365-Tenant hat und bereits unsere Services nutzt, kann er das Upgrade auf 365 Total Protection (siehe [Über 365 Total Protection](#) auf Seite 6) über das Control Panel selbst durchführen (siehe [Auf 365 Total Protection upgraden](#) auf Seite 25).

Kunden, die auf die Version Enterprise oder Enterprise Backup upgraden und bisher einen lokalen Exchange-Server verwendet haben, können während des Upgrades Postfachdaten von ihrem lokalen Exchange-Server zu ihrem Microsoft-365-Tenant migrieren (siehe [Über die Postfachmigration](#) auf Seite 43). Dadurch wird den Kunden der Umstieg auf Microsoft 365 erleichtert.

Beim Upgrade auf 365 Total Protection werden alle in Microsoft 365 erstellten Domains und Postfächer automatisch in das Control Panel übernommen.

Auf 365 Total Protection upgraden



Sie haben einen Microsoft-365-Tenant und nutzen unsere Services.

Als bestehender Kunde können Sie im Control Panel auf 365 Total Protection (siehe [Über 365 Total Protection](#) auf Seite 6) upgraden.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie Ihre Domain in der Bereichsauswahl aus.
3. Navigieren Sie zu **365 Total Protection > 365 Total Protection**.



4.

! Wichtig:

Bei dem Upgrade auf 365 Total Protection werden die Postfächer und Domains im Control Panel mit Microsoft 365 synchronisiert. Neue Postfächer werden zum Control Panel hinzugefügt und bestehende Postfächer werden gemäß den Einstellungen in Microsoft 365 aktualisiert.

! Wichtig:

Das Upgrade kann nicht durchgeführt werden, falls im Modul **Spam and Malware Protection** die Option **POP3/IMAP** als primäre Umgebung ausgewählt ist (siehe [Primäre Umgebungseinstellungen vornehmen](#)).

! Wichtig:

Die Option **Enterprise Backup** kann nur ausgewählt werden, falls der Partner 365 Total Backup aktiviert hat (siehe [365 Total Backup aktivieren](#)).

Klicken Sie auf die Version von 365 Total Protection, auf die Sie upgraden möchten. Sie haben die folgenden Optionen:

- **Business**
- **Enterprise**
- **Enterprise Backup**

i Hinweis:

Für weitere Informationen zu den Versionen siehe [Über 365 Total Protection](#) auf Seite 6.



Abbildung 21: Version auswählen





Falls die Multi-Faktor-Authentifizierung für die Domain im Control Panel freigeschaltet ist (siehe [Multi-Faktor-Authentifizierung freischalten](#)), wird eine Meldung zur Multi-Faktor-Authentifizierung angezeigt. Andernfalls wird eine Warnmeldung angezeigt.

5.

! Wichtig:

Das Upgrade auf 365 Total Protection ist nur möglich, falls die Multi-Faktor-Authentifizierung im Control Panel deaktiviert ist. Nach dem Upgrade auf 365 Total Protection melden sich die Benutzer aus dem Microsoft-365-Tenant mit ihren Zugangsdaten aus Microsoft 365 im Control Panel an und es gelten die Authentifizierungsrichtlinien aus dem Tenant (siehe [Multi-Faktor-Authentifizierung freischalten](#)).

Falls eine Meldung zur Multi-Faktor-Authentifizierung angezeigt wird, klicken Sie auf **Bestätigen**.

MULTI-FAKTOR-AUTHENTIFIZIERUNG

Die Multi-Faktor-Authentifizierung ist für Ihre Benutzer im Control Panel freigeschaltet. Sie können nur zu 365 Total Protection migrieren, falls die Multi-Faktor-Authentifizierung im Control Panel deaktiviert ist. Kunden von 365 Total Protection können die Multi-Faktor-Authentifizierung stattdessen in ihrem Tenant in Microsoft 365 konfigurieren. Falls Sie fortfahren, wird die Multi-Faktor-Authentifizierung deaktiviert und die Konfiguration für alle Benutzer im Control Panel aufgehoben. Möchten Sie fortfahren?

Abbildung 22: Multi-Faktor-Authentifizierung deaktivieren



Die Multi-Faktor-Authentifizierung wird für die Benutzer der Domain deaktiviert. Für Benutzer, die die Multi-Faktor-Authentifizierung bereits konfiguriert hatten, wird die Konfiguration aufgehoben. Eine Warnmeldung wird angezeigt.



- Um das Upgrade auf 365 Total Protection anzustoßen, klicken Sie auf **Bestätigen**.

MIGRATION ZU 365 TOTAL PROTECTION

Sie sind im Begriff, zu 365 Total Protection zu migrieren. Postfächer aus der primären Umgebung, die nicht in Microsoft 365 verwaltet werden, werden stattdessen der ausgewählten sekundären Umgebung zugewiesen.

Die E-Mails für diese Postfächer werden ab sofort an den Zielsever der sekundären Umgebung geleitet. Falls dieser Zielsever von der primären Umgebung abweicht, schlägt das E-Mail-Routing möglicherweise fehl.

Bei der Migration zu 365 Total Protection werden die Postfächer und Domains im Control Panel mit Microsoft 365 synchronisiert. Neue Postfächer werden zum Control Panel hinzugefügt und bestehende Postfächer werden gemäß den Einstellungen in Microsoft 365 aktualisiert.

Abbildung 23: Bestätigen



7.

**Wichtig:**

Kunden können nicht gleichzeitig 365 Total Protection und LDAP-Verbindungen im Control Panel verwenden. Falls der Kunde aktive LDAP-Verbindungen oder LDAP-Postfächer hat (siehe [LDAP-Verbindung](#)), werden die LDAP-Verbindungen deaktiviert und alle LDAP-Postfächer in normale Postfächer umgewandelt. Benutzer und Gruppen werden nicht mehr mit dem Verzeichnisdienst über LDAP synchronisiert. Die Einstellungen des Kunden im Tab **LDAP-Verbindung** des Moduls **Service Dashboard** werden im Hintergrund gespeichert, aber nicht angezeigt, solange der Kunde 365 Total Protection verwendet.

Falls der Kunde das Upgrade auf 365 Total Protection abbricht oder 365 Total Protection kündigt und seine LDAP-Verbindungen wieder verwenden möchte, können Administratoren auf Kundenebene die LDAP-Verbindungen wieder aktivieren (siehe [LDAP-Verbindung aktivieren](#)). Postfächer, die mit dem Verzeichnisdienst synchronisiert werden, werden dann innerhalb von 24 Stunden wieder zu LDAP-Postfächern.

Um Ihre aktiven LDAP-Verbindungen zu deaktivieren und Ihre LDAP-Postfächer in normale Postfächer umzuwandeln, klicken Sie auf **Bestätigen**.

LDAP-VERBINDUNG DEAKTIVIEREN

Ihre Domain hat eine aktive LDAP-Verbindung oder LDAP-Postfächer. 365 Total Protection kann nur ohne aktive LDAP-Verbindung und ohne LDAP-Postfächer verwendet werden. Falls Sie fortfahren, wird die LDAP-Verbindung deaktiviert und alle LDAP-Postfächer werden im Control Panel zu normalen Postfächern. Falls Sie die LDAP-Verbindung später erneut aktivieren, werden diese Postfächer innerhalb von 24 Stunden wieder zu LDAP-Postfächern. Möchten Sie fortfahren?

✘ Abbrechen**✔ Bestätigen****Abbildung 24: LDAP-Verbindung deaktivieren**

Der erste Schritt für die Einrichtung von 365 Total Protection wird angezeigt.



- Wählen Sie aus, ob bestehende Postfächer aus der primären Umgebung, die nicht im Microsoft-365-Tenant des Kunden verwaltet werden, nach dem Upgrade einer bestehenden oder einer neuen sekundären Umgebung zugewiesen werden sollen.

**Hinweis:**

Nach dem Upgrade auf 365 Total Protection dürfen der primären Umgebung nur noch Microsoft-365-Postfächer aus dem Tenant des Kunden zugewiesen sein. Daher müssen andere Postfächer, die bereits im Control Panel vorhanden sind und derzeit der primären Umgebung zugewiesen sind, stattdessen einer sekundären Umgebung zugewiesen werden. Diese Postfächer können entweder einer bestehenden sekundären Umgebung oder einer neuen sekundären Umgebung zugewiesen werden.

Falls für den Kunden noch keine sekundäre Umgebung vorhanden ist, wird die Option **Bestehende Umgebung** ausgeblendet.

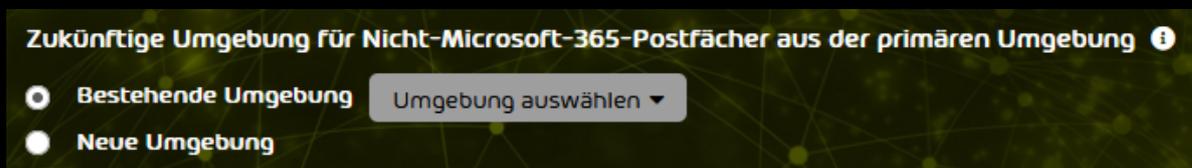


Abbildung 25: Umgebung für Nicht-Microsoft-365-Postfächer aus der primären Umgebung auswählen



Falls die Option ausgewählt worden ist, wird ein Formular zur Erstellung einer sekundären Umgebung angezeigt.

- Falls Sie die Option **Bestehende Umgebung** ausgewählt haben, wählen Sie aus dem Drop-down-Menü **Umgebung auswählen** eine sekundäre Umgebung aus.

**Hinweis:**

Falls für den Kunden nur eine sekundäre Umgebung vorhanden ist, ist diese bereits ausgewählt.



10. Falls Sie die Option **Neue Umgebung** ausgewählt haben, erstellen Sie eine sekundäre Umgebung in dem Formular.

Neue Umgebung

Individuell POP3/IMAP Hornet.email

Name der Umgebung im Control Panel

Adresse des Zielservers ⓘ

✕ Abbrechen ✓ Hinzufügen

Abbildung 26: Umgebung erstellen

i Hinweis:

Für weitere Informationen zur Erstellung von sekundären Umgebungen siehe [Sekundäre Umgebung erstellen](#).

11. Klicken Sie auf **Weiter**.



Der nächste Schritt für die Einrichtung von 365 Total Protection wird angezeigt.



12. Optional: Falls Sie die Postfachmigration freischalten möchten, setzen Sie ein Häkchen in der Checkbox **Postfachmigration freischalten**.

**Hinweis:**

Die Postfachmigration erleichtert Kunden den Umstieg von einem lokalen Exchange-Server auf Microsoft 365. Mit diesem Feature kann der Kunde Postfachdaten von seinem lokalen Exchange-Server in seinen Microsoft-365-Tenant übertragen. Für weitere Informationen siehe [Über die Postfachmigration](#) auf Seite 43.

**Hinweis:**

Die Postfachmigration ist nur in den Versionen Enterprise und Enterprise Backup von 365 Total Protection verfügbar. In der Version Business ist die Checkbox ausgegraut.

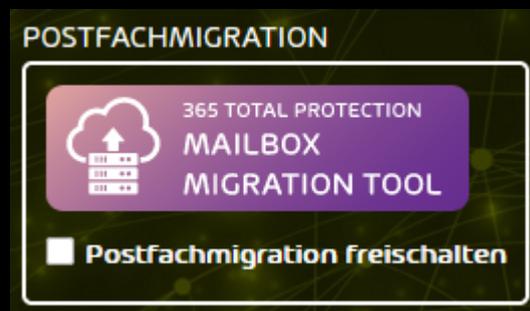


Abbildung 27: Postfachmigration freischalten

13. Klicken Sie auf **Weiter**.



Falls ein Häkchen in der Checkbox **Postfachmigration freischalten** gesetzt worden ist, wird ein Bestätigungsfenster angezeigt. Andernfalls wird der nächste Schritt für die Einrichtung von 365 Total Protection angezeigt.



14. Falls ein Bestätigungsfenster angezeigt wird, klicken Sie auf **Bestätigen**.

The screenshot shows a confirmation dialog with a blue header bar containing the text "POSTFACHMIGRATION FREISCHALTEN". Below the header, the main text reads: "Sie sind im Begriff, die Postfachmigration freizuschalten. Dieser Service ist kostenpflichtig. Für weitere Informationen kontaktieren Sie bitte Ihren Ansprechpartner. Möchten Sie fortfahren?". At the bottom of the dialog, there are two buttons: "X Abbrechen" (Cancel) and "✓ Bestätigen" (Confirm).

Abbildung 28: Freischaltung der Postfachmigration bestätigen



Die Postfachmigration wird freigeschaltet. Sobald der Kunde das Upgrade auf 365 Total Protection angestoßen hat, kann der Kunde Postfachdaten von seinem lokalen Exchange-Server in seinen Microsoft-365-Tenant übertragen.

Der nächste Schritt für die Einrichtung von 365 Total Protection wird angezeigt.



15. Wählen Sie aus, welcher Umgebung Microsoft-365-Postfächer zugewiesen werden sollen, die bereits im Control Panel vorhanden sind und aktuell einer sekundären Umgebung zugewiesen sind. Betätigen Sie den Schalter der gewünschten Option.

**Hinweis:**

Nach dem Upgrade auf 365 Total Protection wird der Microsoft-365-Tenant des Kunden im Control Panel als primäre Umgebung eingestellt (siehe **Primäre Umgebungseinstellungen**). Microsoft-365-Postfächer, die erst nach dem Upgrade auf 365 Total Protection im Zuge der Synchronisation mit Microsoft 365 zum Control Panel hinzugefügt werden, werden automatisch der primären Umgebung zugewiesen.

Die Auswahlmöglichkeiten beziehen sich auf Microsoft-365-Postfächer, die bereits vor dem Upgrade im Control Panel vorhanden sind und einer sekundären Umgebung zugewiesen sind. Diese Microsoft-365-Postfächer können nach dem Upgrade entweder der primären Umgebung zugewiesen werden oder in ihrer bisherigen Umgebung verbleiben. Unabhängig davon, ob solche Postfächer im Control Panel tatsächlich existieren, muss für den Kunden eine Option ausgewählt werden.

**Hinweis:**

Falls die Postfachmigration freigeschaltet worden ist, kann diese Einstellung nicht bearbeitet werden. Falls im Control Panel Postfächer aus dem Microsoft-365-Tenant des Kunden vorhanden sind, die aktuell einer sekundären Umgebung zugewiesen sind, werden diese Postfächer nach dem Upgrade auf 365 Total Protection der neuen primären Umgebung zugewiesen.

Zukünftige Umgebung für Microsoft-365-Postfächer aus sekundären Umgebungen ⓘ

- Microsoft-365-Postfächer aus sekundären Umgebungen in die neue primäre Umgebung verschieben
- Microsoft-365-Postfächer in ihrer aktuellen sekundären Umgebung belassen

Abbildung 29: Umgebung für Microsoft-365-Postfächer aus sekundären Umgebungen auswählen

16. Klicken Sie auf **Weiter**.



Ein Formular wird angezeigt.



17. Geben Sie Ihre Kontaktdaten in das Formular ein.

Hinweis:

Anhand der Kontaktdaten können wir Sie bei Problemen oder Rückfragen kontaktieren.

ONBOARDING

 **Firma**

Anrede **Vorname** **Nachname**

E-Mail **Telefon**

IT Security News
 Ich möchte regelmäßig die IT Security News erhalten.

 **Jetzt migrieren**

Abbildung 30: Kontaktdaten eingeben

18. Falls Sie unsere IT Security News erhalten möchten, setzen Sie ein Häkchen in der Checkbox **Ich möchte regelmäßig die IT Security News erhalten.**

19. **Achtung:**

Sobald 365 Total Protection aktiviert wird, startet eine 14-tägige kostenfreie Testphase. Damit ein Kunde den Service nach Ende der Testphase weiterhin verwenden kann, muss der Kunde den Service erwerben (siehe [365 Total Protection bestellen](#) auf Seite 111).

Um das Upgrade anzustoßen, klicken Sie auf **Jetzt migrieren**.



Die Anmeldeseite von Microsoft 365 wird angezeigt.



20. Melden Sie sich mit administrativen Zugangsdaten des Microsoft-365-Tenants des Kunden an.

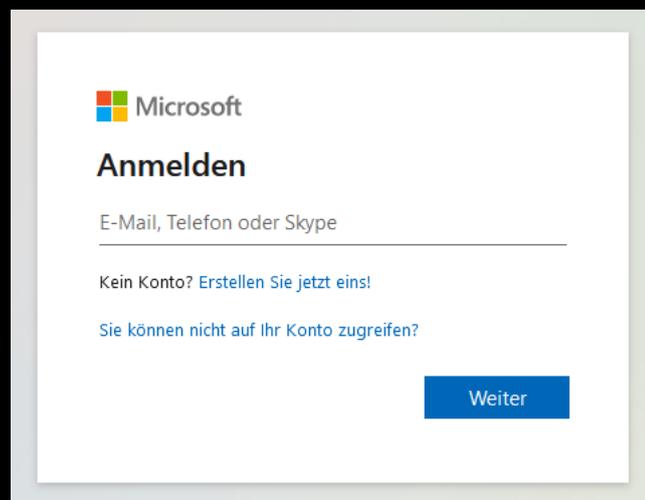


Abbildung 31: Anmelden



21. Um unsere Services mit Microsoft 365 zu synchronisieren, akzeptieren Sie die angeforderten Berechtigungen.



Hinweis:

Bei der Synchronisation werden Domains und Postfächer aus Microsoft 365 in das Control Panel übertragen. Die Konfigurationseinstellungen von Microsoft werden nicht geändert.

Falls im Control Panel Gruppen vorhanden sind, die den gleichen Namen wie Gruppen in Microsoft 365 haben, wird die Zugehörigkeit von Microsoft-365-Postfächern zu diesen Gruppen ebenfalls im Control Panel synchronisiert (siehe [Gruppenverwaltung im Control Panel](#) auf Seite 114 und [Gruppen aus Microsoft 365 im Control Panel synchronisieren](#) auf Seite 114).

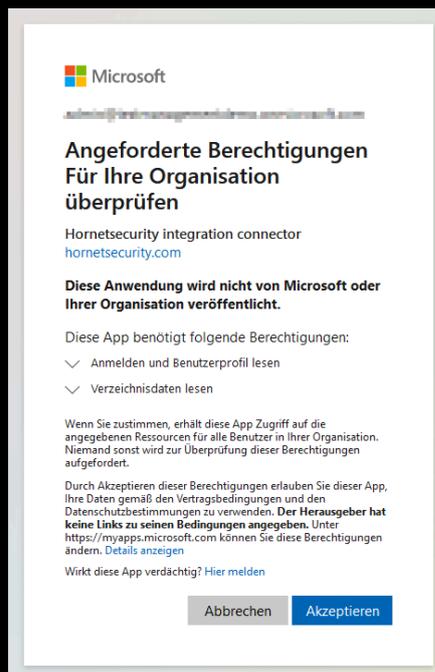


Abbildung 32: Berechtigungen akzeptieren



22. Falls Sie die Postfachmigration freigeschaltet haben (siehe Schritt 12 auf Seite 32), akzeptieren Sie die angeforderten Berechtigungen.

**Hinweis:**

Diese Berechtigungen gewähren uns Zugriff auf die Postfächer im Microsoft-365-Tenant und sind nur für die Durchführung der Postfachmigration erforderlich. Wir empfehlen, die Berechtigungen der App Hornetsecurity Mailbox Migration nach dem Abschluss des Upgrades auf 365 Total Protection wieder aus dem Microsoft-365-Tenant des Kunden zu entfernen.

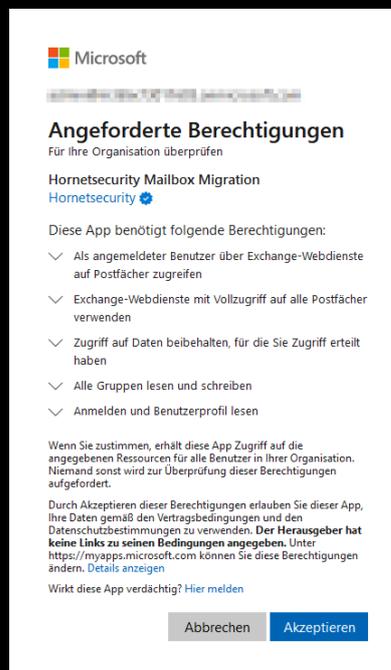


Abbildung 33: Berechtigungen für die Postfachmigration akzeptieren



Falls die Postfachmigration freigeschaltet worden ist (siehe Schritt 12 auf Seite 32), wird das Upgrade auf 365 Total Protection unterbrochen, damit der Kunde Postfachdaten von seinem lokalen Exchange-Server in seinen Microsoft-365-Tenant übertragen kann (siehe **Über die Postfachmigration** auf Seite 43). Erst nachdem der Kunde die Postfachmigration abgeschlossen hat, wird das Upgrade auf 365 Total Protection durchgeführt.

Falls die Postfachmigration nicht freigeschaltet worden ist, wird das Upgrade auf 365 Total Protection direkt durchgeführt. Sobald das Upgrade erfolgreich abgeschlossen



worben ist, wird die Anzahl der synchronisierten Domains und Postfächer angezeigt. Die Domains und Postfächer aus Microsoft 365 sind im Control Panel unter dem Kunden erstellt worden. Die Domains werden zum Modul **Kundeneinstellungen > Domains** (siehe **Domains**) hinzugefügt. Die Domains erhalten in der Spalte **Verifiziert** zunächst den Status



Nicht verifiziert. Nach wenigen Minuten wird geprüft, ob die Domains verifiziert werden können (siehe [Verifizierung von Domains](#)).



Hinweis:

Im Rahmen des Upgrades werden verschiedene Aktionen durchgeführt, wie zum Beispiel die Erstellung oder Änderung von Umgebungen, E-Mail-Adressen, Domains und Postfächern. Diese Aktionen werden im Modul **Auditing 2.0** dokumentiert (siehe [Auditing 2.0](#)).

Einrichtungsstatus 365 Total Protection Enterprise

MICROSOFT 365 WURDE VERBUNDEN.
3 Postfächer | 2 Lizenzen | 2 Domains

Konfigurieren Sie die DNS-Einstellungen Ihrer Domains
Die DNS-Einstellungen von mindestens einer synchronisierten Domain wurden noch nicht gesetzt oder sind falsch konfiguriert. Folgen Sie der Anleitung im Handbuch, um die DNS-Einstellungen richtig zu konfigurieren.
[Jetzt konfigurieren](#)

Ausgehenden E-Mail-Verkehr konfigurieren
Sie müssen Ihren ausgehenden E-Mail-Verkehr konfigurieren. Eine Anleitung dazu finden Sie in unserem [Handbuch](#).
[Automatisch konfigurieren](#)

Installation des Hornetsecurity Outlook Add-ins
Sie können das Hornetsecurity Outlook Add-in automatisch in den Outlook-Anwendungen Ihrer Benutzer installieren. Nach der Installation können Ihre Benutzer verschiedene Funktionen des Control Panels direkt in Ihren Outlook-Anwendungen ausführen.
[Installieren](#)

Vertragsstatus: Testvorbereitung

Abbildung 34: Erfolgreiches Upgrade



Wichtig:

Falls das Upgrade fehlschlägt, wird der Grund dafür angezeigt. Sobald der Fehler behoben worden ist, kann das Upgrade erneut angestoßen werden.



Einrichtungsstatus 365 Total Protection Enterprise DIE SYNCHRONISATION IST FEHLGESCHLAGEN.

Status der Synchronisation:	
Auf Microsoft-Berechtigungen warten	✓
Vorprüfungen	✗
Migration	⊙
Domains ermitteln	⊙
Delta ermitteln	⊙
Administratoren ermitteln	⊙
Benutzer ermitteln	⊙
Domains schreiben	⊙
Benutzer schreiben	⊙
Einstellungen schreiben	⊙

✗ Die Ziel-IP und der Ziel-Hostname müssen unter Spam and Malware Protection definiert werden.

Abbildung 35: Fehlgelagertes Upgrade



Die Domains und Postfächer aus Microsoft 365 sind zu 365 Total Protection übertragen worden. Die Domains und Postfächer sind im Control Panel erstellt worden. Von jetzt an können Sie sich mit Ihren Microsoft-365-Zugangsdaten im Control Panel anmelden und die Services einstellen.

Um unsere Services in vollem Umfang nutzen zu können, passen Sie die Einstellungen der synchronisierten Domains an (siehe [Konfiguration der Services von Microsoft](#) auf Seite 95) und konfigurieren Sie den ausgehenden E-Mail-Verkehr.

Falls Sie 365 Total Protection Enterprise Backup ausgewählt haben, müssen Sie zusätzlich 365 Total Backup konfigurieren (siehe [365 Total Backup konfigurieren](#) auf Seite 84), damit die Daten aus Ihrem Microsoft-365-Tenant gesichert werden.

Sprache und Symbole in der Dokumentation

Gender-Erklärung

Aus Gründen der besseren Lesbarkeit wird in dieser Dokumentation die Sprachform des generischen Maskulinums verwendet. Es wird an dieser Stelle darauf hingewiesen, dass die ausschließliche Verwendung der männlichen Form genderunabhängig verstanden werden soll.



Verwendete Symbole

Zur besseren Kenntlichkeit relevanter Schritte innerhalb handlungsanleitender Kapitel werden folgende Symbole verwendet:

Symbol	Bedeutung	Erklärung
	Voraussetzung	Bedingung, die vor dem nächsten Schritt erfüllt sein muss
	Zwischenresultat	Resultat, welches nach einem Schritt zwischenzeitlich erzielt wird
	Endresultat	Resultat, welches nach der Schrittreihenfolge eines handlungsanleitenden Kapitels erzielt wird

Warn- und Sicherheitshinweise

Die Warn- und Sicherheitshinweise werden eingesetzt, um Benutzer über Restrisiken und Gefahren zu informieren und diese mit einer empfohlenen Vorgehensweise zu vermeiden. Folgende Warn- und Sicherheitshinweise werden in dieser Dokumentation verwendet:

Symbol	Bedeutung	Erklärung
	HINWEIS	Weiterführende Informationen innerhalb eines bestimmten Absatzes, die für die Ausführung weiterer Schritte relevant sind.
	TIPP	Hinweis zu Konfigurationsmöglichkeiten.
	WICHTIG	Warnhinweis mit Informationen über Einschränkungen oder wichtige Konfigurationsmöglichkeiten des Services.
	ACHTUNG	Warnhinweis über zusätzliche Kosten, die, abhängig von gebuchten Serviceleistungen, möglicherweise entstehen können.
	WARNUNG	Warnhinweis zum möglichen Verlust von Daten.



Symbol	Bedeutung	Erklärung
	GEFAHR	Sicherheitshinweis zur möglichen System-Infizierung mit einer Malware.

Über die Postfachmigration

Wir möchten bestehenden Kunden, die bisher einen lokalen Exchange-Server verwendet haben, den Umstieg auf Microsoft 365 erleichtern. Daher bieten wir Kunden, die auf 365 Total Protection Enterprise oder Enterprise Backup upgraden (siehe [Upgrade auf 365 Total Protection als Kunde](#)), die Möglichkeit, die Daten der Postfächer aus ihrem lokalen Exchange-Server in ihren Microsoft-365-Tenant zu übertragen.



Hinweis:

Die Postfachmigration wird für Exchange Server ab der Version 2007 unterstützt.

Bei der Postfachmigration werden die folgenden Daten übertragen:

- E-Mails einschließlich Anhängen
- Kontakte
- Kalender
- Aufgaben
- Notizen



Hinweis:

Falls möglich, werden die Kennzeichnungen von E-Mails (z. B. gelesen, ungelesen, wichtig) im Microsoft-365-Tenant beibehalten.



Hinweis:

Die folgenden Daten von Postfächern können nicht migriert werden:

- Öffentliche Ordner
- Archive
- Journals
- Benutzerspezifische Einstellungen
- Verteilerlisten
- Postfachberechtigungen



Hinweis:

Für Informationen zu weiteren Einschränkungen der Postfachmigration siehe [Einschränkungen der Postfachmigration](#) auf Seite 45.

Administratoren auf Partner- und Kundenebene können die Postfachmigration während des Upgrades des Kunden auf 365 Total Protection freischalten (siehe [Auf 365 Total Protection upgraden](#)). Falls die Postfachmigration freigeschaltet wird, wird das Upgrade pausiert, damit Administratoren die Daten aller gewünschten Postfächer von einem lokalen Exchange-Server in den Microsoft-365-Tenant des Kunden übertragen können.



Achtung:

Die Postfachmigration verursacht zusätzliche Kosten gemäß der Preisliste.

Vor der Postfachmigration müssen jedoch Voraussetzungen auf dem lokalen Exchange-Server, im Microsoft-365-Tenant und im Control Panel erfüllt sein (siehe [Voraussetzungen für die Postfachmigration](#) auf Seite 46). Sobald diese Vorbereitungen getroffen worden sind, können Administratoren im Control Panel die Migration von Postfachdaten durchführen (siehe [Migration von Postfachdaten](#) auf Seite 65).

**Hinweis:**

Eine Postfachmigration kann mehrere Tage dauern. Konkrete Zeitangaben sind nicht möglich, da die Dauer von den folgenden Faktoren abhängt:

- Anzahl und Größe der zu migrierenden Postfächer
- Gesamtlast durch andere Postfachmigrationen in der Warteschlange

Administratoren werden über Zustandsänderungen per E-Mail informiert. Außerdem können Administratoren den aktuellen Zustand jederzeit im Modul **365 Total Protection > 365 Total Protection** einsehen. Während der Postfachmigration kann das Control Panel wie gewohnt verwendet werden.

Sobald Administratoren die Postfachmigration abgeschlossen haben, wird das Upgrade auf 365 Total Protection fortgesetzt.

Einschränkungen der Postfachmigration

Die Postfachmigration (siehe [Über die Postfachmigration](#) auf Seite 43) unterliegt Einschränkungen. Die Einschränkungen wirken sich auf die Daten aus, die migriert werden können. Nachfolgend werden die Einschränkungen aufgeführt.

Einschränkungen durch Exchange-Webdienste (EWS)

Durch EWS-Einschränkungen werden bei Microsoft die Serverressourcen begrenzt, die ein Benutzer oder eine Anwendung verbrauchen kann. Dadurch werden die Zuverlässigkeit und die Betriebszeit von Servern sichergestellt. Für die Postfachmigration ergeben sich daraus die folgenden Einschränkungen:

- Der Besitzer eines Postfachs wird im Microsoft-365-Tenant zum Organisator aller seiner Termine.
- Der Teilnehmerstatus in Terminen (akzeptiert oder abgelehnt) kann nicht migriert werden.
- Bei der Postfachmigration wird versucht, systeminterne Adressen (z. B. X500-Adressen) aufzulösen und durch eine gültige E-Mail-Adresse zu ersetzen. Falls dieser Vorgang fehlschlägt, wird die Adresse nicht in den Microsoft-365-Tenant übertragen.
- Bei der Postfachmigration werden ungültige Einträge (z. B. ungültige URLs in Website-Feldern) herausgefiltert, da diese von dem Microsoft-365-Tenant abgelehnt werden würden.



Einschränkungen durch den lokalen Exchange-Server

Abhängig von der Version des lokalen Exchange-Servers kann es zusätzlich zu den folgenden Einschränkungen kommen:

- Falls eine E-Mail die Datenmengenbegrenzung des Microsoft-365-Tenants überschreitet, wird die E-Mail nicht migriert. Der Benutzer wird in diesem Fall benachrichtigt.
- E-Mails mit einer Datenmenge von über 64 MB werden nicht migriert.
- Das maximale Datenvolumen pro Postfach darf 50 GB nicht überschreiten.
- Die Darstellung bestimmter E-Mail-Nachrichten (z. B. spezielle MIME-Formate) im Microsoft-365-Tenant weicht von der Darstellung auf dem lokalen Exchange-Server ab.
- Die Zuordnung von Elementeigenschaften ist eingeschränkt (z. B. bei fehlender Unterstützung durch den Microsoft-365-Tenant).
- Die Zuordnung von Ordnerfreigaben ist eingeschränkt.

Voraussetzungen für die Postfachmigration

Vor der Postfachmigration (siehe [Über die Postfachmigration](#) auf Seite 43) müssen Voraussetzungen auf dem lokalen Exchange-Server, im Microsoft-365-Tenant und im Control Panel erfüllt sein. Erst danach können Administratoren auf Kundenebene die Postfachmigration im Control Panel durchführen (siehe [Migration von Postfachdaten](#) auf Seite 65).

Da bei der Postfachmigration nur Daten zwischen bestehenden Postfächern migriert werden können, müssen die Postfächer bereits auf dem lokalen Exchange-Server, im Microsoft-365-Tenant und im Control Panel vorhanden sein (siehe [Voraussetzungen für Postfächer](#) auf Seite 47).

Auf dem lokalen Exchange-Server muss eine weitere Voraussetzung erfüllt sein. Da wir während der Postfachmigration über die Zugangsdaten eines Administrators auf die zu migrierenden Postfächer auf dem lokalen Exchange-Server zugreifen, muss der Administrator des lokalen Exchange-Servers dazu berechtigt sein, sich bei den Postfächern der Benutzer anzumelden. Deshalb muss dem Administrator die Rolle **ApplicationImpersonation** zugewiesen werden (siehe [Rollengruppe auf dem Exchange-Server erstellen](#) auf Seite 48).

Auch im Microsoft-365-Tenant müssen weitere Voraussetzungen erfüllt sein. Ebenso wie dem Administrator des lokalen Exchange-Servers muss dem Administrator des Microsoft-365-Tenants die Rolle **ApplicationImpersonation** zugewiesen werden (siehe [Rollengruppe in Microsoft 365 erstellen](#) auf Seite 53). Um die Validierung von Umgebungen (siehe [Umgebung validieren](#) auf Seite 66) während der Postfachmigration zu beschleunigen, können Sie dem Administrator des Microsoft-365-Tenants Berechtigungen zum Lesen und Verwalten der Postfächer erteilen, zu



denen Daten migriert werden sollen. Sie können dem Administrator entweder über das Exchange Admin Center Zugriff auf einzelne Postfächer erteilen (siehe [Berechtigungen zum Lesen und Verwalten von Postfächern in Microsoft 365 erteilen](#) auf Seite 57) oder den Zugriff auf alle Postfächer des Microsoft-365-Tenants über die PowerShell erteilen (siehe [Berechtigungen zum Lesen und Verwalten von Postfächern in Microsoft 365 über PowerShell erteilen](#) auf Seite 60). Da für den Zugriff auf die Postfächer im Microsoft-365-Tenant die Exchange-Webdienste verwendet werden, müssen auch Vorbereitungen bei den Exchange-Webdiensten getroffen werden. Damit der Zugriff auf die Postfächer über die Exchange-Webdienste möglich ist, muss der Zugriff auf die Exchange-Webdienste erlaubt werden (siehe [Zugriff auf Exchange-Webdienste erlauben](#) auf Seite 61). Zudem muss die Einschränkung der Exchange-Webdienste vorübergehend deaktiviert werden (siehe [Einschränkung der Exchange-Webdienste deaktivieren](#) auf Seite 63), damit Daten mit einer höheren Bandbreite migriert werden können.

Voraussetzungen für Postfächer

Bei der Postfachmigration (siehe [Über die Postfachmigration](#) auf Seite 43) werden über das Control Panel Daten von Postfächern von dem lokalen Exchange-Server eines Kunden in dessen Microsoft-365-Tenant übertragen. Dabei werden jedoch keine neuen Postfächer erstellt. Daher muss der Kunde vor der Postfachmigration sicherstellen, dass die zu migrierenden Postfächer in den folgenden Systemen vorhanden sind:

- Lokaler Exchange-Server
- Microsoft-365-Tenant
- Control Panel



Wichtig:

Damit wir die Postfächer in den verschiedenen Systemen einander zuordnen können, müssen die E-Mail-Adressen eines Postfachs bis zum @-Zeichen genau miteinander übereinstimmen. Die Domains auf dem lokalen Exchange-Server und im Microsoft-365-Tenant müssen sich unterscheiden, da die Postfächer unterschiedlichen Servern zugeordnet sind.

Um mehrere Postfächer auf einmal zum Microsoft-365-Tenant hinzuzufügen, können Administratoren des Kunden zunächst die Postfächer von dem lokalen Exchange-Server exportieren und anschließend die Postfächer als CSV-Datei in den Microsoft-365-Tenant importieren.

Um die Postfächer zum Control Panel hinzuzufügen, können Administratoren auf Kundenebene die Postfächer im Control Panel über eine LDAP-Verbindung mit dem Verzeichnisdienst des lokalen Exchange-Servers synchronisieren (siehe [LDAP-Verbindung](#)), aus einer CSV-Datei



importieren (siehe [Postfächer aus einer CSV-Datei importieren](#)) oder manuell zum Control Panel hinzufügen (siehe [Postfach hinzufügen](#)).

Rollengruppe auf dem Exchange-Server erstellen



Die Postfächer, deren Daten migriert werden sollen, sind auf dem lokalen Exchange-Server vorhanden (siehe [Voraussetzungen für Postfächer](#) auf Seite 47). Sie sind ein Administrator des lokalen Exchange-Servers des Kunden.

Für die Postfachmigration (siehe [Über die Postfachmigration](#) auf Seite 43) ist der Zugriff auf den lokalen Exchange-Server des Kunden erforderlich. Hierfür werden die Zugangsdaten eines Administrators des lokalen Exchange-Servers verwendet. Da bei der Postfachmigration die Daten aller zu migrierenden Postfächer ausgelesen werden müssen, muss der Administrator dazu berechtigt sein, sich bei den Postfächern anzumelden. Um dem Administrator diese Berechtigung zuzuweisen, müssen Sie auf dem lokalen Exchange-Server eine Rollengruppe erstellen. Über die Rollengruppe können Sie dem Administrator die Berechtigungen der Rolle **ApplicationImpersonation** erteilen.

1. Öffnen Sie das Exchange Admin Center des lokalen Exchange-Servers in Ihrem Browser.



Hinweis:

Standardmäßig ist das Exchange Admin Center über den Link <https://<Domain-Name>/ecp> erreichbar. Der Platzhalter **<Domain-Name>** steht für die absolute Adresse des lokalen Exchange-Servers im Domain Name System.

2. Melden Sie sich mit Ihren administrativen Zugangsdaten des lokalen Exchange-Servers im Exchange Admin Center an.
3. Navigieren Sie zu **Berechtigungen**.
4. Wählen Sie den Tab **Administratorrollen** aus.



5. Klicken Sie auf das Pluszeichen.

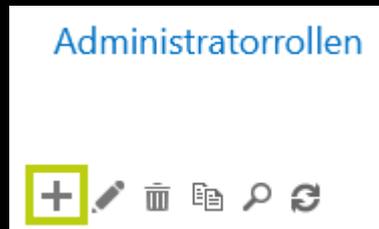


Abbildung 36: Administratorrolle hinzufügen



Das Fenster **Neue Rollengruppe** wird angezeigt.

Abbildung 37: Neue Rollengruppe

6. Geben Sie in das Feld **Name** einen Namen für die neue Rollengruppe ein. Sie können den Namen frei wählen.
7. Optional: Geben Sie in das Feld **Beschreibung** eine Beschreibung der Rollengruppe ein.



8. Klicken Sie unter **Rollen** auf das Pluszeichen.



Abbildung 38: Rolle hinzufügen



Das Fenster **Rolle auswählen** wird angezeigt.

9. Wählen Sie aus der Liste die Rolle **ApplicationImpersonation** aus.



Hinweis:

Die Rolle **ApplicationImpersonation** berechtigt den Administrator dazu, sich im Namen anderer Postfächer beim lokalen Exchange-Server anzumelden.

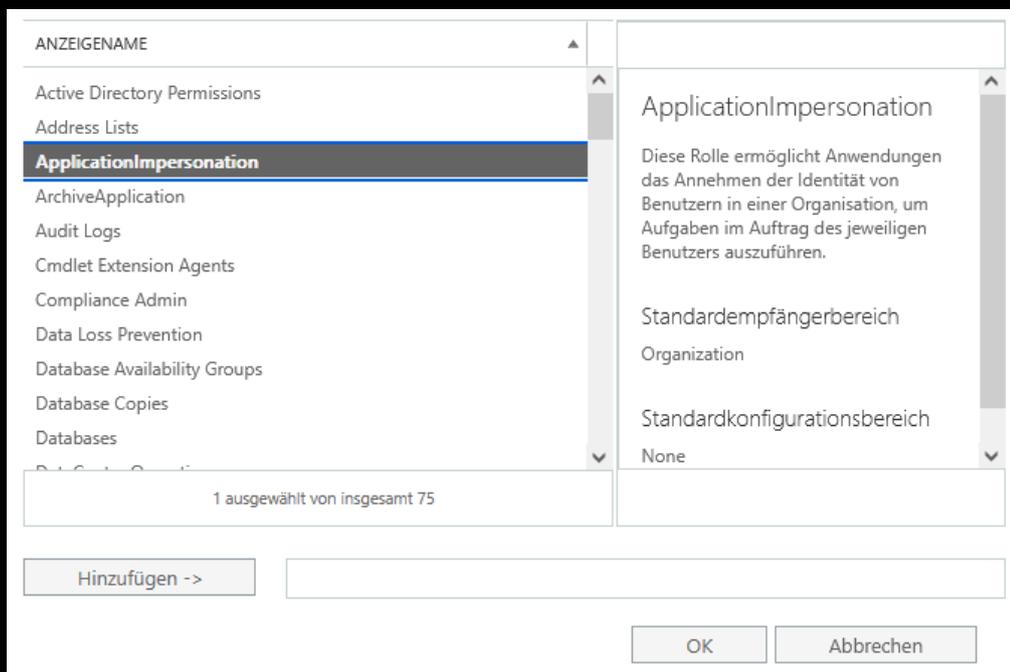


Abbildung 39: ApplicationImpersonation auswählen



10. Klicken Sie auf **Hinzufügen**.



Die Rolle wird ausgewählt.



Abbildung 40: Ausgewählte Rolle

11. Klicken Sie auf **OK**.



Das Fenster **Rolle auswählen** wird geschlossen. Die Rolle **ApplicationImpersonation** wird im Fenster **Neue Rollengruppe** unter **Rollen** angezeigt.

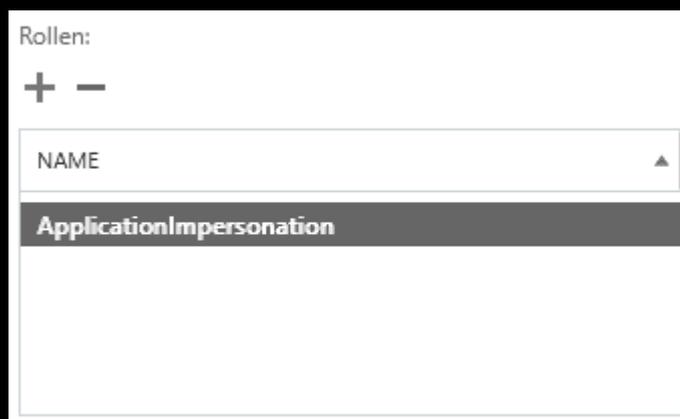


Abbildung 41: Hinzugefügte Rolle

12. Klicken Sie unter **Mitglieder** auf das Pluszeichen.



Abbildung 42: Mitglied hinzufügen



Das Fenster **Mitglieder auswählen** öffnet sich.



13. Wählen Sie aus der Liste im Fenster **Mitglieder auswählen** den Administrator aus, mit dessen Zugangsdaten für den lokalen Exchange-Server die Postfachmigration im Control Panel durchgeführt werden soll (siehe [Migration von Postfachdaten](#) auf Seite 65).

NAME	ANZEIGENAME
Adele Vance	Adele Vance
Administrator	Administrator
Alex Wilber	Alex Wilber
Allan Deyoung	Allan Deyoung
Christie Cline	Christie Cline

Abbildung 43: Administrator auswählen

14. Klicken Sie auf **Hinzufügen**.



Der Administrator wird ausgewählt.



Abbildung 44: Ausgewählter Administrator

15. Klicken Sie auf **OK**.



Das Fenster **Mitglieder auswählen** wird geschlossen. Der ausgewählte Administrator wird im Fenster **Neue Rollengruppe** unter **Mitglieder** angezeigt.

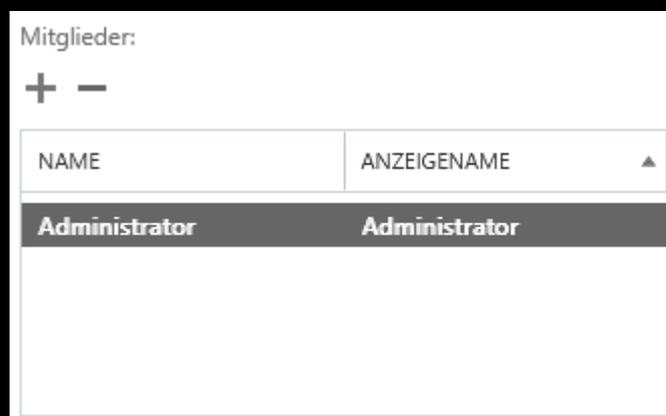


Abbildung 45: Hinzugefügter Administrator



16. Klicken Sie auf **Speichern**.



Das Fenster **Neue Rollengruppe** wird geschlossen. Die Rollengruppe wird zu der Liste im Tab **Administratorrollen** unter **Berechtigungen** im Exchange Admin Center hinzugefügt. Der Administrator ist ab sofort dazu berechtigt, sich bei allen Postfächern des lokalen Exchange-Servers anzumelden.



Einem Administrator sind die Berechtigungen der Rolle **ApplicationImpersonation** auf dem lokalen Exchange-Server des Kunden erteilt worden.

Rollengruppe in Microsoft 365 erstellen



Die Postfächer, zu denen Daten migriert werden sollen, sind bereits im Microsoft-365-Tenant des Kunden vorhanden (siehe **Voraussetzungen für Postfächer** auf Seite 47). Sie sind ein Administrator des Microsoft-365-Tenants.

Für die Postfachmigration (siehe **Über die Postfachmigration** auf Seite 43) ist der Zugriff auf den Microsoft-365-Tenant des Kunden erforderlich. Hierfür werden die Zugangsdaten eines Administrators des Microsoft-365-Tenants verwendet. Da bei der Postfachmigration auf alle Postfächer im Microsoft-365-Tenant zugegriffen werden muss, zu denen Daten migriert werden sollen, muss der Administrator dazu berechtigt sein, sich bei den Postfächern anzumelden. Um dem Administrator diese Berechtigung zuzuweisen, müssen Sie im Microsoft-365-Tenant eine Rollengruppe erstellen. Über die Rollengruppe können Sie dem Administrator die Berechtigungen der Rolle **ApplicationImpersonation** erteilen.

1. Öffnen Sie die Webseite **admin.exchange.microsoft.com**.
2. Melden Sie sich mit Ihren administrativen Zugangsdaten des Microsoft-365-Tenants an.
3. Navigieren Sie zu **Rollen > Administratorrollen**.



4. Klicken Sie auf **Gruppenrolle hinzufügen**.



Abbildung 46: Rollengruppe hinzufügen



Die Seite **Einrichten der Grundlagen** wird angezeigt.

Einrichten der Grundlagen

Um zu beginnen, geben Sie einige grundlegende Informationen über die Rollengruppe ein, die Sie erstellen.

Name *

Beschreibung

Geben Sie eine Beschreibung ein, damit andere Administratoren wissen, welchen Zweck diese Rollengruppe hat.

Schreibbereich ⓘ

Abbildung 47: Einrichten der Grundlagen

5. Geben Sie in das Feld **Name** einen Namen für die neue Rollengruppe ein. Sie können den Namen frei wählen.
6. Optional: Geben Sie in das Feld **Beschreibung** eine Beschreibung der Rollengruppe ein.
7. Klicken Sie auf **Weiter**.



Die Seite **Berechtigungen hinzufügen** wird angezeigt.



8. Wählen Sie aus der Liste der Rollen die Rolle **ApplicationImpersonation** aus.

<input type="checkbox"/>	ApplicationImpersonation	This role enables applications to impersonate users in an organization in order to perform tasks on behalf of the user.	Organization	None
--------------------------	---------------------------------	---	--------------	------

Abbildung 48: ApplicationImpersonation auswählen

9. Klicken Sie auf **Weiter**.



Die Seite **Administratoren zuordnen** wird angezeigt.

Administratoren zuordnen

Wählen Sie die Benutzer aus, die Sie dieser Rollengruppe zuweisen möchten. Sie haben dann die Berechtigung, die Rollen zu verwalten, die Sie im vorherigen Schritt zugewiesen haben.

Mitglieder

Abbildung 49: Weiter

10. Geben Sie in das Feld **Mitglieder** den Namen oder die E-Mail-Adresse des Administrators ein, dessen Zugangsdaten für die Postfachmigration verwendet werden sollen, und wählen Sie den Administrator aus.



11. Klicken Sie auf **Weiter**.



Die Seite **Rollengruppe überprüfen und beenden** wird angezeigt.

Rollengruppe überprüfen und beenden

Wir empfehlen, den Mitgliedern der Rollengruppe mitzuteilen, wie sich diese Änderungen auf sie auswirken werden.

Grundlagen
Name: ApplicationImpersonation
Beschreibung:
Schreibbereich: Default
[Grundlagen bearbeiten](#)

Berechtigungen
ApplicationImpersonation
[Berechtigungen bearbeiten](#)

Administratoren
admin
[Administratoren bearbeiten](#)

Abbildung 50: Seite Rollengruppe überprüfen und beenden



12. Klicken Sie auf **Rollengruppe hinzufügen**.



Die Rollengruppe wird erstellt. Die Erstellung kann bis zu 1 Minute dauern. Sobald die Rollengruppe erstellt worden ist, wird eine Erfolgsmeldung angezeigt.

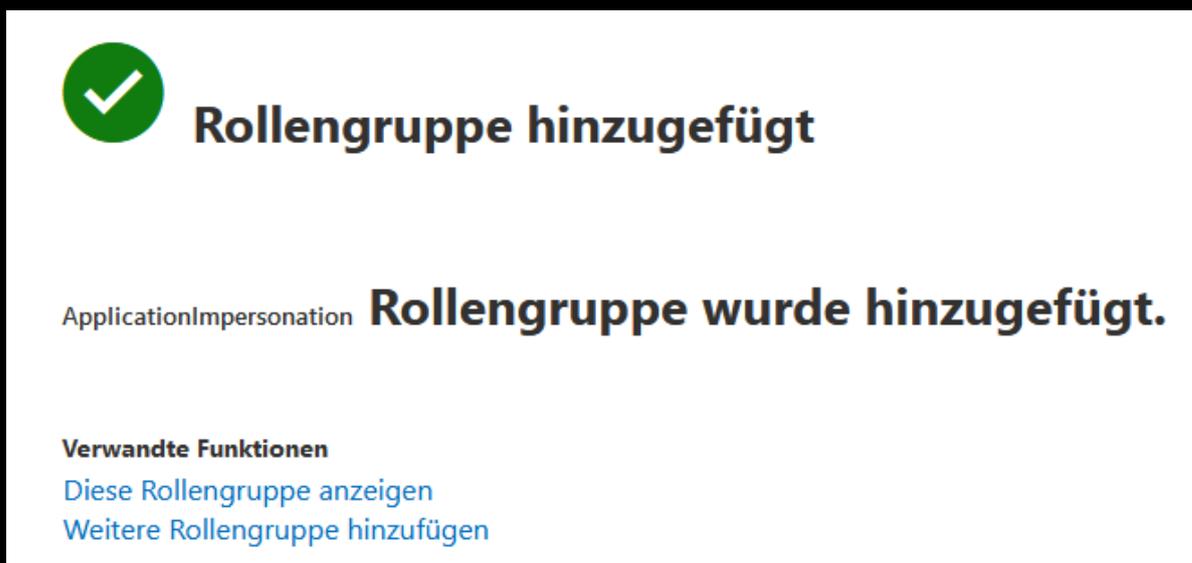


Abbildung 51: Erfolgsmeldung

13. Klicken Sie auf **Fertig**.



Die Erfolgsmeldung wird geschlossen. Das Modul **Rollen > Administratorrollen** wird wieder angezeigt. Die neue Rollengruppe wird in der Liste der Rollengruppen angezeigt.



Einem Administrator sind die Berechtigungen der Rolle **ApplicationImpersonation** im Microsoft-365-Tenant des Kunden erteilt worden.

Berechtigungen zum Lesen und Verwalten von Postfächern in Microsoft 365 erteilen



Die Postfächer, zu denen Daten migriert werden sollen, sind bereits im Microsoft-365-Tenant des Kunden vorhanden (siehe **Voraussetzungen für Postfächer** auf Seite 47). Sie sind ein Administrator des Microsoft-365-Tenants.

Um die Validierung von Umgebungen (siehe **Umgebung validieren** auf Seite 66) für die Postfachmigration (siehe **Über die Postfachmigration** auf Seite 43) zu beschleunigen, können



Sie dem Administrator, dessen Zugangsdaten für den Microsoft-365-Tenant des Kunden für die Postfachmigration verwendet werden sollen, Berechtigungen zum Lesen und Verwalten der zu migrierenden Postfächer erteilen. Dadurch erhält der Administrator direkten Zugriff auf die Postfächer.



Hinweis:

Bei der Validierung von Umgebungen (siehe [Umgebung validieren](#) auf Seite 66) für die Postfachmigration wird zunächst geprüft, ob mit den Zugangsdaten des Administrators direkt auf die zu migrierenden Postfächer zugegriffen werden kann. Falls der direkte Zugriff nicht möglich ist, wird stattdessen über die Rolle **ApplicationImpersonation** (siehe [Rollengruppe in Microsoft 365 erstellen](#) auf Seite 53) auf die Postfächer zugegriffen. Dadurch dauert die Validierung länger.

Wir empfehlen, für die Postfachmigration als erstes eine Umgebung mit wenigen Postfächern zu validieren und dem Administrator im Microsoft-365-Tenant direkten Zugriff auf diese Postfächer zu gewähren. Dadurch liegt das Ergebnis der Validierung schnell vor und der Administrator kann sich mit dem Vorgang vertraut machen.



Hinweis:

Im Microsoft Admin Center kann dem Administrator die Berechtigung für den direkten Zugriff nur für einzelne Postfächer erteilt werden. Nur über die PowerShell ist es möglich, dem Administrator direkten Zugriff auf alle Postfächer auf einmal zu gewähren (siehe [Berechtigungen zum Lesen und Verwalten von Postfächern in Microsoft 365 über PowerShell erteilen](#) auf Seite 60).

1. Öffnen Sie die Webseite **admin.microsoft.com**.
2. Melden Sie sich mit Ihren administrativen Zugangsdaten des Microsoft-365-Tenants an.
3. Navigieren Sie zu **Benutzer > Aktive Benutzer**.



Eine Liste mit allen aktiven Benutzern des Microsoft-365-Tenants wird angezeigt.

4. Klicken Sie in der Liste auf den Anzeigenamen eines Benutzers, in dessen Postfach später Daten aus dem lokalen Exchange-Server des Kunden migriert werden sollen.



Auf der rechten Seite des Fensters werden Informationen zum Benutzer angezeigt.



5. Wählen Sie den Tab **E-Mail** aus.

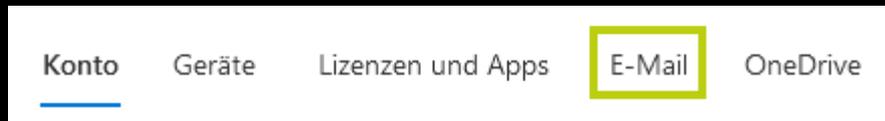


Abbildung 52: Tab E-Mail auswählen

6. Klicken Sie unter **Postfachberechtigungen** auf "**Lesen und Verwalten**"-Berechtigungen.

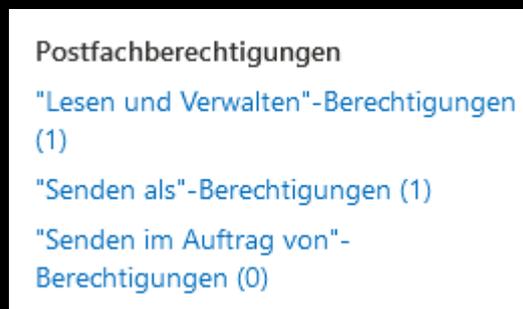


Abbildung 53: Berechtigungen auswählen



Die Seite "**Lesen und Verwalten**"-Berechtigungen wird angezeigt.

7. Klicken Sie auf **Berechtigungen hinzufügen**.

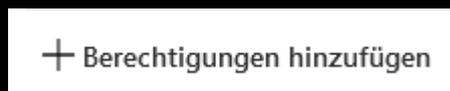


Abbildung 54: Berechtigungen hinzufügen



Die Seite **Fügen Sie Benutzerpostfachberechtigungen hinzu** wird angezeigt.



Abbildung 55: Seite Fügen Sie Benutzerpostfachberechtigungen hinzu

8. Suchen Sie nach dem Administrator, dessen Zugangsdaten für den Microsoft-365-Tenant später für die Postfachmigration verwendet werden sollen, und wählen Sie den Administrator aus.



9. Klicken Sie auf **Hinzufügen**.



Die Seite "**Lesen und Verwalten**"-Berechtigungen wird wieder angezeigt. Der Administrator wird in der Liste der Berechtigungen angezeigt. Dem Administrator werden Berechtigungen zum Lesen und Verwalten für das Postfach erteilt. Es kann bis zu 1 Stunde dauern, dass die Änderungen wirksam werden.

10. Klicken Sie oben rechts auf das Kreuzsymbol.



Die Seite wird geschlossen. Das Modul **Benutzer > Aktive Benutzer** wird wieder angezeigt.

11. Wiederholen Sie die Schritte **4** auf Seite 58 bis **10** auf Seite 60 für alle Postfächer, an die später Daten aus dem lokalen Exchange-Server des Kunden übertragen werden sollen.



Einem Administrator sind Berechtigungen zum Lesen und Verwalten von Postfächern im Microsoft-365-Tenant des Kunden erteilt worden.

Berechtigungen zum Lesen und Verwalten von Postfächern in Microsoft 365 über PowerShell erteilen



Die Postfächer, zu denen Daten migriert werden sollen, sind bereits im Microsoft-365-Tenant des Kunden vorhanden (siehe **Voraussetzungen für Postfächer** auf Seite 47). Sie sind ein Administrator des Microsoft-365-Tenants.

Um die Validierung von Umgebungen (siehe **Umgebung validieren** auf Seite 66) für die Postfachmigration (siehe **Über die Postfachmigration** auf Seite 43) zu beschleunigen, können Sie dem Administrator, dessen Zugangsdaten für den Microsoft-365-Tenant des Kunden für die Postfachmigration verwendet werden sollen, Berechtigungen zum Lesen und Verwalten der zu migrierenden Postfächer erteilen. Dadurch erhält der Administrator direkten Zugriff auf die Postfächer. Statt dem Administrator den Zugriff auf einzelne Postfächer zu erteilen (siehe **Berechtigungen zum Lesen und Verwalten von Postfächern in Microsoft 365 erteilen** auf Seite 57), können Sie dem Administrator über die PowerShell Zugriff auf alle Postfächer des Microsoft-365-Tenants auf einmal erteilen.

1. Öffnen Sie die PowerShell Ihres Microsoft-365-Tenants.



2. Führen Sie den folgenden Befehl aus und ersetzen Sie den Platzhalter **<E-Mail-Adresse des Administrators>** durch die E-Mail-Adresse des Administrators, der Berechtigungen zum Lesen und Verwalten aller Postfächer des Microsoft-365-Tenants erhalten soll:

```
get-mailbox | add-mailboxpermission -User <E-Mail-Adresse des Administrators> -  
AccessRights FullAccess
```



Der Administrator erhält Berechtigungen zum Lesen und Verwalten aller Postfächer des Microsoft-365-Tenants. In der PowerShell werden die Benutzer aufgelistet, auf die der Administrator nun vollen Zugriff hat.



Einem Administrator sind Berechtigungen zum Lesen und Verwalten aller Postfächer im Microsoft-365-Tenant des Kunden erteilt worden.

Zugriff auf Exchange-Webdienste erlauben



Sie sind ein Administrator des Microsoft-365-Tenants des Kunden.

Während der Postfachmigration (siehe **Über die Postfachmigration** auf Seite 43) müssen wir auf die Daten der Postfächer im Microsoft-365-Tenant des Kunden zugreifen. Für den Zugriff verwenden wir die Exchange-Webdienste. Daher müssen Sie den Zugriff auf die Exchange-Webdienste des Microsoft-365-Tenants erlauben.

1. Öffnen Sie die Webseite aad.portal.azure.com.
2. Melden Sie sich mit Ihren administrativen Zugangsdaten des Microsoft-365-Tenants an.



3. Navigieren Sie zu **Azure Active Directory Admin Center**.

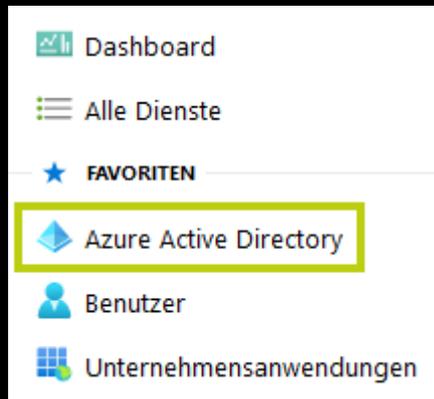


Abbildung 56: Azure Active Directory öffnen

4. Klicken Sie unter **Verwalten** auf **Eigenschaften**.

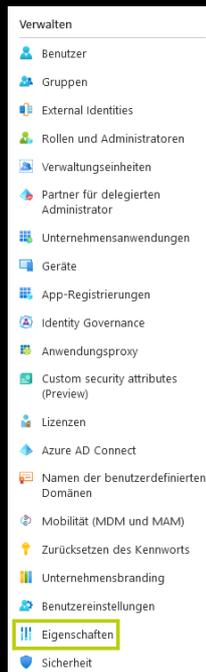


Abbildung 57: Einstellungen öffnen



5. Klicken Sie unten auf der Seite auf den Link **Sicherheitsstandards verwalten**.

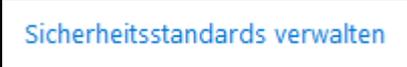


Abbildung 58: Sicherheitsstandards öffnen



Die Seite **Sicherheitsstandards aktivieren** wird angezeigt.



Abbildung 59: Sicherheitsstandards

6. Klicken Sie auf **Nein**.
7. Klicken Sie auf **Speichern**.



Die Änderungen werden gespeichert.



Der Zugriff auf die Exchange-Webdienste ist erlaubt worden.

Einschränkung der Exchange-Webdienste deaktivieren



Sie sind ein Administrator des Microsoft-365-Tenants des Kunden.

Um Daten bei der Postfachmigration (siehe **Über die Postfachmigration** auf Seite 43) mit einer höheren Bandbreite in den Microsoft-365-Tenant des Kunden migrieren zu können, müssen Sie die Einschränkung der Exchange-Webdienste vorübergehend deaktivieren.



1. Öffnen Sie die Webseite admin.microsoft.com.
2. Melden Sie sich mit Ihren administrativen Zugangsdaten des Microsoft-365-Tenants an.
3. Geben Sie in das Eingabefeld den folgenden Text ein: **EWS Throttling**.
4. Klicken Sie auf **Tests ausführen**.

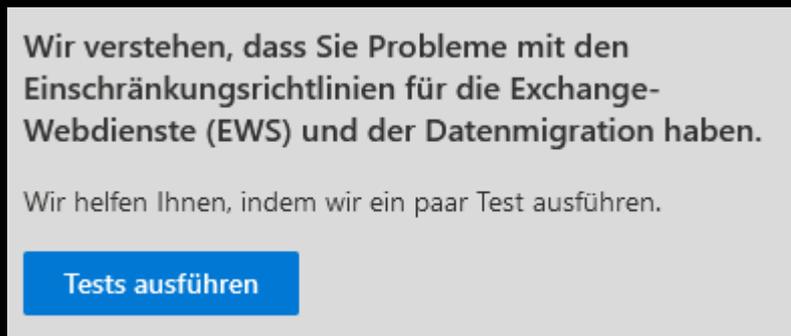


Abbildung 60: Tests durchführen



Die Tests werden durchgeführt. Falls die Exchange-Webdienste eingeschränkt sind, wird der folgende Text angezeigt.

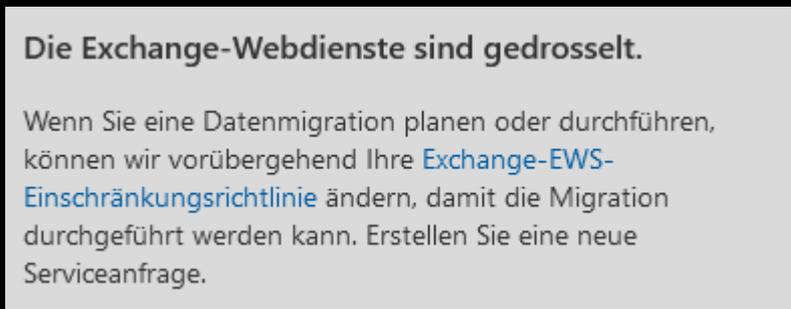


Abbildung 61: Einschränkung aktiv

5. Erstellen Sie eine Support-Anfrage bei Microsoft, um die Einschränkung der Exchange-Webdienste für 30 Tage aufzuheben.



Der Support von Microsoft deaktiviert die Einschränkung der Exchange-Webdienste vorübergehend.



Die Einschränkung der Exchange-Webdienste ist vorübergehend deaktiviert worden.



Migration von Postfachdaten

Administratoren auf Partner- und Kundenebene können während des Upgrades eines bestehenden Kunden auf 365 Total Protection Enterprise oder Enterprise Backup (siehe [Auf 365 Total Protection upgraden](#)) Postfachdaten von einem lokalen Exchange-Server in den Microsoft-365-Tenant des Kunden übertragen (siehe [Über die Postfachmigration](#) auf Seite 43).

! Wichtig:

Bevor Administratoren die Postfachmigration im Control Panel durchführen können, müssen die Voraussetzungen auf dem lokalen Exchange-Server, im Microsoft-365-Tenant und im Control Panel erfüllt sein (siehe [Voraussetzungen für die Postfachmigration](#) auf Seite 46).

i Hinweis:

Eine Postfachmigration kann mehrere Tage dauern. Konkrete Zeitangaben sind nicht möglich, da die Dauer von den folgenden Faktoren abhängt:

- Anzahl und Größe der zu migrierenden Postfächer
- Gesamtlast durch andere Postfachmigrationen in der Warteschlange

Administratoren werden über Zustandsänderungen per E-Mail informiert. Außerdem können Administratoren den aktuellen Zustand jederzeit im Modul **365 Total Protection** > **365 Total Protection** einsehen. Während der Postfachmigration kann das Control Panel wie gewohnt verwendet werden.

Um Postfachdaten zu migrieren, müssen Administratoren mehrere Schritte im Control Panel durchführen. Zunächst müssen Administratoren die Umgebung der Postfächer, deren Daten sie in den Microsoft-365-Tenant des Kunden übertragen möchten, validieren (siehe [Umgebung validieren](#) auf Seite 66). Mit der Validierung stellen wir sicher, dass der Zugriff auf den lokalen Exchange-Server und den Microsoft-365-Tenant möglich ist.

i Hinweis:

Administratoren können mehrere Umgebungen validieren. Auf diese Weise ist es möglich, Postfachdaten von verschiedenen Exchange-Servern in den Microsoft-365-Tenant des Kunden zu übertragen.



Sobald ein Administrator eine Umgebung validiert hat, kann der Administrator ein oder mehrere Postfächer aus der Umgebung auswählen und die Daten dieser Postfächer migrieren (siehe [Postfächer migrieren](#) auf Seite 73).

! Wichtig:

Administratoren können nur Postfächer aus Umgebungen migrieren, die sie selbst validiert haben.

Sobald die Daten aller gewünschten Postfächer in den Microsoft-365-Tenant des Kunden übertragen worden sind, können Administratoren die Postfachmigration abschließen (siehe [Postfachmigration abschließen](#) auf Seite 82). Danach wird das Upgrade auf 365 Total Protection automatisch fortgesetzt (siehe [Auf 365 Total Protection upgraden](#)).

! Wichtig:

Die Postfachmigration ist nur einmalig möglich. Nach dem Abschluss der Postfachmigration ist es nicht mehr möglich, weitere Postfachdaten zu migrieren.

Umgebung validieren



Sie haben das Upgrade auf 365 Protection Enterprise oder Enterprise Backup angestoßen und die Postfachmigration freigeschaltet (siehe [Auf 365 Total Protection upgraden](#)). Sie haben die Vorbereitungen für die Postfachmigration auf dem lokalen Exchange-Server, im Microsoft-365-Tenant und im Control Panel getroffen (siehe [Voraussetzungen für die Postfachmigration](#) auf Seite 46). Sie haben Postfächer zu der Umgebung hinzugefügt, die Sie validieren möchten (siehe [Sekundäre Umgebungen](#)).

Während des Upgrades eines bestehenden Kunden auf 365 Total Protection Enterprise oder Enterprise Backup (siehe [Auf 365 Total Protection upgraden](#)) können Sie Postfachdaten von einem lokalen Exchange-Server in den Microsoft-365-Tenant des Kunden übertragen (siehe [Über die Postfachmigration](#) auf Seite 43). Die Migration von Postfachdaten (siehe [Migration von Postfachdaten](#) auf Seite 65) ist nur mit Zugriff auf den lokalen Exchange-Server und den Microsoft-365-Tenant möglich. Bevor Sie Daten von Postfächern migrieren können (siehe [Postfächer migrieren](#) auf Seite 73), müssen Sie daher die Umgebung (siehe [Sekundäre Umgebungen](#)) validieren, der die Postfächer des lokalen Exchange-Servers im Control Panel zugewiesen sind. Dazu müssen Sie die Zugangsdaten des lokalen Exchange-Servers eingeben. Mit der Validierung stellen wir sicher, dass der Zugriff auf den lokalen Exchange-Server möglich ist.



Hinweis:

Administratoren können mehrere Umgebungen validieren. Auf diese Weise ist es möglich, Postfachdaten von verschiedenen Exchange-Servern in den Microsoft-365-Tenant des Kunden zu übertragen.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie in der Bereichsauswahl die Domain aus, für die Sie eine Umgebung validieren möchten.
3. Navigieren Sie zu **365 Total Protection > 365 Total Protection**.



In dem Modul wird die Seite **Postfachmigration** angezeigt.



4.

**ACHTUNG:**

Falls die eingegebenen Zugangsdaten des lokalen Exchange-Servers während der Postfachmigration ungültig werden, können keine weiteren Daten vom lokalen Exchange-Server in den Microsoft-365-Tenant übertragen werden. Dadurch können die Postfachdaten im Microsoft-365-Tenant unvollständig bleiben. Damit die Postfachdaten vollständig übertragen werden, ändern Sie die Zugangsdaten des lokalen Exchange-Servers nicht, bevor die Postfachmigration abgeschlossen ist (siehe [Postfachmigration abschließen](#) auf Seite 82).

Füllen Sie in der Spalte **Umgebungsvalidierung** das Formular **Lokaler Exchange-Server** aus.

LOKALER EXCHANGE-SERVER**Umgebung**

Primäre Umgebung ▾

IP-Adresse oder Hostname**E-Mail-Adresse des Administrators****Passwort des Administrators****Abbildung 62: Formular ausfüllen**

- Wählen Sie aus dem Drop-down-Menü **Umgebung** die Umgebung der Postfächer aus, deren Daten Sie migrieren möchten.
- Geben Sie in das Feld **IP-Adresse oder Hostname** die IP-Adresse oder den Hostname des lokalen Exchange-Servers ein, auf dem sich die Daten der Postfächer befinden.
- Geben Sie in das Feld **E-Mail-Adresse des Administrators** die E-Mail-Adresse eines Administrators des lokalen Exchange-Servers ein.
- Geben Sie in das Feld **Passwort des Administrators** das Passwort des Administrators des lokalen Exchange-Servers ein.



5. Klicken Sie auf **Umgebung validieren**.

✓ Umgebung validieren

Abbildung 63: Umgebung validieren



Die Umgebung wird zu der Liste in der Spalte **Validierte Umgebungen** hinzugefügt. Die Umgebung wird validiert. Sobald das Ergebnis der Validierung vorliegt, wird die Umgebung diesem Ergebnis innerhalb der Liste zugeordnet. Falls die Liste mindestens eine erfolgreich



validierte Umgebung enthält, wird der Button **Postfächer für die Migration auswählen** unterhalb der Liste freigeschaltet.



Hinweis:

Die Liste in der Spalte **Validierte Umgebungen** wird nicht automatisch aktualisiert. Administratoren können die Liste mit einem Klick auf den Button **Aktualisieren** neu laden.



Hinweis:

Während der Validierung prüfen wir, ob der Zugriff auf den lokalen Exchange-Server und den Microsoft-365-Tenant mit den eingegebenen Zugangsdaten möglich ist. Außerdem prüfen wir stichprobenartig, ob der Administrator auf dem lokalen Exchange-Server und im Microsoft-365-Tenant Zugriff auf die Postfächer hat, die der Umgebung im Control Panel zugewiesen sind.

VALIDIERTE UMGEBUNGEN: ⓘ

In Bearbeitung ⓘ

Exchange  Zurücksetzen

Abbildung 64: Validierung in Bearbeitung

VALIDIERTE UMGEBUNGEN: ⓘ

Fertig ⓘ

Exchange  Zurücksetzen

Abbildung 65: Erfolgreiche Validierung

VALIDIERTE UMGEBUNGEN: ⓘ

Fehlgeschlagen ⓘ

Exchange ⓘ  Zurücksetzen

Abbildung 66: Fehlgeschlagene Validierung

**Hinweis:**

Falls die Validierung fehlgeschlagen ist, werden bei einem Klick auf den Button mit den drei Punkten Informationen zum Grund angezeigt. Um die Validierung der Umgebung erneut zu versuchen, muss die Validierung zunächst zurückgesetzt werden (siehe [Validierung einer Umgebung zurücksetzen](#) auf Seite 71).



Die Umgebung ist validiert worden.

**Wichtig:**

Die Zugangsdaten des lokalen Exchange-Servers und des Microsoft-365-Tenants dürfen nicht geändert werden, solange die Migration der Postfachdaten dieser Umgebung nicht abgeschlossen ist.

Anschließend können Sie die Daten von Postfächern von dem lokalen Exchange-Server in den Microsoft-365-Tenant des Kunden übertragen (siehe [Postfächer migrieren](#) auf Seite 73).

Validierung einer Umgebung zurücksetzen



Sie haben eine Umgebung validiert (siehe [Umgebung validieren](#) auf Seite 66). Für die Umgebung wird derzeit keine Postfachmigration durchgeführt (siehe [Postfächer migrieren](#) auf Seite 73).

Sie können die Validierung einer Umgebung für die Postfachmigration (siehe [Über die Postfachmigration](#) auf Seite 43) zurücksetzen. Das Zurücksetzen der Validierung ist sinnvoll, falls sich die Zugangsdaten des lokalen Exchange-Servers oder des Microsoft-365-Tenants seit der Validierung geändert haben oder die Validierung fehlgeschlagen ist. Nachdem Sie auf dem lokalen Exchange-Server, im Microsoft-365-Tenant oder im Control Panel mögliche Fehler für die Validierung behoben haben und die Validierung der Umgebung zurückgesetzt haben, können Sie die Umgebung später erneut validieren.

**Hinweis:**

Jeder Administrator sieht im Modul **365 Total Protection > 365 Total Protection** nur die Validierungen, die er selbst durchgeführt hat. Deshalb kann ein Administrator nur seine eigenen Validierungen zurücksetzen.

**Wichtig:**

Solange eine Umgebung für einen Administrator nicht validiert ist, kann der Administrator keine Daten von Postfächern dieser Umgebung migrieren (siehe [Postfächer migrieren](#) auf Seite 73).

**Wichtig:**

Die Validierung kann nur für Umgebungen zurückgesetzt werden, für die derzeit keine Postfachmigration durchgeführt wird.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie in der Bereichsauswahl die Domain aus, für die Sie die Validierung einer Umgebung zurücksetzen möchten.
3. Navigieren Sie zu **365 Total Protection > 365 Total Protection**.
4. Klicken Sie in der Spalte **Validierte Umgebungen** in der Zeile der Umgebung, deren Validierung Sie zurücksetzen möchten, auf **Zurücksetzen**.

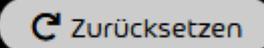
Exchange   Zurücksetzen

Abbildung 67: Validierung zurücksetzen



Ein Bestätigungsfenster wird angezeigt.



5. Klicken Sie auf **OK**.

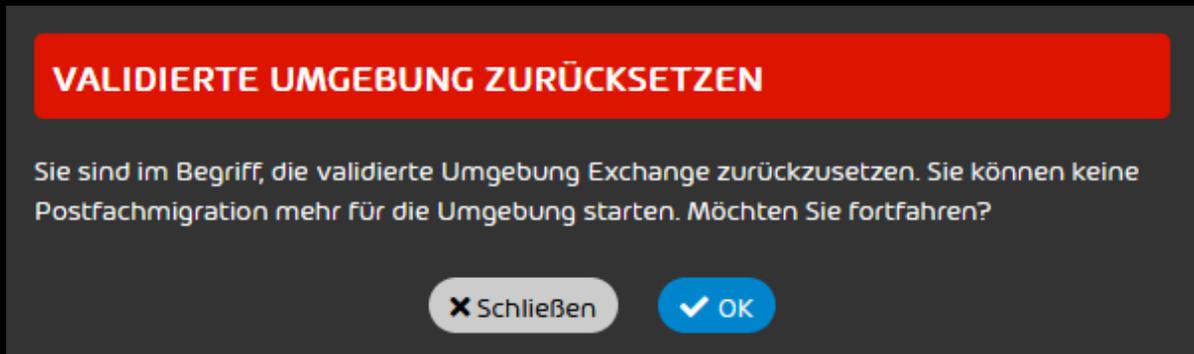


Abbildung 68: Zurücksetzen der Validierung bestätigen



Die Validierung der Umgebung wird zurückgesetzt. Die Umgebung wird aus der Liste in der Spalte **Validierte Umgebungen** entfernt.

Anschließend können Sie die Umgebung erneut validieren (siehe [Umgebung validieren](#) auf Seite 66).

Postfächer migrieren



Sie haben die Vorbereitungen für die Postfachmigration auf dem lokalen Exchange-Server, im Microsoft-365-Tenant und im Control Panel getroffen (siehe [Voraussetzungen für die Postfachmigration](#) auf Seite 46). Sie haben die Umgebung der Postfächer validiert, deren Daten Sie migrieren möchten (siehe [Umgebung validieren](#) auf Seite 66).

Mit der Postfachmigration (siehe [Über die Postfachmigration](#) auf Seite 43) können Sie die Daten von Postfächern validierter Umgebungen (siehe [Umgebung validieren](#) auf Seite 66) migrieren. Im Modul **Kundeneinstellungen** > **Postfächer** können Sie ein oder mehrere Postfächer für die Migration auswählen.



Hinweis:

Nur die Daten von Postfächern der Typen **LDAP-Postfach** und **Postfach** können migriert werden (siehe [Postfachtypen](#)).



Hinweis:

Wir empfehlen, beim ersten Mal nur wenige Postfächer auszuwählen, um sich mit dem Prozess vertraut zu machen.

Grundsätzlich empfehlen wir, die Daten der Postfächer einer Umgebung in Gruppen von 50 bis 100 Postfächern zu migrieren.



Hinweis:

Eine Postfachmigration kann mehrere Stunden oder Tage dauern. Konkrete Zeitangaben sind nicht möglich, da die Dauer von den folgenden Faktoren abhängt:

- Anzahl und Größe der zu migrierenden Postfächer
- Gesamtlast durch andere Postfachmigrationen in der Warteschlange

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie in der Bereichsauswahl die Domain des Kunden aus, dessen Postfachdaten Sie migrieren möchten.
3. Navigieren Sie zu **Kundeneinstellungen > Postfächer**.



Hinweis:

Alternativ können Administratoren mit einem Klick auf den Button **Postfächer für die Migration auswählen** im Modul **365 Total Protection > 365 Total Protection** zum Modul **Kundeneinstellungen > Postfächer** navigieren.

4. Filtern Sie die angezeigten Postfächer nach Ihren Wünschen (siehe [Postfächer](#)).



Hinweis:

Es ist auch möglich, die Postfächer nach dem Status der Postfachmigration zu filtern.



5. Falls Sie die Daten aller angezeigten Postfächer migrieren möchten, gehen Sie wie folgt vor:
- Klicken Sie auf **Alle Postfächer zu Microsoft 365 migrieren**.



Abbildung 69: Alle angezeigten Postfächer migrieren



Ein Bestätigungsfenster wird angezeigt.

- Klicken Sie auf **OK**.

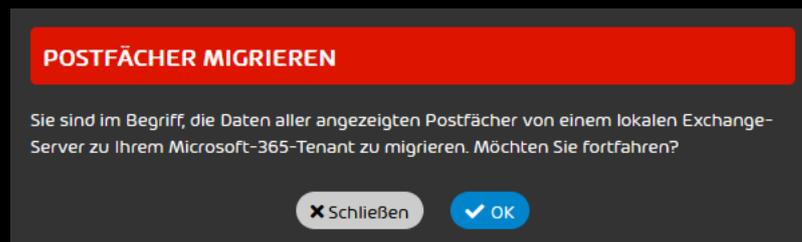


Abbildung 70: Migration aller angezeigten Postfächer bestätigen



Das Fenster wird geschlossen.

Falls die Migration für die Postfächer gestartet werden kann, wird eine Erfolgsmeldung angezeigt.

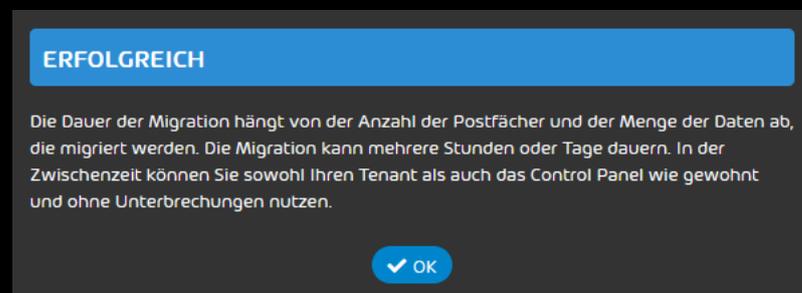


Abbildung 71: Erfolgsmeldung

Falls die Migration nicht für alle ausgewählten Postfächer gestartet werden kann, wird eine Fehlermeldung oder eine Warnmeldung angezeigt. In dem Fall wird die Migration auch für die übrigen Postfächer nicht gestartet.



Hinweis:

Eine Fehlermeldung wird beispielsweise angezeigt, falls für eines der ausgewählten Postfächer bereits eine Migration durchgeführt wird, da für jedes Postfach nur eine Migration durchgeführt werden kann.

Eine Warnmeldung wird beispielsweise angezeigt, falls die Umgebung eines ausgewählten Postfachs noch nicht vom angemeldeten Administrator validiert worden ist. In dem Fall muss der Administrator die Umgebung zunächst validieren (siehe [Umgebung validieren](#) auf Seite 66).



Für mindestens ein
ausgewähltes Postfach wird
bereits eine Migration
durchgeführt.

Abbildung 72: Fehlermeldung



UMGEBUNGSVALIDIERUNG ERFORDERLICH

Die folgenden Umgebungen wurden noch nicht validiert:

- Primäre Umgebung

Bevor Sie Postfachdaten aus diesen Umgebungen migrieren können, müssen Sie die Umgebungen im Modul „365 Total Protection“ validieren.

X Schließen

Zur Validierung **>**

Abbildung 73: Warnmeldung zu nicht validierten Umgebungen



6. Falls Sie nur die Daten ausgewählter Postfächer migrieren möchten, gehen Sie wie folgt vor:

a) Klicken Sie auf .



In der Liste der Postfächer wird eine Spalte mit Checkboxes angezeigt.

b) Setzen Sie ein Häkchen in den Checkboxes der Postfächer, deren Daten Sie migrieren möchten.

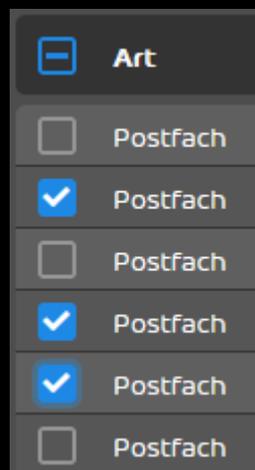


Abbildung 74: Postfächer auswählen



Der Button **Ausgewählte Postfächer zu Microsoft 365 migrieren** wird freigeschaltet.

c) Klicken Sie auf **Ausgewählte Postfächer zu Microsoft 365 migrieren**.



Abbildung 75: Ausgewählte Postfächer migrieren



Ein Bestätigungsfenster wird angezeigt.

d) Klicken Sie auf **OK**.

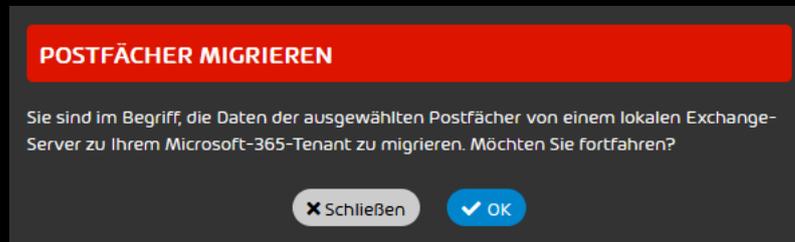


Abbildung 76: Migration der ausgewählten Postfächer bestätigen



Das Fenster wird geschlossen.

Falls die Migration für die Postfächer gestartet werden kann, wird eine Erfolgsmeldung angezeigt.

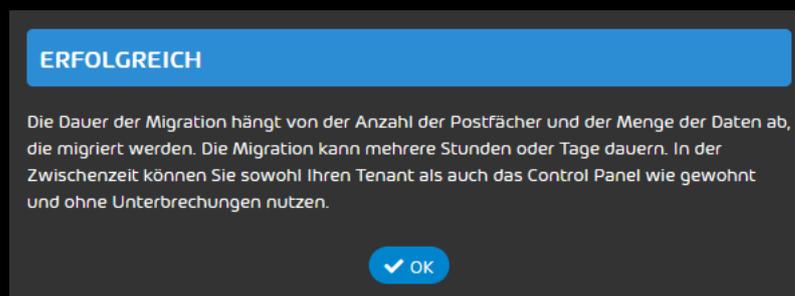


Abbildung 77: Erfolgsmeldung

Falls die Migration nicht für alle ausgewählten Postfächer gestartet werden kann, wird eine Fehlermeldung oder eine Warnmeldung angezeigt. In dem Fall wird die Migration auch für die übrigen Postfächer nicht gestartet.



Hinweis:

Eine Fehlermeldung wird beispielsweise angezeigt, falls für eines der ausgewählten Postfächer bereits eine Migration durchgeführt wird, da für jedes Postfach nur eine Migration durchgeführt werden kann.

Eine Warnmeldung wird beispielsweise angezeigt, falls die Umgebung eines ausgewählten Postfachs noch nicht vom angemeldeten Administrator validiert worden ist. In dem Fall muss der Administrator die Umgebung zunächst validieren (siehe [Umgebung validieren](#) auf Seite 66).



Abbildung 78: Fehlermeldung



Abbildung 79: Warnmeldung zu nicht validierten Umgebungen

7. Falls eine Erfolgsmeldung angezeigt wird, klicken Sie auf **OK**.



8. Navigieren Sie zu **365 Total Protection > 365 Total Protection**.



Der neue Migrationsauftrag wird in der Spalte **Derzeit laufende Migrationen** angezeigt. Falls Postfächer mehrerer Umgebungen für die Migration ausgewählt worden sind, werden statt eines einzigen Auftrags einzelne Aufträge für jede Umgebung angezeigt.



Hinweis:

Die Migration besteht aus den folgenden Phasen:

- **in Warteschlange:** Der Migrationsauftrag befindet sich in der Warteschlange und hat noch nicht begonnen.
- **in Verarbeitung:** Die Verarbeitung des Migrationsauftrags hat begonnen.
- **Migration wird durchgeführt:** Die Postfachdaten der Postfächer werden vom lokalen Exchange-Server in den Microsoft-365-Tenant migriert.
- **bereit für die Umleitung:** Die Migration der Postfachdaten ist abgeschlossen worden. Sobald dieser Zustand erreicht worden ist, hat der Administrator 14 Tage Zeit, um die migrierten Postfächer im Control Panel umzuleiten (siehe Schritt 9 auf Seite 81).
- **Umleitung läuft:** Der Administrator hat die Umleitung der migrierten Postfächer durchgeführt. Als Umgebung der migrierten Postfächer wird im Control Panel nicht mehr der lokale Exchange-Server, sondern der Microsoft-365-Tenant verwendet. Dadurch leiten unsere Server den E-Mail-Verkehr der migrierten Postfächer nun an den Microsoft-365-Tenant.

Falls während der Migration ein Fehler auftritt, wird die Migration pausiert und erhält den Zustand **angehalten**. In dem Fall muss der Administrator in die Migration eingreifen.



Hinweis:

Mit einem Klick auf den Button  neben dem Migrationsauftrag wird ein Protokoll der Migration heruntergeladen. Das Protokoll enthält Informationen zu den migrierten Postfächern und möglichen Fehlern.



9. Sobald der Migrationsauftrag den Zustand **bereit für die Umleitung** erreicht hat, klicken Sie auf den Button  neben dem Migrationsauftrag.



Ein Bestätigungsfenster wird angezeigt.

10. Klicken Sie auf **Umleitung starten**.

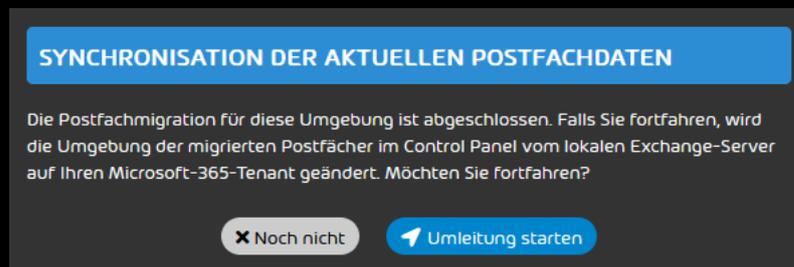


Abbildung 80: Umleitung bestätigen



Die Umgebung der migrierten Postfächer wird im Control Panel vom lokalen Exchange-Server auf den Microsoft-365-Tenant geändert. Falls die Umleitung innerhalb von 14 Tagen nach der Migration der Postfachdaten durchgeführt wird, werden die Daten der migrierten Postfächer, die sich in der Zwischenzeit auf dem lokalen Exchange-Server geändert haben, im Microsoft-365-Tenant synchronisiert.

! Wichtig:

Nach 14 Tagen ist es nicht mehr möglich, die aktuellen Postfachdaten auf dem lokalen Exchange-Server im Microsoft-365-Tenant automatisch zu synchronisieren.

Der Migrationsauftrag wird abgeschlossen und durch einen grünen Haken gekennzeichnet. Sobald alle Migrationsaufträge abgeschlossen sind, wird in der Spalte **Derzeit laufende Migrationen** der Button **Postfachmigration abschließen** freigeschaltet.

2 Postfächer
Exchange

Umleitung läuft
2 / 2 migriert



Abbildung 81: Abgeschlossener Migrationsauftrag





Die Daten von Postfächern sind von einem lokalen Exchange-Server in den Microsoft-365-Tenant des Kunden migriert werden.

Sobald alle Migrationsaufträge abgeschlossen sind, können Sie die Postfachmigration abschließen (siehe [Postfachmigration abschließen](#) auf Seite 82).

Postfachmigration abschließen



Sie haben die Daten aller gewünschten Postfächer migriert (siehe [Postfächer migrieren](#) auf Seite 73).

Sobald alle Migrationsaufträge (siehe [Postfächer migrieren](#) auf Seite 73) abgeschlossen worden sind, können Sie die Postfachmigration (siehe [Über die Postfachmigration](#) auf Seite 43) abschließen. Danach wird das Upgrade des Kunden auf 365 Total Protection automatisch fortgesetzt (siehe [Auf 365 Total Protection upgraden](#)). Erst nachdem das Upgrade auf 365 Total Protection abgeschlossen worden ist, werden die Postfächer, Gruppen und Domains des Microsoft-365-Tenants des Kunden im Control Panel synchronisiert.



Wichtig:

Nach Abschluss der Postfachmigration können keine weiteren Postfachdaten mehr migriert werden. Stellen Sie daher sicher, dass die Daten aller gewünschten Postfächer migriert worden sind.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie in der Bereichsauswahl die Domain aus, für die Sie die Postfachmigration abschließen möchten
3. Navigieren Sie zu **365 Total Protection > 365 Total Protection**.



4. Klicken Sie in der Spalte **Derzeit laufende Migrationen** auf **Postfachmigration abschließen**.

 **Hinweis:**

Der Button ist nur freigeschaltet, falls alle Postfachmigrationen in der Spalte **Derzeit laufende Migrationen** abgeschlossen sind.



Abbildung 82: Postfachmigration abschließen



Ein Bestätigungsfenster wird angezeigt.

5. Klicken Sie auf **Postfachmigration abschließen**.

POSTFACHMIGRATION ABSCHLIESSEN

Sie sind im Begriff, die Postfachmigration abzuschließen.

STELLEN SIE SICHER, DASS SIE ALLE GEWÜNSCHTEN POSTFÄCHER MIGRIERT HABEN, BEVOR SIE FORTFAHREN. DIESE AKTION IST DAUERHAFT. SIE KÖNNEN DANACH KEINE WEITEREN POSTFÄCHER MEHR MIGRIEREN.

Falls Sie fortfahren, wird das Upgrade auf 365 Total Protection abgeschlossen und im Control Panel beginnt die Synchronisation mit Ihrem Microsoft-365-Tenant.

Möchten Sie fortfahren?

Abbildung 83: Abschluss der Postfachmigration bestätigen



Die Postfachmigration wird abgeschlossen. Das Upgrade des Kunden auf 365 Total Protection wird fortgesetzt (siehe [Auf 365 Total Protection upgraden](#)).



Die Postfachmigration ist abgeschlossen worden.



365 Total Backup konfigurieren



Sie sind zu 365 Total Protection Enterprise Backup migriert (siehe [Auf 365 Total Protection upgraden](#) auf Seite 25).

Der Service 365 Total Protection Enterprise Backup kombiniert die Services 365 Total Protection Enterprise und 365 Total Backup miteinander (siehe [Über 365 Total Protection](#) auf Seite 6). Sobald Sie als Kunde zu 365 Total Protection Enterprise Backup migriert sind, können Sie 365 Total Backup konfigurieren. Mit diesem Vorgehen richten Sie 365 Total Backup nach den Standardeinstellungen ein. In dem Fall werden alle Microsoft-365-Postfächer, Dateien in OneDrive-for-Business-Konten und SharePoint-Dokumentbibliotheken sowie Teams-Chats für Benutzer und Gruppen aus Ihrem Tenant gesichert.



Hinweis:

Administratoren auf Kundenebene oder Partnerebene können 365 Total Backup mit anderen Einstellungen konfigurieren, indem sie 365 Total Backup über das Modul **Backup > 365 Total Backup** öffnen (siehe [365 Total Backup starten](#)).

Mit 365 Total Backup können auch Daten von Windows-basierten Endpunkten gesichert werden. Endpunkte werden bei der Standardkonfiguration jedoch nicht berücksichtigt. Nur Administratoren auf Partnerebene können Backups von Endpunkten konfigurieren. Dazu können Administratoren auf Partnerebene 365 Total Backup über das Modul **Backup > 365 Total Backup** öffnen.



Wichtig:

Administratoren auf Kundenebene können 365 Total Backup nur konfigurieren, falls ihr Partner ihnen Zugriff auf 365 Total Backup gewährt hat (siehe [Zugang zu 365 Total Backup gewähren](#)). Andernfalls können nur Administratoren auf Partnerebene 365 Total Backup für den Kunden konfigurieren.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie in der Bereichsauswahl Ihre Domain aus.



3. Navigieren Sie zu **365 Total Protection > 365 Total Protection**.



Der Einrichtungsstatus von 365 Total Protection Enterprise Backup wird angezeigt.

Einrichtungsstatus 365 Total Protection Enterprise Backup

MICROSOFT 365 WURDE VERBUNDEN.

21 Postfächer | 20 Lizenzen | 2 Domains

Konfigurieren Sie die DNS-Einstellungen Ihrer Domains

Die DNS-Einstellungen von mindestens einer synchronisierten Domain wurden noch nicht gesetzt oder sind falsch konfiguriert. Folgen Sie der Anleitung im Handbuch, um die DNS-Einstellungen richtig zu konfigurieren.

Jetzt konfigurieren

365 Total Backup konfigurieren

Klicken Sie auf „Jetzt konfigurieren“, um erforderliche Berechtigungen für die Sicherung Ihres Microsoft-365-Tenants zu gewähren.

Jetzt konfigurieren

Ausgehenden E-Mail-Verkehr konfigurieren

Sie müssen Ihren ausgehenden E-Mail-Verkehr konfigurieren. Eine Anleitung dazu finden Sie in unserem Handbuch.

Automatisch konfigurieren

Abbildung 84: Einrichtungsstatus

4. Klicken Sie unter **365 Total Backup konfigurieren** auf **Jetzt konfigurieren**.



In einem neuen Tab öffnet sich eine Seite zur Konfiguration von 365 Total Backup. Die Daten des Kunden sind voreingestellt.



Hinweis:

Auf der Seite wird die Sprache verwendet, die für den übergeordneten Partner des Kunden im Control Panel eingestellt ist (siehe **Standardwerte für Zeitzone und Sprache einstellen**).



5. Klicken Sie auf **Weiter**.

365 Total Backup konfigurieren

Schritt 1
Office-365-Organisation hinzufügen

2 Beenden
Zugang gewähren

Office-365-Organisation hinzufügen

Wählen Sie die Office-365-Organisation aus, die hinzugefügt werden soll.

Kunde auswählen
blueberry.com

Unternehmensname der Office-365-Organisation
onmicrosoft.com

Office-365-Organisation
onmicrosoft.com

Abbrechen Weiter

Abbildung 85: Angaben prüfen



Ein Fenster mit einer Übersicht der Konfigurationsschritte öffnet sich.



6. Klicken Sie auf Schritt 1.

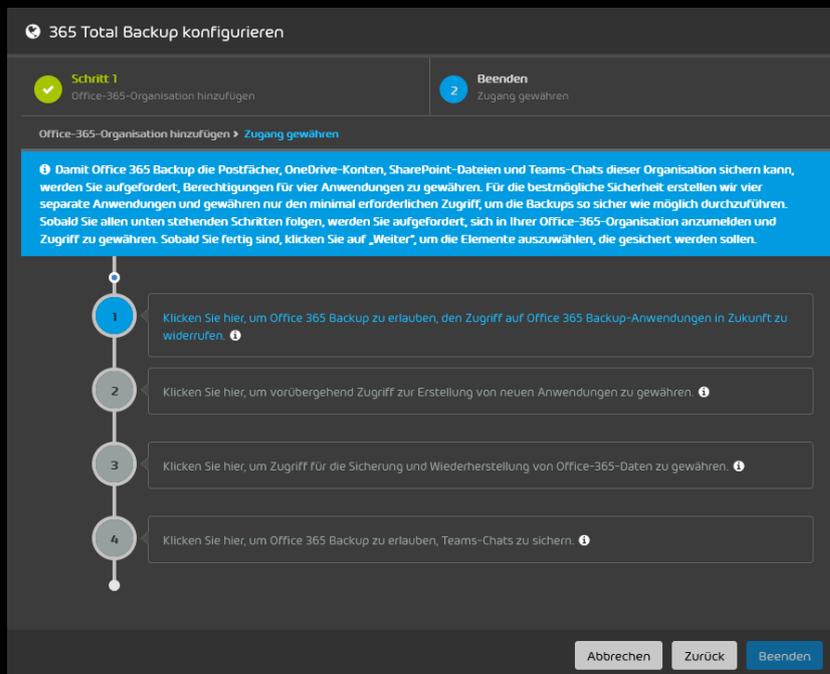


Abbildung 86: Schritt 1 durchführen



Die Anmeldeseite von Microsoft 365 öffnet sich in einem neuen Tab.

7. Melden Sie sich mit den administrativen Zugangsdaten des Kunden bei Microsoft 365 an.



Eine Seite mit angeforderten Berechtigungen wird angezeigt.



8. Gewähren Sie die angeforderten Berechtigungen.

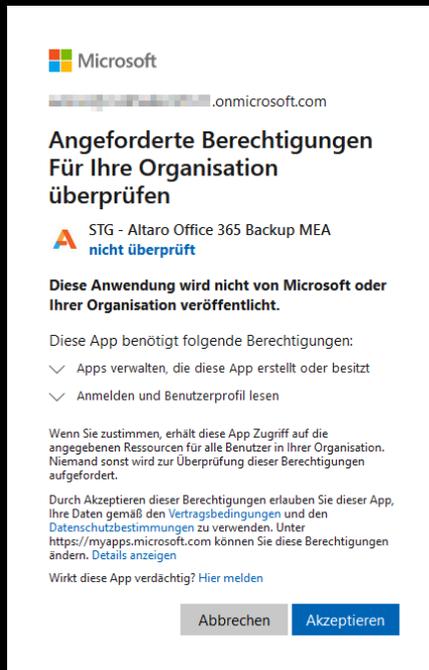


Abbildung 87: Berechtigungen gewähren



Die Berechtigungen werden gewährt. Eine Bestätigungsmeldung wird angezeigt.



Abbildung 88: Bestätigungsfenster

9. Klicken Sie auf **Schließen**.



Der Tab wird geschlossen. Die Übersicht der Konfigurationsschritte wird wieder angezeigt.



10. Klicken Sie auf Schritt 2.

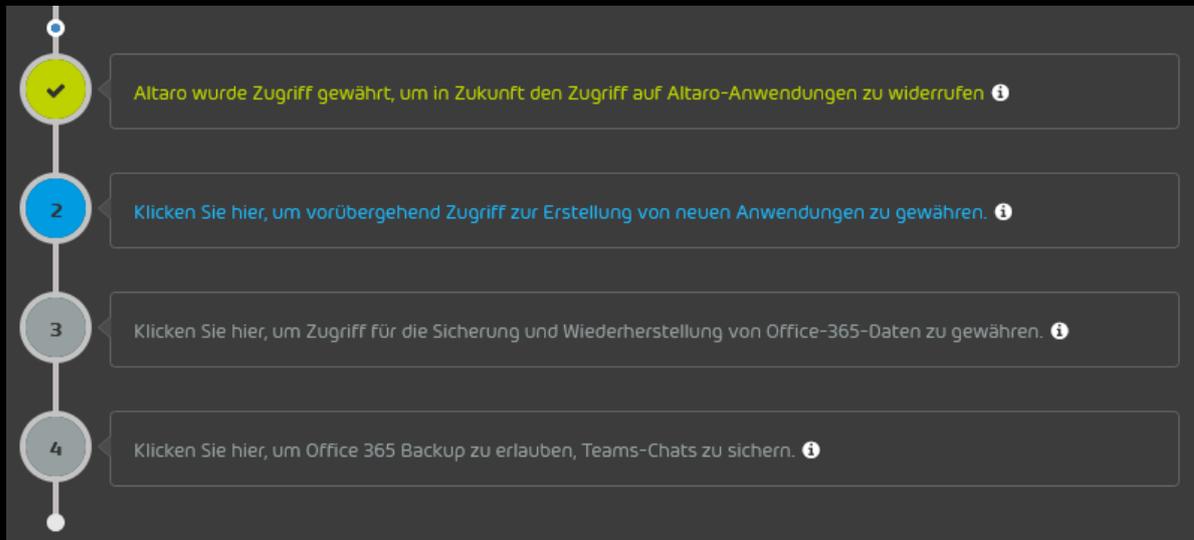


Abbildung 89: Schritt 2 durchführen



Die Anmeldeseite von Microsoft 365 öffnet sich in einem neuen Tab.

11. Melden Sie sich mit den administrativen Zugangsdaten des Kunden bei Microsoft 365 an.



365 Total Backup wird Zugang zum Tenant des Kunden gewährt. Eine Bestätigungsmeldung wird angezeigt.



Abbildung 90: Bestätigungsfenster

12. Klicken Sie auf **Schließen**.



Der Tab wird geschlossen. Die Übersicht der Konfigurationsschritte wird wieder angezeigt.



13. Klicken Sie auf Schritt 3.

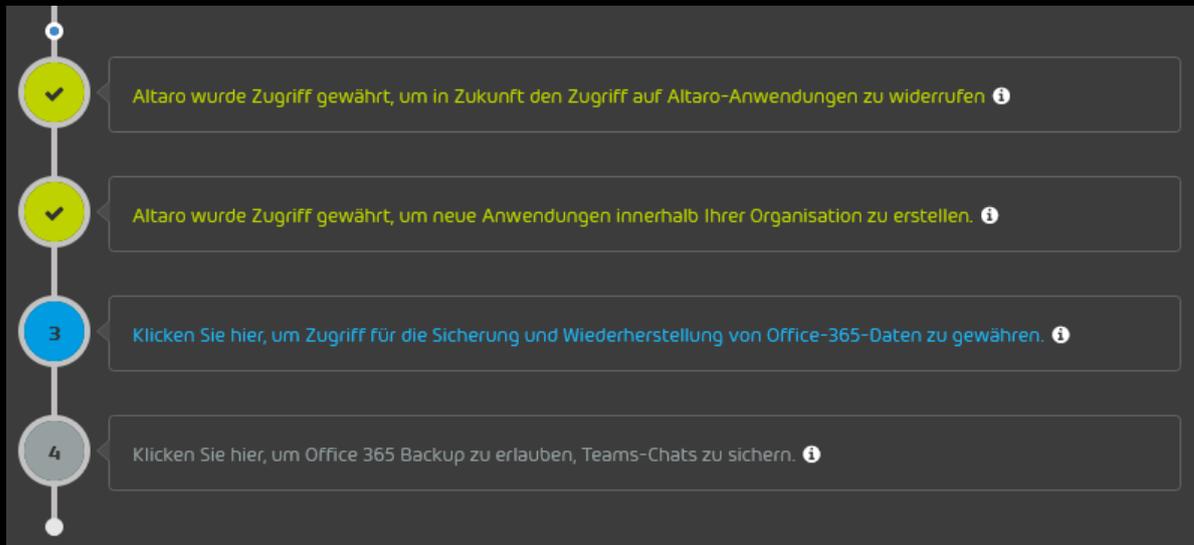


Abbildung 91: Schritt 3 durchführen



Die Anmeldeseite von Microsoft 365 öffnet sich in einem neuen Tab.

14. Melden Sie sich mit den administrativen Zugangsdaten des Kunden bei Microsoft 365 an.



Eine Seite mit angeforderten Berechtigungen wird angezeigt.



15. Gewähren Sie die angeforderten Berechtigungen.

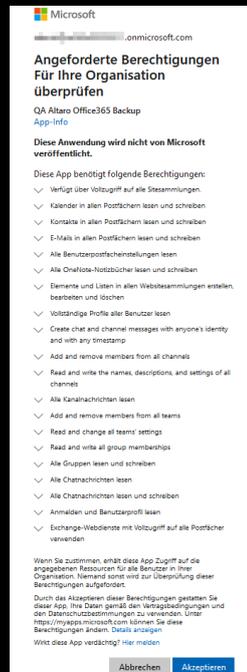


Abbildung 92: Berechtigungen gewähren



Die Berechtigungen werden gewährt. Eine Bestätigungsmeldung wird angezeigt.



Abbildung 93: Bestätigungsfenster



16. Klicken Sie auf Schritt 4.

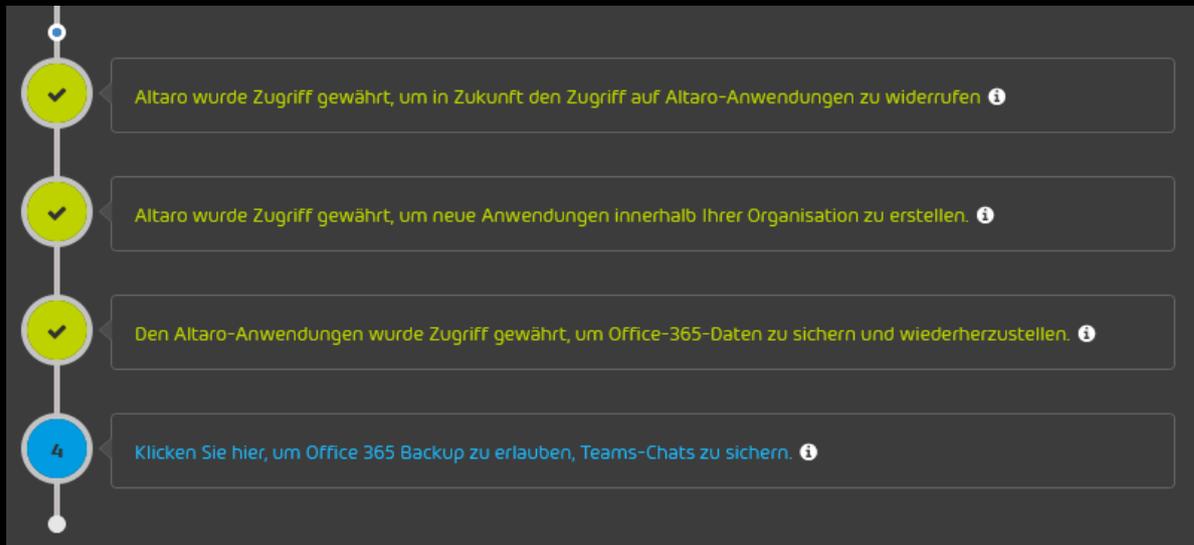


Abbildung 94: Schritt 4 durchführen



Die Anmeldeseite von Microsoft 365 öffnet sich in einem neuen Tab.

17. Melden Sie sich mit den administrativen Zugangsdaten des Kunden bei Microsoft 365 an.



Eine Seite mit angeforderten Berechtigungen wird angezeigt.



18. Gewähren Sie die angeforderten Berechtigungen.

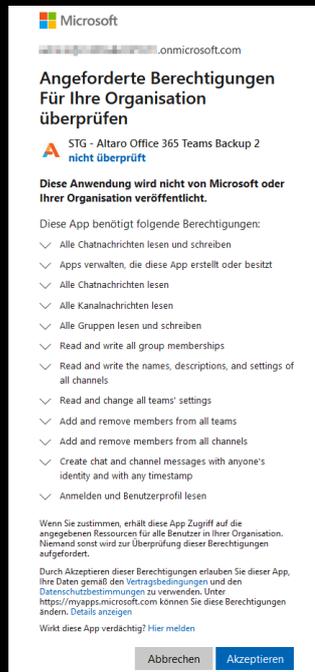


Abbildung 95: Berechtigungen gewähren



Die Berechtigungen werden gewährt. Eine Bestätigungsmeldung wird angezeigt.



Abbildung 96: Bestätigungsfenster

19. Klicken Sie auf **Schließen**.



Der Tab wird geschlossen. Die Übersicht der Konfigurationsschritte wird wieder angezeigt.



20. Klicken Sie auf **Beenden**.

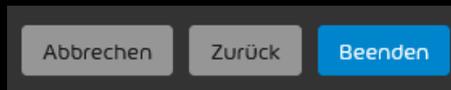


Abbildung 97: Konfiguration beenden



Der Tab wird geschlossen. Im Control Panel wird die Konfiguration von 365 Total Backup im Modul **365 Total Protection** > **365 Total Protection** als abgeschlossen angezeigt.



Abbildung 98: Status der Konfiguration von 365 Total Backup



365 Total Backup ist konfiguriert worden.



Konfiguration der Services von Microsoft

Um den korrekten Betrieb von 365 Total Protection (siehe [Über 365 Total Protection](#) auf Seite 6) zu gewährleisten, müssen nach der Synchronisation der Postfächer die Services von Microsoft für alle erstellten Domains konfiguriert werden. Die folgenden Einstellungen können angepasst werden:

- **Grundlegende Einstellungen** auf Seite 95: Diese Einstellungen sind für den korrekten Betrieb von 365 Total Protection erforderlich.
- **Erweiterte Einstellungen** auf Seite 109: Diese Einstellungen sind nur für optionale Services von 365 Total Protection erforderlich.

Grundlegende Einstellungen

Grundlegende Einstellungen

365 Total Protection (siehe [Über 365 Total Protection](#) auf Seite 6) kann Ihre Postfächer nur schützen, falls alle eingehenden E-Mails von Absendern außerhalb Ihrer Organisation sowie alle ausgehenden E-Mails an Empfänger außerhalb Ihrer Organisation an unsere Server geleitet werden. Dafür gelten die folgenden Voraussetzungen:

- Die MX-Einträge der DNS-Zonen Ihrer Domains zeigen auf unsere Server (siehe [MX-Einträge anpassen](#) auf Seite 96). Dadurch werden eingehende E-Mails der Domains zunächst an unsere Server geleitet. Unsere Server leiten die eingehenden E-Mails anschließend an Microsoft 365 weiter.



Hinweis:

Unsere Server leiten eingehende E-Mails an die Adresse des Zielservers von Microsoft 365 weiter, die bei der erstmaligen Synchronisation (siehe [365 Total Protection einrichten](#) auf Seite 10) automatisch ermittelt worden ist. Diese Adresse muss uns daher nicht gesondert mitgeteilt werden.

Sobald Postfächern eine primäre oder sekundäre Umgebung zugewiesen wird, leiten unsere Server die eingehenden E-Mails der Postfächer nicht mehr an die automatisch ermittelte Adresse, sondern an die Adressen der zugewiesenen Umgebungen (siehe [Primäre Umgebungseinstellungen vornehmen](#) und [Sekundäre Umgebungen](#)).

- Ihre Postfächer können nur E-Mails empfangen, die von unseren Services verarbeitet worden sind. Dafür muss in Microsoft 365 ein Connector für den eingehenden E-Mail-Verkehr



eingrichtet werden, der nur E-Mails aus unseren IP-Adressbereichen zulässt. Dieser Connector kann automatisch erstellt werden (siehe [Eingehenden und ausgehenden E-Mail-Verkehr automatisch konfigurieren](#) auf Seite 99).

- Der Spamfilter von Microsoft 365 ist für die IP-Adressbereiche unserer Server deaktiviert (siehe [Spamfilter von Microsoft 365 für den IP-Adressbereich von Hornetsecurity deaktivieren](#) auf Seite 102). Ansonsten würde der Spamfilter von Microsoft 365 die von uns verarbeiteten E-Mails als Spam einstufen.

**Wichtig:**

Der Spamfilter von Microsoft 365 kann für unseren IP-Adressbereich erst deaktiviert werden, nachdem in Exchange Online Anpassungen für die Microsoft-365-Organisation freigeschaltet worden sind (siehe [Organisationsanpassungen freischalten](#) auf Seite 101).

- Für den ausgehenden E-Mail-Verkehr ist ein Connector eingerichtet worden, der die ausgehenden E-Mails Ihrer Postfächer an unseren Smarthost umleitet. Nur so können unsere Services alle ausgehenden E-Mails an Postfächer außerhalb Ihrer Organisation verarbeiten. Nach der Verarbeitung sendet unser Smarthost die ausgehenden E-Mails an ihre Empfänger. Dieser Connector kann automatisch erstellt werden (siehe [Eingehenden und ausgehenden E-Mail-Verkehr automatisch konfigurieren](#) auf Seite 99).
- Die SPF-Einträge Ihrer Domains zeigen auf unsere SPF-Einträge (siehe [SPF-Einträge anpassen](#) auf Seite 108). Nur so können die E-Mails, die über unseren Smarthost gesendet worden sind, bei einer SPF-Prüfung (siehe [SPF-Prüfung](#)) von den Posteingangsservern der Empfänger als legitim erkannt und angenommen werden.

MX-Einträge anpassen



Sie haben Ihre Domains konfiguriert.

**Hinweis:**

Falls Sie nicht sicher sind, ob die Konfiguration Ihrer Domains abgeschlossen ist, kontaktieren Sie den Support.

MX-Einträge zeigen auf die Server, die eingehende E-Mails für Postfächer einer Domain empfangen. Sie können unsere Server in den MX-Einträgen Ihrer Domain eintragen, damit die eingehenden E-Mails Ihrer Domain zunächst an unsere Server geleitet werden. Dadurch können die E-Mails gefiltert werden, bevor Sie an Microsoft 365 weitergeleitet werden.



1. Setzen Sie die MX-Einträge in Abhängigkeit von Ihrer Region. Sie können aus den folgenden Regionen wählen.
 - Europa (siehe [MX-Einträge für Kunden aus Europa](#) auf Seite 98)
 - USA (siehe [MX-Einträge für Kunden aus den USA](#) auf Seite 98)
 - Kanada (siehe [MX-Einträge für Kunden aus Kanada](#) auf Seite 99)

**Hinweis:**

Kunden, deren Organisation sich außerhalb der genannten Regionen befindet, können eine Region nach datenschutzrechtlichen Kriterien auswählen.

2. Um zu prüfen, ob die MX-Einträge richtig eingestellt sind, klicken Sie auf **Konfiguration zeigen**.

**Abbildung 99: Zeige Konfiguration**

Der Statusbericht zeigt die erfolgreiche Umstellung der MX-Einträge an.

MX-Statusbericht:

Domain	MX umgestellt
example.com	✓

Abbildung 100: Statusbericht

Die MX-Einträge sind angepasst worden.

Anschließend können Sie den eingehenden und ausgehenden E-Mail-Verkehr automatisch konfigurieren (siehe [Eingehenden und ausgehenden E-Mail-Verkehr automatisch konfigurieren](#) auf Seite 99).



MX-Einträge für Kunden aus Europa

Kunden aus Europa müssen in der DNS-Zone ihrer Domains die MX-Einträge aus der folgenden Tabelle setzen, damit unsere Services ihre eingehenden E-Mails filtern und verarbeiten können (siehe [#unique_40](#)). Der Platzhalter **<domain.tld>** steht für die Domain des Kunden.

Tabelle 1: MX-Einträge für Kunden aus Europa

Domain	Klasse	Typ	Priorität	E-Mail-Server
<domain.tld>	IN	MX	10	mx01.hornetsecurit
<domain.tld>	IN	MX	20	mx02.hornetsecuril
<domain.tld>	IN	MX	30	mx03.hornetsecuril
<domain.tld>	IN	MX	40	mx04.hornetsecuril

Für Kunden des DNS-Anbieters 1&1 gelten stattdessen die folgenden MX-Einträge:

Tabelle 2: MX-Einträge für Kunden des DNS-Anbieters 1&1

Domain	Klasse	Typ	Priorität	E-Mail-Server
<domain.tld>	IN	MX	10	mx23a.antispameu
<domain.tld>	IN	MX	20	mx23b.antispameu
<domain.tld>	IN	MX	30	mx23c.antispameu
<domain.tld>	IN	MX	40	mx23d.antispameu

MX-Einträge für Kunden aus den USA

Kunden aus den USA müssen in der DNS-Zone ihrer Domains die MX-Einträge aus der folgenden Tabelle setzen, damit unsere Services ihre eingehenden E-Mails filtern und verarbeiten können (siehe [#unique_40](#)). Der Platzhalter **<domain.tld>** steht für die Domain des Kunden.

Tabelle 3: MX-Einträge

Domain	Klasse	Typ	Priorität	E-Mail-Server
<domain.tld>	IN	MX	10	mx-cluster- usa01.hornetsecuri



Domain	Klasse	Typ	Priorität	E-Mail-Server
<domain.tld>	IN	MX	20	mx-cluster- usa02.hornetsecuri
<domain.tld>	IN	MX	30	mx-cluster- usa03.hornetsecuri
<domain.tld>	IN	MX	40	mx-cluster- usa04.hornetsecuri

MX-Einträge für Kunden aus Kanada

Kunden aus Kanada müssen in der DNS-Zone ihrer Domains die MX-Einträge aus der folgenden Tabelle setzen, damit unsere Services ihre eingehenden E-Mails filtern und verarbeiten können (siehe [#unique_40](#)). Der Platzhalter **<domain.tld>** steht für die Domain des Kunden.

Tabelle 4: MX-Einträge für Kunden aus Kanada

Domain	Klasse	Typ	Priorität	E-Mail-Server
<domain.tld>	IN	MX	10	mx-cluster- ca01.hornetsecurity
<domain.tld>	IN	MX	20	mx-cluster- ca02.hornetsecurity
<domain.tld>	IN	MX	30	mx-cluster- ca03.hornetsecurity
<domain.tld>	IN	MX	40	mx-cluster-ca- fallback.hornetsecu

Eingehenden und ausgehenden E-Mail-Verkehr automatisch konfigurieren

Connectoren für den eingehenden und ausgehenden E-Mail-Verkehr gewährleisten, dass alle E-Mails von Absendern und an Empfänger außerhalb Ihrer Organisation an unsere Server geleitet werden. Sie können diese Connectoren auf der Statusseite von **365 Total Protection** (siehe [Über 365 Total Protection](#) auf Seite 6) automatisch konfigurieren.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie Ihre Domain in der Bereichsauswahl aus.
3. Navigieren Sie zu **365 Total Protection > 365 Total Protection**.



4. Klicken Sie auf **Automatisch konfigurieren**.



Abbildung 101: Automatisch konfigurieren



Hinweis:

Bei der automatischen Konfiguration des ausgehenden E-Mail-Verkehrs wird auch der eingehende E-Mail-Verkehr automatisch konfiguriert.



Der eingehende und der ausgehende E-Mail-Verkehr werden konfiguriert.



Für den eingehenden und ausgehenden E-Mail-Verkehr sind Connectoren konfiguriert worden.



Abbildung 102: Erfolgreiche Konfiguration



Wichtig:

Bereits installierte Connectoren können Fehler bei der automatischen Konfiguration des ausgehenden E-Mail-Verkehrs verursachen.

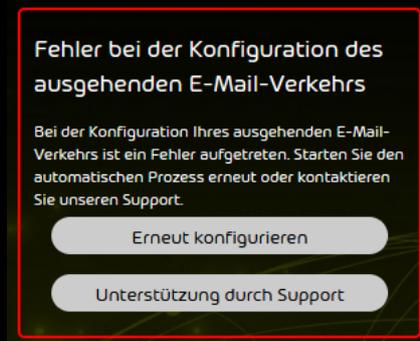


Abbildung 103: Fehler in der Konfiguration

Problembeseitigung

- Entfernen Sie bereits konfigurierte Connectoren und klicken Sie auf **Erneut konfigurieren**, um die Konfiguration neu zu starten ODER
- klicken Sie auf **Support-Unterstützung**, um den Support zu kontaktieren.

Anschließend können Sie den Spamfilter von Microsoft 365 für unseren IP-Adressbereich deaktivieren (siehe [Spamfilter von Microsoft 365 für den IP-Adressbereich von Hornetsecurity deaktivieren](#) auf Seite 102).

Organisationsanpassungen freischalten

Microsoft-365-Organisationen sind in Exchange Online standardmäßig komprimiert. Das bedeutet, dass einige Objekte in den Rechenzentren von Microsoft zusammengeführt sind, um Speicherplatz zu sparen. Aus diesem Grund können für komprimierte Microsoft-365-Organisationen einige Objekte in Exchange Online nicht bearbeitet werden. Bevor Sie diese Objekte bearbeiten können, müssen Sie über einen Befehl einmalig Anpassungen für Ihre Microsoft-365-Organisation in Exchange Online freischalten. Auch den Spamfilter von Microsoft 365 können Sie für unseren IP-Adressbereich erst deaktivieren (siehe [Spamfilter von Microsoft 365 für den IP-Adressbereich von Hornetsecurity deaktivieren](#) auf Seite 102), nachdem Sie den Befehl ausgeführt haben. Durch den Befehl wird die Organisation dekomprimiert.



Wichtig:

Der Befehl kann nur einmal ausgeführt werden und kann nicht rückgängig gemacht werden.

1. Öffnen Sie die Exchange Online PowerShell.



- Optional: Um zu prüfen, ob bereits Anpassungen für Ihre Microsoft-365-Organisation in Exchange Online freigeschaltet sind, führen Sie den folgenden Befehl aus: **Get-OrganizationConfig | fl IsDehydrated**.



Falls die Anpassungen bereits freigeschaltet sind, wird der Wert **False** ausgegeben. Falls die Anpassungen noch nicht freigeschaltet sind, wird der Wert **True** ausgegeben.

- Führen Sie den folgenden Befehl aus: **Enable-OrganizationCustomization**.



Die Microsoft-365-Organisation wird in Exchange Online dekomprimiert. Anpassungen für die Microsoft-365-Organisation werden in Exchange Online freigeschaltet. Es kann einige Zeit dauern, bis die Änderungen wirksam werden.



Anpassungen für eine Microsoft-365-Organisation sind in Exchange Online freigeschaltet worden.

Anschließend können Sie den Spamfilter von Microsoft 365 für unseren IP-Adressbereich deaktivieren (siehe [Spamfilter von Microsoft 365 für den IP-Adressbereich von Hornetsecurity deaktivieren](#) auf Seite 102).

Spamfilter von Microsoft 365 für den IP-Adressbereich von Hornetsecurity deaktivieren



Sie haben für Ihre Microsoft-365-Organisation Anpassungen in Exchange Online freigeschaltet (siehe [Organisationsanpassungen freischalten](#) auf Seite 101).

Sobald Sie eingehende E-Mails durch unsere Services filtern lassen möchten, müssen Sie den Spamfilter von Microsoft 365 deaktivieren. Ansonsten würde der Spamfilter von Microsoft 365 eingehende E-Mails Ihrer Domains als Spam klassifizieren. Unsere Services filtern Ihre eingehenden E-Mails nach Spam.



Hinweis:

Die E-Mail-Authentifizierung über SPF ist nicht automatisch aktiviert. Die Einrichtung der SPF-Prüfung ist nicht zwingend erforderlich, aber empfehlenswert. Für Informationen zur Einrichtung siehe [Über Email Authentication](#).

- Melden Sie sich unter admin.microsoft.com mit Ihren administrativen Zugangsdaten an.



2. Wählen Sie unter **Admin Center** den Menüpunkt **Sicherheit** aus.



Hinweis:

Sollten die Admin Centers in Ihrer Standardansicht nicht angezeigt werden, erweitern Sie das Menü mit **Alle anzeigen**.



Die Startseite von **Microsoft 365 Defender** öffnet sich.

3. Klicken Sie auf der linken Seite auf den Menüpunkt **Richtlinien und Regeln**.

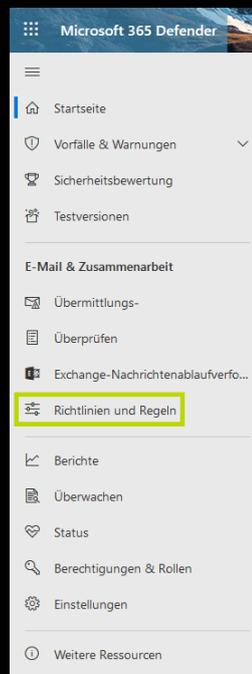


Abbildung 104: Menüpunkt auswählen



4. Klicken Sie auf **Bedrohungsrichtlinien**.

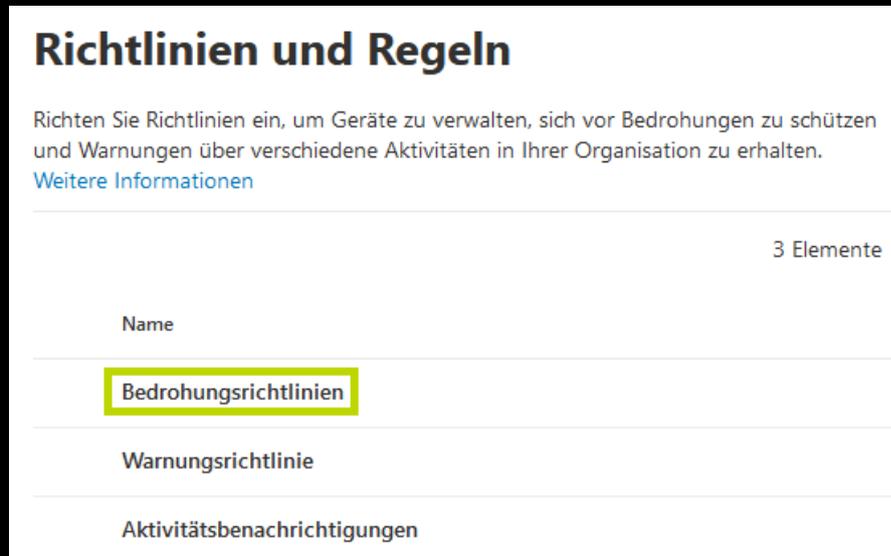


Abbildung 105: Bedrohungsrichtlinien auswählen



5. Klicken Sie unter **Richtlinien** auf **Antispam**.

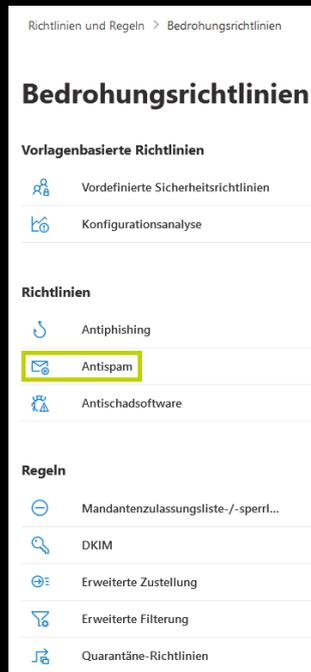


Abbildung 106: Antispam auswählen



Die Seite **Antispamrichtlinien** öffnet sich.



6. Klicken Sie auf **Verbindungsfilterrichtlinie (Standard)**.

Richtlinien und Regeln > Bedrohungsrichtlinien > Antispamrichtlinien

ⓘ Gehen Sie zur Seite mit den Quarantänerrichtlinien, um die Spam-Benachrichtigung für Benutzer zu konfigurieren, da wir die Konfiguration im Dezember 2021 aus der Anti-Spam-Richtlinie entfernen werden. [Erfahren Sie mehr über Quarantänerrichtlinien](#)

Auf dieser Seite können Sie zum Antispamschutz gehörende Richtlinien konfigurieren. Diese Richtlinien umfassen Verbindungsfilterung, Spamfilterung, ausgehende Spamfilterung und Spoof Intelligence. [Weitere Informationen](#)

+ Richtlinie erstellen ▾ ↻ Aktualisieren 1 von 3 ausgewählt 🔍 Suchen ☰ ▾

Name	Status	Priorität	Typ
Antispam-Eingangsrichtlinie (Standard)	● Immer aktiviert	Niedrigste	
<input checked="" type="checkbox"/> Verbindungsfilterrichtlinie (Standard)	● Immer aktiviert	Niedrigste	
Antispam-Ausgangsrichtlinie (Standard)	● Immer aktiviert	Niedrigste	

Abbildung 107: Verbindungsfilterrichtlinie (Standard) auswählen



Die Einstellungen der Richtlinie öffnen sich.



7. Klicken Sie auf **Verbindungsfilterrichtlinie bearbeiten**.

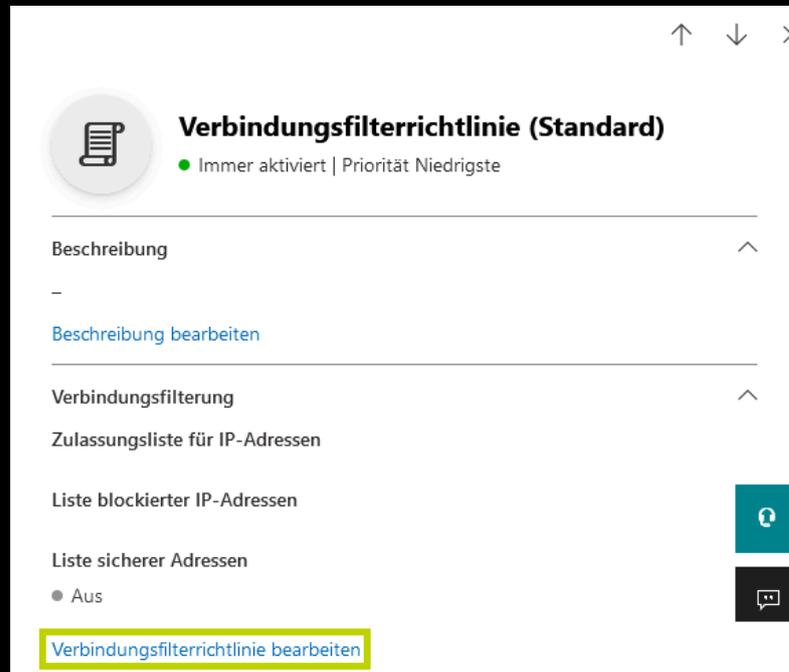


Abbildung 108: Richtlinie bearbeiten



Weitere Einstellungen werden angezeigt.

8. Geben Sie nacheinander die folgenden IP-Adressen in das Eingabefeld unter **Always allow messages from the following IP addresses or address range:** ein.

83.246.65.0/24	94.100.128.0/24	94.100.129.0/24
94.100.130.0/24	94.100.131.0/24	94.100.132.0/24
94.100.133.0/24	94.100.134.0/24	94.100.135.0/24
94.100.136.0/24	94.100.137.0/24	94.100.138.0/24
94.100.139.0/24	94.100.140.0/24	94.100.141.0/24
94.100.142.0/24	94.100.143.0/24	173.45.18.0/24
185.140.204.0/24	185.140.205.0/24	185.140.206.0/24



185.140.207.0/24

**Hinweis:**

Kunden aus Kanada müssen zusätzlich die folgenden IP-Adressen eintragen:

108.163.133.224/27 199.27.221.64/27 209.172.38.64/27
216.46.2.48/29 216.46.11.224/27

← ×

Verbindungsfilterrichtlinie (Standard)
● Immer aktiviert | Priorität Niedrigste

Always allow messages from the following IP addresses or address range:

94.100.131.0/24

Always block messages from the following IP addresses or address range:

Turn on safe list

Speichern Abbrechen

Abbildung 109: IP-Adressen in die Liste zugelassener IP-Adressen eintragen

9. Klicken Sie auf **Speichern**.



Die Einstellungen werden gespeichert.



Der Spamfilter von Microsoft 365 ist für E-Mails aus unserem IP-Adressbereich deaktiviert worden.

SPF-Einträge anpassen

Die SPF-Einträge Ihrer Domains müssen auf unsere eigenen SPF-Einträge verweisen. Somit wird Hornetsecurity als gültiger Absender von den Posteingangsservern anerkannt und die Über



unseren Smarthost versendeten E-Mails werden bei der SPF-Prüfung (siehe [SPF-Prüfung](#)) nicht als Spam eingestuft.

**Hinweis:**

Unser SPF-Eintrag ist nicht erforderlich für Kunden, die ihre primäre Umgebung mit der Option **IP/Hostname** eingestellt haben, jedoch keine Adressen von Relay-Servern für ausgehende E-Mails hinterlegt haben. Für weitere Informationen zur Einstellung der primären Umgebung siehe [Primäre Umgebungseinstellungen](#).

1. Melden Sie sich in der Administrationsumgebung von Microsoft 365 an.
2. Navigieren Sie zu **Setup > Domänen**.
3. Wählen Sie die Domain aus, die Sie bei Hornetsecurity registriert haben.
4. Fügen Sie folgenden SPF-Eintrag hinzu: **TXT "v=spf1 include:spf.protection.outlook.com include:spf.hornetsecurity.com ~all"**

**Wichtig:**

Falls Sie zusätzliche Systeme haben, die ausgehende E-Mails für die betroffene Domain senden, fügen Sie auch diese zu dem SPF-Eintrag hinzu.



Ihre SPF-Einträge sind angepasst worden.

Erweiterte Einstellungen

Erweiterte Einstellungen

Neben den grundlegenden Einstellungen (siehe [Grundlegende Einstellungen](#) auf Seite 95) können für 365 Total Protection (siehe [Über 365 Total Protection](#) auf Seite 6) auch erweiterte Einstellungen vorgenommen werden, um zusätzliche Möglichkeiten nutzen zu können oder Probleme bei der automatischen Einstellung zu umgehen.

- Um den Einrichtungsprozess von Benutzerkonten in E-Mail-Programmen zu erleichtern, kann der Autodiscover-Service eingerichtet werden (siehe [Autodiscover einrichten](#) auf Seite 110).
- Falls die automatische Einrichtung der Connectoren für den ein- und ausgehenden E-Mail-Verkehr (siehe [Eingehenden und ausgehenden E-Mail-Verkehr automatisch konfigurieren](#) auf Seite 99) fehlschlägt, besteht die Möglichkeit, die Connectoren manuell zu erstellen. In



diesem Fall ist es nötig, die Archivierung des E-Mail-Verkehrs innerhalb Ihres Unternehmens durch die Erstellung einer Journalregel zu ermöglichen. Weitere Informationen hierzu finden Sie in der Anleitung [Manuelle Ersteinrichtung der Services mit Microsoft 365](#)

- Falls Sie die Postfächer einer Domain teilweise über eine primäre Umgebung in Microsoft 365 und teilweise über andere sekundäre Umgebungen verwalten (siehe [Sekundäre Umgebungen](#)), müssen Sie eine Weiterleitung an die sekundären Umgebungen einrichten. Andernfalls werden E-Mails an Postfächer der sekundären Umgebungen abgewiesen. Weitere Informationen zur Einrichtung der Weiterleitung finden Sie in der Anleitung [Weiterleitung von E-Mails aus Microsoft 365](#).
- Die Multi-Faktor-Authentifizierung für Microsoft-365-Konten wird auch für die Anmeldung im Control Panel verwendet (siehe [Multi-Faktor-Authentifizierung](#) auf Seite 110).

Autodiscover einrichten

Das Konfigurieren des Autodiscover-Services erleichtert den Einrichtungsprozess von Benutzerkonten in E-Mail-Programmen. Benutzer brauchen damit keinen Servernamen oder Port-Nummer einzutragen: diese Informationen werden durch den Autodiscover-Service automatisch weitergegeben.

Setzen Sie einen CNAME-Eintrag für den Autodiscover-Service:

Tabelle 5: MX-Einträge setzen

TYP	PRIORITÄT	HOSTNAME	ZEIGT AUF	TTL
CNAME		autodiscover	autodiscover.hornetsecurity.com	1 Stunde



Der Autodiscover-Service ist erfolgreich eingerichtet worden.

Multi-Faktor-Authentifizierung

Alle Benutzer einer Domain, die durch 365 Total Protection geschützt wird, melden sich mit ihren Zugangsdaten aus Microsoft 365 im Control Panel an. Falls die Multi-Faktor-Authentifizierung bei Microsoft 365 aktiviert ist, wird diese auch im Control Panel verwendet.



365 Total Protection bestellen

Sie können 365 Total Protection (siehe [Über 365 Total Protection](#) auf Seite 6) direkt im Control Panel bestellen, falls Sie das Produkt nach der 14-tägigen Teststellung weiterhin nutzen möchten.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie in der Bereichsauswahl die Domain aus, für die Sie 365 Total Protection bestellen möchten.
3. Wählen Sie **365 Total Protection** aus.
4. Klicken Sie auf **Jetzt erwerben**.



Es erscheint eine Übersicht über die Anzahl Ihrer Postfächer und den Preis.

◀ Erwerb von 365 Total Protection

Sie sind im Begriff, 365 Total Protection im Abonnement Enterprise für 2 Postfächer zu einem monatlichen Nettopreis von 4,00€ pro Postfach zu bestellen. Der Gesamtpreis wird anhand der höchsten Postfach-Anzahl im Abrechnungsmonat berechnet.

Hier finden Sie unsere [Allgemeinen Geschäftsbedingungen](#) und die [Leistungsbeschreibung](#) zu 365 Total Protection Enterprise.

Erwerben

5. Klicken Sie auf **Erwerben**, um 365 Total Protection zu kaufen.



Sie erhalten eine Bestätigungs-E-Mail mit der Übersicht über Ihr Produkt.



365 Total Protection ist bestellt worden.



Anzeige der Anzahl von Postfächern, Lizenzen und Domains

Nach dem Onboarding wird bei Kunden von 365 Total Protection (siehe [Über 365 Total Protection](#) auf Seite 6) die Anzahl der Postfächer, Lizenzen und Domains unter **365 Total Protection > 365 Total Protection** angezeigt.



Abbildung 110: Anzahl von Postfächern, Lizenzen und Domains

Unter **Postfächer** wird die Anzahl der Postfächer angezeigt, die mit Microsoft 365 synchronisiert werden. Diese Anzahl enthält sowohl Postfächer von einfachen Benutzern als auch von Administratoren.

Unter **Lizenzen** wird die Anzahl der Lizenzen angezeigt, die abgerechnet werden. Die Lizenzanzahl richtet sich nach der Anzahl der Hauptpostfächer der Benutzer von 365 Total Protection, wobei Hauptpostfächer von Administratoren nicht mitgezählt werden. Die angezeigte Anzahl hat verschiedene Bedeutungen je nach Lizenzstatus:

- Während der Testphase von 365 Total Protection wird jeweils die Anzahl der Hauptpostfächer angezeigt, die bei der letzten Synchronisation mit Microsoft 365 übermittelt worden ist.
- Im ersten Monat nach dem Ende der Testphase oder dem Erwerb der kostenpflichtigen Version von 365 Total Protection wird die Anzahl der Hauptpostfächer angezeigt, die durch 365 Total Protection geschützt worden sind, als die Testphase abgelaufen ist oder die kostenpflichtige Version erworben worden ist. Diese Anzahl ist für die Abrechnung im ersten Monat maßgeblich.
- Ab dem zweiten Monat nach dem Ende der Testphase oder dem Erwerb der kostenpflichtigen Version von 365 Total Protection wird die maximale Anzahl der Hauptpostfächer angezeigt, die im laufenden Monat gleichzeitig durch 365 Total Protection geschützt worden sind. Diese Anzahl ist für die Abrechnung des laufenden Monats ausschlaggebend.

Unter **Domains** wird die Anzahl der Domains angezeigt, für die 365 Total Protection aktiviert ist. Diese Anzahl enthält sowohl die Hauptdomain als auch die Aliasdomains des Kunden.



Verwaltung von Postfächern

Im Modul **Kundeneinstellungen** > **Postfächer** können Postfächer verwaltet werden (siehe "**Kundeneinstellungen**" im Control-Panel-Handbuch). 365-Total-Protection-Kunden (siehe **Über 365 Total Protection** auf Seite 6) können sowohl Microsoft-365-Postfächer als auch manuell erstellte Postfächer anderer E-Mail-Anbieter verwalten (siehe **Postfachtypen**). Für Microsoft-365-Postfächer und für manuell erstellte Postfächer stehen im Control Panel unterschiedliche Funktionen zur Verfügung.

Im Gegensatz zu Microsoft-365-Postfächern werden manuell erstellte Postfächer (siehe "**Postfach hinzufügen**" im Control-Panel-Handbuch) nicht mit Microsoft 365 synchronisiert. Auf manuell erstellte Postfächer können alle Funktionen des Moduls **Postfächer** angewendet werden. Diesen Postfächern müssen sekundäre Umgebungen zugewiesen werden (siehe "**Sekundäre Umgebungen**" im Control-Panel-Handbuch).

Für Microsoft-365-Postfächer sind die Funktionen des Moduls **Postfächer** eingeschränkt:

- Microsoft-365-Postfächer können nicht manuell hinzugefügt werden.
- Microsoft-365-Postfächer können nicht entfernt werden.
- Die Grunddaten von Microsoft-365-Postfächern können nicht bearbeitet werden.
- Die Passwörter von Microsoft-365-Postfächern können nicht geändert werden.
- Microsoft-365-Postfächern können keine Aliasadressen zugewiesen werden.

Zur Unterscheidung zwischen Microsoft-365-Postfächern und manuell erstellten Postfächern bietet das Modul **Postfächer** 365-Total-Protection-Kunden zusätzlich die folgenden Postfachtypen für Microsoft-365-Postfächer:

- **Microsoft 365 Postfach**
- **Microsoft 365 Funktionspostfach**
- **Microsoft 365 Administrationspostfach**



Gruppenverwaltung im Control Panel

Im Control Panel können Postfächer zu Gruppen zusammengefasst werden (siehe "**Gruppen**"). Falls Gruppen vorhanden sind, können Einstellungen gruppenweit statt nur für einzelne Postfächer vorgenommen werden. Die Gruppenzugehörigkeit von Microsoft-365-Postfächern (siehe "**Postfachtypen**") wird ausschließlich in Microsoft 365 verwaltet. Microsoft-365-Postfächer können also nicht zu Gruppen aus dem Control Panel hinzugefügt werden. Es ist jedoch möglich, Gruppen aus Microsoft 365 im Control Panel abzubilden, indem im Control Panel gleichnamige Gruppen erstellt werden (siehe "**Gruppen aus Microsoft 365 im Control Panel synchronisieren**" auf Seite 114). Die Synchronisierung ist für Microsoft-365-Gruppen, Verteilerlisten, Sicherheitsgruppen und Sicherheitsgruppen mit E-Mail-Unterstützung möglich.

Bis auf einige Beschränkungen, die im Control-Panel-Handbuch beschrieben werden, sind für synchronisierte Gruppen dieselben Optionen wie für nicht synchronisierte Gruppen im Control Panel verfügbar (siehe "**Gruppen**"). Zusätzlich zu Microsoft-365-Postfächern können auch Postfächer aus sekundären Umgebungen (siehe "**Sekundäre Umgebungen**") zu synchronisierten Gruppen im Control Panel hinzugefügt werden. Diese Postfächer werden bei der Synchronisierung mit Microsoft 365 nicht berücksichtigt und bleiben erhalten.

Gruppen aus Microsoft 365 im Control Panel synchronisieren

Sie können Gruppen aus Microsoft 365 im Control Panel synchronisieren lassen (siehe "**Gruppenverwaltung im Control Panel**" auf Seite 114). Dadurch enthält das Control Panel Informationen über den Zusammenhalt von Ihren Microsoft-365-Gruppen, damit gruppenspezifische Einstellungen gemacht werden können.



Hinweis:

Die Synchronisierung ist für Microsoft-365-Gruppen, Verteilerlisten, Sicherheitsgruppen und Sicherheitsgruppen mit E-Mail-Unterstützung möglich.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie in der Bereichsauswahl den Kunden aus, für den Sie eine Gruppe mit Microsoft 365 synchronisieren möchten.
3. Navigieren Sie zu **Kundeneinstellungen > Gruppen**.



- 4. Klicken Sie auf **Hinzufügen**.



Ein Drop-down-Menü öffnet sich.

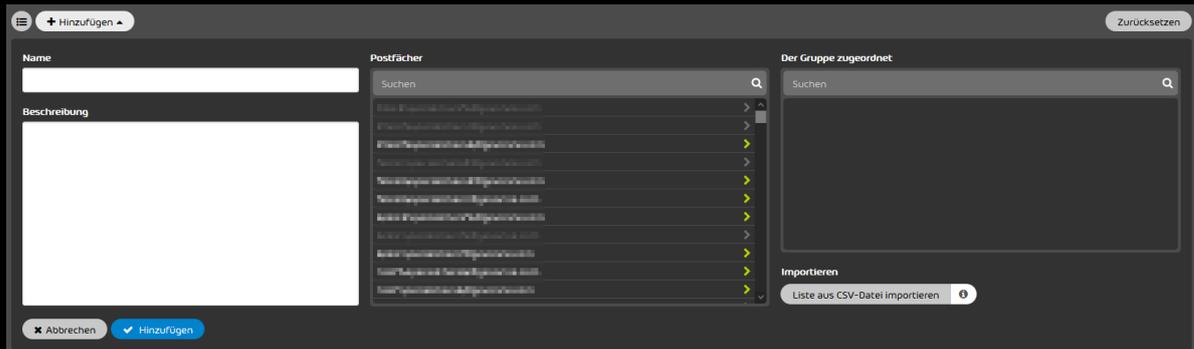


Abbildung 111: Neue Gruppe hinzufügen

- 5.

! Wichtig:

Der Name der Gruppe im Control Panel muss exakt mit dem Namen der Gruppe in Microsoft 365 übereinstimmen, damit das Control Panel die beiden Gruppen miteinander verbinden kann. Andernfalls kann die Gruppe nicht synchronisiert werden.

Geben Sie unter **Name** den Namen der Gruppe aus Microsoft 365 ein, die Sie im Control Panel synchronisieren möchten.

- 6. Klicken Sie auf **Hinzufügen**.



Die Gruppe wird zum Control Panel hinzugefügt. Bei der nächsten Synchronisierung werden die Gruppenmitglieder aus Microsoft 365 zur Gruppe hinzugefügt.

i Hinweis:

Die Daten im Control Panel werden mehrmals pro Stunde mit Microsoft 365 synchronisiert. Daher kann es mehrere Minuten dauern, bis die Daten der Gruppe im Control Panel verfügbar sind.



Eine Gruppe aus Microsoft 365 ist im Control Panel abgebildet und mit Microsoft 365 synchronisiert worden.



Zusammenspiel von 365 Total Protection mit weiteren Services

365 Total Protection enthält mehrere Services (siehe [Über 365 Total Protection](#) auf Seite 6), die von den Einstellungen von 365 Total Protection abhängig sind. Nachfolgend werden einige Zusammenhänge beschrieben.



Hinweis:

Für eine vollständige und aktuelle Liste der Features von 365 Total Protection siehe [365 Total Protection](#) auf der Website von Hornetsecurity.

- Administratoren müssen den Service Email Encryption gesondert aktivieren (siehe [Email Encryption](#) auf Seite 116).
- Administratoren müssen den Continuity Service, der nur in 365 Total Protection Enterprise enthalten ist, gesondert aktivieren (siehe [Continuity Service aktivieren \(Nur 365 Total Protection Enterprise\)](#) auf Seite 117).
- Für den Service Signature and Disclaimer werden Attribute aus dem Azure Active Directory, dem Verzeichnisdienst von Microsoft 365, weitgehend synchronisiert (siehe [Synchronisierte Attribute aus dem Azure Active Directory](#) auf Seite 119).

Email Encryption

Email Encryption ist Bestandteil der Produkte 365 Total Protection Business und Enterprise (siehe [Über 365 Total Protection](#) auf Seite 6). Email Encryption wird manuell aktiviert, da einige Einstellungen vorgenommen werden müssen. Folgen Sie dazu den Anweisungen im Kapitel ["Email Encryption"](#).



Wichtig:

Im Modul **Email Encryption** können Administratoren auf Kundenebene S/MIME-Zertifikate für Benutzer bestellen. Ein S/MIME-Zertifikat ist an die Hauptadresse eines Benutzers gebunden. Falls sich die E-Mail-Adresse des Benutzers ändert, verliert das S/MIME-Zertifikat für den Benutzer seine Gültigkeit.

Falls die E-Mail-Adresse eines Benutzers in Microsoft 365 umbenannt wird, wird die E-Mail-Adresse des Benutzers während der nächsten Synchronisation auch im Control Panel umbenannt. Die Administratoren des Kunden werden per E-Mail über die Umbenennung von synchronisierten Benutzern informiert, die bisher ein gültiges S/MIME-Zertifikat hatten. Für weitere Informationen siehe [S/MIME-Benutzer hinzufügen](#).

Continuity Service aktivieren (Nur 365 Total Protection Enterprise)

Sollte es zu einem Ausfall der Microsoft-Services kommen oder die Services temporär nicht erreichbar sein, beeinträchtigt dies ebenfalls den Zugriff auf Ihr E-Mail-Postfach. E-Mails können dann weder empfangen noch verschickt werden, was sich auf Ihre gesamten Geschäftsprozesse auswirken kann. Für solch einen Fall ist der Continuity Service Ihr Stand-by-System, das – innerhalb weniger Sekunden aktiviert – Ihren E-Mail-Verkehr am Laufen hält. Für weitere Informationen siehe [Über den Continuity Service](#).



Hinweis:

Der Continuity Service ist nur in 365 Total Protection Enterprise enthalten und Sie müssen ihn manuell aktivieren und einige Einstellungen vornehmen.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie die Domain in der Bereichsauswahl aus.
3. Navigieren Sie zu > .
4. Betätigen Sie den Schalter .

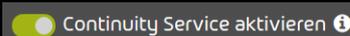


Abbildung 112: Continuity Service aktivieren



Ein Bestätigungsfenster wird angezeigt.



5.

Achtung:

Sobald der Continuity Service aktiviert wird, startet eine 30-tägige kostenfreie Testphase. Nach Ende der Testphase wird der Service kostenpflichtig.

Der Continuity Service wird pro Kunde berechnet, nicht pro Benutzer.

Wichtig:

Administratoren können den Continuity Service nicht selbst deaktivieren. Nur der Support kann den Continuity Service für eine Domain deaktivieren.

Klicken Sie auf .

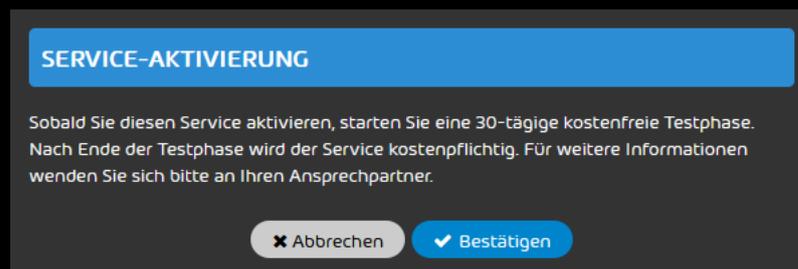


Abbildung 113: Bestätigen



Der Continuity Service wird aktiviert.

6. Wählen Sie aus, für welche Benutzer Sie den Continuity Service aktivieren möchten. Sie haben zwei Optionen:

- **Alle Benutzer**: Alle Benutzer der Domain werden zum Continuity Service hinzugefügt. Für weitere Schritte siehe [#unique_49](#).
- **Nur ausgewählte Benutzer**: Nur einzelne Benutzer der Domain werden zum Continuity Service hinzugefügt. Für weitere Schritte siehe [#unique_50](#).

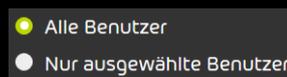


Abbildung 114: Option auswählen



Der Continuity Service ist aktiviert worden.



Synchronisierte Attribute aus dem Azure Active Directory

Mit dem Azure Active Directory von Microsoft werden bestimmte Attribute für Signature and Disclaimer (siehe [#unique_51](#)) synchronisiert.

! Wichtig:

Es ist nicht möglich, die Synchronisation der Attribute gleichzeitig über Microsoft 365 und LDAP (siehe "[LDAP-Verbindung](#)") zu verwenden. Für Microsoft-365-Postfächer (siehe [Postfachtypen](#)) werden nur die Attribute aus der unten stehenden Tabelle synchronisiert. Für manuell erstellte Postfächer werden die Grunddaten (siehe [#unique_52](#)) verwendet. Die LDAP-Attribute werden nicht synchronisiert und können nicht verwendet werden.

Folgende Attribute werden für Microsoft-365-Postfächer synchronisiert und können für die Erstellung von Signaturen und Disclaimern verwendet werden:

AD-Variable	Bedeutung
countryCode	Land/Region
department	Abteilung
displayName	Anzeigename – kompletter Name
givenName	Vorname
info	Jobtitel/Position
I (kleines L)	Stadt
mail	E-Mail-Adresse

i Hinweis:

Das Feld title wird vielfach anders verwendet. Deshalb wird hier für das LDAP-Attribut Title (Jobtitel/Position) die Bezeichnung info verwendet.



HORNETSECURITY

Zusammenspiel von 365 Total Protection mit
weiteren Services

AD-Variable	Bedeutung
mobile	Mobiltelefonnummer
postalCode	Postleitzahl
sn	Nachname
st	Bundesland/Kanton
streetAddress	Straße
telephoneNumber	Telefonnummer



Offboarding nach Beenden der Teststellung oder Kündigung

Falls ein Kunde die Teststellung von 365 Total Protection (siehe [Über 365 Total Protection](#) auf Seite 6) beendet hat und das Produkt nicht weiter verwenden möchte oder er 365 Total Protection zu einem bestimmten Zeitpunkt gekündigt hat, muss er einige Einstellungen in seiner Microsoft-365-Konfiguration rückgängig machen, damit seine E-Mails weiterhin zugestellt werden.

1. Der Kunde muss den Connector für den eingehenden E-Mail-Verkehr löschen oder deaktivieren. (Firewall-Einstellung)
2. Falls der Kunde den ausgehenden E-Mail-Verkehr umgestellt hat, muss er auch diesen Connector löschen oder deaktivieren. (Relaying)



Hinweis:

Für Informationen zum Löschen oder Deaktivieren von Connectoren in der Microsoft-365-Umgebung siehe [Connector löschen oder deaktivieren](#) auf Seite 121.

3. Der Kunde muss die MX-Einträge in der DNS-Zone seiner Domains löschen.

Anschließend werden die E-Mails des Kunden nicht mehr über unsere Services geleitet.

Administratoren auf Partnerebene können den Kunden aus dem Control Panel löschen (siehe [Kunden löschen](#) auf Seite 122).

Connector löschen oder deaktivieren

Falls Sie 365 Total Protection (siehe [Über 365 Total Protection](#) auf Seite 6) nicht mehr verwenden möchten (siehe [Offboarding nach Beenden der Teststellung oder Kündigung](#) auf Seite 121), müssen Sie die Connectoren für den eingehenden und ausgehenden E-Mail-Verkehr in Microsoft 365 löschen oder deaktivieren.

1. Öffnen Sie Office.com und melden Sie sich mit den administrativen Benutzerdaten an.
2. Navigieren Sie zu **Administrator > Admin Center > Exchange**.
3. Wählen Sie **E-Mail-Fluss** und anschließend den Tab **Connectors** aus.
4. Wählen Sie den entsprechenden Connector aus.



5. Sie haben die Wahl, den Connector zu löschen oder zu deaktivieren:
- Um den Connector zu löschen, klicken Sie auf **Entfernen**.
 - Um den Connector zu deaktivieren, klicken Sie in der Übersicht des Connectors auf **Deaktivieren**.

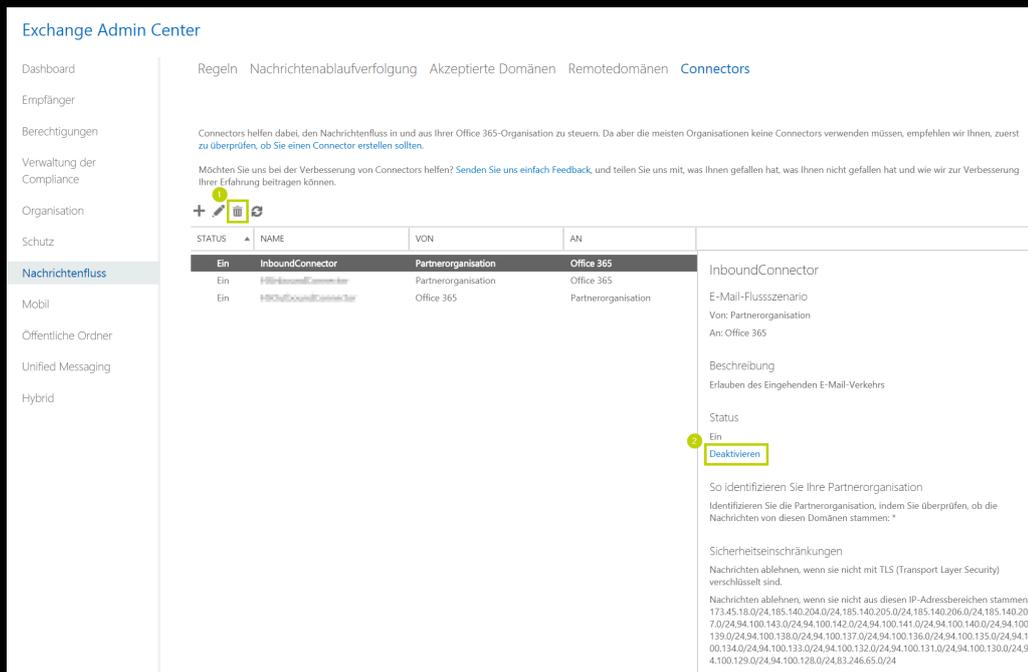


Abbildung 115: Connector löschen oder deaktivieren

6. Bestätigen Sie den Hinweis mit **Ja**.



Ein Connector ist gelöscht oder deaktiviert worden.

Kunden löschen

Als Administrator auf Partnerebene können Sie einen bestehenden 365-Total-Protection-Kunden (siehe **Über 365 Total Protection** auf Seite 6) während oder nach Ablauf der Testphase löschen.



ACHTUNG:

Sobald Sie einen Kunden löschen, werden alle Kundendaten aus dem Control Panel gelöscht. Die Kundendaten können nicht wiederhergestellt werden. Vergewissern Sie sich, dass Sie den Kunden löschen möchten.



1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie in der Bereichsauswahl den Partner aus, dessen Kunden Sie löschen möchten.
3. Navigieren Sie zu **Service Dashboard**.
4. Wählen Sie den Tab **Service Dashboard** aus.
5. Klicken Sie auf den Menüpfel neben dem Kunden, den Sie löschen möchten.

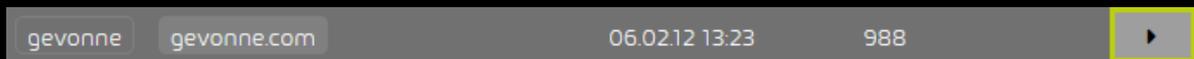


Abbildung 116: Menü öffnen



Ein Menü öffnet sich.

6. Klicken Sie auf **Ausgewählten Kunden löschen**.

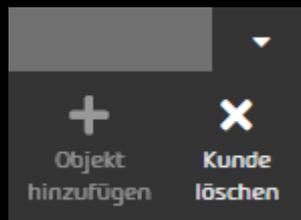


Abbildung 117: Kunde löschen



Eine Warnmeldung wird angezeigt.



7. Klicken Sie auf **Bestätigen**.

KUNDE LÖSCHEN

Vorsicht: Sie sind im Begriff, den Kunden talltara.com zu löschen. Alle Daten des Kunden einschließlich der Backup-Daten werden gelöscht. Dieser Vorgang kann nicht rückgängig gemacht werden.

Falls Sie fortfahren möchten, geben Sie bitte den Namen des Kunden ein, den Sie löschen möchten:

Abbildung 118: Bestätigen



Der Kunde wird gelöscht.



Der 365-Total-Protection-Kunde ist gelöscht worden.

Numerische Stichwörter

- 365 Total Backup
 - konfigurieren [14](#), [84](#)
- 365 Total Protection
 - Erklärung [6](#)
 - Postfachmigration, *Siehe* Postfachmigration Erklärung
 - Upgrade [25](#)
 - upgraden [25](#)

A

- abschließen
 - Postfachmigration, *Siehe* Postfachmigration abschließen
- aktivieren
 - Continuity Service [117](#)
- anpassen
 - MX-Eintrag [96](#)
 - SPF-Eintrag [108](#)
- ausfüllen
 - Onboarding-Formular [10](#)
- Autodiscover
 - konfigurieren [110](#)

B

- Berechtigungen
 - zum Lesen und Verwalten von Postfächern in Microsoft 365 erteilen, *Siehe* Microsoft 365 Berechtigungen zum Lesen und Verwalten von Postfächern erteilen

C

- CNAME-Eintrag
 - hinzufügen, *Siehe* Autodiscover konfigurieren
- Connector
 - deaktivieren [121](#)
 - löschen [121](#)
- Continuity Service
 - aktivieren [117](#)

D

- deaktivieren
 - Connector [121](#)
 - Drosselung der Exchange-Webdienste, *Siehe* Exchange-Webdienste Drosselung deaktivieren
 - Spamfilter von Microsoft 365, *Siehe* Microsoft 365 Spamfilter deaktivieren
- DNS-Einstellung
 - konfigurieren, *Siehe* MX-Eintrag anpassen
- Dokumentation
 - Hinweise [4](#), [41](#)
 - Symbole [4](#), [41](#)

E

Einschränkungen

Postfachmigration, *Siehe* Postfachmigration Einschränkungen

Erklärung

365 Total Protection, *Siehe* 365 Total Protection Erklärung

Postfachmigration, *Siehe* Postfachmigration Erklärung

Sicherheitshinweise [4, 41](#)

Warnhinweise [4, 41](#)

erlauben

Zugriff auf Exchange-Webdienste, *Siehe* Exchange-Webdienste Zugriff erlauben

erstellen

Kunde [9](#)

Onboarding-Link [8](#)

Rollengruppe auf Exchange-Server, *Siehe* Postfachmigration Rollengruppe auf Exchange-Server erstellen

Rollengruppe in Microsoft 365, *Siehe* Microsoft 365 Rollengruppe erstellen

erteilen

Berechtigungen zum Lesen und Verwalten von Postfächern in Microsoft 365, *Siehe* Microsoft 365 Berechtigungen zum Lesen und Verwalten von Postfächern erteilen

Europa

MX-Einträge, *Siehe* MX-Einträge Europa

Exchange Online

Organisationsanpassungen freischalten [101](#)

Exchange-Server

Rollengruppe erstellen, *Siehe* Postfachmigration Rollengruppe auf Exchange-Server erstellen

Exchange-Webdienste

Drosselung deaktivieren [63](#)

Zugriff erlauben [61](#)

F

freischalten

Organisationsanpassungen, *Siehe* Exchange Online Organisationsanpassungen freischalten

H

Hinweise

Dokumentation [4, 41](#)

hinzufügen

CNAME-Eintrag [110](#)

K

Kanada

MX-Einträge, *Siehe* MX-Einträge Kanada

konfigurieren

365 Total Backup, *Siehe* 365 Total Backup konfigurieren

Autodiscover [110](#)

DNS-Einstellung [96](#)

Kunde

erstellen [9](#)

löschen [122](#)

Onboarding, *Siehe* Kunde erstellen

Kündigung, *Siehe* Offboarding

L

Link

erstellen, *Siehe* Onboarding-Link erstellen

löschen

Connector [121](#)

Kunde [122](#)

M

Microsoft 365

Berechtigungen zum Lesen und Verwalten von Postfächern erteilen [57](#)

Rollengruppe erstellen [53](#)

Spamfilter deaktivieren [102](#)

Migration

Postfächer [65](#)

migrieren

Postfächer, *Siehe* Postfächer migrieren

Multi-Faktor-Authentifizierung [110](#)

MX-Eintrag

anpassen [96](#)

MX-Einträge

Europa [98](#)

Kanada [99](#)

USA [98](#)

O

Offboarding [121](#)

Onboarding

Kunde, *Siehe* erstellen Kunde

Onboarding-Formular

ausfüllen [10](#)

Onboarding-Link

erstellen [8](#)

Organisationsanpassungen

freischalten, *Siehe* Exchange Online Organisationsanpassungen freischalten

P

Postfächer

Migration [65](#)

migrieren [73](#)

Voraussetzungen für Postfachmigration, *Siehe* Postfachmigration Voraussetzungen zu Postfächern

Postfachmigration

abschließen [82](#)

Durchführung, *Siehe* Postfächer Migration

Einschränkungen [45](#)

Erklärung [43](#)

Rollengruppe auf Exchange-Server erstellen [48](#)

Umgebung validieren [66](#)

Validierung einer Umgebung zurücksetzen [71](#)

Voraussetzungen [46](#)

Voraussetzungen zu Postfächern [47](#)

R

Rollengruppe
in Microsoft 365 erstellen, *Siehe* Microsoft 365 Rollengruppe erstellen

S

Sicherheitshinweise
Erklärung [4, 41](#)
Spamfilter
deaktivieren, *Siehe* Microsoft 365 Spamfilter deaktivieren
SPF-Eintrag
anpassen [108](#)
Symbole
Dokumentation [4, 41](#)

U

Umgebung
validieren, *Siehe* Postfachmigration Umgebung validieren
Upgrade
365 Total Protection, *Siehe* 365 Total Protection Upgrade
upgraden
365 Total Protection, *Siehe* 365 Total Protection upgraden
USA
MX-Einträge, *Siehe* MX-Einträge USA

V

validieren
Umgebung, *Siehe* Postfachmigration Umgebung validieren
Validierung
zurücksetzen, *Siehe* Postfachmigration Validierung einer Umgebung zurücksetzen
Voraussetzungen
Postfächer für Postfachmigration, *Siehe* Postfachmigration Voraussetzungen zu Postfächern
Postfachmigration, *Siehe* Postfachmigration Voraussetzungen

W

Warnhinweise
Erklärung [4, 41](#)

Z

Zugriff
auf Exchange-Webdienste erlauben, *Siehe* Exchange-Webdienste Zugriff erlauben
zurücksetzen
Validierung einer Umgebung, *Siehe* Postfachmigration Validierung einer Umgebung zurücksetzen
Zwei-Faktor-Authentifizierung, *Siehe* Multi-Faktor-Authentifizierung
Zwei-Faktor-Authentisierung, *Siehe* Multi-Faktor-Authentifizierung
zweistufige Überprüfung, *Siehe* Multi-Faktor-Authentifizierung



HORNETSECURITY

Hornetsecurity GmbH
Am Listholze 78 | 30177 Hannover
Tel.: +49 511 515 464-0 | info@hornetsecurity.com
www.hornetsecurity.com