

# M07\_Administrator-Einstellungen im Power BI Verwaltungsportal

In diesem Lab geht es um einen strukturierten Überblick über die wesentlichen Administrator-Einstellungen im Power BI Verwaltungsportal. Dieses Lab richtet sich an Administratoren, die den Power BI Service verwalten und kontrollieren möchten.

---

## Lab: Power BI Service verwalten – Überblick über das Verwaltungsportal

### 1. Zielsetzung

In diesem Lab lernen Sie:

- Den Zugang zum Power BI Verwaltungsportal und dessen grundlegende Navigation.
- Die wichtigsten Tenant-Einstellungen kennen, die steuern, welche Funktionen den Endanwendern zur Verfügung stehen.
- Wie Überwachungs-, Audit- und Sicherheitsfunktionen eingesetzt werden, um den Betrieb und die Compliance des Power BI Service zu gewährleisten.

### 2. Voraussetzungen

- **Power BI-Konto mit Administratorrechten:** Stellen Sie sicher, dass Sie ein entsprechendes Konto besitzen.
- **Zugang zum Power BI Service:** Melden Sie sich unter [powerbi.com](https://powerbi.com) an.
- **Grundkenntnisse in Power BI:** Basiswissen im Umgang mit Berichten, Dashboards und Datenmodellen ist hilfreich.
- Zugriff auf das **Power BI Admin-Portal**

### 3. Lab-Schritte

#### Schritt 1: Zugang zum Verwaltungsportal

- **Anmeldung:** Logge Dich in den Power BI Service ein.
- **Navigation:** Klicken Sie auf das **Zahnradsymbol** oben rechts und wähle „**Verwaltungsportal**“ aus.  
**Ziel:** Einen ersten Überblick über das Dashboard und die verfügbaren Bereiche erhalten.

## Schritt 2: Überblick über Tenant-Einstellungen

- **Mandanteneinstellungen öffnen:** Im Admin-Portal findest Du den Menüpunkt „Mandanteneinstellungen“.

Verwaltungsportal



## Tenant Settings (Mandanteneinstellungen)

Hier legen Sie fest, welche Aktionen Benutzer im Power BI Service durchführen dürfen.

### Wichtige Einstellungen:

#### A. Einstellungen für Export und Freigabe

- **Export von Daten:**  
Steuern Sie, ob Benutzer Daten aus Berichten exportieren dürfen (z.B. nach Excel, PDF oder als PBIT-Datei).

**Empfehlung:** Beschränken Sie den Export sensibler Daten.



- **Freigabe von Inhalten:**  
Legen Sie fest, ob Benutzer Berichte und Dashboards für externe Benutzer freigeben können.  
**Empfehlung:** Aktivieren Sie die Option „Nur bestimmte Sicherheitsgruppen“, um Kontrolle zu behalten.

**Erkunden der Kategorien:** Gehen Sie die einzelnen Kategorien durch, z. B.:

- **Externe Datenfreigabe:** Bestimmen Sie, wie Berichte und Dashboards innerhalb und außerhalb des Unternehmens geteilt werden können.

## Einstellungen für Export und Freigabe

### Externe Datenfreigabe Für die gesamte Organisation deaktiviert

Benutzer\*innen können einen schreibgeschützten Link zu in OneLake gespeicherten Daten mit Mitarbeitenden außerhalb Ihrer Organisation teilen. Wenn Sie ihnen die entsprechende Berechtigung erteilen, können Benutzer\*innen einen Link zu Daten in Lakehouses und zusätzlichen Fabric-Elementen freigeben. Mitarbeiter\*innen, die den Link erhalten, können die Daten sowohl innerhalb ihrer eigenen Fabric-Mandanten als auch über ihre eigenen Fabric-Mandanten hinaus anzeigen, freigeben und darauf aufbauen, indem sie die Lizenzen und Kapazitäten ihrer Organisation verwenden. [Weitere Informationen](#)

☐ Deaktiviert

ⓘ Die Verwendung freigegebener Daten innerhalb eines Empfängermandanten ist durch keine Richtlinien innerhalb Ihres Mandanten eingeschränkt, wie z. B. bedingter Zugriff, Information Protection, Microsoft Cloud App Security usw. Freigegebene Daten können auch außerhalb der Region verarbeitet werden, in der sie gespeichert sind.

Übernehmen

Abbrechen

- **App-Einstellungen:** Steuern Sie, wie Inhalte bereitgestellt und verwaltet werden.

### Veröffentlichen von Apps für die gesamte Organisation Für die gesamte Organisation aktiviert

Benutzer in der Organisation können Apps für die gesamte Organisation veröffentlichen.

☒ Aktiviert

Übernehmen für:

☒ Gesamte Organisation

☐ Sicherheitsgruppen angeben

☐ Ausgenommen spezifische Sicherheitsgruppen

Übernehmen

Abbrechen

- **Dokumentation:** Notieren Sie sich die Wirkung und empfohlene Best Practices zu den einzelnen Einstellungen.

## B. Integration mit anderen Diensten

- **Power BI-Integration in Microsoft Teams:**  
Ermöglichen oder blockieren Sie die Einbettung von Power BI-Inhalten in Teams.

### Microsoft Teams-Integration aktivieren Für die gesamte Organisation aktiviert

Mithilfe dieser Einstellung können Personen in der Organisation auf Features zuzugreifen, die mit der Integration von Microsoft Teams und Power BI verbunden sind. Dazu gehören das Starten von Teams-Funktionen aus dem Power BI-Dienst (beispielsweise Chats), die Power BI-App für Teams und der Empfang von Power BI-Benachrichtigungen in Teams. Arbeiten Sie mit Ihrem Teams-Administrator zusammen, um die Teams-Integration vollständig zu aktivieren oder zu deaktivieren.

☒ Aktiviert

Übernehmen für:

☒ Gesamte Organisation

☐ Sicherheitsgruppen angeben

☐ Ausgenommen spezifische Sicherheitsgruppen

Übernehmen

Abbrechen

- **SharePoint- und OneDrive-Integration:**  
Steuern Sie, ob Berichte in SharePoint oder OneDrive gespeichert werden können.

⚠ Benutzer können in OneDrive und SharePoint gespeicherte Power BI-Dateien anzeigen (Vorschau)  
Für die gesamte Organisation aktiviert

Benutzer in der Organisation können Power BI-Dateien anzeigen, die in OneDrive for Business- oder SharePoint-Dokumentbibliotheken gespeichert sind. Die Berechtigungen zum Speichern und Freigeben Power BI-Dateien in OneDrive- und SharePoint-Dokumentbibliotheken werden durch Berechtigungen gesteuert, die in OneDrive und SharePoint verwaltet werden. [Weitere Informationen](#)

☒ Aktiviert

🔒 Diese Einstellung gilt für die gesamte Organisation.

Übernehmen

Abbrechen

## C. Entwickler- und API-Einstellungen

- **APIs und Embedded Analytics:**  
Erlauben Sie die Nutzung der Power BI-REST-APIs für automatisierte Workflows.
- **Benutzerdefinierte Visuals:**  
Beschränken Sie die Verwendung benutzerdefinierter Visuals aus dem Marketplace, um Sicherheitsrisiken zu minimieren.

⚠ Downloads von benutzerdefinierten Visuals zulassen  
Für die gesamte Organisation deaktiviert

Wenn Sie diese Einstellung aktivieren, können benutzerdefinierte Visuals alle für das Visual verfügbaren Informationen (z. B. zusammengefasste Daten und visuelle Konfiguration) mit Benutzereinstimmung herunterladen. Dies ist nicht von Downloadeinschränkungen betroffen, die in den Export- und Freigabeeinstellungen Ihrer Organisation gelten. [Weitere Informationen](#)

☐ Deaktiviert

🔒 Wenn der Bericht oder das zugrunde liegende semantische Modell über eine angewendete Vertraulichkeitsbezeichnung verfügt, werden die Bezeichnung und die zugehörigen Schutzeinstellungen (z. B. die Verschlüsselung) nicht auf die exportierte Datei angewendet. [Weitere Informationen](#)

Übernehmen

Abbrechen

## D. Kapazitätseinstellungen (Premium)

- **Dedizierte Kapazitäten verwalten:**  
Weisen Sie Arbeitsbereiche dedizierten Kapazitäten zu, um Leistung und Ressourcen zu optimieren.

---

## Sicherheit und Compliance

### A. Datensicherheit

- **Datenklassifizierung:**  
Aktivieren Sie die **Sensitivity Labels** (Empfindlichkeitslabels) aus Microsoft Purview, um Daten nach Vertraulichkeit zu kennzeichnen (z.B. „Vertraulich“, „Öffentlich“).

- ⚡ Vertraulichkeitsbezeichnungen aus Datenquellen auf Daten in Power BI anwenden  
Für die gesamte Organisation deaktiviert

Es werden nur Vertraulichkeitsbezeichnungen aus unterstützten Datenquellen angewendet. In der Dokumentation finden Sie Details zu den unterstützten Datenquellen und zur Anwendung ihrer Vertraulichkeitsbezeichnungen in Power BI. [Informationen zu unterstützten Datenquellen](#)

☐ Deaktiviert

🔔 In Zukunft werden möglicherweise zusätzliche Datenquellen unterstützt. Wenn dieses Feature aktiviert ist, werden die Vertraulichkeitsbezeichnungen aus diesen Datenquellen auch in Power BI angewendet.

Übernehmen

Abbrechen

## B. Audit Logs

- **Aktivieren Sie die Überwachungsprotokolle:**

Verfolgen Sie Benutzeraktivitäten wie Anmeldungen, Datenfreigabe oder Berichtsänderungen.

*Navigationspfad:* Admin-Portal > „**Überwachungsprotokolle**“ > Aktivieren und in Microsoft 365 Compliance Center anzeigen.

Überwachungsprotokolle werden im Microsoft 365 Admin Center verwaltet.

Wechseln Sie dorthin, um Protokolle zu Mandantenaktivität und Exporten anzuzeigen.

Die Überwachung ist nur in bestimmten Regionen verfügbar, während sich das Feature in der Vorschauphase befindet. [Weitere Info](#)

[Zu Microsoft 365 Admin Center wechseln](#)

---

## Workspace-Einstellungen

- **Workspace-Erstellung:**

Steuern Sie, wer neue Arbeitsbereiche erstellen darf (z.B. nur Administratoren oder alle Benutzer).

*Empfehlung:* Beschränken Sie dies auf erfahrene Benutzer, um Chaos zu vermeiden.

Arbeitsbereichseinstellungen

- ⚡ Arbeitsbereiche erstellen  
Für die gesamte Organisation aktiviert

Benutzer\*innen in der Organisation können App-Arbeitsbereiche für die Zusammenarbeit an Dashboards, Berichten und anderen Inhalten erstellen. Selbst wenn diese Einstellung deaktiviert ist, wird ein Arbeitsbereich erstellt, wenn eine Vorlagen-App installiert wird.

☒ Aktiviert

Übernehmen für:

☒ Gesamte Organisation

☐ Sicherheitsgruppen angeben

☐ Ausgenommen spezifische Sicherheitsgruppen

Übernehmen

Abbrechen

---

## Nutzungsmetriken und Berichte

- **Nutzungsüberwachung:**

Analysieren Sie, wie Berichte und Dashboards genutzt werden (Admin-Portal >

## „Nutzungsmetriken“).

**Wichtig:** Identifizieren Sie inaktive Inhalte, um Kosten zu optimieren.

### Nutzungsmetriken

Diese Seite wird mit einer neuen Oberfläche für Überwachung und Metriken aktualisiert. In der Zwischenzeit finden Sie das neueste Dashboard im Arbeitsbereich für die Administratorüberwachung.

Um zum Arbeitsbereich für die Administratorüberwachung zu navigieren, wählen Sie den Link unten aus.

[Arbeitsbereich für die Administratorüberwachung öffnen](#) 

---

## Datenquellen und Gateways

- **Gateway-Verwaltung:**  
Verwalten Sie On-Premises-Gateways, um lokale Datenquellen mit Power BI zu verbinden.  
*Navigationspfad:* Admin-Portal > „**Gateways verwalten**“.
- **Datenquellen-Zertifikate:**  
Stellen Sie sicher, dass SSL-Zertifikate für sichere Verbindungen zu Datenbanken gültig sind.

---

## Benutzer- und Lizenzverwaltung

- **Lizenzen zuweisen:**  
Verwalten Sie Power BI Pro- und Premium-Lizenzen über das **Microsoft 365 Admin Center**.
- **Benutzerrollen:**  
Weisen Sie Rollen wie **Berichts-Ersteller**, **Mitwirkender** oder **Leser** zu, um Zugriffsrechte zu steuern.

---

## Best Practices und häufige Fehler

### Best Practices:

1. **Least Privilege-Prinzip:** Gewähren Sie nur die notwendigsten Berechtigungen.
2. **Regelmäßige Audits:** Überprüfen Sie monatlich Freigaben, Nutzungsdaten und Compliance-Einstellungen.
3. **Schulungen:** Schulen Sie Benutzer im Umgang mit Sensitivity Labels und Sicherheitsrichtlinien.

### Häufige Fehler:

- **Zu offene Freigabe:** Unkontrollierte Freigabe externer Links führt zu Datenlecks.

- **Veraltete Gateways:** Nicht aktualisierte Gateways verursachen Verbindungsfehler.
  - **Fehlende Backup-Strategie:** Sichern Sie kritische Berichte regelmäßig über **Power BI Deployment Pipelines**.
- 

### Schritt 3: Verwaltung von Kapazitäten (bei Power BI Premium)

- **Kapazitätsüberwachung:** Falls in Ihrer Organisation Power BI Premium verwendet wird, öffnen Sie den Bereich „**Kapazitätseinstellungen**“.
- **Leistungsparameter:** Überwachen Sie die Auslastung, Zuweisung und Leistungsdaten Ihrer Kapazitäten.
- **Optimierung:** Identifizieren Sie Engpässe und passen Sie ggf. die Zuweisungen an, um eine optimale Performance zu gewährleisten.

### Schritt 4: Praktische Änderungen testen

- **Änderungen vornehmen:** Wähle einzelne Einstellungen aus, ändere diese (idealerweise in einer Testumgebung) und beobachte die Auswirkungen.
- **Dokumentation:** Halte fest, welche Änderungen welchen Effekt hatten – dies dient als wertvolle Referenz für zukünftige Anpassungen.

### Schritt 6: Zusammenfassung

- **Erkenntnisse zusammenfassen:** Erstelle einen kurzen Bericht, in dem Du die wichtigsten Einstellungen und deren Auswirkungen zusammenfasst.
  - **Diskussion:** Überlege, welche Einstellungen in Deiner Organisation besonders relevant sind und welche Best Practices angewendet werden können.
  - **Weiterführende Schritte:** Plane, wie regelmäßige Überprüfungen der Tenant-Einstellungen und der Überwachungstools in den administrativen Alltag integriert werden können.
- 

### Fazit

Dieses Lab bietet Dir einen praxisnahen Einstieg in die Verwaltung des Power BI Service über das Admin-Portal. Mit dem gewonnenen Überblick kannst Du sicherstellen, dass die für Deine Organisation wichtigen Einstellungen optimal konfiguriert sind, um sowohl die Sicherheit als auch die Leistungsfähigkeit des Systems zu gewährleisten.