Verzeichnisschutz für Middleware-Webservice

In diesem Artikel erfahren Sie, wie Sie einen Verzeichnisschutz für den Middleware-Webservice anlegen, damit kein unbefugter Zugriff auf die Schnittstelle möglich ist. Ziel ist es, den Zugriff auf den Webservice von außen zu sperren, aber den Zugriff für die Middleware weiterhin zu ermöglichen.

> ⚠ **Beachten Sie:**
>
> Das Vorgehen unterscheidet sich je nach Hoster und je nach Shopsystem! Sprechen Sie diese Änderung auf jeden Fall mit dem Betreiber des Servers und mit Ihrem Shopbetreuer ab und testen Sie, ob nach der Einrichtung Ihr Shop wie gewohnt funktioniert.

Verzeichnisschutz für alle Shop-Systeme außer Magento

Die Dateien des Middleware-Webservices werden in Ihrem Shop-Verzeichnis an folgender Stelle abgelegt:

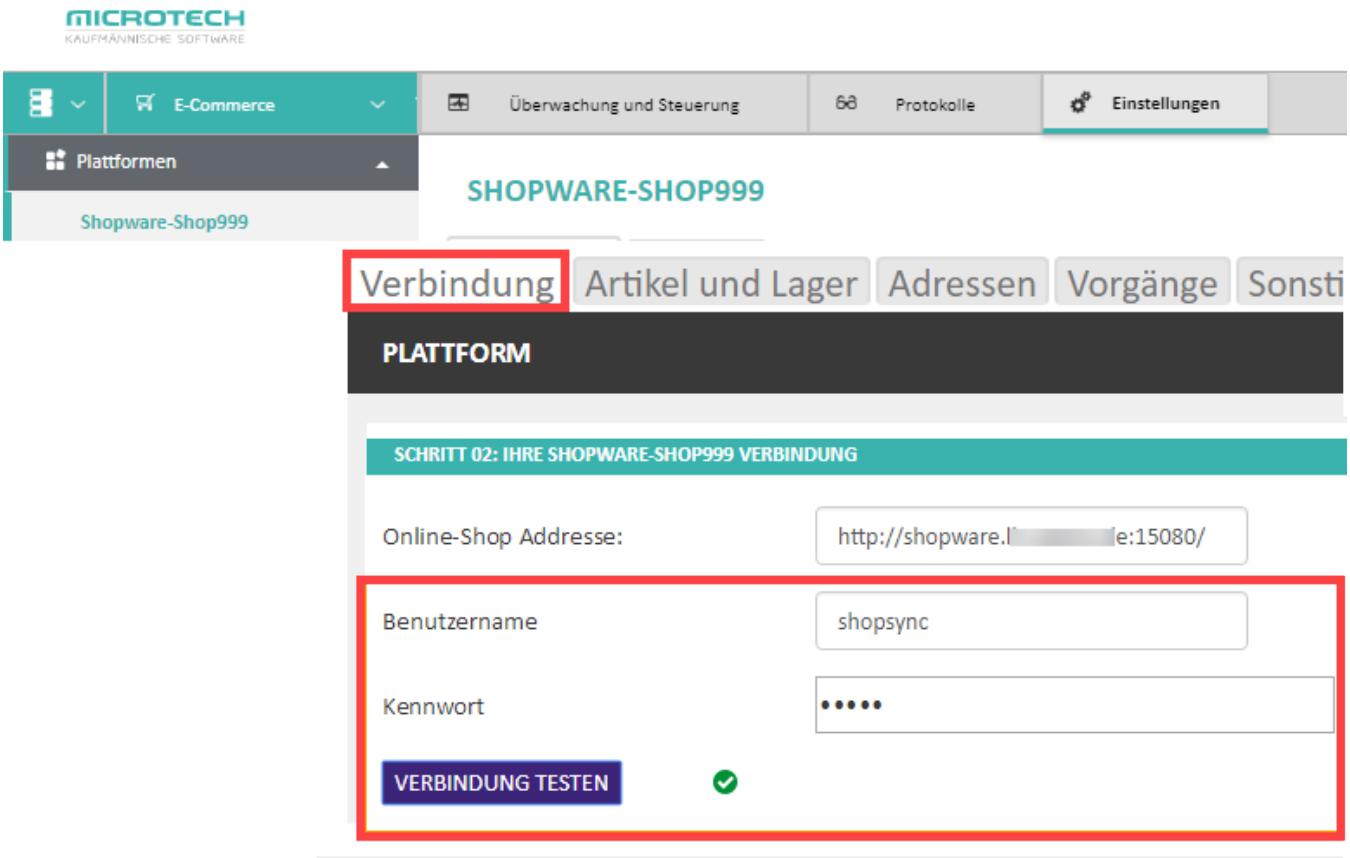
`.../[Ihr Shopverzeichnis]/`**`shopsync`**

Das Verzeichnis ***shopsync*** sollte mit einem Verzeichnisschutz versehen werden.

Den Verzeichnisschutz müssen Sie in der Regel über Ihren Account beim Provider einrichten. Wenden Sie sich hierzu bei Fragen an Ihren Shop-Betreuer oder den Provider selbst.

Ansonsten besteht auch die Möglichkeit für das *shopsync*-Verzeichnis eine .htaccess- und passende .htpasswd-Datei zu hinterlegen. Auch hierzu wenden Sie sich bei Fragen bitte an Ihren Shop-Betreuer.

Nachdem der Verzeichnisschutz angelegt wurde, müssen Sie Benutzernamen und Kennwort in der Middleware hinterlegen. Wechseln Sie in der Middleware in folgenden Bereich: **E-Commerce** > **[Profil Ihres Shops]** > **Einstellungen** > **Verbindung.** Tragen Sie an dieser Stelle die Daten bei *Schritt 02* ein und klicken Sie auf **Verbindung testen**:



Wenn die eingegebenen Daten korrekt sind wird durch das grüne Symbol eine entsprechende Bestätigung ausgegeben.

Verzeichnisschutz für Magento

Für das Shopsystem Magento gehen Sie wie folgt vor:

1. Ergänzen Sie die Datei **.htaccess** im Stammverzeichnis des Shops am unteren Ende mit folgenden Einstellungen:
   .htaccess

```
############################################
## microtech Middleware-Webservice Access control - BEGIN

      AuthType Basic
      AuthName "ShopSync - Zugangskontrolle"
      AuthUserFile "<Pfad zur Datei>/.htpasswd"
      Require valid-user

      ## Deny access for any shopsync uri
      SetEnvIf Request_URI "/shopsync/" DENY_ACCESS=1
      ## Allow WSDL path for anyone
      SetEnvIf Request_URI "/shopsync/.*/wsdl" !DENY_ACCESS
      ## Server's remote address for internal access
      SetEnvIf Remote_Addr "<interne IP-Adresse>" !DENY_ACCESS
      ## ERP's remote address to allow access
      SetEnvIf Remote_Addr "<externe IP-Adresse>" !DENY_ACCESS

      Order Allow,Deny
      Allow from all
      Deny from env=DENY_ACCESS
      Satisfy any

## microtech Middleware-Webservice Access control - END
############################################
```

2. Passen Sie die Angaben in spitzen Klammern (<Pfad zur Datei>, <interne IP-Adresse>, <externe IP-Adresse>) in Abstimmung mit Ihrem Shopbeteuer an.

Zur Erklärung:

1. **Basis** - Dies ist der auf jeden Fall notwendige Teil, der alle URIs der Middleware schützt. Der WSDL-Pfad muss explizit für den Server, auf dem der Shop läuft, freigegeben werden, um die internen Aufrufe des SOAP-Servers nicht zu blockieren. Optional kann man den WSDL-Pfad auch generell freigeben.
   ## Deny access for any shopsync uri
   SetEnvIf Request_URI "/shopsync/" DENY_ACCESS=1
   ## Allow WSDL path for anyone (optional)
   #SetEnvIf Request_URI "/shopsync/./wsdl" !DENY_ACCESS*
   ## Server's remote address for internal access
   SetEnvIf Remote_Addr "<interne IP-Adresse>" !DENY_ACCESS

   Order Allow,Deny
   Allow from all
   Deny from env=DENY_ACCESS
   Satisfy any
2. **Zugangskontrolle**
   a. **Passwortschutz** - Dies ist die Passwortabfrage, die alle Benutzer und Maschinen aussperrt, die den Zugang nicht haben.
      AuthType Basic
      AuthName "ShopSync - Zugangskontrolle"
      AuthUserFile "<Pfad zur Datei>/.htpasswd"
      Require valid-user
   b. **IP-Adressen-Freigabe** - Hierüber wird durch Freigabe einer kompletten IP-Adresse die Passwortabfrage ausgehebelt.
      SetEnvIf Remote_Addr "<externe IP-Adresse>" !DENY_ACCESS