



# Update-Services: Windows

## Servicename

Services im Zusammenhang mit Updates für die Windows-Plattform

## Kurzbeschreibung

Das Rechenzentrum der Universität Freiburg hostet WSUS-Server, die von Einrichtungen und Instituten der Universität für Updates von Microsoft-Produkten der Windows-Umgebung verwendet werden können. Services werden für verschiedene Umgebungstypen bereitgestellt. Diese Umgebungen stellen verschiedene Grade der Betreuung von Einrichtungen durch das Rechenzentrum dar. Mit diesem Angebot wird angestrebt, campusweit eine Maximierung des Patchlevels von Maschinen zu erreichen und die Sicherheit der Umgebungen durch Reduzierung von Schwachstellen zu erhöhen.

Das Angebot steht kostenfrei für die Einrichtungen und Institute zur Verfügung.

Die auf den WSUS-Server bereitgestellten Patches stehen über das Netzwerk der Universität bereit. Ungemanagte Umgebungen im gerouteten Uninetz haben Zugriff auf den öffentlichen WSUS-Server. Gemanagte Umgebungen erhalten Zugang zum WSUS-Server durch die Anbindung an das Active-Directory der Universität (PUBLIC). Für administrative Umgebungen führen die IT-Beauftragte, die durch den IT-Verantwortlichen ihrer Einrichtung oder ihres Institutes autorisiert sind, die Updates durch.

Besonderes Kennzeichen dieses Services ist der Beratungsanteil des Windows-Team, der eine eigenständige Entscheidung der Einrichtungen und Institute für Teildienste des Update-Services begleitet.

Die den *Update-Service Windows* nutzenden Einrichtungen tragen dazu bei, das Level der Patches campusweit zu heben.

## Ziele

Das Ziel dieses Services ist ein Teilziel im Zusammenhang der Informationssicherheit.

Aktuell gehaltene Betriebssysteme und Softwareapplikationen sind notwendig, um Risiken für die IT-Systeme der Universität zu senken.

In dieser Beschreibung werden die Update-Services für Windows erläutert. Der Umfang des Dienstes richtet sich dabei nach den Anforderungen des Campus und den Möglichkeiten zur Diensterbringung.

Die hier beschriebenen Update-Services adressieren dies für Windows sowie weitere Applikationen, die von Microsoft entwickelt wurden und auf dem Campus eingesetzt werden. Der Reviewprozess ist mehrstufig mit dem Ziel, die Funktionalität der campusspezifischen Use-Cases bestmöglich aufrechtzuerhalten. Im Fall erwartbarer instabiler Zustände von Zielsystemen werden Patches zurückgehalten. Im weiteren Fall festgestellter Inkompatibilitäten werden Patches zurückgezogen oder gesperrt.



## Zielgruppe

Die Zielgruppe sind alle Einrichtungen der Universitäten, die eigene Umgebungen administrieren. Ansprechpartner in den Einrichtungen sind die IT-Beauftragten/IT-Betreuer bzw. die IT-Verantwortlichen, falls kein IT-Betreuer für die betreffende Umgebung benannt ist.

## Leistungsumfang

Die Update-Services für Windows bestehen aus Teilleistungen. Diese Teilleistungen gliedern sich nach Zielumgebungen sowie Zielgruppen und deren Ansprechpartner. Je nach Umgebung sind Teilleistungen anwendbar, die im Abschnitt „Teilleistungen der Update-Services“ beschrieben werden.

### Gemanagte Umgebung

Gemanagte Umgebungen sind Mitglieder der Domäne PUBLIC. Die Konfiguration der Client-Updatedienste erfolgt durch Gruppenrichtlinien (*Group Policy Objects*, GPO).

### Ungemanagte Umgebung

In ungemanagten Umgebungen (UU) befindet sich die Windowsclients, die nicht vom Rechenzentrum betreut sind. Die Konfiguration des Updatemanagements obliegt dem lokalen IT-Beauftragten.

## Teilleistungen der Update-Services

Folgende Teilleistungen gehören zu den Update-Services:

- **Updates mit LAN-Geschwindigkeit:** WSUS-Server liefert Updates mit der maximalen Geschwindigkeit der *virtuellen Maschinen* (VM) im ESX-Cluster.
- **Express-Updates:** Kunden erhalten eine schnellere Installation, verglichen mit den publizierten Standard-Updates.
- **Peergruppen-Verfahren:** Im Rahmen des Patch-Risikomanagement gibt es Peergruppen, in denen an ausgewählten Systemen Patches vor einem allgemeinen Ausrollen eingespielt und hinsichtlich ihrer Auswirkung auf die Stabilität beobachtet und bewertet werden.
- **Patch-Management:** Im Rahmen der Möglichkeiten des WSUS-Servers wird der Lifecycle von Patches gemanagt.
- **Interventionsverfahren für Einzelpatches:** Bei Einschränkungen der Umgebung durch Einzelpatches wird nach Abschätzung der Risiken für Kunden und den Campus interveniert.
- **Clientgruppen:** Clientgruppen ermöglichen die Zusammenfassung von Systemen für administrativ gezieltes Patchen.
- **Reports:** Kooperativ sind im Rahmen der Möglichkeiten des WSUS-Servers Reports erstellbar.
- **Regelbasierter Approval-Prozess:** Für Clientgruppen besteht die Möglichkeit, metatag-basierte Regeln für den Approval-Prozess zu customizen.



## Matrix von Leistungen auf Umgebungstyp

Die folgende Matrix bildet ab, dass Teilleistungen nicht vollständig für alle Umgebungstypen anwendbar sind. Die Teilleistungen, die in einer Spalte für einen Umgebungstypen aufgeführt sind, müssen nicht zwingend vollständig abgerufen werden.

Teilleistung	GU	UU
Updates mit LAN-Geschwindigkeit	x	x
Express-Updates	x	x
Patch-Risikomanagement Peer-Gruppen	x	
Patch-Lifecycle-Verfahren (WSUS)	x	x
Clientgruppen	x	
Regelbasierter Approval-Prozess	x	

## Betreiber / Admin / Verantwortliche

Betreiber dieses Services ist das *Windows-Team* als Teil der Abteilung *Zentrale Dienste*. Der Teamleiter dieser Abteilung ist mit Stand Dezember 2017 Matthias Scharring, der dem Leiter der Abteilung Zentrale Dienste berichtet.

## Technische Beschreibung

Die WSUS-Server sind virtuelle Server und physische Server. Nähere Details geben die jeweiligen Dokumente der Cluster und Maschinensäle, auf denen diese Server laufen.

### WSUS-Server

#### WSUS1

Als WSUS1 wird der WSUS-Server bezeichnet, über den gemanagte Umgebungen ihre Updates beziehen können. Dieser Server läuft als virtuelle Maschine auf dem ESX-Cluster. FQDN: `wsus.public.ads.uni-freiburg.de:8531`

#### WSUS2

Als WSUS2 wird der WSUS-Server bezeichnet, über den ungemanagte Umgebungen ihre Updates beziehen können. Er hostet Patches in den Systemsprachen Englisch und Deutsch und enthält alle Klassifikationen von Microsoft außer die der Klassifikation *Treiber (Driver)*. FQDN: `wsus.uni-freiburg.de:80`

## Zuständigkeiten

Ungemanagte Umgebungen (UU) können den WSUS-Server ohne explizite Bestellung nutzen. Troubleshooting wird geleistet, wenn es Störungen beim WSUS-Server gibt. Ein Erstgespräch mit dem Windows-Team erfolgt, wenn aus einer UU oder direkt eine Nutzung als Gemanagte Umgebung (GU) erwogen wird.



Eskalationen werden in erster Stufe vom Teamleiter entgegengenommen. Eskalationen in zweiter Stufe werden vom Abteilungsleiter der Abteilung „Zentrale Dienste“ bearbeitet.

## Auftragsgrundlage

Das Rechenzentrum der Universität Freiburg ist die zentrale Einrichtung für IT-Dienstleistungen, die von Mitgliedern und weiteren Einrichtungen, den Dienstnehmern, in Anspruch genommen werden können. Basisdienste, zu denen die Update-Services zählen, werden als campusweit verfügbare Dienste nach dem Fair-Use-Prinzip kostenfrei bereitgestellt. Das beinhaltet eine Steuerung dieses Dienstes, bei der die Bedienung der Bedarfe des Campus mit den von der Universität bereitgestellten Ausstattung in Übereinstimmung gebracht wird.

## Bestellwege

Die Bestellung einzelner oder mehrerer Teilleistungen im Rahmen der Update-Services wird eingeleitet durch eine Anfrage per Mail an die Ticketqueue [mits-team@rz.uni-freiburg.de](mailto:mits-team@rz.uni-freiburg.de). Nach der Anfrage erfolgt eine Beratung, die die Voraussetzungen der anfragenden Einrichtung berücksichtigt, entlang der Teildienstleistungen der Update-Services. Unterstützt vom RZ-Dienst fällt die dienstnehmende Einrichtung die Entscheidung, welche dieser Dienste in Anspruch genommen werden sollen. Entscheidungen können von der Einrichtung im laufenden Dienst modifiziert werden.

Der IT-Verantwortliche der dienstnehmenden Einrichtung bestätigt die Vereinbarungen über die bestellten Teilleistungen des Update-Services enthält. Die Bestätigung erfolgt in Form einer E-Mail vom IT-Verantwortlichen, die mit einer elektronischen Signatur auf der Basis eines PKI-Zertifikats des DFN beglaubigt ist. Bei dieser Bestätigung muss der IT-Beauftragte als technischer Ansprechpartner der Einrichtung namentlich benannt werden, der für Rückfragen durch das RZ-Team zur Verfügung steht.

Die Teilleistung *Updates mit LAN-Geschwindigkeit* bedarf keiner expliziten Bestellung. Diese Leistung ist durch jede Unieinrichtung innerhalb des Netzes der Universität Freiburg nutzbar.

## Finanzierung / Budget / Verrechnungsmodell

Die Update-Services des Rechenzentrums gehören zur kostenfreien Grundversorgung für Einrichtungen der Universität. Erstgespräche und Support werden als Teil dieses Services ebenso kostenfrei erbracht.

## Kontakt

E-Mail: [mits-team@rz.uni-freiburg.de](mailto:mits-team@rz.uni-freiburg.de)

Telefon:

1. Zentrale Supportnummer: 0761 203 4666



2. Nummer Windowsabteilung: 0761 203 4680
3. Nummer Volker-Henning Winterer: 0761 203 4646