

# Novell® Sentinel™

[www.novell.com](http://www.novell.com)

5.1.3

Band V - Handbuch für Drittanbieter-Integration

7. Juli 2006

# N

Novell®

## Rechtliche Hinweise

Novell, Inc., übernimmt keine Gewährleistung oder Haftung in Bezug auf den Inhalt und die Verwendung dieser Dokumentation und schließt insbesondere jede ausdrückliche oder stillschweigende Gewährleistung bezüglich der handelsüblichen Qualität sowie der Eignung für einen bestimmten Zweck aus. Darüber hinaus behält sich Novell, Inc., das Recht vor, diese Veröffentlichung ohne vorherige Ankündigung zu überarbeiten und inhaltliche Änderungen vorzunehmen, ohne dass für Novell die Verpflichtung entsteht, Personen oder Organisationen über die vorgenommenen Änderungen zu informieren.

Novell, Inc., übernimmt ferner keine Gewährleistung oder Haftung in Bezug auf Software und schließt insbesondere jede ausdrückliche oder stillschweigende Gewährleistung bezüglich der handelsüblichen Qualität sowie der Eignung für einen bestimmten Zweck aus. Darüber hinaus behält sich Novell, Inc., das Recht vor, die Novell-Software vollständig oder teilweise zu ändern, ohne dass für Novell die Verpflichtung entsteht, Personen oder Organisationen über die vorgenommenen Änderungen zu informieren.

Sämtliche Produkte und technischen Informationen, die im Rahmen dieser Vereinbarung bereitgestellt werden, unterliegen möglicherweise den US-Exportbestimmungen und den Handelsgesetzen anderer Länder. Hiermit erklären Sie sich bereit, sämtliche Exportbestimmungen einzuhalten und ggf. die erforderlichen Lizenzen oder Berechtigungen für den Export, die Wiederausfuhr oder den Import einzuholen. Sie erklären sich bereit, keinen Export oder keine Wiederausfuhr an natürliche oder juristische Personen zu tätigen, die zurzeit auf den Exportausschlusslisten der USA aufgeführt sind, oder in Länder, die einem Embargo unterliegen oder die den US-Exportbestimmungen zufolge den Terrorismus unterstützen. Sie erklären sich bereit, die Lieferbestandteile nicht für die Endnutzung in verbotenen nuklearen, chemischen oder biologischen Waffen oder Raketen einzusetzen. Weitere Informationen zum Export von Novell-Software finden Sie unter [www.novell.com/info/exports/](http://www.novell.com/info/exports/). Novell übernimmt keinerlei Verantwortung, wenn Sie es versäumen, die erforderlichen Exportgenehmigungen einzuholen.

Copyright © 1999–2006, Novell, Inc. Alle Rechte vorbehalten. Ohne ausdrückliche, schriftliche Genehmigung des Herausgebers darf kein Teil dieser Veröffentlichung reproduziert, fotokopiert, übertragen oder in einem Speichersystem verarbeitet werden.

Novell, Inc., besitzt Rechte an geistigem Eigentum für die Technologie, die in das in dieser Dokumentation beschriebene Produkt integriert ist. Diese Rechte an geistigem Eigentum umfassen im Besonderen eines oder mehrere der unter <http://www.novell.com/company/legal/patents/> aufgelisteten Patente sowie ein oder mehrere andere Patente oder Patentanmeldungen in den USA und in anderen Ländern, sind jedoch nicht darauf beschränkt.

Novell, Inc.  
404 Wyman Street, Suite 500  
Waltham, MA 02451  
U.S.A.  
[www.novell.com](http://www.novell.com)

*Online-Dokumentation:* Zugriff auf die Online-Dokumentation für dieses und andere Novell-Produkte sowie auf Aktualisierungen erhalten Sie unter [www.novell.com/documentation](http://www.novell.com/documentation).

## Novell-Marken

Informationen zu Novell-Marken finden Sie in der Liste der Marken und Dienstleistungsmarken von Novell (<http://www.novell.com/company/legal/trademarks/tmlist.html>).

## Materialien von Drittanbietern

Alle Marken von Drittanbietern sind Eigentum der jeweiligen Inhaber.

## Rechtliche Hinweise zu Drittanbieterprodukten

Sentinel 5 enthält möglicherweise folgende Drittanbietertechnologien:

- Apache Axis und Apache Tomcat, Copyright © 1999 bis 2005, Apache Software Foundation. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter <http://www.apache.org/licenses/>
- ANTLR. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter <http://www.antlr.org>
- Boost, Copyright © 1999, Boost.org.
- Bouncy Castle, Copyright © 2000–2004, the Legion of Bouncy Castle. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter <http://www.bouncycastle.org>.
- Checkpoint. Copyright © Check Point Software Technologies Ltd.
- Concurrent, Dienstprogrammpaket. Copyright © Doug Lea. Wird ohne die Klassen CopyOnWriteArrayList und ConcurrentReaderHashMap verwendet.
- Crypto++ Compilation. Copyright © 1995–2003, Wei Dai, beinhaltet folgende durch Copyright geschützte Werke: mars.cpp von Brian Gladman und Sean Woods. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter <http://www.eskimo.com/~weidai/License.txt>.
- Crystal Reports Developer und Crystal Reports Server. Copyright © 2004 Business Objects Software Limited.
- DataDirect Technologies Corp. Copyright © 1991–2003.
- edpFTPj, lizenziert unter: Lesser GNU Public License. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter <http://www.enterisedt.com/products/edftpj/purchase.html>.
- Enhydra Shark, lizenziert unter: Lesser General Public License, verfügbar unter: <http://shark.objectweb.org/license.html>.
- ICEsoft ICEbrowser. ICEsoft Technologies, Inc. Copyright © 2003–2004.
- ILOG, Inc. Copyright © 1999–2004.
- Installshield Universal. Copyright © 1996–2005, Macrovision Corporation und/oder Macrovision Europe Ltd.
- Java 2 Platform, Standard Edition. Copyright © Sun Microsystems, Inc. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter [http://java.sun.com/j2se/1.4.2/j2re-1\\_4\\_2\\_10-license.txt](http://java.sun.com/j2se/1.4.2/j2re-1_4_2_10-license.txt).

Java 2 Platform kann außerdem folgende Drittanbieterprodukte enthalten:

- CoolServlets © 1999
- DES and 3xDES © 2000, Jef Poskanzer
- Crimson © 1999–2000, The Apache Software Foundation
- Xalan J2 © 1999–2000, The Apache Software Foundation
- NSIS 1.0j © 1999–2000, Nullsoft, Inc.

- Eastman Kodak Company © 1992
- Lucinda, eine eingetragene Marke oder Marke von Bigelow and Holmes
- Taligent, Inc.
- IBM, einige Teile verfügbar unter: <http://oss.software.ibm.com/icu4j/>

Weitere Informationen zu diesen Drittanbietertechnologien und den zugehörigen Haftungsausschlüssen und Einschränkungen finden Sie unter: [http://java.sun.com/j2se/1.4.2/j2se-1\\_4\\_2-thirdpartylicensereadme.txt](http://java.sun.com/j2se/1.4.2/j2se-1_4_2-thirdpartylicensereadme.txt).

- JavaBeans Activation Framework (JAF). Copyright © Sun Microsystems, Inc. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter <http://www.java.sun.com/products/javabeans/glasgow/jaf.html>, klicken Sie auf „Download“ > „License“.
- JavaMail. Copyright © Sun Microsystems, Inc. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter <http://www.java.sun.com/products/javamail/downloads/index.html>, klicken Sie auf „Download“ > „License“.
- Java Ace von Douglas C. Schmidt und seiner Forschungsgruppe an der Washington University und Tao (mit ACE-Wrappers) von Douglas C. Schmidt und seiner Forschungsgruppe an der Washington University, University of California, Irvine, und Vanderbilt University. Copyright © 1993–2005. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter <http://www.cs.wustl.edu/~schmidt/ACE-copying.html> und <http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html>
- Java Authentication and Authorization Service Modules, lizenziert unter: Lesser General Public License. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter <http://free.tagish.net/jaas/index.jsp>.
- Java Network Launching Protocol (JNLP). Copyright © Sun Microsystems, Inc. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter <http://www.java.sun.com/products/javawebstart/download-jnlp.html>, klicken Sie auf „Download“ > „License“.
- Java Service Wrapper. Teile wie folgt durch Copyright geschützt: Copyright © 1999, 2004 Tanuki Software und Copyright © 2001 Silver Egg Technology. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter <http://wrapper.tanukisoftware.org/doc/english/license.html>.
- JIDE. Copyright © 2002 bis 2005, JIDE Software, Inc.
- jTDS ist lizenziert unter: Lesser GNU Public License. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter <http://jtds.sourceforge.net/>.
- MDateSelector. Copyright © 2005, Martin Newstead, lizenziert unter: Lesser General Public License. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter <http://web.ukonline.co.uk/mseries>
- Monarch Charts. Copyright © 2005, Singleton Labs.
- Net-SNMP. Teile des Codes unterliegen dem Copyright verschiedener juristischer Personen, die sich alle Rechte vorbehalten. Copyright © 1989, 1991, 1992 by Carnegie Mellon University; Copyright © 1996, 1998 bis 2000, the Regents of the University of California; Copyright © 2001 bis 2003 Networks Associates Technology, Inc.; Copyright © 2001 bis 2003, Cambridge Broadband, Ltd.; Copyright © 2003 Sun Microsystems, Inc., und Copyright © 2003 bis 2004, Sparta, Inc. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter <http://net-snmp.sourceforge.net>.
- The OpenSSL Project. Copyright © 1998–2004, The Open SSL Project. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter <http://www.openssl.org>.
- Oracle Help für Java. Copyright © 1994–2006, Oracle Corporation.
- RoboHELP Office. Copyright © Adobe Systems Incorporated, vormals Macromedia.
- Skin Look and Feel (SkinLF). Copyright © 2000–2006 L2FProd.com. Lizenziert unter der Apache-Softwarelizenz. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter <https://skinlf.dev.java.net/>.
- Sonic Software Corporation. Copyright © 2003–2004. Die SSC-Software enthält Sicherheitssoftware, die von RSA Security, Inc., lizenziert wurde.

- Tinyxml. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter <http://grinninglizard.com/tinyxmldocs/index.html>.
- SecurityNexus. Copyright © 2003 bis 2006. SecurityNexus, LLC. Alle Rechte vorbehalten.
- Xalan und Xerces, jeweils von der Apache Software Foundation lizenziert, Copyright © 1999–2004. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter <http://xml.apache.org/dist/LICENSE.txt>.
- yWorks. Copyright © 2003 bis 2006, yWorks.

---

**HINWEIS:** Zum Zeitpunkt der Veröffentlichung dieser Dokumentation waren die oben stehenden Links aktiv. Sollten Sie feststellen, dass einer der oben angegebenen Links unterbrochen oder die verlinkten Webseiten inaktiv sind, wenden Sie sich an Novell, Inc., 404 Wyman Street, Suite 500, Waltham, MA 02451 U.S.A.

---

# Inhalt

<b>1 Remedy-Integration</b>	<b>1-1</b>
Konfiguration .....	1-2
Datenfluss von Remedy zu Sentinel .....	1-6
Installation von Sentinel.....	1-10
Konfiguration des Datenflusses von Remedy zu Sentinel .....	1-11
<b>2 Remedy Help Desk-Vorgänge</b>	<b>2-1</b>
Remedy Help Desk-Vorgänge.....	2-1
Manuelles Neukonfigurieren der Einstellungen für die Remedy-Schnittstelle .....	2-2
Remedy-Einstellungen .....	2-2
Zurücksetzen des Remedy-Passworts .....	2-2
<b>3 Installieren von HP OpenView Service Desk unter Windows</b>	<b>3-1</b>
Systemanforderungen .....	3-2
Installation .....	3-2
Konfigurieren von HP OpenView Service Desk .....	3-3
Aktivieren der (bidirektionalen) Service Desk-Sentinel-Schnittstelle.....	3-4
<b>4 HP OpenView Service Desk-Integration</b>	<b>4-1</b>
HP OpenView Service Desk.....	4-1
Senden von Vorfällen an HP OpenView Service Desk.....	4-2
HP OpenView Service Desk Client.....	4-4
HP OpenView Service Desk – Bidirektionale Schnittstelle .....	4-5
Manuelles Neukonfigurieren der Einstellungen der HP OpenView Service Desk-Schnittstelle .....	4-6

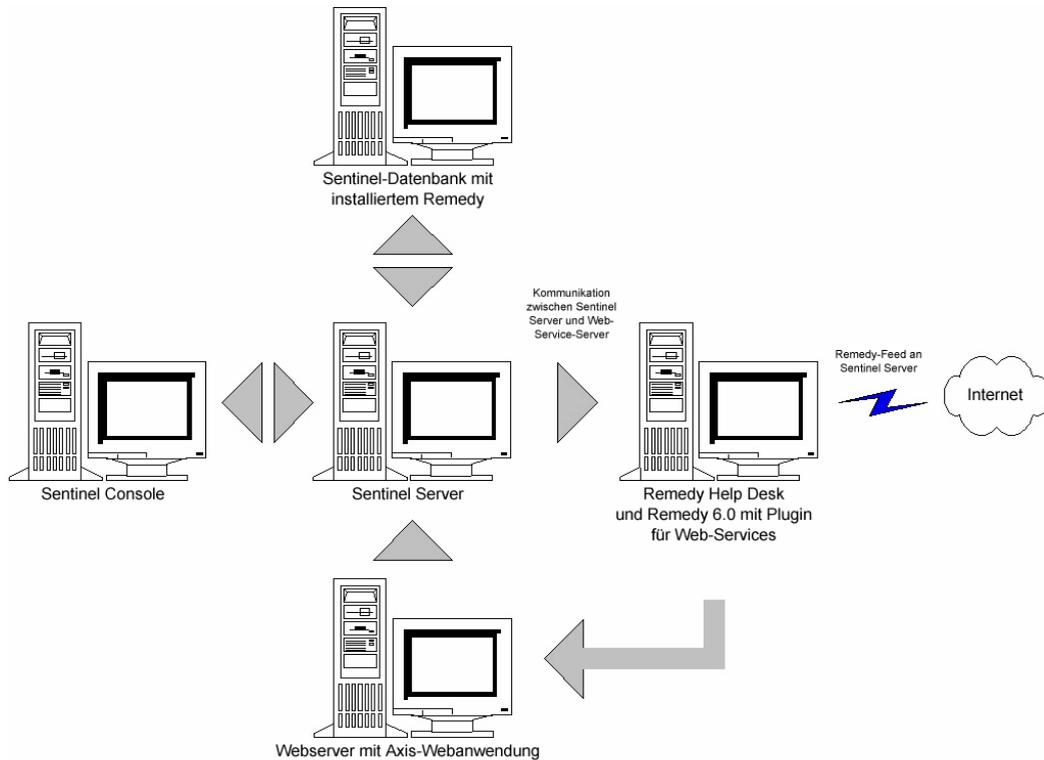


# 1

## Remedy-Integration

Mithilfe der Remedy-Integration für Sentinel v4.2 bzw. v5 können Workflow-Anwendungen erstellt werden, die sowohl mit dem Remedy Trouble Ticketing System als auch mit dem Sentinel-System integriert sind. Die Hauptfunktionen der Remedy-Integration sind:

- Die Möglichkeit, auf der Grundlage eines Vorfalls in Sentinel einen neuen Fall in Remedy Help Desk zu erstellen.
- Die Möglichkeit, bei der Aktualisierung eines Sentinel-Vorfalls den zugehörigen Fall in Help Desk zu aktualisieren.
- Die Möglichkeit, einen Sentinel-Vorfall zu aktualisieren, wenn ein zugehöriger Fall in Help Desk aktualisiert wird.



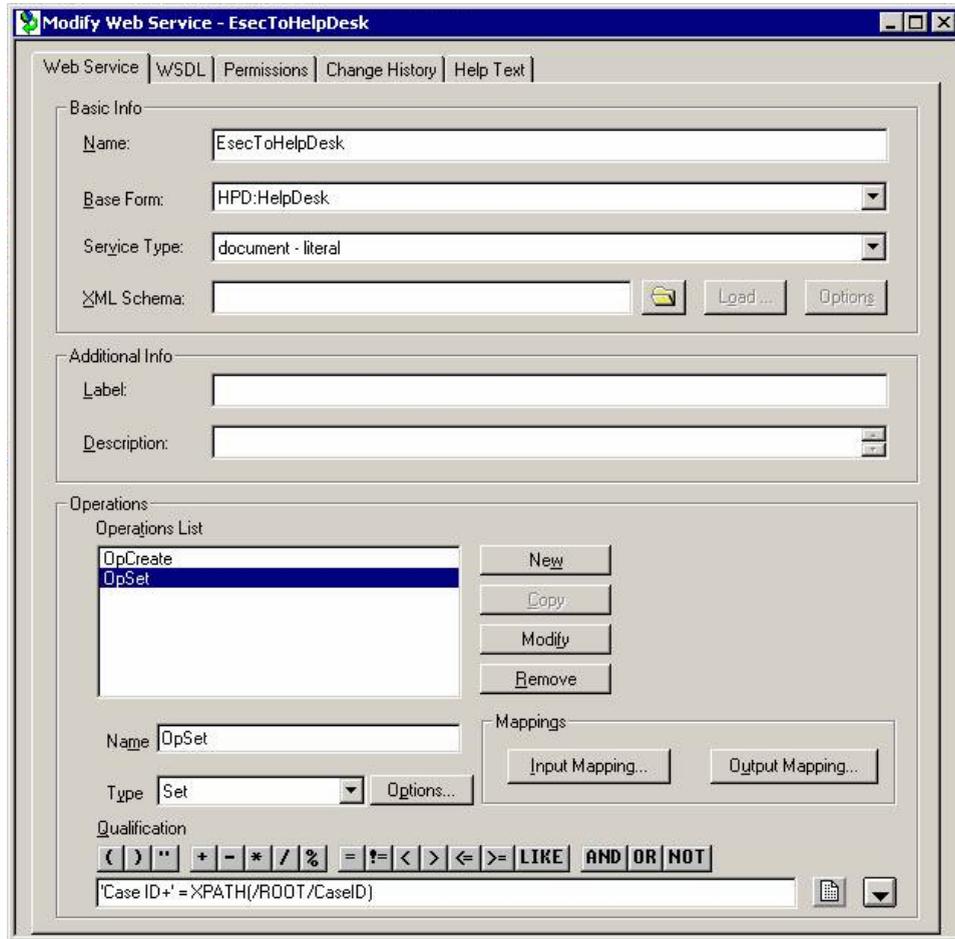
# Konfiguration

## So ändern Sie das Formular für Remedy Help Desk-Fälle

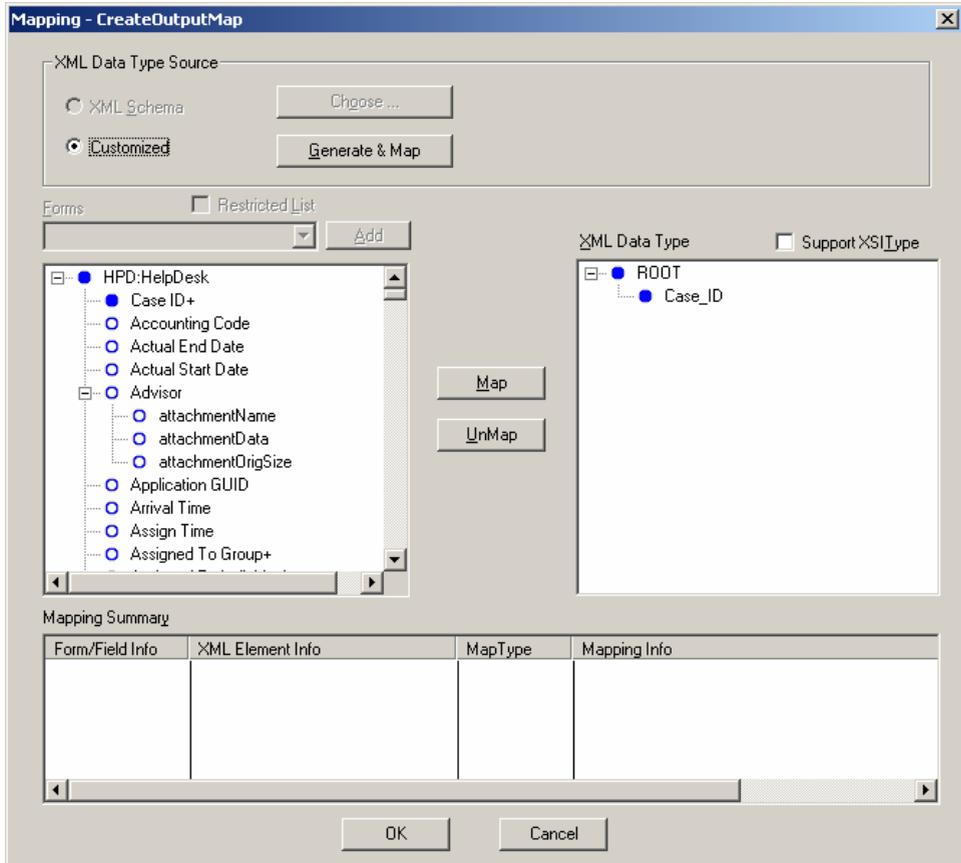
1. Melden Sie sich bei *Remedy Administrator* (Remedy-Administrator) > *Forms* (Formulare) an und doppelklicken sie auf *HPD HelpDesk*.
2. Um die Integration mit Sentinel zu unterstützen, muss zum Help Desk-Fallformular ein Merkmalsfeld (EsecIncidentId) und ein Anlagenpoolfeld (Attachment Pool) hinzugefügt werden. Mithilfe dieser Feldeinträge können Vorfallsanlagen zum Formular hinzugefügt werden.
3. So fügen Sie das Merkmalsfeld „EsecIncidentId“ hinzu:
  - Klicken Sie auf die Schaltfläche „New Character Field“ (Neues Merkmalsfeld) und platzieren Sie es an einer beliebigen Stelle des Formulars.
  - Legen Sie auf der Registerkarte „Display“ (Anzeigen) eine Bezeichnung fest.
  - Setzen Sie auf der Registerkarte „Database“ (Datenbank) im Feld „Name“ (Name) den Namen auf „EsecIncidentID“.
4. So fügen Sie das Merkmalsfeld „Attachment Pool“ (Anlagenpool) mit folgenden drei Feldern hinzu: „EsecEvents“, „EsecVuln“ und „EsecAdv“.
  - Klicken Sie auf die Schaltfläche *Create Attachment Pool* (Anlagenpool erstellen).
  - Geben Sie auf der Registerkarte „Display“ (Anzeigen) im Feld „Label“ (Bezeichnung) einen Bezeichnungsnamen ein (z. B.: esec-Anlagen).
  - Geben Sie unter „Attach Fields“ (Felder beifügen) in „Enter Attachments Field Label“ (Feldbezeichnung für Anlagen eingeben) Folgendes ein:
    - „EsecEvent“ und klicken Sie auf „Add“ (Hinzufügen).
    - „EsecVuln“ und klicken Sie auf „Add“ (Hinzufügen).
    - „EsecAdv“ und klicken Sie auf „Add“ (Hinzufügen).
5. Klicken Sie auf *Save* (Speichern).

## Erstellen des Web-Service

1. Markieren Sie unter „Remedy Administrator“ (Remedy-Administrator), im Navigationsfenster die Option *Web Services* (Web-Services). Klicken Sie mit der rechten Maustaste auf *New Web Services* (Neue Web-Services) und klicken Sie auf die Registerkarte *Web Services* (Web-Services).

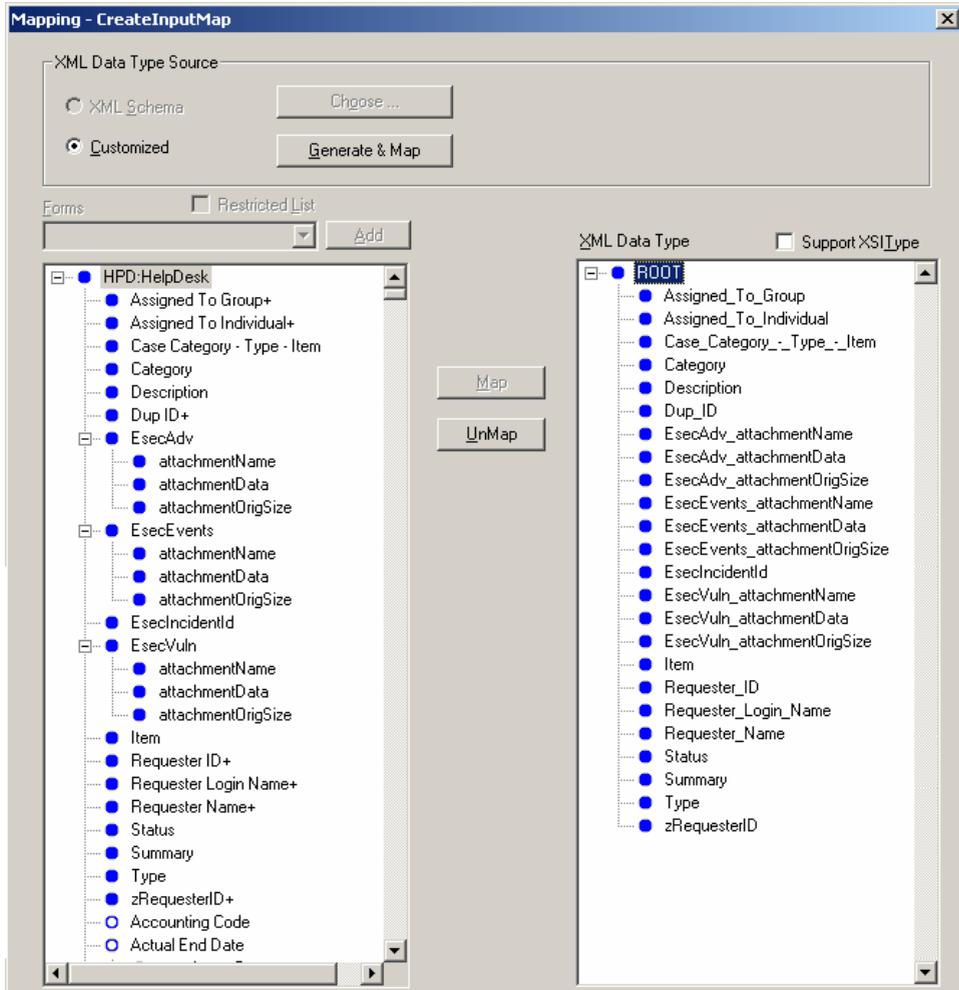


2. Erstellen Sie unter Verwendung von „Help Desk Case“ (Help Desk-Fall) als Grundformular einen Web-Service mit der Bezeichnung *EsecToHelpDesk* und wählen Sie unter „Base Form“ (Basisformular) „HPD HelpDesk“ aus.
3. Erstellen Sie zwei Operationen für diesen Web-Service namens:
  - opCreate
  - opSet
 indem Sie die anderen Operationen entfernen.
4. Wählen Sie „OpCreate“ und klicken Sie auf die Schaltfläche „Output Mapping“ (Ausgabebezuordnung). Stellen Sie sicher, dass der Bildschirm wie folgt aussieht.



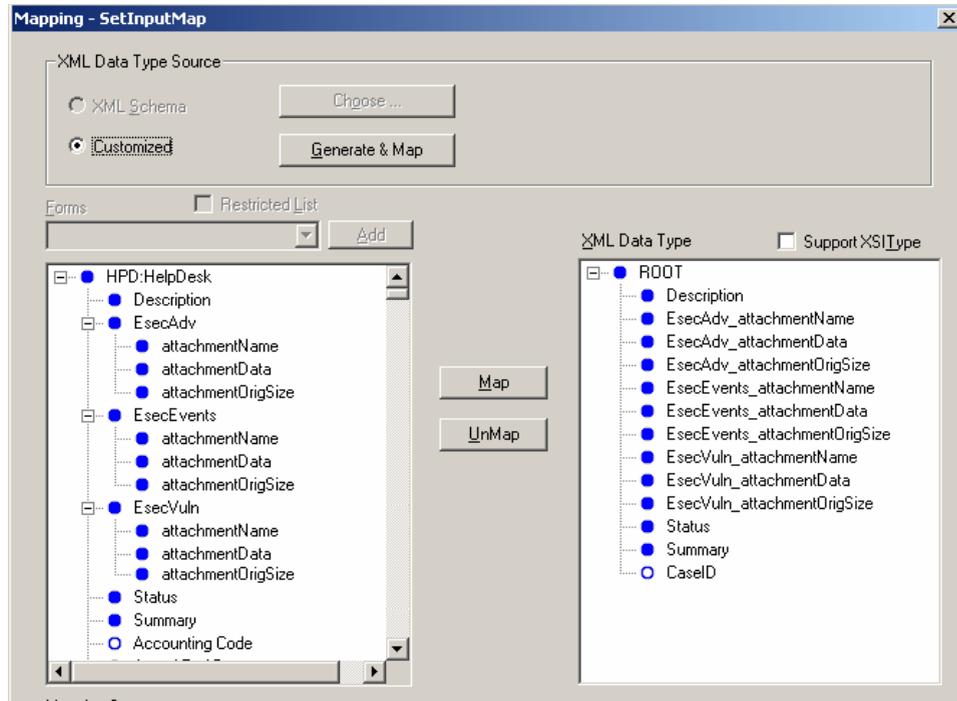
Wählen Sie die Schaltfläche „Input Mapping“ (Eingabezuordnung) für opCreate aus. Stellen Sie sicher, dass der Bildschirm wie folgt aussieht

**HINWEIS:** Um ein Element zu entfernen, markieren Sie es > *klicken Sie mit der rechten Maustaste* > *schneiden Sie es aus*.



Klicken Sie auf *Save* (Speichern).

Wählen Sie die Schaltfläche „Input Mapping“ (Eingabezuordnung) für opSet aus. Stellen Sie sicher, dass der Bildschirm wie folgt aussieht.



Für opSet gibt es keine Ausgabezuordnung. Für opSet müssen Sie eine Qualifizierung angeben:



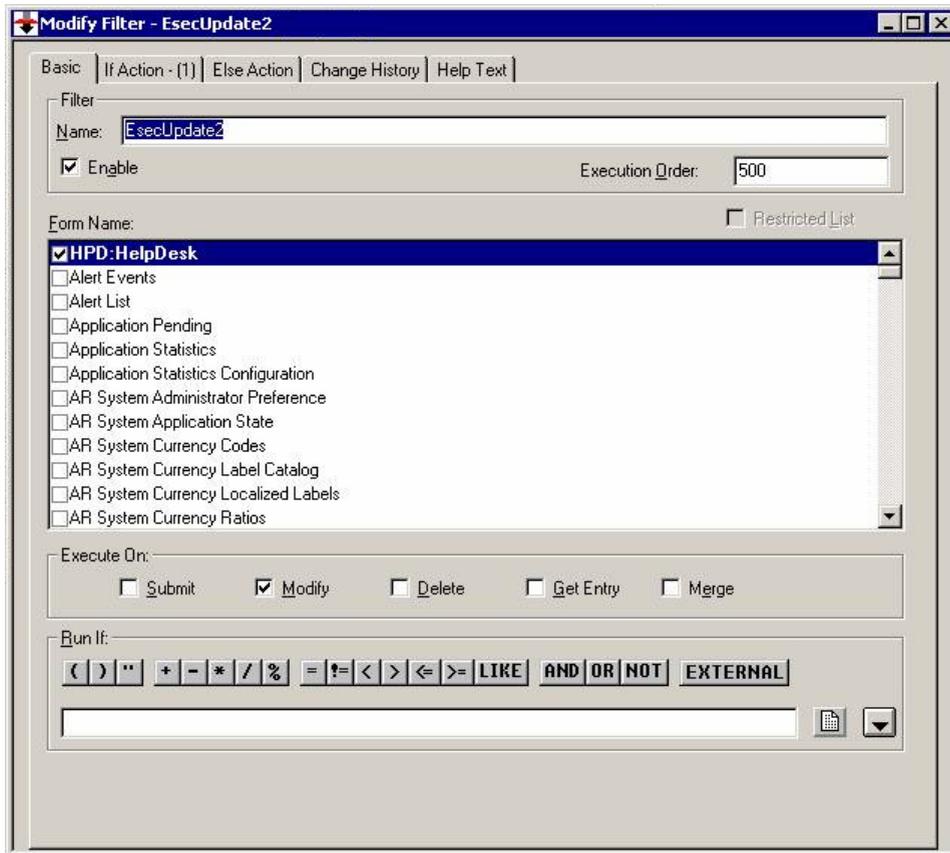
5. Wechseln Sie zur Registerkarte „Permissions“ (Berechtigungen) und verschieben Sie den Service in den Bereich „Public“ (Öffentlich), indem Sie „Public“ (Öffentlich) von links nach rechts verschieben. Klicken Sie auf *Save* (Speichern).

## Datenfluss von Remedy zu Sentinel

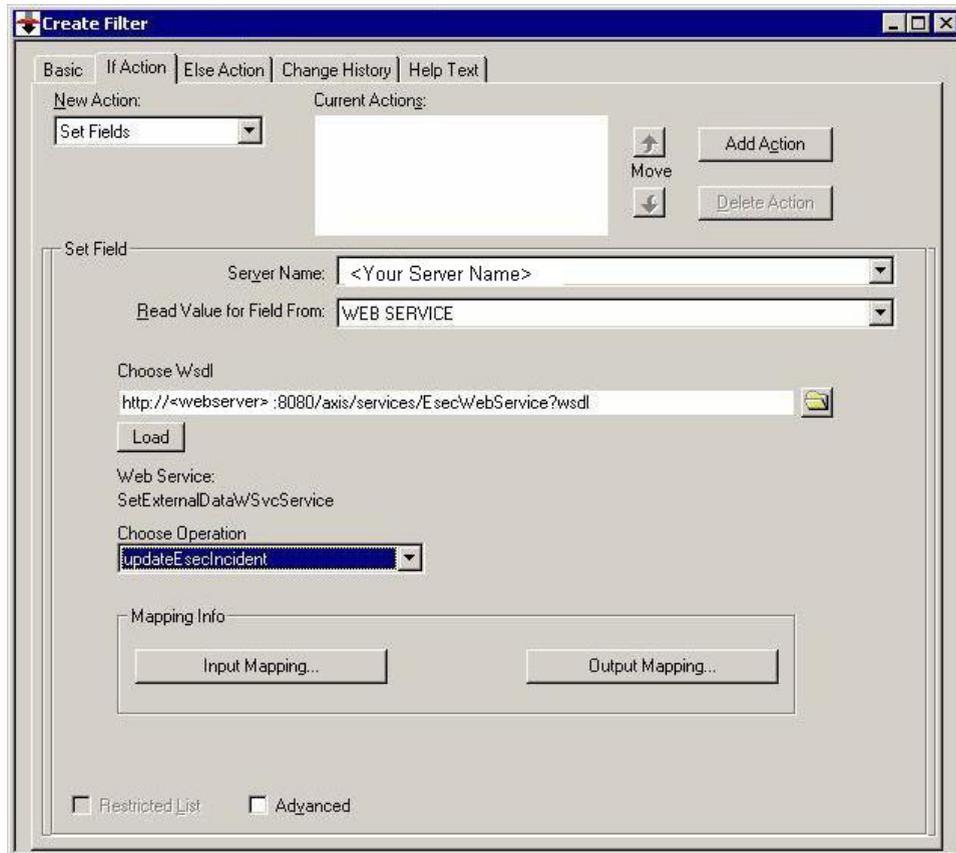
Für den Zugriff auf Sentinel Webservice ist ein Webserver erforderlich, auf dem zum Zeitpunkt des Starts von Sentinel Server die Webanwendung Axis ausgeführt wird.

### Datenfluss von Remedy zu Sentinel

1. Markieren Sie in „Remedy Administrator“ (Remedy-Administrator) die Option „Filters“ (Filter) und klicken Sie mit der rechten Maustaste auf „Add Filter“ (Filter hinzufügen).
2. Erstellen Sie einen Filter für das Help Desk-Fallformular, das für ein bearbeitetes Ereignis ausgeführt wird. Stellen Sie sicher, dass der Bildschirm wie folgt aussieht.

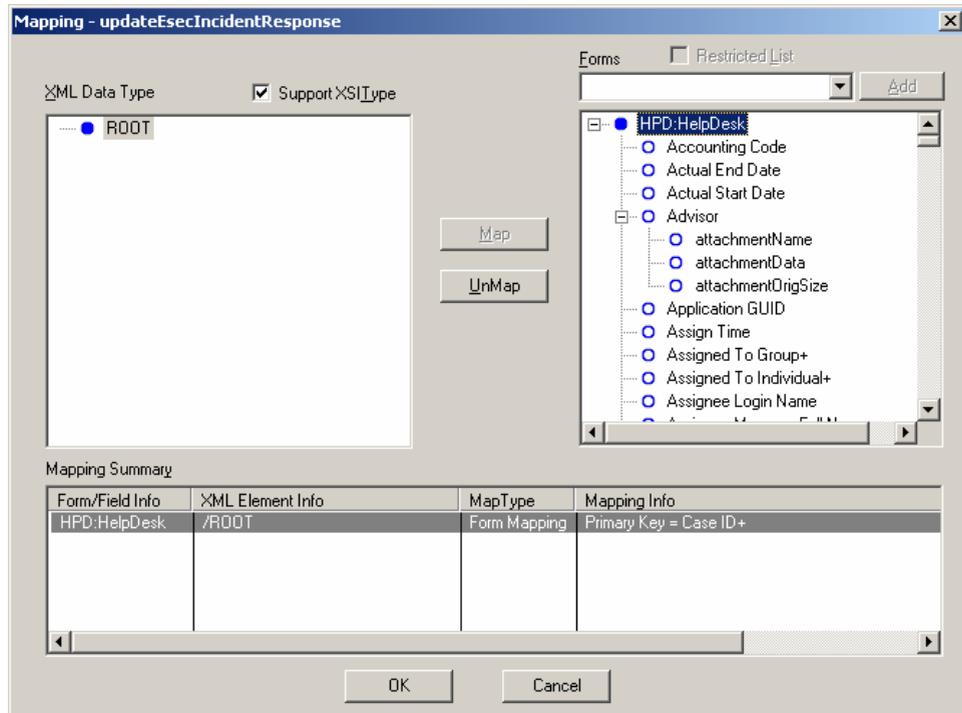


3. Wählen Sie auf der Registerkarte *If Action* (Wenn-Aktion) im Dropdown-Menü *New Action* (Neue Aktion) die Aktion *Set field* (Feld festlegen), wählen Sie im Bereich *Set Field* (Feld festlegen) *WEB SERVICE* aus und geben Sie die URL für Sentinel Webservice an (<http://<Webserver-IP bzw. DNS-Name>:8080/axis/services/EsecWebService?wsdl>).



4. Wählen Sie im Dropdown-Menü *Choose Operation* (Operation auswählen) die Methode *updateEsecIncident* aus und legen Sie die Zuordnung für Eingabe und Ausgabe fest.

Klicken Sie auf die Schaltfläche „Output Mapping“ (Ausgabezuordnung). Stellen Sie sicher, dass der Bildschirm wie folgt aussieht.

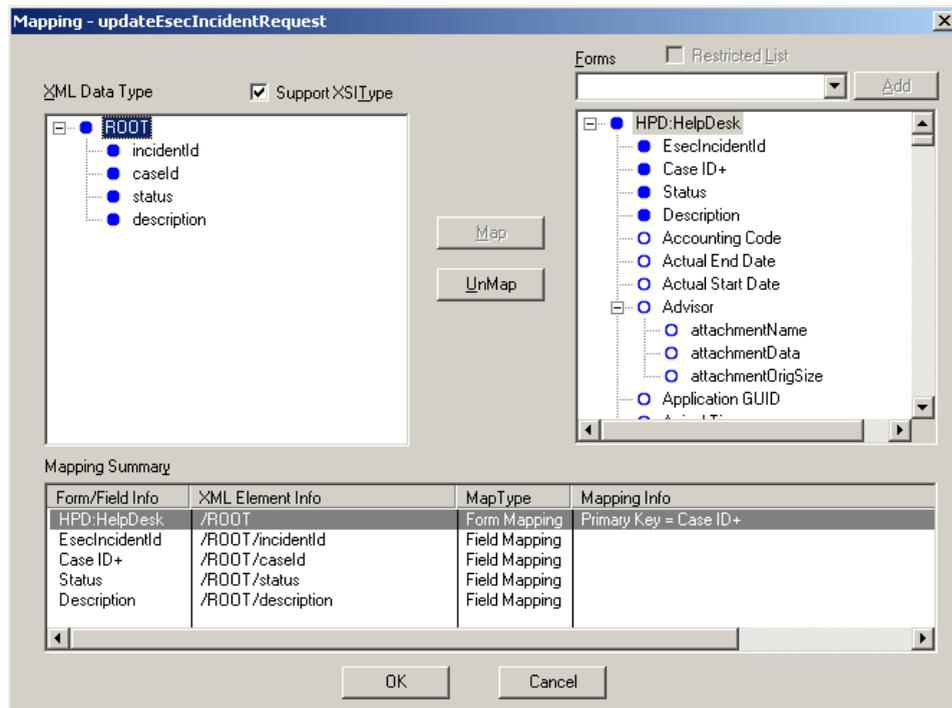


Klicken Sie auf die Schaltfläche „Input Mapping“ (Eingabezuordnung). Stellen Sie sicher, dass der Bildschirm wie folgt aussieht.

---

**HINWEIS:** Zur Festlegung der Zuordnung müssen Sie ein Element auf der linken Seite (z. B. incidentId) und ein Element auf der rechten Seite (z. B. EsecIncidentId) auswählen und auf die Schaltfläche „Map“ (Zuordnen) klicken.

---



**HINWEIS:** Nach der Einrichtung wird bei jeder Speicherung einer Änderung im Help Desk-Fallformular die betreffende Änderung an einen Sentinel-Service gesendet.

5. Klicken Sie auf *Save* (Speichern).

## Installation von Sentinel

Bei der Installation von Sentinel mit Remedy, benötigen Sie ein Konto bei Remedy. Über dieses Konto werden Sie zur Eingabe folgender Informationen aufgefordert.

**HINWEIS:** Sie benötigen die Berechtigung „Remedy Integration“.

- Benutzername
- Passwort
- Requester-Name
- Requester-ID
- Requester-Anmeldung
- Gruppenname (kann leer gelassen werden)
- Individueller Name (kann leer gelassen werden)
- Servername
- Service-Name

Für den Datenfluss von Remedy zu Sentinel werden Sie zur Eingabe folgender Informationen aufgefordert:

- Sentinel-Webserver (<Computername:Port>)
- Sentinel-Benutzername (z. B. esecadm)
- Sentinel-Benutzer-ID
- Sentinel-UUID
- Sentinel-Sperr-ID (normalerweise auf 1 oder 2 gesetzt; dies ist....)

## Installation von Sentinel

1. Wählen Sie während der Installation die Option „Remedy Integration“ aus.
2. Halten Sie die oben angegebenen Informationen während des Installationsvorgangs bereit.

## Konfiguration des Datenflusses von Remedy zu Sentinel

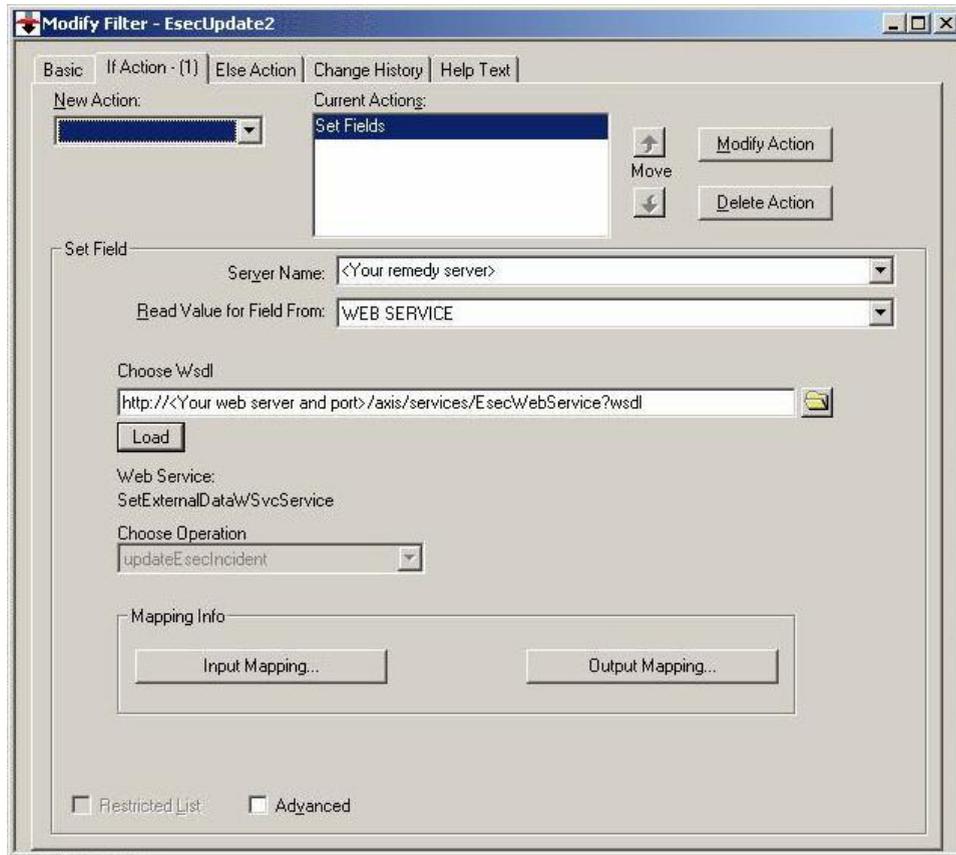
Bei Verwendung der Drittanbieterintegration (Remedy-Integration) sollten Sie Installation und Konfiguration in folgender Reihenfolge ausführen:

- Installieren Sie Remedy Help Desk und Remedy 6.0 mit dem Plugin für Web-Services.
- Konfigurieren Sie neue Filter und Web-Services in Remedy Help Desk.
- Installieren Sie Sentinel.

Um den Datenfluss von Remedy zu Sentinel zu ermöglichen, müssen Sie wie folgt vorgehen:

- Für den Zugriff auf Sentinel Webservice ist ein Webserver erforderlich, auf dem die Webanwendung Axis ausgeführt wird, bevor Sentinel Server gestartet wird.
- Kopieren Sie alle jar-Dateien aus dem folgenden Speicherort auf Ihrer Sentinel Server-Instanz in <Axis-Webanwendung>\webclient\lib.
  - %ESEC\_HOME%\lib
  - %ESEC\_HOME%\sentinel\console
  - %ESEC\_HOME%\communicator (nur bei v4.2)
- Kopieren Sie die Sentinel Server-Datei configuration.xml und die.keystore-Datei in einen beliebigen Speicherort auf dem Webserver. Beide Dateien befinden sich unter %ESEC\_HOME%.
  - Bearbeiten Sie die Datei configuration.xml auf dem Webserver so, dass sie auf die.keystore-Datei verweist.
  - Fügen Sie folgende JVM-Option zu Ihrem Webserver hinzu:

```
Dcom.esecurity.configurationfile=<Pfad zu
configuration.xml>\configuration.xml
```
- Sie müssen einen Filter für das Help Desk-Fallformular erstellen, das für ein Ereignis vom Typ „Modified“ (Bearbeitet) ausgeführt wird. Dieser Filter ruft den Sentinel-Webserver auf.



# 2

## Remedy Help Desk-Vorgänge

Die Remedy-Integration kann zur Erstellung von Workflow-Anwendungen verwendet werden. Funktionen der Remedy-Integration:

- Die Möglichkeit, auf der Grundlage eines Vorfalls in Sentinel einen neuen Fall in Remedy Help Desk zu erstellen.
- Die Möglichkeit, bei der Aktualisierung eines Sentinel-Vorfalles den zugehörigen Fall in Help Desk zu aktualisieren.
- Die Möglichkeit, einen Sentinel-Vorfall zu aktualisieren, wenn ein zugehöriger Fall in Help Desk aktualisiert wird.

### Remedy Help Desk-Vorgänge

So senden Sie einen Vorfall hinsichtlich Remedy Help Desk (v5.0.1 und höher):

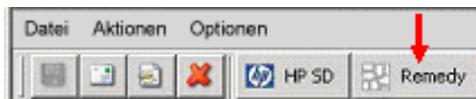
1. Klicken Sie auf die Registerkarte *Vorfälle*.
2. Erweitern Sie im Navigationsbereich den Ordner *Vorfallsansichten* und markieren Sie *Vorfallsansichts-Manager*.

---

**HINWEIS:** Wenn bereits ein Vorfall für ein anderes externes System festgelegt wurde, ist die Änderung nicht möglich.

---

3. Erweitern Sie eine der Vorfallsansichten und doppelklicken Sie auf Ihren Vorfall. Daraufhin wird Ihr Vorfall geöffnet.
4. Klicken Sie auf die Schaltfläche *Remedy* (Remedy).



Der Vorfall wird aktualisiert und weist im Anschluss eine Registerkarte mit der Bezeichnung „Externe Daten“ und eine Schaltfläche mit der Bezeichnung „Remedy“ (Remedy) auf.



So aktualisieren Sie einen Vorfall für Remedy Help Desk (v5.0.1. und höher):

1. Klicken Sie auf die Registerkarte *Vorfälle*.
2. Erweitern Sie den Navigationsbereich auf der linken Seite und doppelklicken Sie auf einen Vorfall, für den „Remedy Help Desk“ (Remedy Help Desk) angegeben ist.
3. Klicken Sie im Vorfall auf die Schaltfläche *Remedy*. Unterhalb der Extern-Registerkarte wird eine Anmerkung hinzugefügt.

## Manuelles Neukonfigurieren der Einstellungen für die Remedy-Schnittstelle

Bei der anfänglichen Installation der HP OpenView Service Desk-Drittanbieterschnittstelle werden die Service Desk- und OpenView-Einstellungen in der Datei `das_query.xml` gespeichert. Ziehen Sie die Informationen in diesem Abschnitt der Dokumentation zurate, wenn Sie diese Einstellungen nach der Installation ändern müssen.

### Remedy-Einstellungen

Remedy-Einstellungen werden in der Datei `das_query.xml` unter der `RemedyARServerService`-Komponente wie folgt gespeichert:

### Zurücksetzen des Remedy-Passworts

Die Remedy-Passwörter werden in der Datei `das_query.xml` im verschlüsselten Format gespeichert. Folglich müssen Sie, wenn Sie die in dieser Datei gespeicherten Passwörter zurücksetzen müssen, das nachfolgend beschriebene Dienstprogramm verwenden.

So setzen Sie das Passwort für die Remedy-Schnittstelle zurück:

1. Wechseln Sie zum Verzeichnis `%ESEC_HOME%/sentinel/bin/`
2. Geben Sie Folgendes ein:

```
extconfig -n das_query.xml [-r remedy_password]
```

- `-r` steht für das Remedy-Passwort

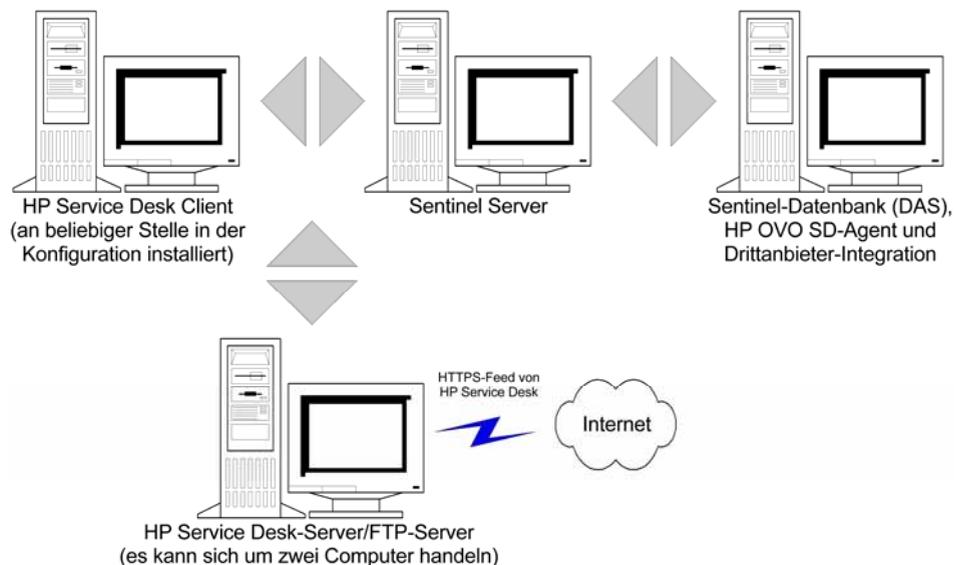
# 3

## Installieren von HP OpenView Service Desk unter Windows

Durch die bidirektionale HP OpenView Service Desk-Integration von Sentinel (separate Lizenz) wird Sentinel Console um neue nützliche Funktionen ergänzt. Sentinel nutzt die Bestandsverwaltungsfunktionen von HP OpenView Service Desk optimal und stellt so referenzielle Informationen bereit, die sich bei der Reaktion auf Sicherheitsbedrohungen und -angriffe als hilfreich erweisen. Mithilfe dieser neuen Funktionen können folgende Schritte durchgeführt werden:

- Vorfälle an HP Service Desk (SD) senden
- Ereignisse an einen HP SD-Vorfall anfügen
- Informationen zur Anfälligkeit an einen HP SD-Vorfall anfügen
- Informationen zu Konfigurationselementen (Bestand) sowohl von Sentinel Console-Vorfällen als auch von SD abfragen und füllen
- Round-Trip-Integration: SD sendet Aktualisierungen an Novell und Novell sendet Aktualisierungen an SD
- SD-Vorfallsstatus über Novell Sentinel Console aktualisieren
- Sentinel-Vorfallsstatus über HP SD aktualisieren

Nachfolgend ist eine typische Installationskonfiguration dargestellt. Ihre eigene Konfiguration kann abweichen.



# Systemanforderungen

Informationen zu Hardware- und Software-Anforderungen für HP OpenView Service Desk Client, Server und Agent finden Sie im Installationshandbuch zu HP OpenView Service Desk.

Sentinel unterstützt folgende Versionen von HP OpenView Service Desk:

- HP OpenView Service Desk Server – Version 4.5 mit Service Pack 8 (4.5.0588.0802 SP 8)
- HP OpenView Service Desk Client – Version 4.5 mit Service Pack 8
- HP OpenView Service Desk Agent – Version 4.5 mit Service Pack 8
- Sentinel 4.2.1.8 oder 4.2.1.15 für Windows
- Sämtliche Drittanbieter-FTP-Server

HP OpenView Service Desk Server und Client müssen auf einem Computer installiert werden, der als Service Desk-Server konfiguriert werden muss. Ziehen Sie hinsichtlich der Installation von Service Desk das Installationshandbuch zu HP OpenView Service Desk zurate.

Zur Aktivierung dieser bidirektionalen Schnittstelle muss eine HP OpenView Agent-Instanz auf dem Computer installiert werden, auf dem sich die Datei `das_cmd.bat` befindet. Über die bidirektionale Schnittstelle kann HP Service Desk Sentinel über jede Statusänderung eines Vorfalles informieren, der seinen Ursprung in Sentinel hat und von einem Service Desk-Benutzer geändert wurde. Diese Vorfälle müssen ihren Ursprung in Sentinel Console haben.

Damit Service Desk Anlagen verarbeiten kann, muss ein FTP-(File Transfer Protocol-)Server installiert werden (normalerweise auf einer Service Desk Server-Instanz) und Service Desk muss für die Kommunikation mit diesem Server konfiguriert werden. Es kann ein beliebiger Drittanbieter-FTP-Server verwendet werden. Ziehen Sie hinsichtlich der Installation des FTP-Servers das Installationshandbuch zu Ihrem FTP-Server zurate.

## Installation

Wenn Sie HP OpenView Operations ebenfalls installieren möchten, empfiehlt es sich, HP OpenView Operations vor HP OpenView Service Desk zu installieren.

---

**HINWEIS:** Bei der anfänglichen Installation der HP OpenView Service Desk-Drittanbieterschnittstelle werden die Service Desk- und OpenView-Einstellungen in der Datei `das_query.xml` gespeichert. Ziehen Sie hinsichtlich der Änderungen dieser Einstellungen (z. B. des Benutzernamens oder des Passworts) die Informationen zum *Betrieb von HP OpenView und Service Desk unter Windows 2000* zurate.

---

Es empfiehlt sich, die Installationen in dieser Reihenfolge vorzunehmen:

- FTP-Server:

---

**HINWEIS:** Ziehen Sie hinsichtlich der Installation Ihres FTP-Servers das Installationshandbuch zu Ihrem FTP-Server zurate.

---

- HP OpenView Service Desk Server mit Service Pack 8 – kann sich auf demselben Computer wie der FTP-Server befinden
- HP OpenView Service Desk Client mit Service Pack 8

- HP OpenView Service Desk Agent mit Service Pack 8 (zur Aktivierung der bidirektionalen Schnittstelle) – muss auf dem Computer installiert werden, auf dem sich DAS befindet

---

**HINWEIS:** Ziehen Sie hinsichtlich der Installation der HP OpenView Service Desk-Software das Installationshandbuch zu HP OpenView Service Desk zurate.

---

- Installieren Sie die Sentinel-Drittanbieter-Integration
  - HP OpenView Service Desk

---

**HINWEIS:** Informationen zur Installation finden Sie in den Versionshinweisen zu Sentinel v4.2.1.8 sowie im Installationshandbuch zu Sentinel v4.2 für Windows und Solaris.

---

## Konfigurieren von HP OpenView Service Desk

Die Konfiguration von HP OpenView Service Desk erfolgt über die Service Desk Client-Instanz. Sie benötigen folgende Informationen, bevor Sie die HP Service Desk-Konfiguration für die Kommunikation mit dem FTP-Server ändern:

- Name (Name) – IP-Adresse Ihres FTP-Servers
- Username/Password (Benutzername/Passwort) – Sämtliche für den FTP-Server festgelegte Benutzer
- Target Folder (Zielordner) – Empfohlene Eingabe: „/“. Hierdurch wird Ihr FTP-Verzeichnis auf das aktuelle FTP-Verzeichnis eingestellt.
- Deaktivieren Sie „Use Passive FTP“ (Passiv-FTP verwenden)
- Aktivieren Sie „Save attachment in background“ (Anlage im Hintergrund speichern)

---

**HINWEIS:** Weitere Informationen sowie detaillierte Anweisungen zur Konfiguration finden Sie im Abschnitt zu den nach der Installation durchzuführenden Aufgaben im Installationshandbuch zu HP OpenView Service Desk.

---

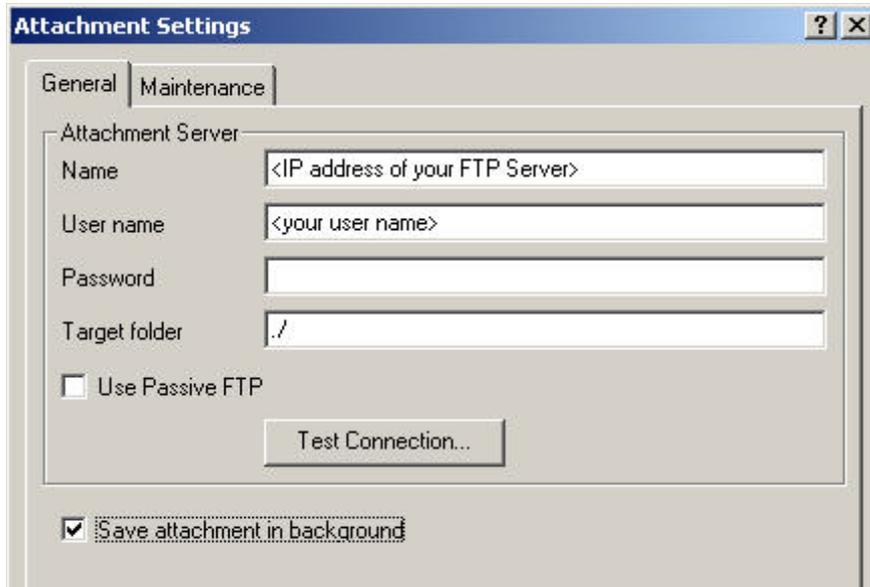
So legen Sie Einstellungen für Anlagen fest:

1. Starten Sie HP Service Desk Client.
2. Wählen Sie die Optionsfolge *Tools* (Tools) > *System* (System).
3. Klicken Sie im Navigationsbereich auf der linken Seite auf *System Panel* (Systemsteuerung).
4. Doppelklicken Sie auf *Attachment Settings* (Einstellungen für Anlagen). Geben Sie Folgendes ein:
  - Name (Name) – IP-Adresse Ihres FTP-Servers
  - Username/Password (Benutzername/Passwort) – Sämtliche für den FTP-Server festgelegte Benutzer
  - Target Folder (Zielordner) – Empfohlene Eingabe: „/“. Hierdurch wird Ihr FTP-Verzeichnis auf das aktuelle FTP-Verzeichnis eingestellt.
  - Deaktivieren Sie *Use Passive FTP* (Passiv-FTP verwenden)
  - Aktivieren Sie *Save attachment in background* (Anlage im Hintergrund speichern)

---

**HINWEIS:** Weitere Informationen sowie detaillierte Anweisungen zur Konfiguration finden Sie im Abschnitt zu den nach der Installation durchzuführenden Aufgaben im Installationshandbuch zu HP OpenView Service Desk.

---



5. Klicken Sie auf *Test Connection* (Verbindung testen).
6. Klicken Sie auf *Apply* (Übernehmen) und dann auf *OK* (OK).

## Aktivieren der (bidirektionalen) Service Desk-Sentinel-Schnittstelle

Dank dieser Option kann HP OVO OpenView Service Desk Sentinel über jede Statusänderung eines Vorfalls informieren, der seinen Ursprung in Sentinel hat und von einem Service Desk-Benutzer geändert wurde. Auf diese Weise kann die Verfolgung des aktuellen Status der einzelnen Vorfälle ermöglicht werden, die zuvor an HP OVO OpenView Service Desk gesendet wurden.

Zur Aktivierung dieser Funktion muss eine HP OVO OpenView Service Agent-Instanz auf dem Computer installiert werden, auf dem sich Sentinel (das\_cmd.bat) befindet. So kann HP Service Desk das das\_cmd-Dienstprogramm von Sentinel ausführen.

### Aktivieren der bidirektionalen Schnittstelle

1. Starten Sie Service Desk Client.
2. Rufen Sie die Administratorkonsole über *Tools* (Tools) > *System* (System) auf.
3. Klicken Sie im Navigationsbereich auf der linken Seite auf „Business Logic“ (Geschäftslogik).
4. Doppelklicken Sie auf *Database Rules* (Datenbankregeln).
5. Doppelklicken Sie auf *Incident* (Vorfall). Daraufhin wird das Fenster mit der Liste der Datenbankregeln eingeblendet.
6. Klicken Sie im Bereich mit den Datenbankregeln mit der rechten Maustaste und wählen Sie dann *New Database Rule* (Neue Datenbankregel).
7. Markieren Sie *When incident is modified* (Wenn Vorfall geändert wird) und klicken Sie dann auf *Next* (Weiter).

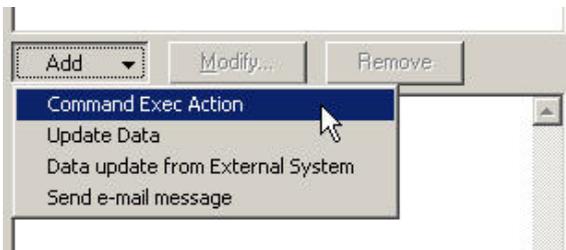
When incident is created or modified  
 When incident is created  
**When incident is modified**  
 When incident is deleted

8. Klicken Sie auf die Schaltfläche *Condition...* (Bedingung...).
9. Klicken Sie auf die Schaltfläche *Add Criterion...* (Kriterium hinzufügen...).
10. Klicken Sie auf die Schaltfläche für *Quick Find* (Schnellsuche), wählen Sie *Status* (Status) und wählen Sie dann im Operator-Feld *is anything* (beliebig).



Klicken Sie auf *OK* (OK) und dann erneut auf *OK* (OK).

11. Klicken Sie auf *Add* (Hinzufügen). Wählen Sie *Command Exec Action* (Aktion für Befehlsausführung).



12. Fügen Sie eine neue „Command Exec Action“ (Aktion für Befehlsausführung) hinzu, damit das `das_cmd.bat`-Skript bei jeder Auswertung der Regel in Sentinel Server ausgeführt wird.

Geben Sie beim Konfigurieren der Aktion in jedem Fall den Namen (bzw. die IP-Adresse) der Sentinel Server-Instanz als „Host“ (Host) an; hierbei handelt es sich um den Computer, auf dem sich `das_cmd.bat` befindet. Zudem muss der vollständige Pfad der Datei `das_cmd.bat` der Sentinel Server-Instanz unter „Command Line“ (Befehlszeile) angegeben werden. Beispiel:

```
c:\progra~1\esecur~1\sentinel\bin\das_cmd.bat
```

---

**HINWEIS:** Bei der Angabe von Verzeichnisnamen mit Leerschritten müssen Sie sich an die DOS 8.3-Benennungskonvention halten. Beispiel: Verwenden Sie „progra~1“ anstatt „Program Files“.

---

Bei der Angabe der „Parameters“ (Parameter) für die Aktion müssen Sie abschließend wie folgt vorgehen:

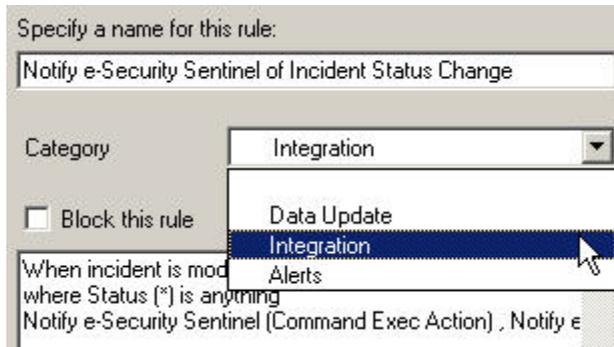
```
UpdateIncident servicedesk esecadm [Source ID] [ID]
„[Status]“
```

The screenshot shows a dialog box titled "Command Exec Action". It has several fields and controls:

- Name:** Notify e-Security Sentinel
- Description:** Notify e-Security Sentinel of a change in Incident Status.
- Host:** This command will be executed on the following host: <IP of Sentinel Server (where das\_cmd.bat is)
- Blocked:**  Blocked
- Command line:** c:\progra~1\esecur~1\sentinel\bin\das\_cmd.bat
- Parameters:** UpdateIncident servicedesk esecadm [Source ID] [ID] "[Status]"
- Insert at cursor position:** Field
- Buttons:** OK, Cancel

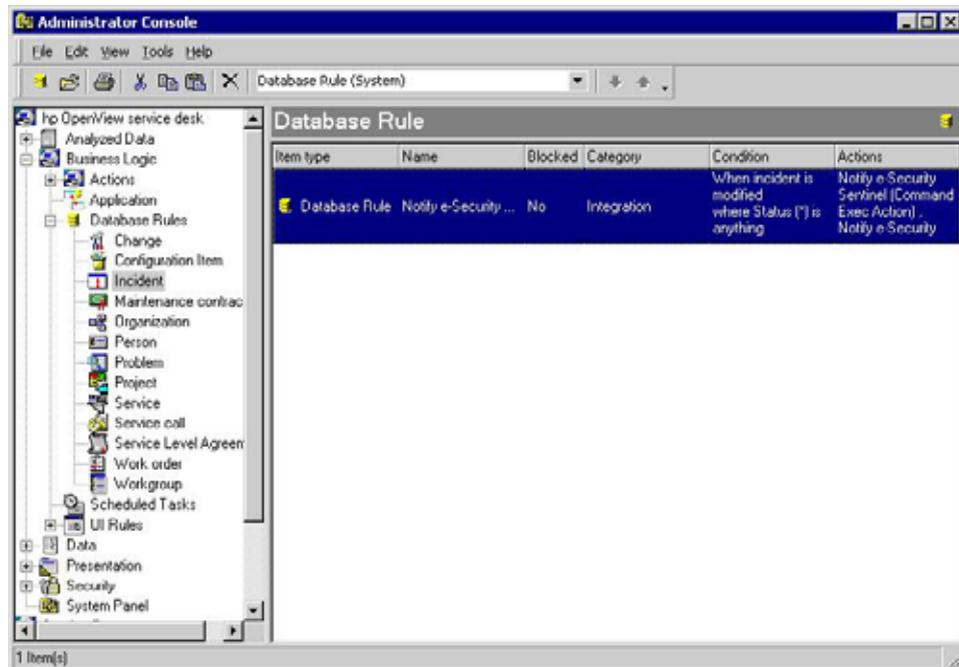
Vergeben Sie einen beliebigen Namen für die neue Datenbankregel und fügen Sie eine Beschreibung hinzu. Klicken Sie auf *OK* (OK) und dann auf *Next* (Weiter).

13. Wählen Sie im Feld „Category“ (Kategorie) den Eintrag „Integration“ (Integration) aus und geben Sie einen Namen für diese Regel an. Belassen Sie *Block this rule* (Diese Regel blockieren) deaktiviert.



Klicken Sie auf *Finish* (Fertig stellen).

14. Nachdem die Erstellung der neuen Datenbankregel abgeschlossen ist, sollte in der Liste der Datenbankregeln eine neue Regel aufgeführt werden.





# 4

## HP OpenView Service Desk-Integration

Mit HP OpenView für Sentinel können Sie von jedem Bildschirm mit Vorfällen und Ereignissen aus Ereignisse an HP OpenView Service Desk senden.

### HP OpenView Service Desk

Durch die Sentinel-Integration in HP OpenView Service Desk verfügen Sie über eine zusätzliche Funktion für die Bestandsverwaltung. Mithilfe dieser zusätzlichen Funktion für die Bestandsverwaltung können folgende Schritte durchgeführt werden:

- Vorfälle an HP Service Desk (SD) senden
  - Ereignisse an einen HP SD-Vorfall anfügen
  - Informationen zur Anfälligkeit an einen HP SD-Vorfall anfügen
  - Advisor-Informationen an einen HP SD-Vorfall anfügen
  - Informationen zu Konfigurationselementen (Bestand) von der Sentinel-Steuerungskonsole abfragen und auffüllen
- SD-Vorfallsstatus über die Sentinel-Steuerungskonsole aktualisieren
- Sentinel-Vorfallsstatus über HP SD aktualisieren

Die an HP OpenView Service Desk gesendeten Sentinel-Vorfallsinformationen umfassen:

- Sentinel-Vorfalls-ID
- Status
- Titel
- Anmerkungen/Verlauf
- Ereignisse (Anlage)
- Informationen zur Anfälligkeit (Anlage)
- Advisor-Informationen (Anlage)

Wenn Informationen an HP OpenView Service Desk gesendet bzw. von dort empfangen werden, werden automatische Statusermittlungs-, Statuszuordnungs- sowie Umwandlungsschritte ausgeführt.

Die Service Desk-Statuszuordnung und -umwandlung für Sentinel-Statusangaben gestaltet sich wie folgt:

Sentinel-Status	Service Desk-Status
Offen	Registered (Registriert)
Bestätigt	Waiting (Warten)
Zugewiesen	Informed (Benachrichtigt)
Wird untersucht	In Progress (Läuft)
Falsch positiv	Closed (Geschlossen)
Überprüft	Completed (Abgeschlossen)
Genehmigt	In Progress (Läuft)
Geschlossen	Closed (Geschlossen)

Die Sentinel-Statuszuordnung und -umwandlung für Service Desk-Statusangaben gestaltet sich wie folgt:

Service Desk-Status	Sentinel-Status
Registered (Registriert)	Offen
In Progress (Läuft)	Wird untersucht
Waiting (Warten)	Bestätigt
Completed (Abgeschlossen)	Überprüft
Informed (Benachrichtigt)	Zugewiesen
Closed (Geschlossen)	Geschlossen

## Senden von Vorfällen an HP OpenView Service Desk

So senden Sie einen Vorfall an HP OpenView Service Desk

1. Klicken Sie auf die Registerkarte *Vorfälle*.
2. Erweitern Sie im Navigationsbereich den Ordner *Vorfallsansichten* und markieren Sie *Vorfallsansichts-Manager*.

---

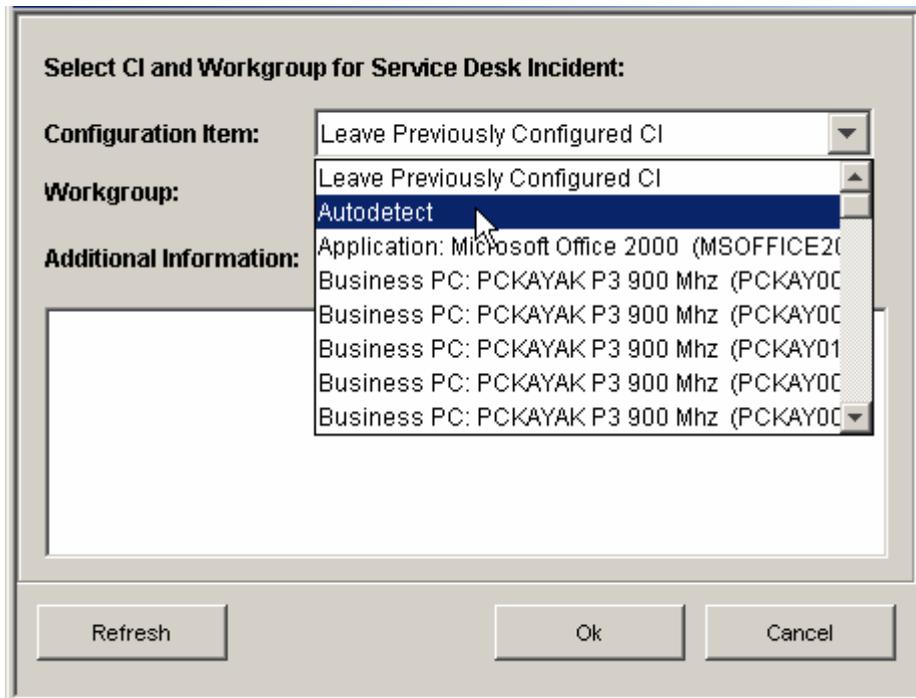
**HINWEIS:** Wenn bereits ein Vorfall für ein anderes externes System festgelegt wurde, ist die Änderung nicht möglich.

---

3. Erweitern Sie eine der Vorfallsansichten und doppelklicken Sie auf Ihren Vorfall. Daraufhin wird Ihr Vorfall geöffnet.
4. Klicken Sie auf die Schaltfläche für *HP SD*.



5. Daraufhin wird das Fenster *Vorfall an HP Service Desk senden* angezeigt. Im Dropdown-Menü *An Service Desk senden* finden Sie eine Konfigurationselement-Auswahlliste, die mit von HP Service Desk abgerufenen Konfigurationselementen gefüllt ist.



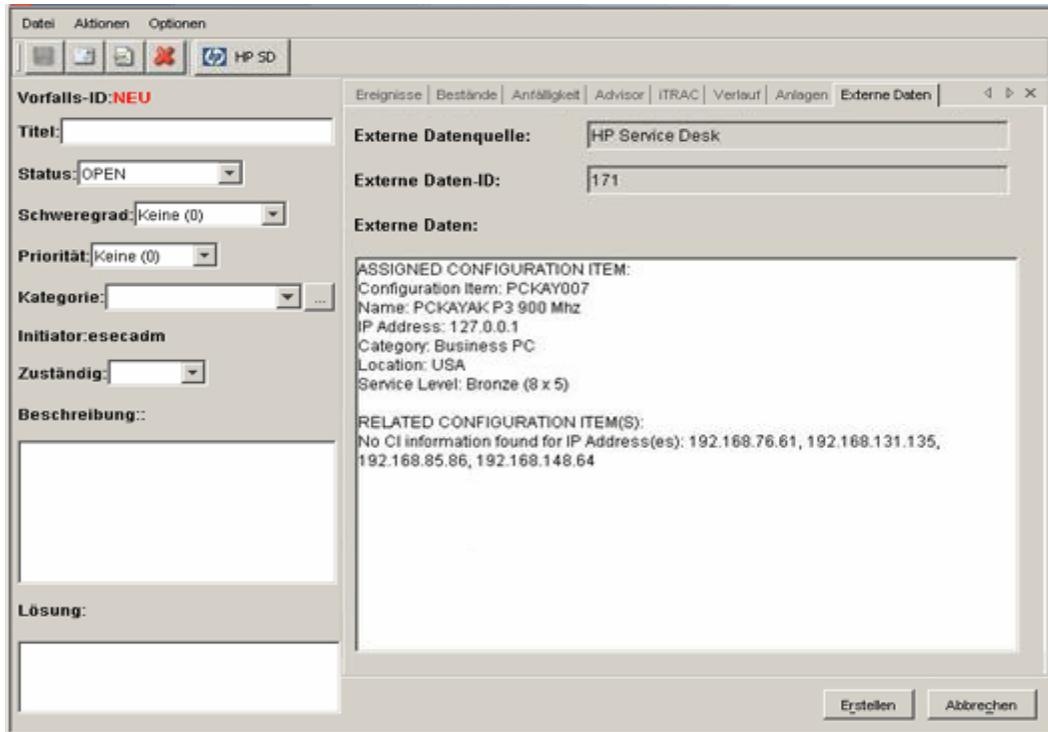
In der Auswahlliste mit Konfigurationselementen steht eine Option namens *Autom. Erkennung* zur Verfügung. Wenn Sie die Option *Autom. Erkennung* aktivieren, versucht Sentinel, anhand der Ziel-IP-Adressen der mit dem Sentinel-Vorfall verknüpften Ereignisse automatisch den zugehörigen Service Desk-Konfigurationseintrag zu ermitteln.

6. (Optional) Das Dialogfeld *An Service Desk senden* enthält zudem eine Arbeitsgruppen-Auswahlliste, die mit von Service Desk abgerufenen Arbeitsgruppen gefüllt ist.
7. Mit *OK* wird der Vorfall an *HP OpenView Service Desk* weitergeleitet.

---

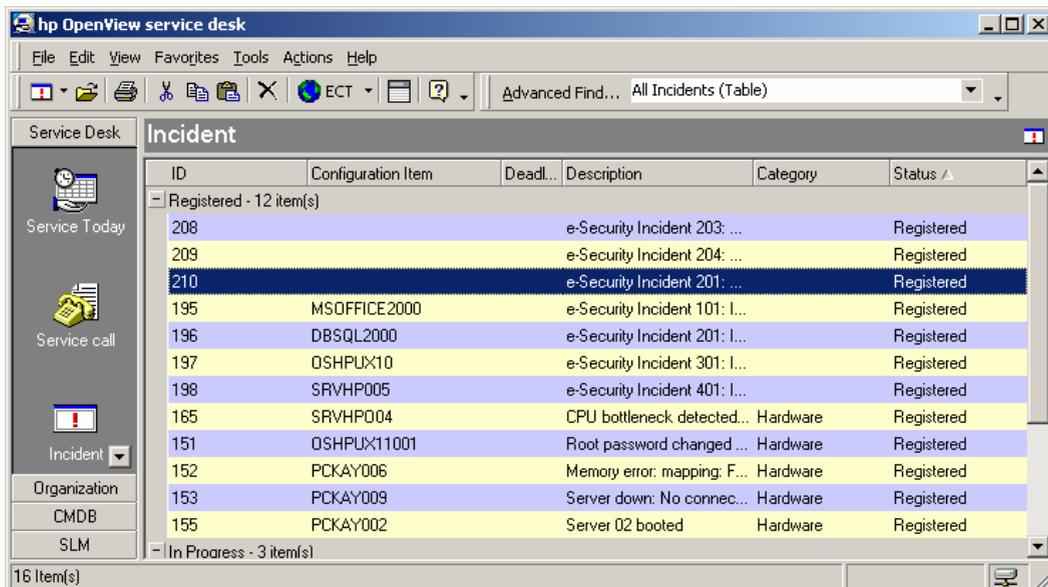
**HINWEIS:** Die Sentinel-Vorfallsanzeige wird aktualisiert und weist im Anschluss eine Registerkarte mit der Bezeichnung „Externe Daten“ auf. Aus der Registerkarte „Externe Daten“ gehen die Service Desk-Vorfalls-ID sowie der Service Desk-Konfigurationseintrag hervor, dem der neue Service Desk-Vorfall zugewiesen wurde.

---



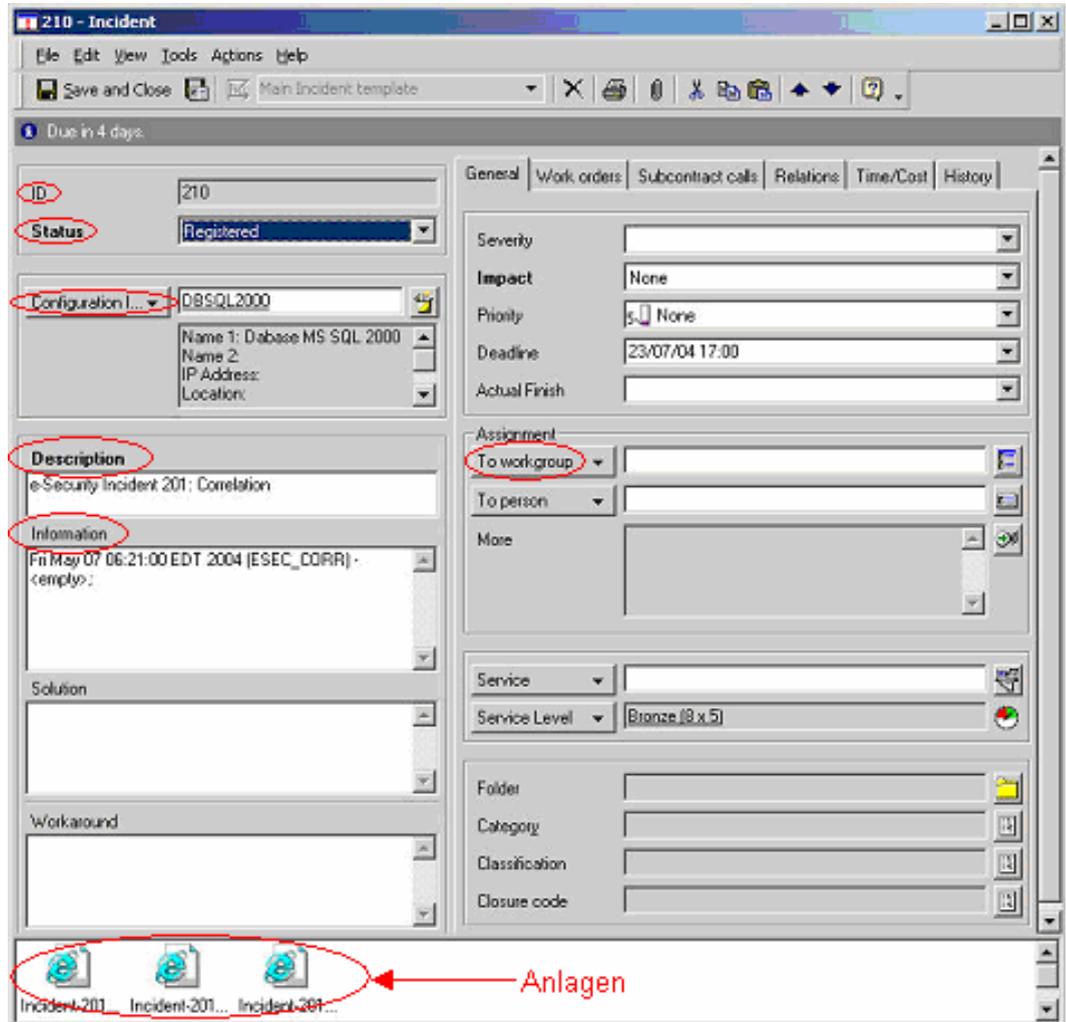
## HP OpenView Service Desk Client

Nachdem ein Vorfall an HP OpenView Service Desk gesendet wurde, wird der Vorfall in HP OpenView Service Desk Client angezeigt. In Service Desk Client wird der Vorfall anhand der erweiterten Daten-ID aufgelistet, nicht anhand der Vorfalls-ID-Nummer.



Wenn Sie auf einen Vorfall doppelklicken, werden die Details zu diesem Vorfall angezeigt.

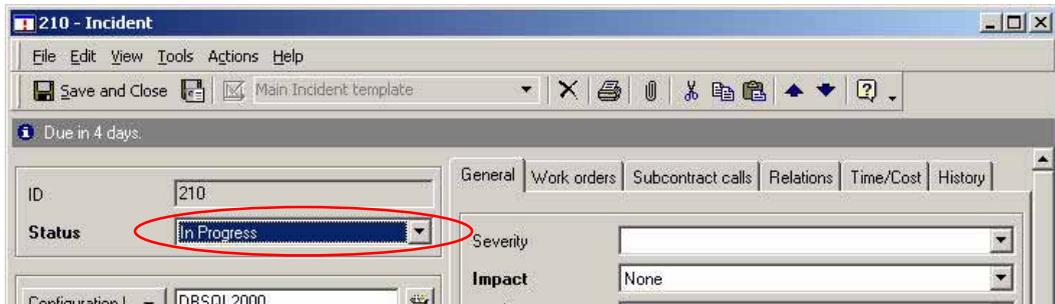
- Erweiterte Quell-ID
- Status
- Konfigurationseintrag
- Beschreibung
- Informationen
- Arbeitsgruppe
- Ereignisinformationen (Anlage)
- Informationen zur Anfälligkeit (Anlage)
- Advisor-Informationen (Anlage)



## HP OpenView Service Desk – Bidirektionale Schnittstelle

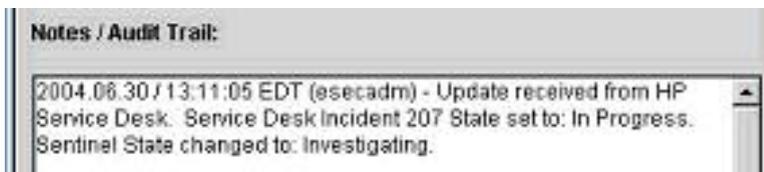
Wenn diese Option aktiviert ist (siehe Sentinel-Installationshandbuch), informiert Service Desk Sentinel über jede Statusänderung eines Vorfalls, der seinen Ursprung in Sentinel hat und von einem Service Desk-Benutzer geändert wurde. Auf diese Weise können Sentinel-Benutzer den aktuellen Status der einzelnen Vorfälle verfolgen, die an Service Desk gesendet wurden.

Wenn Sie die Detailanzeige einblenden, sie ändern und dann speichern, geht aus der Detailanzeige hervor, dass ein Vorgang läuft.



Diese Aktualisierung wird auch in HP OpenView Service Desk Client und dem Vorfallesfenster von Sentinel Console angezeigt.

In Progress - 4 item(s)			
207	DBSQL2000	e-Security Incident 205: ...	In Progress
210	DBSQL2000	e-Security Incident 201: ...	In Progress
201		e-Security Incident 701: I...	In Progress



## Manuelles Neukonfigurieren der Einstellungen der HP OpenView Service Desk-Schnittstelle

Bei der anfänglichen Installation der HP OpenView Service Desk-Drittanbieterschnittstelle werden die Service Desk-Einstellungen in der Datei `das_query.xml` gespeichert. Ziehen Sie die Informationen in diesem Abschnitt der Dokumentation zurate, wenn Sie diese Einstellungen nach der Installation ändern müssen.

### HP OpenView Service Desk-Einstellungen

HP OpenView Service Desk-Einstellungen werden folgendermaßen in der Datei `das_query.xml` unter der `HpServiceDeskService`-Komponente gespeichert:

- `server` – Wird auf den Hostnamen/die IP-Adresse von Service Desk Server eingestellt.
- `username` – Wird auf den Benutzernamen von Service Desk Server eingestellt.
- `password` – Wird mithilfe des im Abschnitt [Zurücksetzen von HP OpenView-Passwörtern](#) erläuterten Dienstprogramms auf das verschlüsselte Service Desk Server-Passwort eingestellt.
- `attachment_path` – Wird automatisch auf das Drittanbieter-„attach“-Verzeichnis eingestellt.
- `ftp_server` – Wird auf den Hostnamen/die IP-Adresse des FTP-Servers (den Service Desk für Anlagen verwendet) eingestellt.
- `ftp_username` – Wird auf den FTP-Benutzernamen (den Service Desk für Anlagen verwendet) eingestellt.
- `ftp_password` – Wird mithilfe des im Abschnitt [Zurücksetzen von HP OpenView-Passwörtern](#) erläuterten Dienstprogramms auf das verschlüsselte FTP-Benutzerpasswort (das Service Desk für Anlagen verwendet) eingestellt.
- `ftp_user_home` – Wird auf den vollständigen Verzeichnispfad des FTP-Benutzers eingestellt.

- attachment.events – Wird auf „yes“ (ja) eingestellt, um anzugeben, dass die Ereignisanlage verwendet wird.
- attachment.events.filename – Der für Ereignisanlagendateien verwendete Dateiname.
- attachment.vuln – Wird auf „yes“ (ja) eingestellt, um anzugeben, dass die Anfälligkeitsanlage verwendet wird.
- attachment.vuln.filename – Der für Anfälligkeitsanlagendateien verwendete Dateiname.
- attachment.adv.attack – Wird auf „yes“ (ja) eingestellt, um anzugeben, dass die Advisor-Angriffsanlage verwendet wird.
- attachment.adv.attack.filename – Der für Advisor-Angriffsanlagendateien verwendete Dateiname.

## Zurücksetzen von HP OpenView-Passwörtern

Die HP OpenView-Passwörter werden in der Datei das\_query.xml im verschlüsselten Format gespeichert. Folglich müssen Sie, wenn Sie die in dieser Datei gespeicherten Passwörter zurücksetzen müssen, das nachfolgend beschriebene Dienstprogramm verwenden.

So setzen Sie die Einstellungen für die HP OpenView Service Desk-Schnittstelle zurück:

1. Wechseln Sie zum Verzeichnis %ESEC\_HOME%/sentinel/bin/
2. Geben Sie Folgendes ein:

```
extconfig -n das_query.xml [-s sd_password] [-f
sd_ftp_password]
```

- „-s“ steht für das HP OpenView Service Desk Server-Passwort
- „-f“ steht für das FTP-Serverpasswort (für den FTP-Server, den Service Desk für Anlagen verwendet)



Bidirektionale Schnittstelle	
HP OpenView Service Desk.....	3-4
HP – Service Desk.....	4-1
HP OpenView Service Desk .....	3-1, 4-1
Installation .....	3-2
Konfigurieren für FTP-Server .....	3-3
Senden eines Vorfalls (v5.0) .....	4-2
So legen Sie Einstellungen für Anlagen fest.....	3-3
HP SD .....	4-1
HP Service Desk .....	3-1, 4-1
Installation .....	3-2
Konfiguration für FTP-Server.....	3-3
Senden eines Vorfalls (v5.0) .....	4-2
So legen Sie Einstellungen für Anlagen fest.....	3-3
HP-OpenView-Vorgänge.....	4-1
HP-OVO .....	4-1

Installation	
HP OpenView Service Desk.....	3-2
Sentinel .....	1-11
Installation Sentinel .....	1-11
Remedy .....	1-1
Remedy Help Desk .....	2-1
Ändern des Fallformulars .....	1-2
Datenfluss .....	1-6
Datenfluss – Ausgabezuordnung.....	1-9
Datenfluss – Eingangszuordnung.....	1-9
Erstellen des Web-Service .....	1-2
Installation von Sentinel.....	1-11
opCreate – Ausgabe.....	1-3
opCreate – Eingabe.....	1-5
opSet –Eingabe .....	1-6
Senden eines Vorfalls an Remedy Help Desk (v5.0.1 und höher).....	2-1
Vorfallseinrichtung (v5.0.1 und höher).....	2-1

