



# Administratorhandbuch

HP Session Allocation Manager (HP SAM) v.3.2

© Copyright 2007-2010 Hewlett-Packard Development Company, L.P. Änderungen vorbehalten.

Microsoft und Windows sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Die Garantien für HP Produkte werden ausschließlich in der entsprechenden, zum Produkt bzw. Service gehörigen Garantieerklärung beschrieben. Aus dem vorliegenden Dokument sind keine weiteren reichenden Garantiesprüche abzuleiten. Hewlett-Packard („HP“) haftet – ausgenommen für die Verletzung des Lebens, des Körpers, der Gesundheit oder nach dem Produkthaftungsgesetz – nicht für Schäden, die fahrlässig von HP, einem gesetzlichen Vertreter oder einem Erfüllungsgehilfen verursacht wurden. Die Haftung für grobe Fahrlässigkeit und Vorsatz bleibt hiervon unberührt.

Dieses Dokument enthält urheberrechtlich geschützte Informationen. Ohne schriftliche Genehmigung der Hewlett-Packard Company darf dieses Dokument weder kopiert noch in anderer Form vervielfältigt oder übersetzt werden.

MIT-Lizenz

<http://sourceforge.net/projects/expat/>  
<http://www.opensource.org/licenses/mit-license.php>

Jeder Person, die eine Kopie dieser Software und der zugehörigen Dokumentationsdateien (nachstehend „Software“ genannt) erlangt, wird hiermit kostenfrei gestattet, die Software ohne Einschränkungen zu nutzen. Diese Berechtigung gilt uneingeschränkt auch für das Verwenden, Kopieren, Ändern, Zusammenführen, Veröffentlichen, Verteilen, Unterlizenzieren und/oder Verkaufen von Kopien dieser Software und das Erteilen der Berechtigung zur Ausübung dieser Tätigkeiten an Personen, denen die Software zur Verfügung gestellt wird, sofern die folgenden Bedingungen erfüllt werden:

Der oben genannte Urheberrechtsvermerk und der vorliegende Genehmigungsvermerk müssen in allen Kopien oder wesentlichen Teilen der Software enthalten sein. DIESE SOFTWARE WIRD „OHNE MÄNGELGEWÄHR“ BEREITGESTELLT, ALSO OHNE JEDLICHE AUSDRÜCKLICHE ODER KONKLUDENTE GEWÄHRLEISTUNG EINSCHLIESSLICH DER GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER DER NICHTVERLETZUNG DER RECHTE DRITTER. DIE URHEBER UND DIE INHABER DER URHEBERRECHTE SIND UNTER

KEINEN UMSTÄNDEN HAFTBAR FÜR JEDLICHE ANSPRÜCHE, SCHÄDEN ODER ANDERE HAFTUNGSANSPRÜCHE, UNABHÄNGIG DAVON, OB SICH DIESE ANSPRÜCHE ODER SCHÄDEN AUS DEM VERTRAG, AUS UNERLAUBTEN HANDLUNGEN ODER AUS ANDEREN GRÜNDEN AUS ODER IM ZUSAMMENHANG MIT DER SOFTWARE ODER DER VERWENDUNG ODER ANDERER VORGÄNGE IN DER SOFTWARE ERGEBEN.

Copyright © 2006 bei Open Source Initiative

Technische Fragen zur Website beantwortet Steve M, Webmaster bei [opensource.org](http://opensource.org/) /  
Rechtliche Fragen zu Open Source beantwortet das Board of Directors.

Die Inhalte dieser Website fallen unter die Bestimmungen der Open Software License 2.1 oder der Academic Free License 2.1. Die Open Source Initiative (OSI) ist eine eingetragene gemeinnützige Organisation gemäß Abschnitt 501(c)(3) der US-Abgabenordnung. Mit Ihrer Spende können Sie die Arbeit der OSI unterstützen.

Bei einem Teil der in dieses Produkt eingebetteten Software handelt es sich um gSOAP-Software.

Mit gSOAP erstellte Abschnitte sind urheberrechtlich geschützt: Copyright (C) 2001-2004 Robert A. van Engelen, Genivia inc. Alle Rechte vorbehalten.

DIE SOFTWARE IN DIESEM PRODUKT WIRD TEILWEISE VON GENIVIA INC BEREITGESTELLT, UND ALLE AUSDRÜCKLICHEN UND KONKLUDENTEN GEWÄHRLEISTUNGEN, UNTER ANDEREM (JEDOCH NICHT AUSSCHLIESSLICH) DIE KONKLUDENTE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, WERDEN AUSGESCHLOSSEN. DER AUTOR HAFTET IN KEINEM FALL WEDER FÜR DIREKTE, INDIREKTE, BEILÄUFIGE, SPEZIELLE UND EXEMPLARISCHE SCHÄDEN NOCH FÜR FOLGESCHÄDEN (DIES SCHLIESST U. A. DIE BESCHAFFUNG VON ERSATZPRODUKTEN ODER -DIENSTLEISTUNGEN, NUTZUNGSSCHÄDEN, DEN VERLUST VON DATEN ODER GEWINNEN UND BETRIEBSUNTERBRECHUNGEN EIN), UNGEACHTET DER URSACHEN UND ZUGRUNDE LIEGENDEN HAFTUNGSTHEORIEN SOWIE UNABHÄNGIG VON VERTRÄGEN, VERSCHULDENSUNABHÄNGIGER HAFTUNG UND UNERLAUBTEN HANDLUNGEN (EINSCHLIESSLICH FAHRLÄSSIGER UND SONSTIGER

HANDLUNGEN), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE ENTSTANDEN SIND, SELBST WENN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE.

Copyright (c) 1998-2007 The OpenSSL Project. Alle Rechte vorbehalten.

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com). Alle Rechte vorbehalten.

## Administratorhandbuch

### HP Session Allocation Manager (HP SAM) Version 3.2

7. Auflage (November 2010)

Sechste Ausgabe (April 2010)

Fünfte Ausgabe (August 2009)

Vierte Ausgabe (November 2008)

Dritte Ausgabe (Dezember 2007)

Zweite Ausgabe (August 2007)

Erste Ausgabe (Juni 2007)

Teilenummer des Dokuments: 453252-047

## Allgemeines

- 
- △ **VORSICHT!** In dieser Form gekennzeichnete(r) Text weist auf Verletzungs- oder Lebensgefahr bei Nichtbefolgen der Anleitungen hin.
  - △ **ACHTUNG:** In dieser Form gekennzeichnete(r) Text weist auf die Gefahr von Hardware-Schäden oder Datenverlust bei Nichtbefolgen der Anleitungen hin.
  - 📄 **HINWEIS:** In dieser Form gekennzeichnete(r) Text weist auf wichtige Zusatzinformationen hin.
-



---

# Inhaltsverzeichnis

<b>1 Einführung .....</b>	<b>1</b>
Was in dieser Version neu ist .....	1
Hauptmerkmale .....	2
Überblick .....	3
Funktionsweise von HP SAM .....	4
HP SAM Software-Komponenten .....	7
Remote Graphics Software (RGS) .....	7
Häufige Aufgaben .....	8
Einrichtung des HP SAM .....	8
Einrichten eines Benutzers mit einer dynamischen Ressource .....	9
Einrichten eines Benutzers mit statischen (dedizierten) Ressourcen .....	10
Konfigurieren eines Monitorlayouts für einen Benutzer .....	11
<b>2 Anforderungen .....</b>	<b>13</b>
HP SAM – Hardware- und Softwareanforderungen .....	13
Architekturempfehlungen und optimale Vorgehensweisen zur Einrichtung einer HP SAM	
Umgebung .....	13
Domänenumgebungsanforderungen für HP SAM .....	16
Anforderungen für HP SAM Web und SQL Server .....	16
Anforderungen für den HP SAM Registrierungsdienst .....	23
Anforderungen für Zugriffsgeräte .....	23
Thin Client .....	24
Mobiler Thin Client .....	24
Desktop- oder Notebook-PC .....	24
Blade Workstation Clients .....	25
Personal Workstation Clients .....	25
Weitere Anforderungen .....	26
Erstellen eines Dienstkontos .....	26
Erlangen von Administratorrechten .....	26
Ändern der Firewall .....	26
Active Directory .....	26
<b>3 Installation .....</b>	<b>27</b>
Installationsreihenfolge .....	27
Neuinstallation .....	27
Upgrade .....	27

Installieren des HP SAM Webservers und der SQL-Software .....	28
Benutzern Administratorzugang zu HP SAM gewähren .....	31
Konfigurieren der HP SAM Systemeinstellungen .....	31
Konfigurieren von Secure Sockets Layer (SSL) .....	32
Installieren und Validieren der HP SAM Registrierungsdienst-Software .....	32
Installieren des HP SAM Registrierungsdienstes .....	32
Erstellen der Konfigurationsdatei für den HP SAM Registrierungsdienst .....	33
Starten/Neustarten des HP SAM Registrierungsdienstes .....	36
Testen des HP SAM Registrierungsdienstes .....	36
Installieren und Validieren der HP SAM Client-Software .....	37
Internet Explorer-basierter Client .....	38
Windows-basierter Client .....	39
Linux-basierter Client .....	40
Konfigurationseinstellungen .....	43
Globale und lokale Client-Konfigurationsdateien .....	53
Banner für rechtliche Hinweise .....	55
Bereitstellen des HP SAM Registrierungsdienstes auf allen HP SAM Rechnerressourcen .....	56
Bereitstellen der HP SAM Client-Software auf allen HP SAM Zugriffsgeräten .....	57

#### **4 Verwaltung ..... 58**

Anmelden .....	58
Allgemeine Navigation und Aufbau der Benutzeroberfläche .....	58
Anzeigen von mehr (oder weniger) Elementen pro Seite .....	58
Verschieben von Spalten .....	58
Sortieren der Ergebnisliste .....	58
Auswählen von mehr als einem Element .....	59
Verwalten der HP SAM Administratorzugangsliste .....	59
Hinzufügen einzelner Benutzer zur Gruppe der HP SAM Administratoren .....	59
Hinzufügen von Sicherheitsgruppen oder organisatorischen Einheiten zur HP SAM Administratorgruppe .....	60
Entfernen von Benutzern oder Gruppen aus der HP SAM Administratorgruppe .....	60
Registerkarten in der HP SAM-Verwaltungskonsole .....	62
Registerkarte „Home“ .....	62
Registerkarte „Benutzer und Rollen“ .....	62
Registerkarte „Ressourcen“ .....	72
Verwalten von Rechenzentren .....	75
Registerkarte „Richtlinien“ .....	76
Registerkarte „Systemeinstellungen“ .....	80
Registerkarte „Berichte“ .....	87
Registerkarte „Protokoll“ .....	91
Einrichten der Smartcard-Anmeldung auf dem Zugangsgerät .....	92

Konfigurieren von Sitzungszeitbeschränkungen für Remote-Sitzungen .....	93
Sitzungszeitgeber für Linux .....	95
Ressourcenreservierungen (auch bekannt als Zugriffsbeschränkungen) .....	96
Vor Zuweisung authentifizieren .....	98
<b>Anhang A Firewall-Regeln .....</b>	<b>99</b>
Webserver .....	99
Clients .....	99
Ressourcen .....	100
SQL-Server .....	100
<b>Anhang B Häufig gestellte Fragen (FAQ) .....</b>	<b>101</b>
<b>Anhang C Registrierungsdienst – Fehlercodes .....</b>	<b>108</b>
<b>Anhang D Glossar .....</b>	<b>111</b>
<b>Index .....</b>	<b>113</b>





# 1 Einführung

HP Remote Client-Lösungen dienen zur Unterstützung des Benutzers bei vielen verschiedenen Aufgaben, von sehr einfachen bis hin zu anspruchsvollen, professionellen und technischen Anwendungen. Gleichzeitig verleihen sie der IT größere Kontrolle über Technologieressourcen, vereinfachen das Desktop Management, erhöhen die Flexibilität und reduzieren in vielen Fällen die Gesamtunterhaltungskosten.

Den HP Remote Client-Lösungen liegt eine einheitliche Infrastruktur zugrunde, die Client-Bereitstellung, Sitzungszuweisung und den Ausgleich von Rechnerressourcen ermöglicht und die Geschäftsanforderungen vieler verschiedener Benutzer mithilfe eines bewährten Tool-Satzes unterstützt.

Das HP Session Allocation Manager-System (HP SAM) ist der Kontrollpunkt für die Verwaltung des Einsatzes von HP Remote Client-Lösungen. HP SAM verwaltet die Zuweisung von Verbindungen von einem Client-Zugriffsgerät eines Endbenutzers zu Desktop-Sitzungen, die auf Rechnerressourcen an einem zentralen Standort (meist einem Rechenzentrum) ausgeführt werden. HP SAM stellt diese Desktop-Sitzungen Benutzern nach Bedarf zur Verfügung.

Weitere Informationen zu HP Remote Client-Lösungen finden Sie unter <http://www.hp.com/go/rcs>.

## Was in dieser Version neu ist

- Option für die bevorzugte Zuweisung von zuletzt verwendeten Ressourcen:
  - Bei den Vorgängerversionen von HP SAM und wenn diese Option deaktiviert ist (was der Standardeinstellung entspricht), weist SAM Ressourcen innerhalb von einer Rolle einem Benutzer zu und stellt dabei vorzugsweise eine Ressource bereit, die nicht zuletzt verwendet wurde. Dies ermöglicht eine gleichmäßigere Auslastung der Ressourcen.
  - Wenn diese neue Option (sie befindet sich auf der Registerkarte General (Allgemein) unter System Settings (Systemeinstellungen) auf der HP SAM-Verwaltungskonsolle) aktiviert ist, weist SAM die Ressourcen innerhalb einer Rolle einem Benutzer zu und bevorzugt dabei die Ressource, die von diesem Benutzer zuletzt verwendet wurde.
  - Wichtiger Hinweis: SAM kann nicht gewährleisten, dass einem Benutzer dessen zuletzt verwendete Ressource zugewiesen wird, weil diese möglicherweise bereits von einem anderen Benutzer verwendet wird. Wenn Sie sicherstellen möchten, dass jedem Benutzer immer dieselbe Ressource zugewiesen wird, sollten Sie nicht mit Rollen, sondern mit Dedicated Resources (Reservierten Ressourcen) arbeiten.
  - Zu beachten ist auch, dass diese Funktion keine Auswirkungen auf die Zuweisung hat, wenn der Benutzer laufende oder getrennte Sitzungen hat. SAM versucht stets, die für den Benutzer reservierten Ressourcen zuzuweisen, unabhängig von dieser Einstellung. Zudem hat die

Funktion keine Auswirkungen auf Dedicated Resources (Reservierte Ressourcen) oder auf die entsprechenden Backup-Ressourcen oder Backup-Rollen.

- Zusätzlicher Support:
  - Linux RHEL6 auf Zugangsgeräten und -ressourcen
  - Ressourcen von VMware Virtual Machine Linux
  - HP T5740e (WES7) Thin Clients
  - Microsoft SQL 2008 R2
- Steuerung der Linux-Ressourcen über die HP SAM-Verwaltungskonsole:
  - SAM 3.2 wurde um den Support für die Remote-Ausführung der folgenden Vorgänge auf Linux-basierten Ressourcen von der Seite Resources (Ressourcen) auf der HP SAM-Verwaltungskonsole aus erweitert:
    - Herunterfahren
    - Neustart
    - Abmelden
  - Diese Vorgänge funktionierten vorher nur bei Windows-basierten Ressourcen.
  - Der Vorgang Send Message (Nachricht senden) wird bei Linux-Ressourcen immer noch nicht unterstützt.
  - Dieser Vorgang funktioniert nur mit den SAM 3.2-Versionen von SAM Linux Blade Service und SAM Server.
  - Ein Zertifikat von der Domain-Zertifizierungsstelle muss auf der HP SAM-Website installiert sein, um diese Funktion zu aktivieren.
- Neue SAM-Policys für RGS Experience-Eigenschaften:
  - In RGS 5.4.5 werden neue RGS-Einstellungen eingeführt, die die Funktionalität in einer WAN-Umgebung mit verringerter Bandbreite optimieren soll: Diese Einstellungen umfassen die Auswahl zwischen fester Bildqualität und automatischer Anpassung der Bildqualität, die Einstellung der Mindestbildqualität und die Aktualisierungsrate bei Verwendung der Option für die automatische Anpassung. SAM 3.2 bietet dem SAM-Administrator die Möglichkeit, diese Einstellungen über die SAM-Server-Policy bei den Endbenutzern zu erzwingen. Nähere Informationen zur Verwendung dieser neuen RGS-Einstellungen sind im RGS-Benutzerhandbuch enthalten.

## Hauptmerkmale

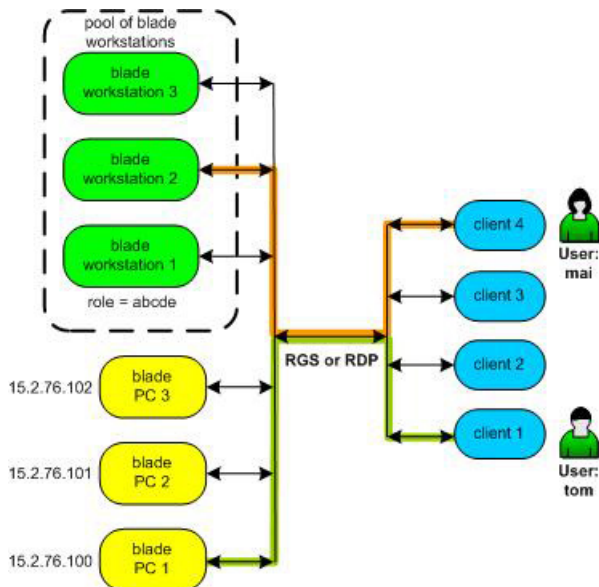
- Zuweisung von Benutzern zu Rechnerressourcen (z. B. Blade-PCs, Workstation Blades oder virtuelle Maschinen)
- Selbstregistrierung der Rechnerressourcen
- Zentrale Verwaltung der Einstellungen für Remote-Verbindungen mit Zugriffsgeräten
- Follow-Me-Roaming und Persistenzunterstützung zur Ermöglichung einer erneuten Verbindung mit einer offenen Sitzung von einem anderen Gerät aus

- Anpassbare Verwaltungsstufen
- Berichte zur Verwendungs- und Kapazitätsplanung
- Dedizierter Benutzer/Dediziertes Display zur Abbildung der Rechnerressourcen

## Überblick

HP SAM ermöglicht die automatische Bereitstellung von Remote-Rechnerressourcen an Benutzer.

**Abbildung 1-1** HP SAM Konfiguration



HP SAM kann so konfiguriert werden, dass ein Benutzer eine Verbindung zur Desktop-Sitzung einer bestimmten Remote-Rechnerressource herstellen kann (identifiziert durch Hostname oder IP-Adresse). Man spricht dabei von einer statischen Verbindung. In [Abbildung 1-1, „HP SAM Konfiguration“, auf Seite 3](#) wurde HP SAM so konfiguriert, dass der Benutzer Tom eine statische Verbindung zum Blade-PC 1 mit der IP-Adresse 15.2.76.100 herstellen konnte. Unabhängig davon, welches Zugriffsgerät Tom verwendet, wird er automatisch mit dem Blade-PC 1 unter der Adresse 15.2.76.100 verbunden.

HP SAM kann auch so konfiguriert werden, dass ein Benutzer eine Verbindung zu einer beliebigen Remote-Rechnerressource herstellen kann. Man spricht dabei von einer dynamischen Verbindung. HP SAM ermöglicht es dem Administrator, eine oder mehrere Rollen für jede Rechnerressource zu definieren. Eine Rechnerressource mit der Rolle „abcde“ kann beispielsweise mit Anwendungen zur Ausführung von Aktientransaktionen oder Buchführungsfunktionen konfiguriert werden. In [Abbildung 1-1, „HP SAM Konfiguration“, auf Seite 3](#) wurde HP SAM so konfiguriert, dass die Benutzerin Mai eine dynamische Verbindung zu einer von drei Blade Workstations herstellen konnte, die die Rolle „abcde“ unterstützen.


HP SAM verwendet die HP Remote Graphics Software (RGS) oder das Microsoft® Remote Desktop Protocol (RDP), um eine Verbindung zwischen Zugriffsgeräten und Rechnerressourcen herzustellen.

RGS verfügt über Funktionen, die sich besonders gut für Remote-Computing eignen. RGS ermöglicht die sehr schnelle Erfassung, Komprimierung und Übertragung des Desktop-Abbilds (die tatsächlichen Rahmenpuffer-Pixel) mithilfe von Standard-TCP/IP-Netzwerken. Weitere Informationen zu RGS finden Sie unter <http://www.hp.com/go/rgs>.

## Funktionsweise von HP SAM


1. Wenn ein Benutzer an einem Zugriffsgerät (Desktop, Notebook, Thin Client) eine Desktop-Sitzung anfordert, sendet der HP SAM Client eine Anfrage an den HP SAM Server.
  - a. Bei entsprechender Konfiguration unterstützt HP SAM einen Server-Failover. Wenn der HP SAM Webserver nicht reagiert, sendet der HP SAM Client die Anfrage an den nächsten HP SAM Webserver in der Liste.
  - b. Der HP SAM Client sendet den Benutzernamen und die Domänendaten an den HP SAM Server.
2. Der HP SAM-Webserver empfängt den Benutzernamen und den Domainnamen vom HP SAM-Client. Der Webserver gleicht diese Informationen mit dem Microsoft Active Directory-Server ab. Das Konto muss gültig und im Active Directory aktiviert sein, damit der Vorgang fortgesetzt werden kann. Normalerweise wird das Passwort noch nicht an diesem Punkt authentifiziert, sondern erst bei der Anmeldung beim Betriebssystem der Ressource. Bei HP SAM 3.0 oder höher kann die Funktion **Authenticate Before Allocation (Vor Zuweisung authentifizieren)** aktiviert werden. Dadurch wird die Passwort-Authentifizierung bereits bei diesem Schritt durchgeführt.
3. Der HP SAM Webserver sendet die entsprechenden Desktop-Sitzungsinformationen an den HP SAM Client zurück.
  - a. Der HP SAM Webserver bestimmt, ob der Benutzer noch eine Desktop-Sitzung ausführt oder nicht. Wenn dem so ist, stellt der Webserver eine neue Verbindung zur selben Sitzung her (daher der Name Follow-Me-Roaming). Wenn der Benutzer über keine bestehende Desktop-Sitzung verfügt, überprüft der HP SAM Webserver seine interne Datenbank auf verfügbare Ressourcen und verbindet den Benutzer mit einer geeigneten Ressource.
  - b. Wenn einem Benutzer mehrere Rollen oder Ressourcen zugeordnet sind, muss er eine bestimmte auswählen.
  - c. Die an den HP SAM Client zurückgesendeten Daten enthalten die IP-Adressen (oder Hostnamen, je nach Konfiguration auf dem HP SAM Webserver) der entsprechenden Ressourcen.
  - d. Wenn keine Rechnerressource verfügbar ist, informiert der HP SAM Client den Benutzer.
4. Der HP SAM Client stellt eine Verbindung zur entsprechenden Desktop-Sitzung her.

---

 **HINWEIS:** HP SAM verwendet die HP Remote Graphics Software (RGS) oder das Microsoft® Remote Desktop Protocol (RDP), um eine Verbindung zwischen Zugriffsgeräten, Rechnerressourcen und organisatorischen Einheiten herzustellen.

---
5. Der Benutzer wird in dem anschließend angezeigten Anmeldefenster zur Passworteingabe aufgefordert. Der Benutzername und die Domain werden automatisch vom HP SAM-Client eingetragen. Dieser Schritt entfällt, wenn der Benutzer das Passwort bereits im HP SAM-Client eingegeben hat und entweder RDP verwendet wird oder RGS im Single Sign-on-Modus aktiviert ist.

---

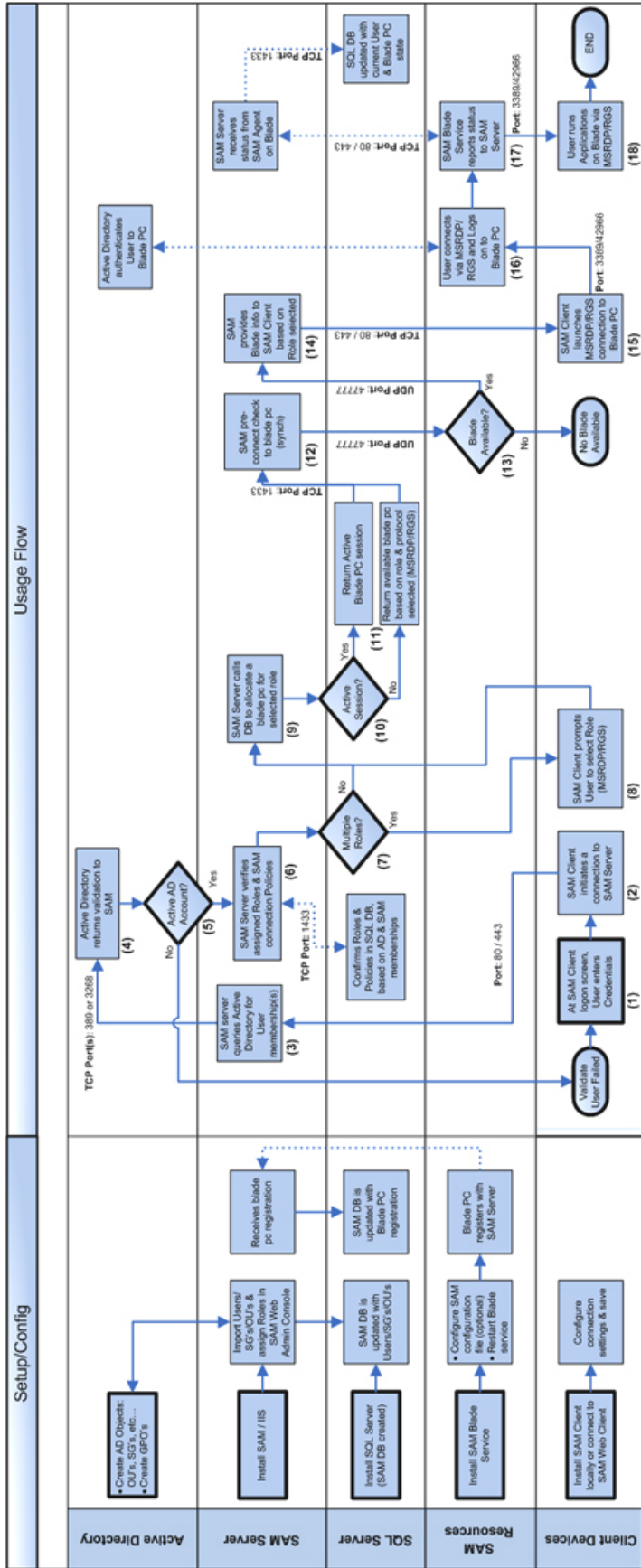
 **HINWEIS:** Mit RDP, RGS 5.1 oder höher oder der Funktion „Vor Zuweisung authentifizieren“ (siehe [„Vor Zuweisung authentifizieren“ auf Seite 98](#)) ermöglicht HP SAM Benutzern mit abgelaufenen Passwörtern die Anmeldung. Diese werden dann aufgefordert, das Passwort umgehend zu aktualisieren.

---

6. Sobald der Benutzer sich anmeldet, benachrichtigt der HP SAM Registrierungsdienst auf der Rechnerressource den HP SAM Webserver.
7. Sobald der Benutzer die Verbindung trennt oder sich abmeldet, aktualisiert der HP SAM Registrierungsdienst den HP SAM Webserver mit den neuen Informationen.



# High-level HP SAM Config & Usage Flow



**Active Directory**

- Minimum Configuration Requirements
  - SAM service account to be identified and created as Domain User
  - Firewall port exceptions and/or application blades to be identified & configured for SAM
  - Remote Desktop Users group to be populated appropriately
  - Terminal Services enabled

**SAM Server**

- Minimum Configuration Requirements
  - Local Admin rights required to install SAM Web Admin console
  - SAM service account used, with local admin rights during install
  - Added to SAM database
  - Added to SAM website
  - Enter SA account (or equivalent) password
  - Open appropriate Firewall ports
  - IIS w/ASP.net enabled
  - Net Framework 2.0
  - After Blade PC registration, it is recommended that you "synchronize" all blade pc's with SAM Server

**SQL Server**

- Minimum Configuration Requirements
  - Configure in "Mixed-Mode"
  - SA account (or equivalent) and password identified for installation only

**Client Devices**

- Minimum Configuration Requirements
  - Ability to install ActiveX controls for SAM
  - Firewall port exceptions applied
  - Need to add the SAM Web Client URL to the IE "Trusted Sites" list

**SAM Resources**

- Minimum Configuration Requirements
  - Firewall port exceptions
  - UDP 47777 (or custom) blade service
  - Local Admin required for service account on blade pc-o perform log-off, reboot, etc...

**Client Devices**

- Minimum Configuration Requirements
  - Ability to install ActiveX controls for SAM
  - Firewall port exceptions applied
  - Need to add the SAM Web Client URL to the IE "Trusted Sites" list

**Legend:**


- Primary Process
- Background/Support Process

**\*Note:** All communication between Client Devices and SAM server is https:// over ports 80/443. All communication between SAM resources and SAM server is https:// by default (47777 by default) for pre-connect check traffic.

## HP SAM Software-Komponenten

Im Folgenden werden die wichtigsten Komponenten von HP SAM aufgelistet.

- **HP SAM Client** – Der HP SAM Client wird auf dem Zugriffsgerät ausgeführt und zeigt die vom Benutzer verwendete Oberfläche an, um eine Verbindung vom Client zu einer Rechnerressource anzufordern. Wenn der Benutzer eine Verbindung anfordert, sendet der HP SAM Client diese Anfrage zur Ausführung an den HP SAM Server.
- **HP SAM Webserver** – Der HP SAM Webserver wird auf Windows Server 2003 oder 2008 ausgeführt und verwaltet den Betrieb von HP SAM. Wenn ein Benutzer an einem Zugriffsgerät eine Verbindung zu einer Rechnerressource anfordert, wird eine Anfrage an den Webserver gesendet. Der Webserver validiert die Anfrage und sendet diese zurück an das Zugriffsgerät, um die Verbindung einzuleiten. Der Webserver unterstützt zudem eine Browser-Oberfläche, die es dem HP SAM Administrator ermöglicht, HP SAM einzurichten, zu konfigurieren und zu verwalten. Außerdem erstellt der Webserver eine Datenbank in Microsoft SQL Server und ermöglicht den Zugriff darauf.
- **HP SAM Registration Service** – Der HP SAM Registration Service (Registrierungsdienst oder Blade-Dienst) wird auf der Rechnerressource ausgeführt und leitet den Status der Rechnerressource und ihrer Verbindungen an den HP SAM Webserver weiter.

 **HINWEIS:** Lesen Sie die Dokumentation Ihres Computers und Ihres Zugriffsgeräts, um zu erfahren, welche der oben genannten Komponenten bereits werkseitig auf der Hardware installiert sind und welche Sie noch installieren müssen. Der HP SAM Client und der RGS Receiver sind beispielsweise auf einigen Clients bereits vorinstalliert. Die übrige RGS-Software ist optional und muss separat erworben werden. Weitere Informationen zu RGS finden Sie unter <http://www.hp.com/go/rgs>.

## Remote Graphics Software (RGS)

RGS ist ein ähnliches Kommunikationsprotokoll wie das Microsoft Remote Desktop Protocol (RDP). Mit HP SAM können Sie entweder RGS oder RDP verwenden.

RGS verfügt im Vergleich zu RDP über einige Vorteile:

- RGS bietet erweiterte Grafikfunktionen, die die Verwendung von Multimedia-Anwendungen und 3D-Grafikanwendungen in einem Standardcomputernetzwerk erleichtern.
- RGS unterstützt mehrere Monitore, die mit einem versetzten Layout konfiguriert sind.

Thin Clients werden wenn möglich auf die Verwendung von RGS eingestellt. Wenn auf einem Zugriffsgerät sowohl RGS als auch RDP installiert sind, wird standardmäßig RGS verwendet. Wenn RGS sowohl auf dem Zugriffsgerät als auch der Rechnerressource installiert ist, wird RGS verwendet. Wenn weder das Zugriffsgerät noch die Rechnerressource über RGS verfügen, wird RDP verwendet.

HP RGS ist optional und muss separat erworben werden. Informationen zu HP RGS finden Sie unter <http://www.hp.com/go/rgs>. Rufen Sie zur Anzeige des *HP Remote Graphics Software-Benutzerhandbuchs* die Seite [http://www.hp.com/support/rgs\\_manuals](http://www.hp.com/support/rgs_manuals) auf, und blättern Sie zur Überschrift **User guide** (Benutzerhandbuch).

# Häufige Aufgaben

## Einrichtung des HP SAM

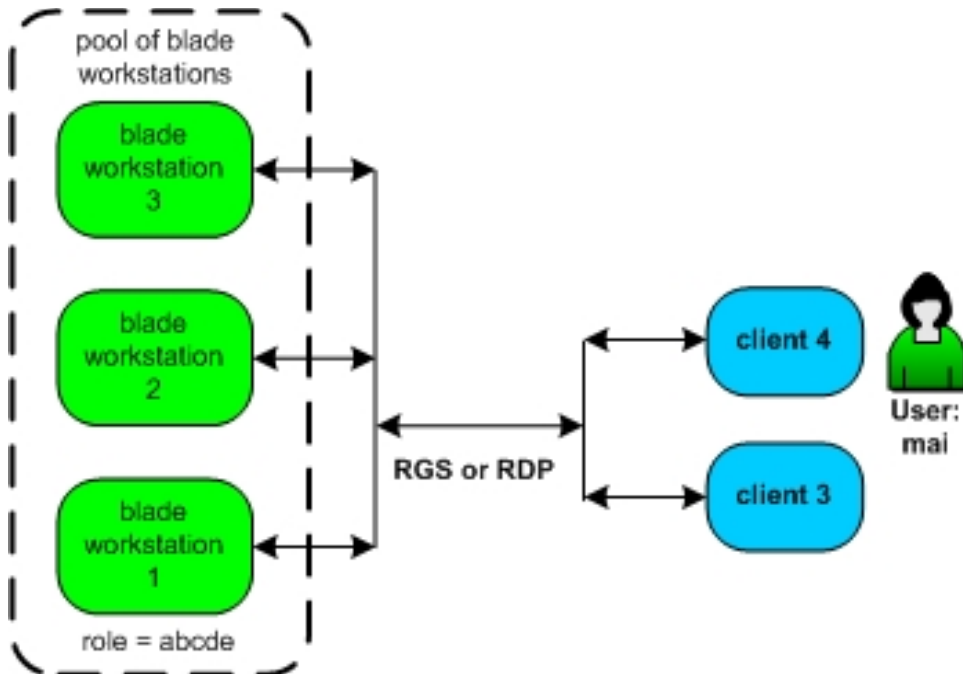
1. Installieren Sie HP SAM. Siehe [„Installation“ auf Seite 27](#).
2. Fügen Sie Benutzer hinzu.
  - a. Fügen Sie neue Benutzer hinzu. Siehe [„Hinzufügen neuer Benutzer“ auf Seite 70](#).
  - b. Erstellen Sie Administratorgruppen, weisen Sie Benutzer zu und passen Sie Berechtigungen an. Siehe [„Administrative Berechtigungen verwalten“ auf Seite 64](#).
3. Erstellen Sie eine Richtlinie. Siehe [„Erstellen oder Aktualisieren einer Richtlinie“ auf Seite 78](#).
4. Erstellen Sie eine Rolle. Siehe [„Verwalten von Ressourcenrollen“ auf Seite 62](#).
5. Weisen Sie den Benutzern Rechnerressourcen oder Rollen zu. Siehe [„Benutzer verwalten“ auf Seite 65](#).



## Einrichten eines Benutzers mit einer dynamischen Ressource

HP SAM ermöglicht die dynamische gemeinsame Nutzung von Rechnerressourcen durch mehrere Benutzer.

**Abbildung 1-2** Dynamische Verbindung – Beispiel



In [Abbildung 1-2, „Dynamische Verbindung – Beispiel“, auf Seite 9](#) müssen wir der Benutzerin Mai den Zugriff auf Rechnerressourcen gewähren. Es wurde eine Gruppe aus drei Blade Workstations erstellt, die jeweils so konfiguriert sind, dass sie die Rolle „abcde“ unterstützen.

▲ Wir weisen Mai die Rolle „abcde“ zu. Siehe [„Benutzer verwalten“ auf Seite 65](#).

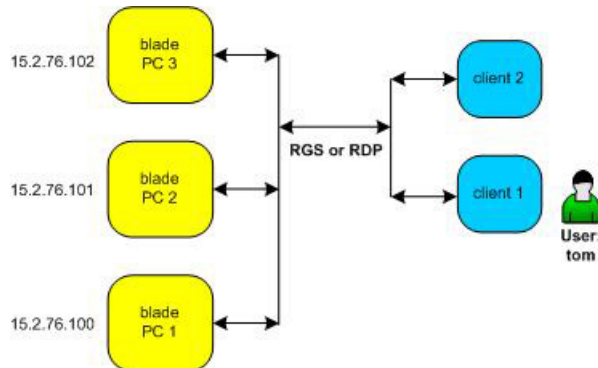
Dies bedeutet, dass Mai jetzt autorisiert ist, auf alle Rechnerressourcen zuzugreifen, die die Rolle „abcde“ unterstützen. Wenn Mai also eine Verbindung zu einer „abcde“-Rechnerressource anfordert, verbindet HP SAM ihr Zugriffsgerät automatisch mit einer der drei Blade Workstations (Verfügbarkeit vorausgesetzt), die diese Rolle unterstützen.

## Einrichten eines Benutzers mit statischen (dedizierten) Ressourcen

Durch die Zuweisung dedizierter (statischer) Ressourcen können eine oder mehrere Rechnerressourcen einem Benutzer zugewiesen werden. Außerdem können eine oder mehrere Rechnerressourcen als Sicherung zugewiesen werden.

Durch die Unterstützung von statischem Roaming können Benutzer von anderen Standorten aus arbeiten. Die unterschiedlichen Anzeigekonfigurationen können auf dem Client-Desktop abgelegt werden, um vollen Zugang mit weniger Monitoren zu ermöglichen.

**Abbildung 1-3** Statische (dedizierte) Verbindung – Beispiel



In [Abbildung 1-3](#), „Statische (dedizierte) Verbindung – Beispiel“, auf Seite 10 müssen wir dem Benutzer Tom den Zugriff auf eine bestimmte Rechnerressource gewähren. Ein Blade-PC wurde für die Unterstützung von Tom konfiguriert.

1. Wir weisen Tom den Blade-PC 1 mit der IP-Adresse 15.2.76.100 zu. Siehe [„So weisen Sie Ressourcen manuell zu“](#) auf Seite 67.
2. Um sicherzustellen, dass Tom auch dann eine Rechnerressource zur Verfügung hat, wenn der Blade-PC 1 ausfällt, weisen wir Blade-PC 3 mit der IP-Adresse 15.2.76.102 als Reserve für Blade-PC 1 zu. Siehe [„So weisen Sie Ressourcen manuell zu“](#) auf Seite 67.

Unabhängig davon, welchen Client-Computer Tom verwendet, wird er automatisch mit dem Blade-PC 1 unter der Adresse 15.2.76.100 verbunden. Wenn der Blade-PC 1 ausfällt, klickt Tom auf **Verbinden** und wird automatisch mit Blade-PC 3 verbunden.

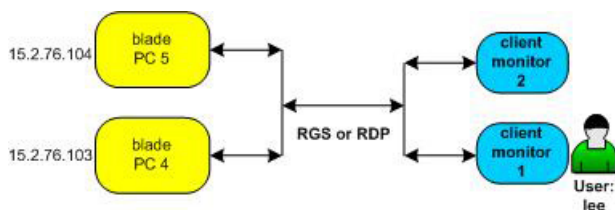
**HINWEIS:** Wenn ein Blade-PC eine dynamische Rolle innehat und als dedizierte Ressource erneut einem Benutzer zugewiesen wird, kann dieser Blade nicht mehr einem anderen Benutzer in dynamischer Rolle zugewiesen werden, auch wenn der aktuelle Status **Verfügbar** lautet. Es empfiehlt sich, dedizierte Ressourcen nicht einer dynamischen Ressourcenrolle zuzuweisen, um die Ressourcenlisten **Verfügbar** und **Verwendet** korrekt verfolgen zu können.

## Konfigurieren eines Monitorlayouts für einen Benutzer

HP SAM ermöglicht es dem Benutzer, eine Verbindung zu mehreren Computern herzustellen, um dadurch gleichzeitig ablaufende Remote-Sitzungen zu erstellen. Ressourcen können dem Benutzer entweder über statische Zuweisung oder durch Zuweisung zu dem Benutzer zugeordneten Rollen zur Verfügung gestellt werden.

Durch die Zuordnung eines statischen Benutzers/einer Anzeige-ID zu einer oder mehreren Rechnerressourcen kann eine spezifische Kombination aus Benutzer-ID und Client-ID zu einer bestimmten Rechnerressource oder zu einer bestimmten Gruppe von Rechnerressourcen zugeordnet werden. Wenn sich der betreffende Benutzer mithilfe von RGS bei dem betreffenden Client anmeldet, werden die vorkonfigurierten Rechnerressourcen an einem bestimmten Speicherort und mit einer bestimmten Auflösung auf dem bzw. den Client-Monitoren angezeigt.

**Abbildung 1-4** Monitorlayout – Beispiel




In [Abbildung 1-4, „Monitorlayout – Beispiel“, auf Seite 11](#) hat der Benutzer Lee statischen Zugriff auf zwei Blade-PCs. HP SAM muss so konfiguriert werden, dass die Informationen dieser Blade-PCs auf Leos zwei Monitoren angezeigt werden.

1. Zunächst erstellen wir eine Monitorlayout-ID. Siehe [„Verwalten des Monitorlayouts“ auf Seite 75](#).
2. Wir weisen die neue Monitorlayout-ID Leos Zugriffsgerät zu. Siehe [„Verwalten von Zugriffsgeräten“ auf Seite 74](#).
3. Wir weisen Lee die Monitorlayout-ID zu und wählen die beiden Blade-PCs, die ihm bereits zugewiesen sind, als Ressourcen für die Monitorlayout-ID aus. Siehe [„Benutzer verwalten“ auf Seite 65](#).

Beide Monitore haben dieselbe horizontale und vertikale Auflösung, also geben wir neben jedem ausgewählten Blade-PC 1280 bzw. 1024 ein.

HP SAM behandelt diese beiden Monitore als Einheit. Um die Ausgabe jedes Blade-PCs wie gewünscht auf einem anderen Monitor anzuzeigen, müssen wir den horizontalen und vertikalen Offset und den Abstand von der oberen linken Ecke angeben.

Die Ausgabe von Blade-PC 4 soll auf Leos linkem Monitor und die Ausgabe von Blade-PC 5 auf Leos rechtem Monitor angezeigt werden (siehe [Abbildung 1-5, „Monitor-Offsetkonfiguration – Beispiel“, auf Seite 12](#)). Für den horizontalen und den vertikalen Versatz wird jeweils der Wert 0 festgelegt, damit die Ausgabe von Blade-PC 4 in der linken oberen Ecke des linken Monitors angezeigt wird. Für die Anzeige der Ausgabe von Blade-PC 5 auf dem rechten Monitor ist es erforderlich, den horizontalen Versatz *einen Schritt über der Monitorauflösung* festzulegen, d. h., der horizontale Versatz wird auf den Wert 1280 eingestellt. Da die Anzeige jedoch nicht nach unten verschoben wird, beträgt der Wert für den vertikalen Versatz weiterhin 0.

 **HINWEIS:** Versätze werden nur bei Verwendung des RGS-Protokolls berücksichtigt. Sitzungen, die das RDP-Protokoll verwenden, sind in der Standardanzeige normalerweise übereinander dargestellt.

---

Durch die Unterstützung von Roaming können Benutzer von anderen Standorten aus arbeiten. Wenn Lee sich von einem anderen Client aus anmeldet, können die unterschiedlichen Anzeigekonfigurationen auf dem Client-Desktop gestaffelt werden, um vollen Zugang mit weniger Monitoren zu ermöglichen.

**Abbildung 1-5** Monitor-Offsetkonfiguration – Beispiel

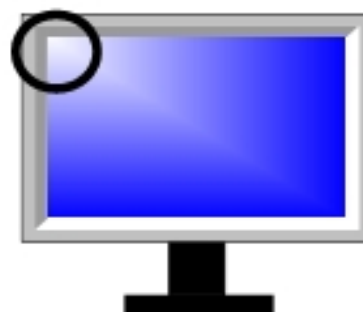
horizontal  
offset "0"

vertical  
offset "0"



horizontal  
offset "1280"

vertical  
offset "0"



---

# 2 Anforderungen

## HP SAM – Hardware- und Softwareanforderungen

### Architekturempfehlungen und optimale Vorgehensweisen zur Einrichtung einer HP SAM Umgebung

#### Bestimmung der Servergröße

Im Allgemeinen kann der HP SAM Server eine theoretische Höchstzahl von 40.000 Benutzern und Ressourcen verwalten.

- Dieser Wert stützt sich auf die Annahme, dass innerhalb eines 30-Sekunden-Fensters nicht mehr als 1 % der Benutzer einen Verbindungsversuch unternimmt.

HP SAM Server kann, bei Minimumspezifikation, nachweislich innerhalb eines Zeitraums von 3 Sekunden mindestens 500 Blade-Anforderungen verarbeiten, ohne Verbindungen zu verweigern. Die tatsächlichen Ergebnisse hängen von der Geschwindigkeit der eingesetzten Server und Infrastruktur ab.

Erweitern Sie den Speicher, wenn die Benutzerzahl steigt.

- In HP SAM durchgeführte Suchvorgänge können speicherintensiv sein, weil der HP SAM Server hierfür eine Kopie der Datenbank aus dem Netzwerk in den Hauptspeicher lädt.
- Eine gute Faustregel ist 1 GB RAM pro 2.000 Benutzer oder Ressourcen (der höhere Wert ist maßgeblich).

Erhöhen Sie die Prozessorgeschwindigkeit und die Anzahl der Cores, wenn die Anzahl der Benutzer steigt.

- Der Hauptspeicher ist der wichtigste Engpass für die Leistung des HP SAM Servers. Bei einer großen Benutzerzahl muss der HP SAM Server eine große Datenbank durchsuchen, um Profile und Ressourcenzuordnungen abzurufen. Nach dem Hauptspeicher bildet die Prozessorleistung den nächsten Engpass.
- 2.000 Benutzer pro CPU-Core ist eine sinnvolle Faustregel.

Die E/A-Leistung des Netzwerks stellt in der Regel keinen Engpass dar.

- Normalerweise werden keine zusätzlichen NIC-Karten benötigt, um höhere Benutzerzahlen zu bewältigen.

#### Empfehlungen für SQL-Datenbanken

Die HP SAM SQL-Datenbank kann auf demselben Server wie der HP SAM Webserver installiert werden, damit keine andere Hardwareplattform oder weitere Lizenz für das Serverbetriebssystem

erworben werden muss. HP empfiehlt jedoch aus folgenden Gründen, Datenbank und Webserver auf separaten Servern zu betreiben:

- Die Wiederherstellung nach Hardwareausfällen geht schneller.
- Wenn die Größe und die Anzahl der Standorte einer Implementierung zunimmt, gibt es in der Regel mehrere HP SAM Webserver, jedoch nur eine zentrale HP SAM SQL-Datenbank.

Die meisten Administratoren kennen sich bereits mit der Größenbemessung einer SQL-Datenbank anhand der erfassten Datenmenge aus; dennoch können gleichzeitige An- und Abmeldungen bei HP SAM die Leistung beeinträchtigen, weil diese Ereignisse in die Datenbank geschrieben werden müssen. Daher sollte diese Möglichkeit im Hinblick auf das Wachstum der Benutzerpopulationen bei der Größenbemessung der SQL-Datenbank berücksichtigt werden.

HP SAM ist eine Multi-Tier-Anwendung, und der eigentliche Benutzer meldet sich niemals direkt bei einer Datenbank an. Für HP SAM ist nur eine Anmeldung erforderlich: die Anmeldung bei dem Konto für den HP SAM-Dienst. Es kann sein, dass Sie sich mehrfach anmelden möchten, um manuell und ohne das Konto für den HP SAM-Dienst auf die HP SAM-Datenbank zuzugreifen.

HP SAM benötigt viele gleichzeitige Verbindungen. HP SAM hat keine Kontrolle über die Anzahl der Verbindungen. Stattdessen bestimmt die Datenbank-Engine von .NET Framework, ob es effizienter ist, auf eine Verbindung zu warten, eine bestehende Verbindung weiterzuverwenden oder eine neue Verbindung herzustellen. Je stärker die Datenbank beansprucht wird, desto mehr Verbindungen werden normalerweise hergestellt. Sie werden nach Abschluss der Vorgänge automatisch wieder beendet.

Sie sollten die Anzahl der gleichzeitigen Verbindungen nicht beschränken. Falls Sie eine Grenze festlegen müssen, empfehlen wir einen Wert von mindestens 200–300.

Die HP SAM Datenbank umfasst zwei Dateien:

- **SAM\_data.mdf**: Sie enthält HP SAM Tabellen
- **SAM\_log.ldf**: Sie enthält die Informationen des Transaktionsprotokolls. SQL Server verwendet diese Datei für die Aufzeichnung von SQL-Transaktionen.

Die Standardgröße der beiden Dateien beträgt 100 MB, aber das tatsächliche in jeder Datei enthaltene Datenvolumen beläuft sich auf etwa 10 MB. Dadurch können die Dateien jeweils noch rund 90 MB Daten aufnehmen, bevor SQL sie erweitern muss.

Die Datei SAM\_data.mdf enthält mehrere HP SAM Tabellen, u. a. für das Verlaufs- und das Prüfprotokoll. In diesen beiden kontinuierlich anwachsenden Tabellen werden HP SAM Verlaufsdaten und Ereignisse gespeichert. Wenn Sie das Verlaufs- und das Prüfprotokoll deaktivieren, wird mit 100 Benutzern die Größenbegrenzung von 100 MB pro Datei nicht überschritten. Wenn Sie die Protokolle nicht deaktivieren, wächst die Datei SAM\_data.mdf täglich um mindestens 100 MB an.

Je aktiver die Datenbank ist, desto mehr Transaktionen werden der Datei SAM\_log.ldf hinzugefügt. Abgeschlossene Transaktionen werden aus der Datei entfernt. Die maximale Größe der Datei wird daher erreicht, wenn sehr viele Transaktionen gleichzeitig ablaufen. Bei 100 Benutzern sollte die durchschnittliche Größe dieser Datei weniger als 2 GB betragen.

Datenbankadministratoren können die Leistung der HP SAM Datenbank durch zwei Maßnahmen optimieren:

- Sie können einen SQL-Wartungsplan entwickeln. Dieser beinhaltet auch die Sicherung der HP SAM Datenbank und die Verkürzung von verwaisten Transaktionsprotokollen in der LDF-Datei. Bei der Datenbanksicherung werden die verwaisten Transaktionen zwar verkürzt, aber die Größe der LDF-Datei wird dadurch nicht verringert. Bei Bedarf kann der Datenbankadministrator die LDF-Datei bis auf die Standardgröße von 100 MB verkleinern.
- Sind das Verlaufs- und das Prüfprotokoll nicht deaktiviert, muss der Datenbankadministrator diese beiden Tabellen regelmäßig abschneiden. Es ist ratsam, dies wöchentlich zu tun, damit SAM\_data.mdf unter 1 GB bleibt.

## Anzahl von HP SAM Servern

Es wird empfohlen, bei steigender Benutzerzahl die Anzahl der HP SAM Server (Gateways) zu erhöhen, um die Arbeitslast zu bewältigen und Reserve-Gateways bereitzuhalten, falls ein Server aus irgendeinem Grund nicht verfügbar ist.

Wenn Sie vermeiden möchten, dem HP SAM Server ständig mehr Speicher und Prozessor-Cores hinzuzufügen, erstellen Sie mehrere Gateway-Server, und teilen Sie den Benutzerkreis auf, um die Anzahl der Benutzer einzugrenzen, die ein bestimmtes Gateway als primäres Ziel verwenden. Sie können auch die Ressourcen auf mehrere HP SAM Server aufteilen, um die Lasten zwischen den Servern zu verteilen.

## Regionalisierung von Rechenzentren

Beachten Sie Folgendes, wenn Sie Benutzer in einer Region und Blades in einer anderen platzieren:

- Wenn die Zahl der Benutzer steigt, sollte sich der HP SAM Server aus folgenden Gründen am Standort der Blades/Ressourcen und nicht am Standort der Benutzer befinden:
  - Da die Benutzerdatenbank über das Netzwerk in den Speicher des HP SAM Servers geladen werden muss, kann das WAN die Geschwindigkeit beeinträchtigen, wenn die Datenbank zu groß wird.
  - Wenn die beiden Server (SQL und HP SAM) sich in demselben Rechenzentrum befinden, können sie über das Hochgeschwindigkeits-Backbone miteinander kommunizieren, und das Netzwerk hat keinen Einfluss auf die Übertragungsgeschwindigkeit.
- Bei einer relativ kleinen Benutzerzahl (weniger als 3.000) können Sie den HP SAM Server aus folgenden Gründen auch am Standort der Benutzer platzieren:
  - Die Benutzerdatenbank, die über das Netzwerk auf den SAM Server geladen wird, ist klein, und ihre Übertragung wird deshalb vom WAN kaum beeinflusst.
  - Beim lokalen HP SAM Server ist die Anzahl der Benutzer begrenzt, die auf diesen Server zugreifen, deshalb kann er kleiner sein.

Konzepte für Disaster Recovery

- Eine Gruppe von HP SAM Servern kann so konfiguriert werden, dass ein Benutzer- und Ressourcen-Failover auf einen anderen HP SAM Server ausgeführt wird, wenn einer der Server nicht mehr erreichbar ist. Die HP SAM Server sollten an verschiedenen Standorten installiert werden, um die Wahrscheinlichkeit zu erhöhen, dass immer mindestens ein Server verfügbar bleibt.

## Mehrere SQL-Datenbanken

In der Regel nutzen alle HP SAM Server gemeinsam eine einzige SQL-Datenbank. Nur in bestimmten Situationen ist es sinnvoll, mehr als eine bestimmte SQL-Datenbank zu verwenden:


- Wenn Benutzer und Ressourcen in voneinander getrennten Supportbereichen verwaltet werden können und keine Migration der Benutzer zwischen diesen Bereichen erforderlich ist.
- Wenn die Benutzerzahl 40.000 übersteigt.
- Wenn sich eine größere Benutzerzahl sehr häufig an- und abmeldet, da dies die Geschwindigkeit der SQL-Datenbank für alle Benutzer beeinträchtigt.

In allen anderen Fällen sollte nur eine einzige SQL-Datenbank eingesetzt werden.

## Domänenumgebungsanforderungen für HP SAM

- HP SAM wird in Domänen unterstützt, auf deren Domänencontroller Windows 2003 Server oder höher läuft.
- HP SAM wird in Domänen mit der Domänenfunktionsebene (Domain Functional Level) Windows 2003, Windows 2008 oder Windows 2008 R2 Server unterstützt.


---

 **HINWEIS:** Wenn die Domäne mit der Domänenfunktionsebene Windows 2008 arbeitet, müssen Sie auf dem HP SAM Server das Service Pack 1 für Microsoft .NET Framework installieren.

---

- HP SAM unterstützt nur Domänen innerhalb desselben Bereichs.
- Für HP SAM sind UPN-Namen für alle Benutzerkonten erforderlich, damit bestimmte HP SAM-Funktionen aktiviert werden können, beispielsweise die Anmeldung bei der Verwaltungskonsole von HP SAM und das Follow-me-Roaming.

---

 **HINWEIS:** Die integrierte Domänenadministratorgruppe und der integrierte Administratorbenutzer auf dem Domänencontroller (Windows 2003 oder frühere Version) können HP SAM nicht hinzugefügt werden.

---

## Anforderungen für HP SAM Web und SQL Server

Sie können HP SAM mit einer zentralen HP SAM SQL-Datenbank auf einem oder mehreren HP SAM Web-Failover-Servern installieren. Sie können HP SAM auch auf einem Server installieren, der sowohl den HP SAM Webserver als auch die SQL-Datenbank hostet.

## Hardwareanforderungen für HP SAM Webserver

### Mindestanforderungen:


x86-kompatibler Server, beispielsweise ein HP Proliant Server mit:

- Prozessor: Pentium 4, 1,0 GHz
- Festplatte: 10 GB (mehr Speicher erforderlich, wenn sowohl der Webserver als auch die SQL-Datenbank gehostet werden)
- Systemspeicher: 1 GB pro 2.000 Ressourcen



## Softwareanforderungen für HP SAM Webserver

---

 **HINWEIS:** Die HP SAM Webserversoftware wird auf Servern, auf denen Windows 2008 R2 Server läuft, nicht unterstützt. Dieses Betriebssystem ist nicht als 32-Bit-Edition verfügbar, und die HP SAM Webserversoftware lässt sich nicht unter einem 64-Bit-Betriebssystem ausführen.

---

### **Mindestanforderungen:**

Eines der folgenden Betriebssysteme muss installiert sein:

- Windows Server 2003 R2, Standard Edition mit Service Pack 2
- Windows Server 2003 R2, Enterprise Edition mit Service Pack 2
- Windows Server 2003 R2, Web Edition mit Service Pack 2
- Windows Server 2008, Standard Edition
- Windows Server 2008, Enterprise Edition
- Windows Server 2008, Web Edition

---

 **HINWEIS:** 64-Bit-Betriebssysteme werden auf dem HP SAM Server nicht unterstützt.

Sie müssen Microsoft .NET Framework Version 2.0 installieren, damit der HP SAM Webserver funktioniert. Es wird empfohlen, Microsoft .NET Framework 2.0 nach IIS zu installieren, um die reibungslose Registrierung von ASP.NET zu gewährleisten.

Wenn Ihr Domaincontroller Windows Server 2008 ausführt und als Domänenfunktionsebene der Windows 2008-Modus festgelegt wurde, müssen Sie das .NET Service Pack 1-Patch installieren, damit HP SAM Web Administrator einwandfrei funktioniert.

---

## HP SAM SQL-Datenbankserver – Hardwareanforderungen

Wenn Sie bereits über einen SQL-Datenbankserver verfügen, können Sie die HP SAM Datenbank auf demselben Server installieren. Es empfiehlt sich jedoch, die HP SQL-Datenbank auf einem separaten Server zu installieren, um die Umgebung in Zukunft besser skalieren zu können. Die Lastverteilung nach diesem Verfahren können Sie den Darstellungen möglicher Konfigurationen entnehmen.

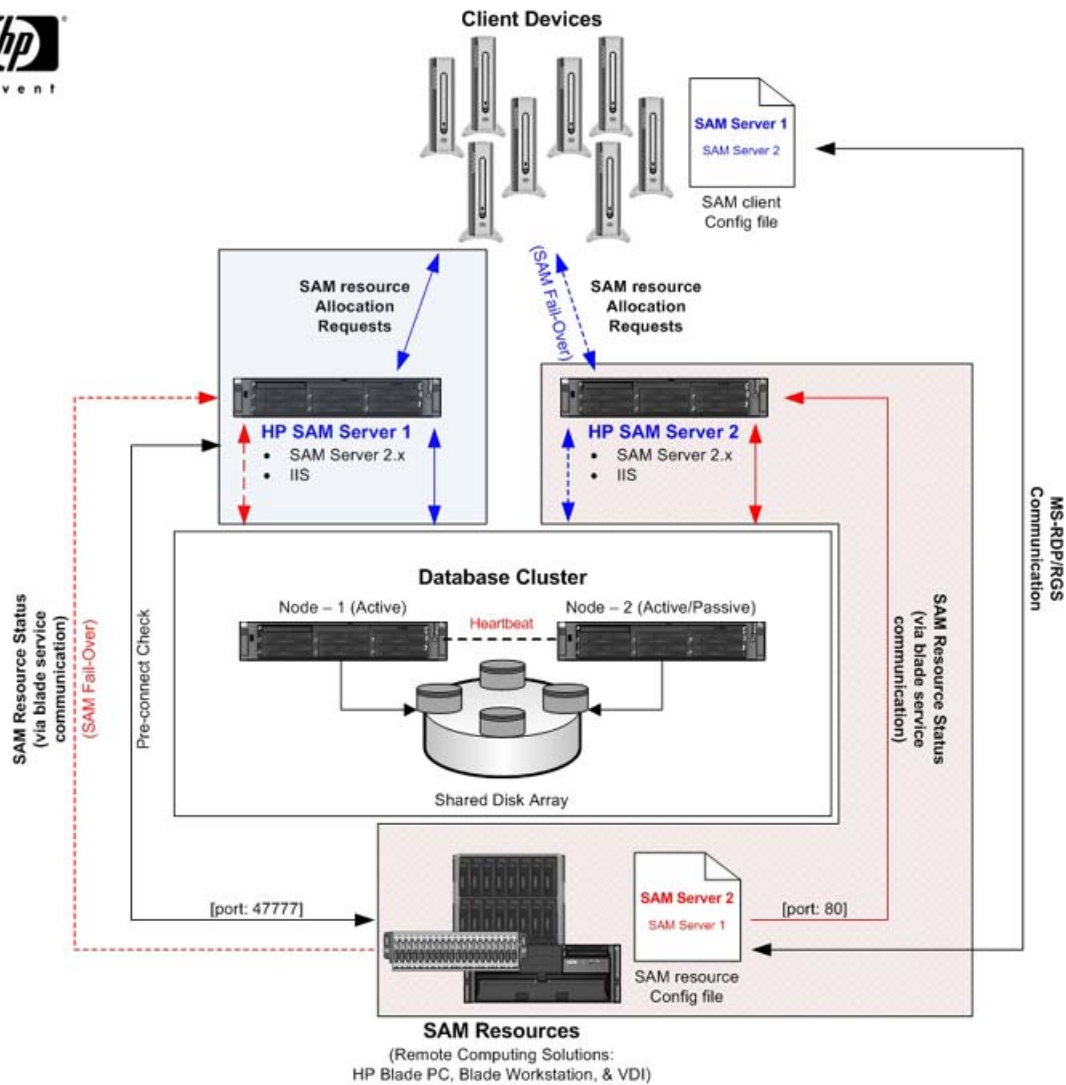
### **Mindestanforderungen:**

x86-kompatibler Server, beispielsweise ein HP Proliant Server mit:

- Prozessor: Pentium 4, 1,0 GHz
- Festplatte: 10 GB (mehr Speicher erforderlich, wenn sowohl der Webserver als auch die SQL-Datenbank ausgeführt werden)
- Systemspeicher: mindestens 1 GB

# SAM Fail-Over & Load Distribution – Option 1

(Tested & Verified)



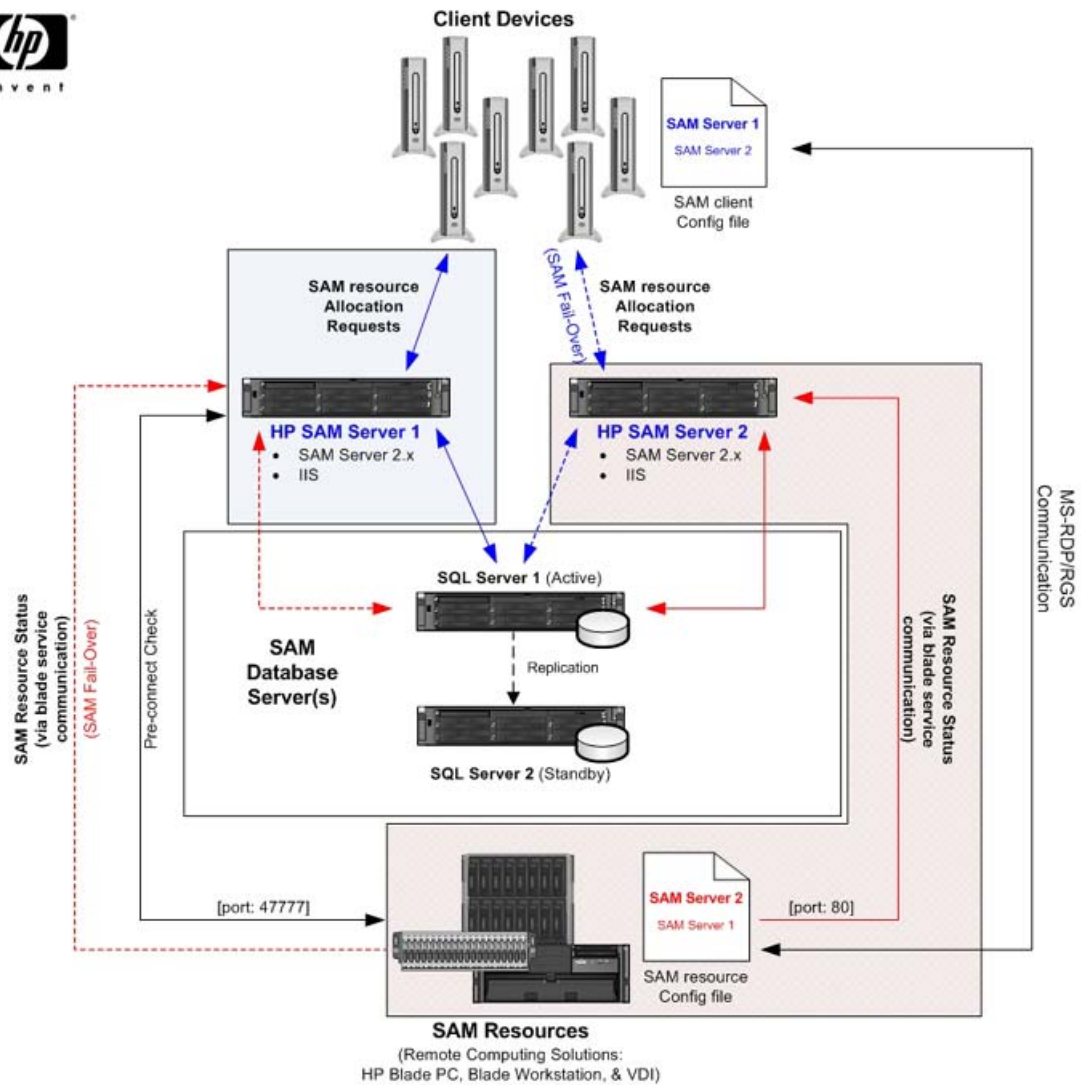
## SAM Load Distribution

- All SAM Resource Allocation requests are routed and handled via SAM Server 1.
- All SAM Resource Status updates are separately routed and handled via SAM Server 2.

## Notes:

- SAM natively provides a method for Fail-Over and Load Distribution. SAM client and resource configuration files allow you specifically identify and point your clients and resources to communicate via multiple SAM servers.
- In this Option, the SAM Resource Allocation requests from the Client Devices are separately routed via SAM Server 1. This allows the SAM Resource Status updates to be isolated by routing via SAM Server 2. This separation allows for load distribution of SAM functionality, where by isolating the SAM Resource Status updates.
  - This configuration has been tested, by 540 clients requesting resources within a three second window, with no request denials or degradation on requests.

## SAM Fail-Over & Load Distribution – Option 1b



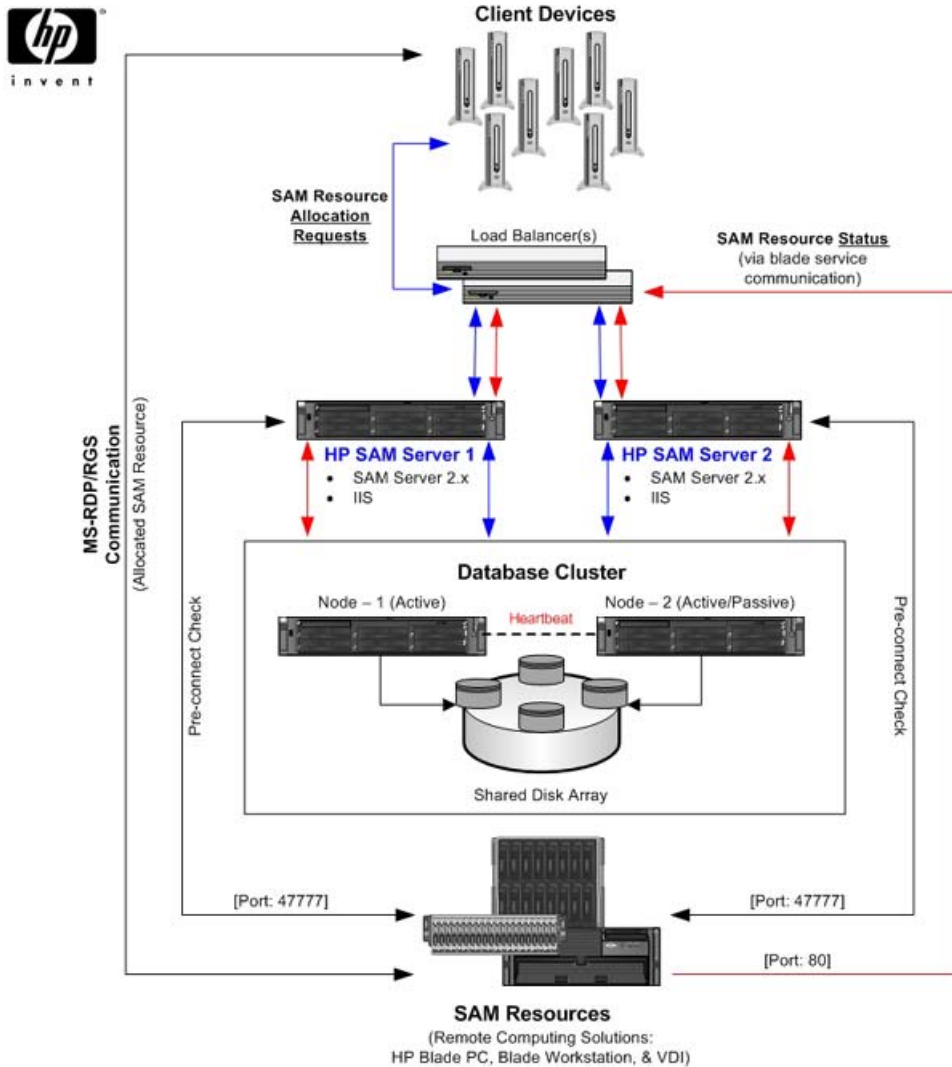
### SAM Load Distribution

- All SAM Resource Allocation requests are routed and handled via SAM Server 1.
- All SAM Resource Status updates are separately routed and handled via SAM Server 2.

### Notes:

- SAM natively provides a method for Fail-Over and Load Distribution. SAM client and resource configuration files allow you specifically identify and point your clients and resources to communicate via multiple SAM servers.
- In this Option, the SAM Resource Allocation requests from the Client Devices are separately routed via SAM Server 1. This allows the SAM Resource Status updates to be isolated by routing via SAM Server 2. This separation allows for load distribution of SAM functionality, where by isolating the SAM Resource Status updates, in order to maintain a more accurate Resource Status.
  - If SAM server 1 goes down, manually re-sync SAM server 2 against the SAM database to acquire the blade resource data faster. The SAM configuration, role assignment, etc... will exist on the 2<sup>nd</sup> SAM server via replication method established.

## SAM High-Availability & Load Balancing – Option 2



### Notes:

SAM natively provides a method for Fail-Over and Load Distribution. SAM client and resource configuration files allow you specifically identify and point your clients and resources to communicate via multiple SAM servers.

- In this Option, a Load Balancer (with or without redundancy) has been introduced to manage and distribute SAM Resource Allocation Requests and SAM Resource Status updates. In this design, the SAM Client and Resource configuration files are pointing to a Virtual IP (VIP). The VIP manages and distribute both the requests and updates, for high-availability and redundancy.
- With this SAM design, both SAM Server 1 and SAM Server 2 are intended to manage an equal load of requests and updates.

## HP SAM SQL-Datenbankserver – Softwareanforderungen

### Mindestanforderungen:

Eine der folgenden Anwendungen muss installiert sein:

- Microsoft SQL Server 2005 Enterprise, Standard oder Express Edition mit Service Pack 1 oder Service Pack 2
- Microsoft SQL Server 2008 Standard oder Enterprise Edition
- Microsoft SQL Server 2008 R2 Standard oder Enterprise Edition

HP empfiehlt Microsoft SQL Server 2005 oder 2008 Standard oder Enterprise Edition. Wenn Sie die SQL Server 2005 oder 2008 Express Edition verwenden, bei der die Datenbankgröße auf 4 GB begrenzt ist, sollten Sie einen der folgenden Schritte ausführen:


- Deaktivieren Sie die Verlaufsdaten- und/oder die Protokollsammlung.  
oder
- Beschränken Sie den Zeitraum, über den das System gespeicherte Verlaufsdaten beibehält, und stellen Sie die Planungsfunktion der Protokollverwaltung so ein, dass die Protokolle häufig und regelmäßig aus der Datenbank entfernt werden.

# Anforderungen für den HP SAM Registrierungsdienst

## Hardwareanforderungen

- HP Blade-PC


---

 **HINWEIS:** Linux wird auf HP Blade-PCs nicht unterstützt.

---

- HP Blade Workstation-Reihe
- HP Personal Workstation
- Virtuelle Maschine auf VMware ESC vSphere 4.X

---

 **HINWEIS:** Die Hardwareanforderungen für die Ausführung von virtuellen VMware-Sitzungen mit VMware sind in der Dokumentation von VMware angegeben.


---

## Softwareanforderungen

Installieren und aktivieren Sie eines der folgenden Betriebssysteme:

- Windows XP Professional 32-Bit oder 64-Bit mit Service Pack 2 oder höher
- Windows Vista mit Service Pack 1 oder höher, 32-Bit oder 64-Bit, wie folgt:
  - Business
  - Enterprise
- Windows 7, 32-Bit oder 64-Bit, wie folgt:
  - Professional
  - Enterprise
- Linux RHEL4 64-Bit (Update 5 oder höher)

---

 **HINWEIS:** HP SAM 2.2 und frühere Clients können keine Verbindungen zu Linux-Ressourcen herstellen.

---

- Linux RHEL5 64-Bit (Update 2 oder höher)
- Linux RHEL6 64-Bit

Installieren und aktivieren Sie mindestens eine der folgenden Anwendungen:

- RGS Sender 5.1.3 oder höher mit aktiviertem Single-Sign-On
- RDP mit Terminaldienst

## Anforderungen für Zugriffsgeräte

Die folgenden Abschnitte enthalten Informationen zu den Anforderungen für Zugriffsgeräte.

## Thin Client

### Hardwareanforderungen

- HP Compaq t5720 Thin Client (mit Windows XP Embedded-Betriebssystem)
- HP Compaq t5730 Thin Client (mit Windows XP Embedded-Betriebssystem)
- HP Compaq t5730w (mit Windows Embedded Standard (WES) als Betriebssystem)
- HP t5630 Thin Client (mit Windows XP Embedded-Betriebssystem)
- HP t5630w (mit Windows Embedded Standard (WES) als Betriebssystem)
- HP t5740 Thin Client (mit Windows Embedded Standard (WES) als Betriebssystem)
- HP t5740e (mit Windows Embedded Standard 7 (WES 7) als Betriebssystem)
- HP t5135 Thin Client (mit HP ThinConnect Embedded-Betriebssystem)
- HP t5145 Thin Client (mit HP ThinConnect Embedded-Betriebssystem)
- HP t5545 Thin Client (mit HP ThinPro-Betriebssystem)
- HP t5745 Thin Client (mit HP ThinPro-Betriebssystem)
- HP gt7725 Thin Client (mit HP ThinPro GT-Betriebssystem)
- HP gt7720 (mit Windows XP Embedded-Betriebssystem)
- HP gt7720w (mit Windows Embedded Standard-Betriebssystem)

Wenn der HP SAM Client bereits vorinstalliert ist, müssen Sie den HP SAM Client nur für die Verbindung mit dem entsprechenden HP SAM Webserver konfigurieren.

### Softwareanforderungen

Installieren und aktivieren Sie mindestens eine der folgenden Anwendungen:

- RGS Receiver 5.1.3 oder höher
- RDP

## Mobiler Thin Client

### Hardwareanforderungen

- HP Compaq 6720t Mobiler Thin Client (mit Windows XP Embedded-Betriebssystem)
- HP Compaq 2533t Mobiler Thin Client (mit Windows XP Embedded-Betriebssystem)
- HP Compaq 4410t Mobile Thin Client (mit Windows Embedded Standard (WES-) Betriebssystem)


## Desktop- oder Notebook-PC

### Softwareanforderungen



Installieren und aktivieren Sie eines der folgenden Betriebssysteme:

- Windows XP Professional, 32-Bit oder 64-Bit, mit Service Pack 2 oder 3

 **HINWEIS:** Von Zugangsgeräten mit Windows XP 64-Bit aus kann der HP SAM-Client keine Verbindung mithilfe der vorinstallierten Version von RDP herstellen. Das liegt am Speicherort (\windows\system32) der Protokolldateien für das vorinstallierte RDP. Für die Herstellung einer Verbindung von einem Zugangsgerät mit Windows XP 64-Bit über RDP muss RDP in einem anderen Ordner als \windows installiert werden.

- Windows Vista, Business oder Enterprise, 32-Bit oder 64-Bit, mit Service Pack 1 oder höher
- Windows 7, Professional oder Enterprise, 32-Bit oder 64-Bit
- Linux RHEL4, 32-Bit oder 64-Bit (Update 5 oder höher)
- Linux RHEL5, 32-Bit oder 64-Bit (Update 2 oder höher)
- Linux RHEL6, 32-Bit oder 64-Bit

Installieren und aktivieren Sie mindestens eine der folgenden Anwendungen:

- RGS Receiver 5.1.3 oder höher
- RDP

## Blade Workstation Clients

### Hardwareanforderungen

- HP Compaq Blade Workstation Client
- HP dc72 Blade Workstation Client
- HP dc73 Blade Workstation Client

### Softwareanforderungen

- Blade Workstation Client-Reihe mit RGS Receiver und HP SAM Client im Abbild

## Personal Workstation Clients

### Hardwareanforderungen

- HP Personal Workstation

### Softwareanforderungen

- Windows XP Professional, 32-Bit oder 64-Bit, mit Service Pack 2 oder 3
- Windows Vista, Business und Enterprise, 32-Bit oder 64-Bit, mit Service Pack 1 oder höher
- Windows 7, Professional oder Enterprise, 32-Bit oder 64-Bit
- Linux RHEL4, 32-Bit oder 64-Bit (Update 5 oder höher)
- Linux RHEL5, 32-Bit oder 64-Bit (Update 2 oder höher)
- Linux RHEL6, 32-Bit oder 64-Bit

# Weitere Anforderungen

## Erstellen eines Dienstkontos

Der HP SAM Webserver muss unter einem Domänenbenutzerkonto ausgeführt werden, mit dem die HP SAM Dienste auf dem lokalen Server ausgeführt werden können.

- Erstellen Sie das Konto vor der Installation der HP SAM Serveranwendung.
- Ändern Sie den Namen und das Passwort für dieses Konto so selten wie möglich, um Unterbrechungen von HP SAM zu minimieren.
- Fügen Sie das Konto zur lokalen Server-Administratorgruppe auf allen HP SAM Webservern hinzu.
- Fügen Sie das Konto zur Administratorgruppe auf allen Ressourcen hinzu (um Abmeldungen und Neustarts zu ermöglichen).
- Das Konto muss in einer Mehrdomänenumgebung als vertrauenswürdig gelten.
- Verwenden Sie das Dienstprogramm HP SAM Configuration Utility, das Sie im Menü **Start** des HP SAM Servers finden, um das Passwort des Dienstkontos für HP SAM zu ändern, wenn dieses aktualisiert wurde.

## Erlangen von Administratorrechten

Für eine vollständige Installation von HP SAM müssen Sie über die folgenden Administratorrechte verfügen:

- Administratorrechte auf allen Rechnerressourcen (z. B. Blade-PCs)
- SQL-Administratorkonto und -passwort: nur während der Installation erforderlich
- Administratorrechte für den HP SAM Webserver


## Ändern der Firewall

Eine in einer Netzwerkumgebung zum Einsatz kommende Hardware- und/oder Software-Firewall muss entsprechend angepasst werden, damit HP SAM ordnungsgemäß funktioniert. Weitere Informationen hierzu finden Sie unter [„Firewall-Regeln“ auf Seite 99](#).

## Active Directory

Active Directory ist nicht Teil von HP SAM, wird aber von HP SAM für die Verwaltung von Benutzerkonten benötigt.

---

 **HINWEIS:** Auf Windows Server 2000-Domänencontrollern ausgeführtes Active Directory wird nicht unterstützt.

---

Unterstützte Domänenfunktionsebenen

- Windows 2003
- Windows 2008
- Windows 2008 R2

---

# 3 Installation

## Installationsreihenfolge

### Neuinstallation

Bei Neuinstallationen wird folgende Installationsreihenfolge empfohlen:

1. [„Installieren des HP SAM Webservers und der SQL-Software“ auf Seite 28](#)
2. [„Installieren und Validieren der HP SAM Registrierungsdienst-Software“ auf Seite 32](#)
3. [„Installieren und Validieren der HP SAM Client-Software“ auf Seite 37](#)
4. [„Bereitstellen des HP SAM Registrierungsdienstes auf allen HP SAM Rechnerressourcen“ auf Seite 56](#)
5. [„Bereitstellen der HP SAM Client-Software auf allen HP SAM Zugriffsgerten“ auf Seite 57](#)

### Upgrade

Bei Upgrades bestehender Installationen wird folgende Installationsreihenfolge empfohlen:

1. Sichern Sie die Datenbank.
2. Verkleinern Sie die Datenbank. (Siehe nachstehende Schritte.)
3. Beenden Sie Internet Information Services (IIS) oder bloß die SAM-Website auf allen HP SAM-Servern. Dadurch werden vorübergehend alle HP SAM-Aktivitäten angehalten.
4. Upgraden Sie die HP SAM-Server (wählen Sie die Installation der HP SAM-Datenbank und des HP SAM-Webadministrators). Sie müssen beides installieren, damit die Datenbankstruktur für den Betrieb mit der neuesten Version von HP SAM aktualisiert wird.
5. Führen Sie das Upgrade des HP SAM Registrierungsdienstes auf allen Rechnerressourcen durch, und starten Sie dann den Dienst (oder das ganze System) neu.
6. Führen Sie das Upgrade der HP SAM Clients durch.

So verkleinern Sie die Datenbank:

1. Verkürzen Sie die Tabellen für das Auditprotokoll und den Verlauf:
  - a. Öffnen Sie SQL Server Management Studio, und erweitern Sie den Ordner „Datenbanken“.
  - b. Klicken Sie mit der rechten Maustaste auf **SAM-Datenbank**, und wählen Sie **Neue Abfrage** aus.
  - c. Geben Sie in der Abfrageregisterkarte auf der rechten Seite Folgendes ein:  
Truncate Table Auditlog

Truncate Table History

- d. Klicken Sie auf **Ausführen**.


Im Meldungsbereich sollte **Befehl(e) wurde(n) erfolgreich abgeschlossen** angezeigt werden.

2. Verkleinern Sie die Datenbank:

- a. Öffnen Sie SQL Server Management Studio, und erweitern Sie den Ordner „Datenbanken“.
- b. Klicken Sie mit der rechten Maustaste auf **SAM-Datenbank**, und wählen Sie **Tasks > Verkleinern > Dateien** aus.
- c. Wählen Sie in der Liste **Dateityp** die Option **Daten** aus.
- d. Wählen Sie im Bereich **Verkleinerungsaktion** die Option **Seiten vor dem Freigeben von nicht verwendetem Speicherplatz neu organisieren** aus.
- e. Stellen Sie unter **Datei verkleinern auf** die Standardgröße **100 MB** ein.
- f. Klicken Sie auf **OK**.

3. Überprüfen Sie, ob die Datei SAM\_data.mdf 100 MB groß ist.


---

 **HINWEIS:** Diese Datei befindet sich standardmäßig im Verzeichnis C:\Programme\Microsoft SQL Server\MSSQL.1\MSSQL\Data.

---

## Installieren des HP SAM Webservers und der SQL-Software

Das Installationspaket installiert die HP SAM-Serveranwendung und/oder die HP SAM-Datenbank (HP SAM-xx ##.EXE, wobei „xx“ für den Sprachcode steht und „##“ für die Softwareversion, die Sie installieren möchten. Folgende Sprachcodes stehen zur Verfügung: EN für Englisch, JP für Japanisch, FR für Französisch, DE für Deutsch, KO für Koreanisch, ZH-CN für Vereinfachtes Chinesisch). Sie müssen bei der Installation sowohl die Webserver- als auch die SQL-Komponente installieren. Die ausgewählte Sprache gilt nur für den Installationsassistenten. Nach der Installation der Anwendung erkennt die Webanwendung die Browsersprache, und die Benutzeroberfläche wird in derselben Sprache angezeigt, sofern die Anwendung die betreffende Sprache unterstützt. Anderenfalls wird die Benutzeroberfläche in Englisch angezeigt.

 **HINWEIS:** Bei HP SAM können mehrere HP SAM Webserver auf eine einzige Datenbank verweisen. Alle HP SAM Webserver bieten den gleichen Funktionsumfang. Sie können HP SAM so konfigurieren, dass zwischen den Servern ein wechselseitiger Lastausgleich erfolgt und die Server als Failover-Server agieren. Darüber hinaus kann jeder Server unabhängig automatisierte Aufgaben ausführen, z. B. das Synchronisieren von Rechnerressourcen oder das Löschen von HP SAM Systemprotokolldaten aus der HP SAM Datenbank. Weitere Informationen zu diesen geplanten Ereignissen finden Sie unter [„Verwaltung“ auf Seite 58](#).


Wenn Sie versuchen, das HP SAM Web Administration-Paket auf einem Microsoft SQL-Server zu installieren, bei dem für die Sortierung die Groß- und Kleinschreibung aktiviert ist, wird die Installation fehlschlagen.

Das HP SAM Web Administration-Paket kann zu Demonstrationszwecken oder für Pilotprojekte auf einem Domänencontroller installiert werden. Es wird allerdings dringend davon abgeraten, diese Verwendung für Produktionsinstallationen zu wählen.

---

So installieren Sie den HP SAM Webserver und die SQL-Software

1. Melden Sie sich beim Server mit einem Konto mit Administratorrechten an.
2. Führen Sie die Installationsdatei **HP SAM-xx ##.EXE** aus (## entspricht der Softwareversionsnummer). Ersetzen Sie xx durch EN für Englisch, JP für Japanisch, FR für Französisch, DE für Deutsch, ZH-CN für vereinfachtes Chinesisch oder KO für Koreanisch.
3. Klicken Sie im Begrüßungsbildschirm auf **Weiter**.
4. Für die Installation von HP SAM-Webserver fragt das Installationsprogramm nach einem Benutzerkonto. Das Benutzerkonto ist der Inhaber (d. h. das HP SAM-Dienstkonto) der HP SAM-Website und des HP SAM-Serverdienstes. Für dieses Konto sind folgende Berechtigungen erforderlich:
  - Administratorrechte auf allen Rechnerressourcen (z. B. Blade-PCs)
  - Administratorrechte auf dem HP SAM-Webserver
  - Domänenbenutzer – kein lokaler Administrator

 **HINWEIS:** HP empfiehlt dringend, den Namen und das Passwort eines Dienstkontos und nicht eines Benutzerkontos anzugeben. Sie sollten den Namen und das Passwort dieses Kontos so selten wie möglich ändern, um Störungen in HP SAM zu vermeiden.

Für die Installation der HP SAM-Webadministrator-Komponente muss der Name des Dienstkontos mit dem Namen im Active Directory übereinstimmen, einschließlich der lokalisierten Zeichen in dem Namen (z. B. ö, ä oder é).

Verwenden Sie das Dienstprogramm HP SAM Configuration Utility, das Sie im Menü **Start** des HP SAM Servers finden, um das Passwort des Dienstkontos für HP SAM zu ändern, wenn dieses aktualisiert wurde.

- 
5. Sie haben die Wahl, entweder nur die HP SAM-Webanwendung zu installieren oder nur die HP SAM-SQL-Datenbank oder beides. Damit HP SAM funktioniert, müssen beide Komponenten installiert sein. Standardmäßig werden beide Komponenten installiert. Klicken Sie auf den Dropdown-Pfeil neben **HP SAM Web Site (HP SAM-Website)** oder **HP SAM Database (HP SAM-Datenbank)**, um die Liste mit Optionen anzuzeigen.

---

△ **ACHTUNG:** Löschen Sie bei einem Upgrade **HP SAM Website** nicht aus dieser Liste, wenn die HP SAM Website und die SQL-Datenbank weiterhin auf demselben Server installiert sein sollen. Durch das Löschen des Eintrags für die HP SAM Website wird die HP SAM Website vom Server entfernt.

---

6. Verwenden Sie den Standardinstallationsordner, oder klicken Sie auf die Schaltfläche **Durchsuchen**, um den Ordner zu ändern. Klicken Sie auf **Weiter**, um fortzufahren.
7. Geben Sie den SQL-Servernamen ein und den **User Name (Benutzernamen)** und das **Password (Passwort)** für die NT-Authentifizierung oder für die SQL-Authentifizierung. Das SQL-Benutzerkonto muss zum Erstellen einer Datenbank auf dem SQL-Server berechtigt sein, damit die Anwendung fehlerfrei installiert werden kann. Wenn keine HP SAM-Datenbank vorhanden ist, wird bei der Installation eine erstellt. Wenn die Datenbank bereits vorhanden ist, wird bei der Installation der Webserver mit dem HP SAM-Datenbankserver verknüpft.
8. Klicken Sie auf dem Bildschirm für die Konfiguration von Webressourcen auf **Weiter**.
9. Wählen Sie **New Web Site (Neue Website)** für eine neue Webinstallation, oder wählen Sie **Existing (Vorhandene)**, um die Installation auf einer vorhandenen Website durchzuführen oder um HP SAM zu upgraden.
10. Klicken Sie auf die Liste mit **IP Address (IP-Adressen)** und ordnen Sie die Website der entsprechenden IP-Adresse zu.
11. Klicken Sie auf **Weiter**, um alle Tests auszuführen. Es wird empfohlen, alle Tests auszuführen, um eine ordnungsgemäße Installation sicherzustellen.

Während der HP SAM-Webserver-Installation werden jetzt Diagnosetests ausgeführt. Diese Tests suchen nach häufig auftretenden Konfigurations- oder Umgebungsproblemen, die zum Misslingen der HP SAM-Installation führen können. HP SAM-Dienstkonto-Berechtigungen; Unterstützung des Betriebssystems, des SQL-Servers und der .NET Framework-Version; Unterstützung der Domain-Umgebung; und die Windows Firewall-Einstellungen werden geprüft.

12. Klicken Sie auf **Weiter**, um die Installation zu starten, oder klicken Sie auf **Abbrechen**, um den Vorgang zu beenden.
13. Klicken Sie auf **Fertig stellen**, wenn die Installation abgeschlossen ist.
14. Wenn Ihre Netzwerkumgebung eine Hardware- und/oder Software-Firewall verwendet, müssen Sie für den HP SAM-Webserver und/oder den SQL-Server folgende Änderungen an den Firewall-Einstellungen vornehmen:
  - Webserver
    - Eingehend:
      - Von den Zugangsgeräten (TCP/ALLE) zum Webserver (TCP/80-HTTP)
      - Von den Blades (TCP/ALLE) zum Webserver (TCP/80-HTTP)
      - Von admin\_workstation (TCP/ALLE) zum Webserver (TCP/443-HTTPS)
      - Von den Blades (UDP/47777) zum Webserver (UDP/47777-Benutzerdefiniert)
    - Abgehend:
      - Vom Webserver (TCP/ALLE) zu SQL\_Server (TCP/1433-MSSQL), sofern die Ausführung nicht auf demselben Rechner erfolgt wie auf dem Webserver

- Vom Webserver (TCP/ALLE) zu den Blades (TCP/139-RPC)
- Vom Webserver (UDP/47777) zu den Blades (UDP/47777-Benutzerdefiniert)
- SQL-Server (nur wenn die Ausführung nicht auf demselben Rechner erfolgt wie dem Webserver)
  - Eingehend: Vom Webserver (TCP/ALLE) zu SQL\_Server (TCP/1433)
  - Ausgehend: Keine

- 15.** Auf einem HP SAM-Server ist ASP.NET 2.0 erforderlich. Wenn noch weitere Versionen installiert sind, aktivieren Sie die **Properties (Eigenschaften)** der HP SAM-Website. Klicken Sie auf die Registerkarte **ASP.NET** und wählen Sie dann **ASP.NET Version 2.0**.

## Benutzern Administratorzugang zu HP SAM gewähren

Der Domänenadministrator, die Domänenbenutzer in der Administratorengruppe auf dem Domaincontroller sowie die Domänenbenutzer in der lokalen Administratorengruppe auf dem HP SAM-Server sind automatisch Mitglieder der HP SAM-Administratorengruppe. HP rät dringend dazu, das System zu aktualisieren und dazu Sicherheitsgruppen oder einzelne Namen zu der HP SAM-Administratorenzugriffsliste hinzuzufügen, anstatt sich über das Administratorkonto anzumelden. Dadurch lässt sich nachverfolgen, wer wann was gemacht hat.

So fügen Sie weitere Benutzer als HP SAM-Administratoren hinzu: Rufen Sie die HP SAM-Verwaltungskonsole auf und fügen Sie diese Benutzer zu der Administratorengruppe hinzu. Zu näheren Informationen siehe [„Registerkarte „Benutzer und Rollen““ auf Seite 62](#).

## Konfigurieren der HP SAM Systemeinstellungen

Melden Sie sich bei der HP SAM-Verwaltungskonsole an, rufen Sie die Registerkarte **System Settings (Systemeinstellungen)** auf und führen Sie die entsprechenden Änderungen durch. Zu näheren Informationen siehe [„Registerkarte „Systemeinstellungen““ auf Seite 80](#).

## Konfigurieren von Secure Sockets Layer (SSL)

### SSL:

Sie können SSL auf dem HP SAM-Webserver konfigurieren (einschließlich der Installation eines Zertifikats), um Ihr Passwort und Ihre Browsersitzung zu verschlüsseln, wenn Sie sich bei der HP SAM-Verwaltungskonsole anmelden.

- Verwalten: Zugriff auf die HP SAM-Verwaltungskonsole
- Web-Client: Kommunikationsleitung zwischen dem Web-Client und dem HP SAM-Server

Nur für bestimmte virtuelle Verzeichnisse unter der HP SAM-Hauptwebsite kann die Option **Require secure channel (SSL) (Sicherer Kanal (SSL) erforderlich)** gewählt werden. Für die HP SAM-Hauptwebsite sollten Sie die Option **Require secure channel (SSL) (Sicherer Kanal (SSL) erforderlich)** nicht wählen.

## Installieren und Validieren der HP SAM Registrierungssoftware

Die manuelle Installation dieser Software umfasst die folgenden Schritte:

1. [„Installieren des HP SAM Registrierungsdienstes“ auf Seite 32](#)
2. [„Erstellen der Konfigurationsdatei für den HP SAM Registrierungsdienst“ auf Seite 33](#)
3. [„Starten/Neustarten des HP SAM Registrierungsdienstes“ auf Seite 36](#)
4. [„Testen des HP SAM Registrierungsdienstes“ auf Seite 36](#)


## Installieren des HP SAM Registrierungsdienstes

- Melden Sie sich mit einem Konto mit lokalen Administratorrechten beim Blade-PC an und führen Sie die Datei `bladeservice_xx##.MSI` aus (wobei „##“ für die Softwareversion steht). Ersetzen Sie „xx“ durch
  - EN = Englisch
  - JA = Japanisch
  - FR = Französisch
  - DE = Deutsch
  - KO = Koreanisch
  - ZH-CN = Vereinfachtes Chinesisch
- Wenn Sie Red Hat Linux verwenden, extrahieren Sie das tar.gz-Paket des HP SAM Linux-Registrierungsdienstes mit dem folgenden Befehl auf dem System: `tar xzvf <Dateiname.tar.gz>`  
Führen Sie dann `./install.sh` aus, um das Paket zu installieren.
- Halten Sie den Dienst ggf. an. Wählen Sie dazu **Systemsteuerung > Verwaltung > Dienste** aus, und suchen Sie nach dem HP SAM Registrierungsdienst. Falls dieser aktiv ist, halten Sie ihn




- an. Wenn Sie Linux verwenden, geben Sie im Terminal den folgenden Befehl ein: `/etc/init.d/daesvc stop`
- Passen Sie die .CFG-Datei des Dienstes an. Bearbeiten Sie die `hpevent.cfg`-Musterdatei. Informationen zum Anpassen dieser Datei finden Sie unter [„Erstellen der Konfigurationsdatei für den HP SAM Registrierungsdienst“ auf Seite 33](#).
  - Benennen Sie die nach der Anpassung der Konfigurationsdatei (erforderlich, siehe [„Erstellen der Konfigurationsdatei für den HP SAM Registrierungsdienst“ auf Seite 33](#)) die Musterdatei um, oder speichern Sie sie mit dem Befehl **Speichern unter** unter dem Namen `hpevent.cfg`.
  - Starten Sie den HP SAM Registrierungsdienst. Wählen Sie dazu **Systemsteuerung > Verwaltung > Dienste** aus, und starten Sie den Dienst mit dem Namen HP SAM Registration Service. Wenn Sie Linux verwenden, geben Sie im Terminal den folgenden Befehl ein: `/etc/init.d/daesvc start`.
  - Wenn der Computer durch eine Firewall geschützt ist, aktivieren Sie die folgenden Anschlüsse.
    - Eingehend:
      - Vom Webserver (UDP/47777) zum Blade (UDP/47777)
      - Vom Webserver (TCP/ALLE) zum Blade (TCP/139)
      - Von Zugriffsgeräten (TCP/BELIEBIG) zu Blade (TCP/3389)—RDP
      - Von Zugriffsgeräten (TCP/BELIEBIG) zu Blade (TCP/42966)—RGS

---

 **HINWEIS:** Der Standard-RGS-Port ist TCP/42966; allerdings kann diese Einstellung in RGS 5.3 und höher geändert werden. Für nähere Informationen wird auf die RGS-Dokumentation verwiesen. In HP SAM 3.0 und höher werden andere als die Standard-RGS-Ports unterstützt.

---
    - Abgehend:
      - Vom Blade (TCP/ALLE) zum Webserver (TCP/80-HTTP)
      - Vom Blade (UDP/47777) zum Webserver (UDP/47777)

---

 **HINWEIS:** Der Port kann auch durch Aktivieren des Softwaredienstes selbst aktiviert werden. Befolgen Sie die Anleitungen für die Firewall, um den HP SAM Registrierungsdienst zu aktivieren.

---

## Erstellen der Konfigurationsdatei für den HP SAM Registrierungsdienst

Die Konfigurationsdatei für den HP SAM Registrierungsdienst ist eine einfache Textdatei mit dem Namen `hpevent.cfg`. Der HP SAM Registrierungsdienst sucht diese Datei an den verschiedenen Speicherorten in der unten genannten Reihenfolge.

- Im selben Verzeichnis, in dem sich auch der Dienst befindet (normalerweise **C:\Programme \Hewlett-Packard\HP SAM Registration Service**)
- In `%SystemRoot%` (in der Regel **C:\Windows\**)
- In `%SystemDrive%` (in der Regel **C:\**)
- Linux: In `/opt/hpsamd/`

Sobald der Dienst die Datei gefunden hat, beendet er die Suche und extrahiert den Inhalt der Datei.

Siehe die folgende Mustervorlage. Sie müssen den Abschnitt [WebServerList] aktualisieren. Der Abschnitt [RolesList] ist optional. Wenn der Abschnitt [RolesList] keine Informationen enthält, wird er in der HP SAM-Verwaltungskonsole ohne Rollen angezeigt. Die Rollen können mithilfe der HP SAM-Verwaltungskonsole zugewiesen werden.

```
[hpEventCfg]
```

```
Gateway=WebServerList
```

```
Role=RolesList
```

```
AssetGroup=AssetGroupList
```

```
;ServicePort=47777
```

```
;DnsDomain=ExampleDomain.com
```

```
[WebServerList]
```

```
server1.yourdomain
```

```
server2.yourdomain
```

```
[RolesList]
```

```
sample-role-1
```

```
sample-role-2
```

```
[AssetGroupList]
```

```
sample-asset-group-1
```

```
sample-asset-group-2
```


## [WebServerList]

Im Abschnitt [WebServerList] werden HP SAM-Webserver aufgelistet. Jeder HP SAM-Webserver (Primärserver und Failover-Server) wird in einer eigenen Zeile genannt. Der Dienst verwendet diese Liste in der angegebenen Reihenfolge. Der erste HP SAM-Webserver in der Liste wird als erster zu verwenden versucht, und der Dienst probiert die übrigen HP SAM-Webserver der Reihe nach durch. Sobald eine Verbindung mit einem HP SAM-Webserver hergestellt werden konnte, werden die übrigen Server nicht mehr verwendet.

Für die Änderung der Serverzeile brauchen Sie lediglich im Ausdruck `server1.ihtdomain` den gewünschten Servernamen einzutragen (Sie können den DNS-Namen oder die statische IP-Adresse des Webserver verwenden). Beispiel:

- *HP SAM Servername*
- *10.1.2.3*


## [RolesList]

 **HINWEIS:** Die Zuweisung von Rollen in der .CFG-Datei ist optional. Normalerweise werden Rollen über die Konfigurationsdatei zugewiesen, weil die Rolle bei dieser Methode automatisch registriert wird. Sind in der .CFG-Datei keine Rollen angegeben, so können Rollen mithilfe der HP SAM-Verwaltungskonsole konfiguriert werden. Für weitere Informationen siehe [„Bereitstellen des HP SAM Registrierungsdienstes auf allen HP SAM Rechnerressourcen“ auf Seite 56](#).

Im Abschnitt [RolesList] sind keine oder mehrere Rollen aufgeführt, denen die Rechnerressource zugeordnet ist. Ein Rolle ist eine funktionale Sammlung von Rechnerressourcen (z. B. Blade-PCs). Die erste Rolle in der Liste ist die primäre Rolle der Rechnerressource. Alle anderen Rollen (falls vorhanden) werden als nicht primär betrachtet.

Wenn ein Benutzer eine Ressource in einer bestimmten Rolle anfordert, werden dem Benutzer Rechnerressourcen nach folgender Priorität zugeordnet:

- Verfügbare Rechnerressourcen, die nur dieser Rolle zugeordnet sind
- Verfügbare Rechnerressourcen, die mehreren Rollen zugeordnet sind, wobei diese Rolle die primäre Rolle ist
- Verfügbare Rechnerressourcen, die mehreren Rollen zugeordnet sind, wobei diese Rolle nicht die primäre Rolle ist

 **HINWEIS:** Wenn die Konfigurationsdatei für die Rechnerressource zu irgendeinem Zeitpunkt geändert wird, müssen Sie den Dienst neu starten, damit die Änderungen wirksam werden.

Diese Einstellung kann durch die über die HP SAM-Verwaltungskonsole zugewiesenen Rollen außer Kraft gesetzt werden.

## [AssetGroupList]

Im Abschnitt [AssetGroupList] sind keine oder mehrere Systemgruppen aufgeführt, denen die Rechnerressource zugeordnet ist. Der HP SAM Administrator oder Domänenadministrator verfügt über umfassende Berechtigungen für alle Systemgruppen auf dem HP SAM Server. Mithilfe von Systemgruppen können HP SAM Administratoren, die über umfassende Rechte verfügen, Objekte (Ressourcen, Benutzer usw.) einschränken oder verbergen, die von anderen Administratoren angezeigt und verwaltet werden dürfen. Weitere Informationen hierzu finden Sie unter [„Verwalten von Systemgruppen“ auf Seite 63](#).

## ServicePort

Mit dieser Einstellung definieren Sie einen nicht standardmäßigen UDP-Port, den HP SAM für die Kommunikation zwischen dem HP SAM Server und den Ressourcen verwendet. Wenn Sie diesen Schritt ausführen, müssen Sie auch noch weitere Einstellungen ändern. Weitere Informationen hierzu finden Sie unter [„Häufig gestellte Fragen \(FAQ\)“ auf Seite 101](#).

## DnsDomain

Mit dieser Einstellung können Sie festlegen, dass die Zeichenfolge eines Domännennamens den erkannten DNS-Namen überschreibt. Wenn beispielsweise die Ressource **Blade1** fälschlicherweise die Domäne als americas.hpinternal.net erkennt, die eigentlich hp.com sein soll, können Sie durch die Festlegung DnsDomain=hp.com erreichen, dass der an HP SAM zurückgegebene vollständige Domänenname Blade1.hp.com lautet.

## Starten/Neustarten des HP SAM Registrierungsdienstes

Sie können den Dienst über das Dienste-Applet (**Systemsteuerung > Verwaltung > Dienste**) oder über die Befehlszeile starten oder anhalten.

- Im Dienste-Applet wird der Dienst als **HP SAM Registrierungsdienst** angezeigt.
- Außerdem können Sie den Dienst über die Befehlszeile durch Eingabe der folgenden Syntax starten bzw. anhalten:

```
C:> net start daesvc
```

und

```
C:> net stop daesvc.
```

Sie können den Dienst auch mit Tools wie dem HP Rapid Deployment Pack starten und anhalten. Anleitungen hierzu finden Sie in der Dokumentation zum HP Rapid Deployment Pack.

Den Linux-Blade-Dienst können Sie durch Eingabe der folgenden Syntax starten bzw. anhalten:

```
/etc/init.d/daesvc start
```

und


```
/etc/init.d/daesvc stop
```

## Testen des HP SAM Registrierungsdienstes

Melden Sie sich bei der HP SAM-Verwaltungskonsole an, klicken Sie auf die Registerkarte **Resources (Ressourcen)** und suchen Sie nach der Rechnerressource innerhalb der Rolle, zu der diese zugewiesen wurde.

- Wenn die Rechnerressource nicht gefunden werden kann, überprüfen Sie die Firewall-Einstellungen und vergewissern Sie sich, dass der Dienst auf dieser Rechnerressource gestartet wurde.
- Wenn die Rechnerressource gefunden wird, klicken Sie auf die Registerkarte **Ressourcen**, wählen Sie in der Liste **Operation** den Eintrag **Synchronisieren** aus, und klicken Sie auf **Los**.

---

 **HINWEIS:** Wenn die Rechnerressource nach dem Synchronisierungsvorgang als offline gekennzeichnet ist, bedeutet dies normalerweise, dass der HP SAM-Webserver nicht mit der Rechnerressource kommunizieren kann. Überprüfen Sie die Firewall-Einstellung auf der Rechnerressource darauf, ob die eingehende Kommunikation auf Port 47777 oder der HP SAM-Registrierungsdienst zugelassen werden. Sie können feststellen, ob die Firewall den erforderlichen Datenverkehr blockiert, indem Sie die Firewall vorübergehend deaktivieren und später wieder aktivieren.

---

# Installieren und Validieren der HP SAM Client-Software

HP SAM umfasst folgende Clients:

- Internet Explorer-basierter Client
- Windows-basierter Client
- Blade Workstation Client-Reihe
- Linux-basierter Client

Der HP SAM Client erfordert, dass RGS (auf dem Windows-basierten Client, der Blade Workstation Client-Reihe oder dem Linux-Client) und/oder Remotedesktopverbindung oder rdesktop für Linux (alle Clients außer der Blade Workstation Client-Reihe) auf dem Zugriffsgerät funktionieren.

 **HINWEIS:** Der Linux-basierte Client unterstützt nur rdesktop-Versionen ab Version 1.3.1.

Zwischen den verschiedenen HP SAM Clients bestehen Unterschiede hinsichtlich ihrer Funktionalität.

**Tabelle 3-1 HP SAM Client-Vergleich**

<b>Funktionen</b>	<b>Internet Explorer-basiert</b>	<b>Windows XP Embedded-basiert</b>	<b>Blade Workstation Client Embedded-Betriebssystem-basiert</b>	<b>Linux-basiert</b>
Betriebssystem-Unterstützung	Windows XP Windows XP, 64-Bit Windows Vista, 32-Bit und 64-Bit Windows 7, 32-Bit und 64-Bit Windows XP Embedded Windows Embedded Standard (WES) WES 7	Windows XP Windows XP, 64-Bit Windows Vista, 32-Bit und 64-Bit Windows 7, 32-Bit und 64-Bit Windows XP Embedded Windows Embedded Standard (WES) WES 7	Blade Workstation Client Embedded-Betriebssystem	HP ThinConnect HP ThinPro HP ThinPro GT RHEL4 32-Bit und 64-Bit RHEL5 32-Bit und 64-Bit RHEL6 32-Bit und 64-Bit
Verbindungsprotokoll	Nur RDP	RGS und RDP	RGS	RGS und rdesktop
Automatische Failover-Unterstützung		X	X	X
Erfordert den Browser Internet Explorer	X			

**Tabelle 3-1 HP SAM Client-Vergleich (Fortsetzung)**


<b>Funktionen</b>	<b>Internet Explorer-basiert</b>	<b>Windows XP Embedded-basiert</b>	<b>Blade Workstation Client Embedded-Betriebssystem-basiert</b>	<b>Linux-basiert</b>
Ausführung erfordert das Herunterladen von ActiveX-Steurelementen	X			
Sprachen	Englisch, Japanisch, Französisch, Deutsch, Koreanisch, Vereinfachtes Chinesisch	Englisch, Japanisch, Französisch, Deutsch, Koreanisch, Vereinfachtes Chinesisch	Englisch	Englisch

## Internet Explorer-basierter Client

Ein Zugriffsgerät kann über den Internet Explorer auf HP SAM zugreifen. Geben Sie den Servernamen (<http://HP SAM Servername>) in die Adresszeile von Internet Explorer ein, um den Internet Explorer-basierten HP SAM Client zu verwenden.

Wenn das Zugriffsgerät zum ersten Mal auf den HP SAM Server zugreift, muss es zwei ActiveX-Steurelemente installieren (HP SAM Web Client Utility Class und Microsoft RDP Client Control). Der Installationsort für diese Steurelemente ist der Ordner %SystemRoot%\Downloaded Program Files\.

Es gibt weitere Internet Explorer-basierte Client-Konfigurationseinstellungen in HP SAM, die Sie vom HP SAM Server aus steuern können. Weitere Informationen finden Sie unter [„Registerkarte „Systemeinstellungen““ auf Seite 80](#).

 **HINWEIS:** HP empfiehlt, den HP SAM-Webserver zu der Liste vertrauenswürdiger Sites hinzuzufügen. Öffnen Sie auf dem Zugangsgerät Internet Explorer und rufen Sie unter **Extras > Internetoptionen >** die Registerkarte **Sicherheit** auf.

Wenn eine Firewall installiert ist, müssen Sie entsprechende Änderungen vornehmen, um den HP SAM Client durchzulassen. Wenn beispielsweise HP Sygate Security Agent installiert ist, fügen Sie eine Regel hinzu, um Port 3389 für die Anwendung **IEXPLORE.EXE** zuzulassen.

Zur Nutzung des Webclients auf einem Zugriffsgerät mit Windows XP 64-Bit müssen Sie den Internet Explorer 32-Bit verwenden.

## HP SAM ActiveX-Steurelemente

Die ActiveX-Steurelemente von HP SAM werden im Zuge des Webserver-Installationsvorgangs als Quelle für die Verbreitung auf dem HP SAM-Webserver gespeichert.

Wenn die ActiveX-Steuerelemente von HP SAM bei einem Upgrade auf dem HP SAM-Webserver ersetzt werden, wird der HP SAM-Client bei der nächsten Verbindung des Zugangsgerätes zum HP SAM-Webserver automatisch auf die neuere Version aktualisiert.

Die ActiveX-Steuerelemente von HP SAM unterstützen nur RDP 5.0, auch wenn RDP 6.0 oder höher oder RGS installiert ist.

Für den HP Thin Client, der Windows XP Embedded oder Windows Embedded Standard ausführt, muss die Installation der HP SAM ActiveX-Steuerelemente unter Umständen bei jedem Neustart des Zugriffsgerätes wiederholt werden, wenn diese nicht als Teil des Thin Client-Abbilds gespeichert sind. Verwenden Sie das Installationsprogramm für die Webclient-Steuerelemente aus dem HP SAM SoftPak, damit Sie keine Steuerelemente automatisch über den Browser herunterladen und installieren müssen.

## Windows-basierter Client

So installieren Sie den HP SAM Client auf einem Windows-basierten Thin Client oder auf einem Desktop-/Notebook-PC mit Windows XP, Windows Vista oder Windows 7:

1. Wenn Sie den HP SAM Client auf einem Windows-basierten Thin Client installieren, müssen Sie den Schreibfilter entsperren.

Wenn Sie den Schreibfilter nicht entsperren, bevor Sie Installations- oder Konfigurationsdaten auf dem XPe-Client speichern, gehen die Installations- oder Konfigurationsdaten beim Abschalten des Clients verloren.

2. Melden Sie sich beim Zugangsgerät mit einem Benutzerkonto an, das über Administratorrechte verfügt, und führen Sie die Datei scw32-xx##.MSI aus („##“ bezeichnet die Softwareversion), um den Windows-XP-basierten Client zu installieren. Ersetzen Sie „xx“ durch:
  - EN = Englisch
  - JA = Japanisch
  - FR = Französisch
  - DE = Deutsch
  - KO = Koreanisch
  - ZH-CN = Vereinfachtes Chinesisch
3. Befolgen Sie die Anleitungen des Installationsassistenten.
4. Vergewissern Sie sich nach der Installation der Software, dass das Programm im Startmenü (**Start > Alle Programme > Hewlett-Packard > HP Session Allocation Client**) aufgeführt wird.
5. Reaktivieren Sie jetzt den in Schritt 1 entsperren Schreibfilter.

## Schritte zur Benutzerdefinition

(Empfohlen)

1. Starten Sie den HP SAM Client.
2. Geben Sie den Namen des HP SAM-Webserver über die Tastatur ein.
3. Klicken Sie auf die Schaltfläche **Optionen**.

4. Ändern Sie die entsprechenden Verbindungseinstellungen.
5. Klicken Sie auf **Einstellungen speichern**.
6. Speichern Sie die Konfigurationsdatei (**hprdc.sam**) am Standardspeicherort, sofern möglich (auf manchen Thin Clients kann diese Funktion gesperrt sein).

Wenn Sie den HP SAM Client starten, werden Ihre gespeicherten Einstellungen wirksam.

Durch manuelle Bearbeitung der .SAM-Dateien (Konfigurationsdateien) können Sie zusätzliche Einstellungen vornehmen.

1. Der HP SAM Verbindungsclient sucht zuerst nach der benutzerspezifischen .SAM-Datei hprdc.sam
2. Anschließend prüft er die Zugriffsgerätedatei hprdc\_accessdevice.sam, die sich im Installationsordner von HP SAM befindet. In der Zugriffsgerätedatei enthaltene Parameter ersetzen die Parameter in der zusammengeführten Datei oder werden dieser hinzugefügt.
3. Anschließend prüft der Verbindungsclient im selben Ordner die Datei hprdc\_admin.sam. In der globalen Datei enthaltene Parameter ersetzen die Parameter in der zusammengeführten Datei oder werden dieser hinzugefügt.

Unter „[Konfigurationseinstellungen](#)“ auf [Seite 43](#) finden Sie eine Liste mit für den Windows-basierten Client verfügbaren Optionen.

## Linux-basierter Client

Zur Installation des Linux-Clients auf den folgenden Plattformen werden verschiedene Verfahren eingesetzt:

- [„HP Blade Workstation Client-Reihe“ auf Seite 40](#)
- [„HP ThinPro GT Client für den HP gt7725 Thin Client“ auf Seite 41](#)
- [„Red Hat Enterprise Linux \(RHEL\) Client“ auf Seite 42](#)

## HP Blade Workstation Client-Reihe

Der HP SAM Client ist auf der HP Blade Workstation Client-Reihe bereits vorinstalliert. So aktualisieren Sie den HP SAM Client: Rufen Sie [www.hp.com](http://www.hp.com) auf, klicken Sie auf **Treiber und Software zum Herunterladen**, wählen Sie den betreffenden Client und das **Embedded-Betriebssystem des Workstation Blade Clients** aus, und erstellen Sie ein neues Abbild des Clients.

### Schritte zur Benutzerdefinition

(Empfohlen)

1. Starten Sie den HP SAM Client.
2. Geben Sie den Namen des HP SAM-Webservers über die Tastatur ein.
3. Geben Sie Benutzername und Domäne an. (Dieser Schritt ist optional.)
4. Klicken Sie auf die Schaltfläche **Optionen**.
5. Ändern Sie die gewünschten Verbindungseinstellungen.



6. Klicken Sie auf **Einstellungen speichern**. Klicken Sie unter der Bestätigungsmeldung zum Speichern der Einstellungen auf **OK**.
7. Wählen Sie **\etc**.
8. Klicken Sie auf **Speichern**.
9. Klicken Sie auf **Verbinden**, um eine Verbindung herzustellen.
10. Wenn der HP SAM Client geschlossen ist, sollte er automatisch starten. Wenn er nicht startet, klicken Sie mit der rechten Maustaste, und wählen Sie **Remote Graphics** aus.

Durch manuelle Bearbeitung der .SAM-Dateien (Konfigurationsdateien) können Sie zusätzliche Einstellungen vornehmen.

1. Der HP SAM Verbindungsclient sucht zuerst nach der benutzerspezifischen .SAM-Datei hprdc.sam
2. Anschließend prüft er die Zugriffsgerätedatei /root/writable/opt/hpsam/hprdc\_accessdevice.sam. In der Zugriffsgerätedatei enthaltene Parameter ersetzen die Parameter in der zusammengeführten Datei oder werden dieser hinzugefügt.
3. Anschließend prüft der Verbindungsclient die Datei /root/writable/opt/hpsam/hprdc\_admin.sam. In der globalen Datei enthaltene Parameter ersetzen die Parameter in der zusammengeführten Datei oder werden dieser hinzugefügt.

Unter [„Konfigurationseinstellungen“ auf Seite 43](#) finden Sie eine Liste der für den Linux-Client verfügbaren Optionen.

## HP ThinPro GT Client für den HP gt7725 Thin Client

Gehen Sie beim HP gt7725 Thin Client mit HP ThinPro GT wie folgt vor, um den HP SAM Client zu installieren oder zu aktualisieren:

1. Bearbeiten Sie die Datei /etc/apt/sources.list und überprüfen Sie, ob die folgende Zeile vorhanden ist (falls nicht, fügen Sie sie ein): deb ftp://ftp.hp.com/pub/tcdebian gt7725 main non-free.
2. Speichern Sie die Datei, und aktualisieren Sie anschließend die Liste mit folgendem Befehl: apt-get update
3. Setzen Sie die Umgebungsvariable „http\_proxy“, falls erforderlich. Führen Sie folgenden Befehl aus: export http\_proxy='http://web-proxy.IhreFirma.com:8080', geben Sie dabei den von Ihnen verwendeten Proxy-Server an. Wenn Sie Synaptic verwenden, geben Sie die Proxy-Informationen unter **Preferences** (Einstellungen) > **Network** (Netzwerk) ein.
4. Führen Sie zum Installieren des HP SAM Clients folgenden Befehl aus: apt-get install hptc-sam-client, oder rufen Sie die Software mithilfe der Anwendung Synaptic ab.

Durch manuelle Bearbeitung der .SAM-Dateien (Konfigurationsdateien) können Sie zusätzliche Einstellungen vornehmen.

1. Der HP SAM Verbindungsclient sucht zuerst nach der benutzerspezifischen .SAM-Datei hprdc.sam
2. Anschließend prüft er die Zugriffsgerätedatei /opt/hpsam/hprdc\_accessdevice.sam. In der Zugriffsgerätedatei enthaltene Parameter ersetzen die Parameter in der zusammengeführten Datei oder werden dieser hinzugefügt.
3. Anschließend prüft der Verbindungsclient die Datei /opt/hpsam/hprdc\_admin.sam. In der globalen Datei enthaltene Parameter ersetzen die Parameter in der zusammengeführten Datei oder werden dieser hinzugefügt.

Unter „[Konfigurationseinstellungen](#)“ auf [Seite 43](#) finden Sie eine Liste der für den HP ThinPro GT-Client verfügbaren Optionen.

## Red Hat Enterprise Linux (RHEL) Client

So installieren Sie den HP SAM Linux-Client auf einem System mit RHEL Version 4 oder 5:

1. Melden Sie sich beim Zugangsgesamt mit einem Benutzerkonto an, das über Stammberechtigungen verfügt.
2. Extrahieren Sie das tar.gz-Paket des Linux-Clients auf dem System, indem Sie den folgenden Terminalbefehl ausführen: tar xzvf <Dateiname.tar.gz>
3. Führen Sie das Installationsskript mit folgendem Befehl aus: ./install.sh
4. Vergewissern Sie sich nach der Installation der Software, dass das Programm in /opt/hpsam installiert wurde.

## Schritte zur Benutzerdefinition

(Empfohlen)

1. Starten Sie den HP SAM Client.

Wenn Sie den HP SAM Client starten (durch Ausführen von /opt/hpsam/hprdccli.sh), werden Ihre gespeicherten Einstellungen wirksam.

2. Geben Sie den Namen des HP SAM-Webservers über die Tastatur ein.
3. Klicken Sie auf **Optionen**.
4. Ändern Sie die entsprechenden Verbindungseinstellungen.
5. Klicken Sie auf **Speichern**.

Durch manuelle Bearbeitung der .SAM-Dateien (Konfigurationsdateien) können Sie zusätzliche Einstellungen vornehmen.

1. Der HP SAM Verbindungsclient sucht zuerst nach der benutzerspezifischen .SAM-Datei hprdc.sam
2. Anschließend prüft er die Zugriffsgerätedatei /opt/hpsam/hprdc\_accessdevice.sam. In der Zugriffsgerätedatei enthaltene Parameter ersetzen die Parameter in der zusammengeführten Datei oder werden dieser hinzugefügt.
3. Anschließend prüft der Verbindungsclient die Datei /opt/hpsam/hprdc\_admin.sam. In der globalen Datei enthaltene Parameter ersetzen die Parameter in der zusammengeführten Datei oder werden dieser hinzugefügt.

Unter [„Konfigurationseinstellungen“ auf Seite 43](#) finden Sie eine Liste der für den RHEL-Client verfügbaren Optionen.

## Konfigurationseinstellungen

### Optionen

Es stehen weitere Optionen zur Konfiguration der Einstellungen zur Verfügung. Durch manuelle Bearbeitung der .SAM-Datei können Sie diese Optionen festlegen. In der folgenden Liste sind im Abschnitt [HPRDC] unterstützte Schlüssel und Werte aufgeführt.


- **Gateways** – String-Wert. Verweist auf den Abschnitt, in dem HP SAM Server aufgelistet sind.
- **DefaultDomain** – Zeichenfolgenwert. Dies ist ein Standardwert, der in das Bearbeitungsfeld **Domain** auf der Benutzeroberfläche des Clients geladen werden kann. Wenn dieser Wert nicht angegeben ist, versucht das Programm die Domain anhand der Zugangsdaten des Benutzers zu ermitteln, kommt dabei aber nicht unbedingt immer zum richtigen Ergebnis.
- **Policies** – String-Wert. Verweist auf den Abschnitt, in dem die Einstellungen aufgelistet sind, die in der Liste **Vordefinierte Einstellungen laden** des Clients auf der Registerkarte **Weitere** im Abschnitt **Optionen** aufgeführt sind. So kann der Administrator mehrere Einstellungen vordefinieren, die mit verschiedenen Verbindungsarten verknüpft sind. Weitere Informationen hierzu finden Sie unter [„Richtlinieneinträge“ auf Seite 50](#).
- **DefaultPolicy** – Zeichenfolgenwert. Diese Policy sollte standardmäßig in der Liste geladener Voreinstellungen des Clients im Bereich Options (Optionen) auf der Registerkarte Other (Sonstige) gewählt sein. Sie hat nichts mit den HP SAM-Policies zu tun, die in der HP SAM-Verwaltungskonsole festgelegt werden.
- **Autodial** – ganze Zahl, 0 oder 1. Wenn der Wert 1 angegeben ist, versucht das Programm beim Starten automatisch eine Verbindung herzustellen, ohne dass der Benutzer vorher die Zugangsdaten eingeben muss. Der Standardwert lautet 0.
- **DefaultUsername** – Zeichenfolgenwert. Wenn dieser Wert nicht angegeben ist, versucht das Programm den Benutzernamen anhand der Zugangsdaten des Benutzers zu ermitteln, kommt dabei aber nicht unbedingt immer zum richtigen Ergebnis.
- **DefaultInsecurePassword** – String-Wert. Mit diesem Feld können Sie das Passwortfeld ausfüllen lassen. Dieses Feld wurde für die automatische Lastüberprüfung in einer Umgebung entwickelt, in der Sicherheit eine sekundäre Rolle spielt.

- △ **ACHTUNG:** Das Feld **DefaultInsecurePassword** enthält unverschlüsselten Text und sollte nicht in einer Produktionsumgebung verwendet werden.
- **Debug** – Ganzzahl, 0 oder 1. Wird der Wert auf 1 festgelegt, werden Debug-Protokolle zu Fehlerbehebungszwecken in der Datei /tmp/hprdc.log erfasst. Diese Option ist nur auf Linux-Clients gültig. Der Standardwert lautet 0.
  - **Failover** – ganze Zahl, 0 oder 1. Wenn der Wert 1 angegeben ist, wird die Failover-Funktion auf dem Zugangsgerät aktiviert. Wenn mehrere Webserver definiert sind, wechselt das Zugangsgerät zum nächsten verfügbaren HP SAM-Webserver, wenn eine Verbindung fehlschlägt. Durch die Aktivierung dieser Funktion kann der Benutzer keinen neuen HP SAM-Server mehr eingeben; er kann aber nach wie vor zwischen den in der Konfigurationsdatei definierten Webservern wählen. Der Standardwert lautet 0 (Aus).
  - **EnablePublicRoles** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 zeigt der HP SAM Client alle verfügbaren öffentlichen Rollen an, mit denen der Benutzer eine Verbindung herstellen kann. Bei Auswahl des Werts 0 verbirgt der HP SAM Client die öffentlichen Rollen. Der Standardwert lautet 1 (anzeigen).
  - **ResetAfterSession** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 werden die Zugriffsgeräteeinstellungen, einschließlich des Benutzernamens, nach jeder Sitzung auf die Standardeinstellungen zurückgesetzt. Dies ist sinnvoll im Kiosk-Modus, um die Einstellungen vorheriger Benutzer zu löschen. Der Standardwert ist 0.
  - **DefaultMonitorLayoutID** – String-Wert. Der String-Wert gibt die Monitorlayout-ID an, die bei der Anmeldung über das Zugriffsgerät standardmäßig verwendet werden soll. Diese Einstellung ist nur wirksam, wenn beim Herstellen der Verbindung neue Zugriffsgeräte registriert werden. Damit diese Einstellung auch für vorhandene Zugriffsgeräte gilt, löschen Sie diese aus HP SAM, damit sie neu registriert werden.
  - **AssetGroup=AssetGroupList** – AssetGroupList verweist auf einen anderen Abschnitt der Datei mit entsprechendem Namen [AssetGroupList], in dem eine oder mehrere Ressourcengruppen aufgeführt sind.
  - **ConnectionBar.Enable** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 wird die HP SAM Verbindungsleiste aktiviert. Bei Auswahl des Werts 1 hat der Benutzer die Möglichkeit, mehrere Verbindungen über die HP SAM Verbindungsleiste zu verwalten. So wird außerdem vermieden, dass der Benutzer den Client mehrmals öffnet. Der Standardwert lautet 1 für die Blade Workstation Client-Reihe sowie den Linux-Client und 0 für alle anderen.
  - **ConnectionBar.FollowMouse** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 wird die Verbindungsleiste an der Position auf dem Bildschirm geöffnet, an der sich der Cursor befindet. Der Standardwert lautet 1.
  - **ConnectionBar.Location** – Ganzzahlwert. Legt die Position der Verbindungsleiste fest (bei 0 oben; bei 1 unten; bei 2 links; bei 3 rechts). Der Standardwert lautet 0 (oben).
  - **ConnectionBar.EnableAddNew** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 wird die Schaltfläche **Neu hinzufügen** in der Verbindungsleiste aktiviert. Der Standardwert lautet 1.
  - **ConnectionBar.EnableCloseAll** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 wird die Schaltfläche **Alle trennen** in der Verbindungsleiste aktiviert. Der Standardwert lautet 1.
  - **ConnectionBar.EnableReconnectAll** – Ganzzahlwert, 0 oder 1. Der Standardwert lautet 1 (aktiviert). Wählen Sie den Wert 0 (deaktiviert) aus, um die Schaltfläche **Alle erneut verbinden** in der Verbindungsleiste auszublenden.

- **ConnectionBar.EnableDisconnectInstance** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 wird die Schaltfläche **Trennen** in der Verbindungsleiste für jede Sitzung aktiviert. Der Standardwert lautet 1.
- **ConnectionBar.EnableContextMenu** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 wird per rechten Mausklick auf ein Sitzungsstatussymbol in der Verbindungsleiste ein Kontextmenü geöffnet. Über dieses Menü kann der Benutzer zur ausgewählten Sitzung wechseln, die ausgewählte Sitzung verschieben oder minimieren oder alle aktuell verbundenen Sitzungen minimieren. Bei Auswahl des Werts 0 wird das Menü nicht angezeigt. Der Standardwert lautet 1.
- **ConnectionBar.EnableSave** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 ist die Schaltfläche **Speichern** in der Verbindungsleiste verfügbar, sodass der Administrator die aktuelle Sitzungskonfiguration als Monitorlayout-ID auf dem Server speichern kann. Sitzungen mit getrennter Verbindung werden nicht in der Datenbank gespeichert. Der Standardwert lautet 0.
- **ConnectionBar.ShowDelay** – Ganzzahlwert. Gibt in Millisekunden an, wie lange es dauert, bis die Verbindungsleiste angezeigt wird, nachdem der Mauszeiger zum Bildschirmrand bewegt wurde. Der Standardwert lautet 500 Millisekunden.
- **ConnectionBar.ShowOnDisconnect** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 wird die Verbindungsleiste beim Schließen einer Sitzung automatisch angezeigt. Der Standardwert lautet 1.
- **ConnectionBar.AutoHideTimeout** – Ganzzahlwert. Gibt die Zeitspanne in Sekunden an, für die die Verbindungsleiste geöffnet bleibt, wenn der Mauszeiger von der Verbindungsleiste weg bewegt wird. 0 = bleibt immer geöffnet. Der Standardwert lautet 3.
- **ConnectionBar.ShowTimingFactor** – Ganzzahlwert. Steuert die Geschwindigkeit der Animation beim Einblenden der Verbindungsleiste auf dem Bildschirm. Ein niedriger Wert hat eine schnellere Animation zur Folge. Die Wahl eines niedrigeren Werts kann bei langsamen Client-Systemen mit zu langsamer Animation der Verbindungsleiste hilfreich sein. Der Standardwert lautet 5.
- **ConnectionBar.HideTimingFactor** – Ganzzahlwert. Steuert die Geschwindigkeit der Animation beim Ausblenden der Verbindungsleiste auf dem Bildschirm. Ein niedriger Wert hat eine schnellere Animation zur Folge. Die Wahl eines niedrigeren Werts kann bei langsamen Client-Systemen mit zu langsamer Animation der Verbindungsleiste hilfreich sein. Der Standardwert lautet 5.
- **ConnectionBar.SessionWindow.EnableIdentify** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 wird eine in der HP SAM Verbindungsleiste ausgewählte RGS-Sitzung hervorgehoben und kann vom Benutzer verschoben werden. Für die Nutzung dieser Funktionen wird RGS 5.1.3 oder höher benötigt. Der Standardwert lautet 1.
- **DisclaimerDisplay.Timeout** – Zeit in Sekunden, die der HP SAM Client im Leerlaufmodus verharrt, bis das Fenster mit dem Haftungsausschluss erneut angezeigt wird. Der Standardwert lautet 30.
- **Resolutions** – String-Wert. Gibt einen anderen Abschnitt in der .SAM-Datei an, der eine Liste mit Auflösungen zur Anzeige auf der Client-Benutzeroberfläche enthält. Öffnen Sie die Standard-.SAM-Datei, um das erforderliche Format anzuzeigen.

- **ConnectionBar.ShowLogoff** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 wird beim Trennen der Verbindung eine Option zum Abmelden der Ressource angezeigt. Der Standardwert lautet 0.
- **ConnectionBar.ShowReboot** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 wird beim Trennen der Verbindung eine Option zum Neustarten der Ressource angezeigt. Der Standardwert lautet 0.


---

 **HINWEIS:** Die Optionen zum Abmelden oder Neustarten von der Verbindungsleiste aus werden in der globalen Policy standardmäßig deaktiviert. Zum Abmelden und Neustarten müssen folgende Voraussetzungen erfüllt sein:

- Ein Zertifikat von der Domain-Zertifizierungsstelle muss auf der HP SAM-Website installiert sein, damit die Benutzernamen und Passwörter an den Server gesendet werden können.
- Das HP SAM-Dienstkonto muss über lokale Administratorrechte auf der Ressource verfügen, damit die Berechtigungen zum Neustarten oder zum Anmelden eines Benutzers vom Blade erteilt werden können.

- **ConnectionBar.ShowHardReboot** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 wird beim Trennen der Verbindung eine Option zum Aus- und erneuten Einschalten der Ressource angezeigt. Der Standardwert lautet 0.


---

 **HINWEIS:** In der globalen Richtlinie ist die Option für das Ausschalten und erneute Einschalten über die Verbindungsleiste standardmäßig deaktiviert. Die folgenden Anforderungen müssen für das Ausschalten und erneute Einschalten erfüllt sein:

- Ein Zertifikat von der Domain-Zertifizierungsstelle muss auf der HP SAM-Website installiert sein, damit die Benutzernamen und Passwörter an den Server gesendet werden können.
- Für die HP BladeSystem PC-Gehäuse muss Integrated Administrator (IA) Software der Version 4.20 oder höher verwendet werden. Standardmäßig weist die IA-Software ein deaktiviertes Konto mit dem Namen **SAM** auf. Sie müssen dieses Konto **SAM** aktivieren und ein Passwort erstellen, damit die Option für das Ausschalten und erneute Einschalten funktioniert.
- Das IA-Passwort für das integrierte **SAM**-Konto muss in HP SAM auf der Seite „Rechenzentren verwalten“ gespeichert sein.
- Es ist einer der folgenden HP BladeSystem Blade-PCs erforderlich:

- HP BladeSystem bc2000 Blade-PC
  - HP BladeSystem bc2200 Blade-PC
  - HP BladeSystem bc2500 Blade-PC
  - HP BladeSystem bc2800 Blade-PC
-

## Smart Card-Einstellungen

 **HINWEIS:** Smart Card-Einstellungen sind für die Blade Workstation Client-Reihe und den Linux-Client nicht gültig.

- **SmartCardAlways** – ganze Zahl, 0 oder 1. Mit dieser Einstellung kann der Benutzer seine Zugangsdaten über eine Smartcard eingeben und sich anmelden. Wenn **UiMode** = 0 oder 1, kann sich der Benutzer mit einer Smartcard anmelden. Wenn **UiMode** = 2, muss sich der Benutzer mit einer Smartcard anmelden. Siehe unter „UiMode“ in [„Einstellungen zur Benutzerdefinition der Oberfläche“ auf Seite 47](#). Der Standardwert lautet 1 (Zulassen).
- **SmartCardRequiresClick** – Ganzzahlwert, 0 oder 1. Wählen Sie den Wert 1, damit der Benutzer auf **Verbinden** klicken muss, nachdem die Smart Card erkannt wurde. Wenn Sie den Wert 0 wählen, wird automatisch eine Verbindung hergestellt, wenn der Benutzer eine Smart Card einsetzt. Der Standardwert lautet 1.
- **SmartCardCSP** – String-Wert. Der beim Zugriff auf eine Smart Card zu verwendende CSP. Dieser muss exakt mit dem Namen des auf dem Rechner installierten CSP übereinstimmen. Die Standardeinstellung lautet „ActivCard Gold Cryptographic Service Provider“. Beispiel: Verwenden Sie für ActivClient 6.x die Einstellung „ActivClient Cryptographic Service Provider“.
- **SmartCardUidType** – Ganzzahlwert, 1 oder 8. Das Feld **Typ** in der Eigenschaftenaufzählung des Smart Card-Zertifikats, das zur Ermittlung des UPN-Namens verwendet werden soll. Der Wert 8 bedeutet CERT\_NAME\_UPN\_TYPE. Wenn Sie den Wert 8 auswählen, müssen Sie **SmartCardUidOid** angeben. Der Standardwert lautet 1 (CERT\_NAME\_EMAIL\_TYPE).
- **SmartCardUidOid** – String-Wert. Die mit dem angegebenen Smart Card-UID-Typ verknüpfte OID. Nicht alle Typen erfordern eine OID. Der Eintrag **SmartCardUidType=8** ist erforderlich. Es ist kein Standardwert angegeben.
- **SmartCardAutoDisconnect** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 wird die Verbindung der Sitzung automatisch getrennt, wenn die Smart Card entfernt wird. Hinweis: Die Richtlinieneinstellungen von Active Directory beeinflussen möglicherweise das tatsächliche Verhalten dieser Eigenschaft. Active Directory-Optionen sind beispielsweise „Beibehalten“, „Passwortsperre“ und „Abmelden“. Active Directory enthält keine Option zum Trennen der Verbindung, daher müssen Sie die Funktion **SmartCardAutoDisconnect** zum Trennen der Verbindung nutzen. Der Standardwert lautet 1.

## Einstellungen zur Benutzerdefinition der Oberfläche


- **UiMode** – Ganzzahlwert, 0, 1 oder 2. Wählen Sie den Typ der anzuzeigenden Benutzeroberfläche aus.
  - 0 (Standard) – Die Felder **HP SAM Server**, **Benutzername** und **Domäne** werden auf der Benutzeroberfläche angezeigt.
  - 1 – Der UPN-Modus wird angezeigt. Das Feld **Domäne** wird nicht angezeigt. Der Benutzer muss das Format Benutzername@Domäne verwenden.
  - 2 – Der Smart Card-Modus wird angezeigt. Die Felder **Benutzername** und **Domäne** sind ausgeblendet und der Benutzer wird aufgefordert, die Smart Card einzusetzen. Die Schaltfläche **Verbinden** ist deaktiviert, wenn keine Smart Card eingesetzt ist. Beim Blade

Workstation Client Embedded-Betriebssystem und beim Linux-Client wird dieser Wert (2) wie der Wert 1 behandelt.

- **Banner** – String-Wert. Ermöglicht das Laden einer bestimmten Datei als Banner-Bild im Hauptdialog des Zugriffsgeräts. Das Bild muss im Format Windows Bitmap (BMP) vorliegen. Die Angabe eines vollständigen Pfads ist erforderlich. Der Bannerbereich umfasst 385 x 60 Pixel und 24 Bit Farbtiefe. Wenn Sie eine Datei mit abweichender Auflösung angeben, wird sie an den Bannerbereich angepasst.
- **TitlebarText** – String-Wert. Ermöglicht das Überschreiben des Standardtexts einer Titelleiste mit einem festgelegten String. Standardmäßig wird der Text in der entsprechenden Sprache angezeigt.
- **ShowVersion** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 wird die Version des HP SAM Clients als Text im Hauptfenster angezeigt. Der Standardwert ist 1.
- **EnableOptionsButton** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 wird die Schaltfläche **Optionen** im Haupt-Anwendungsdialog angezeigt. Bei Auswahl des Werts 0 wird die Schaltfläche nicht angezeigt. Der Standardwert lautet 1.
- **EnablePassword** – Ganzzahlwert, 0 oder 1. Wenn der Wert 1 lautet, wird das Feld **Passwort** auf der Benutzeroberfläche des Zugriffsgeräts angezeigt. Wenn der Wert 0 ausgewählt wird, ist das Passwortfeld nicht verfügbar. Der Standardwert lautet 1.
- **UILanguage** – Sprachkennung. Unterstützte Sprachkennungen:
  - EN = Englisch
  - FR = Französisch
  - DE = Deutsch
  - JA = Japanisch
  - KO = Koreanisch
  - ZH-CN = Vereinfachtes Chinesisch

Wenn die Kennung nicht unterstützt wird oder die Eigenschaft in der Datei nicht vorhanden ist, wird standardmäßig amerikanisches Englisch verwendet. Eine Sprachunterstützungs-DLL muss verfügbar sein. Nicht gültig für die Blade Workstation Client-Reihe und den Linux-Client.

---

 **HINWEIS:** Die angegebene UILanguage muss entweder mit der Sprache der installierten HP SAM Client-Anwendung übereinstimmen, oder die Sprache muss Englisch sein. Wenn Sie die englische HP SAM Client-Anwendung installiert haben, verwenden Sie hier keinen Wert für eine andere Sprache. Um möglichst wenig Festplattenspeicher zu belegen, enthält die englische HP SAM Client-Anwendung keine andere Sprach-DLL für den HP SAM Client.

---

- **EnableServer** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 ist das Feld **HP SAM Server** im Hauptdialog der Anwendung sichtbar. Bei Auswahl des Werts 0 wird das Feld nicht angezeigt. Auch wenn das Feld deaktiviert ist, ist der Wert erforderlich und muss in der Konfigurationsdatei angegeben werden. Der Standardwert lautet 1.
- **EnableDomain** – Ganzzahlwert, 0, 1 oder 2. Bei Auswahl des Werts 1 ist das Domänenfeld im Hauptdialog der Anwendung sichtbar. Bei Auswahl des Werts 0 wird das Feld nicht angezeigt. Wenn das Feld nicht sichtbar ist, wird die angegebene Domäne mit der Einstellung „DefaultDomain“ verwendet (es sei denn, der Benutzername wird als UPN-Name oder im Format Domäne\Benutzername für eine andere Domäne eingegeben). Bei Auswahl des Werts 2 ist das



Feld sichtbar, kann aber nicht bearbeitet werden. Die über die Einstellung „DefaultDomain“ festgelegte Domäne ist stets in Kraft und kann vom Format UPN oder Domäne\Benutzername nicht außer Kraft gesetzt werden. Der Standardwert lautet 1.

- **KioskMode** – Ganzzahlwert. Nicht gültig für Blade Workstation Client-Reihe. Wenn ein anderer Wert als Null ausgewählt ist, wird die Benutzeroberfläche für die Verwendung in einer Kiosk-Modus-Umgebung geändert. Gültige Werte:
  - **Bit 1** – Schaltfläche **Abbrechen** aktivieren/deaktivieren (1 = deaktivieren)
  - **Bit 2** – Aktivieren/deaktivieren der Schaltfläche **Minimieren** in der Symbolleiste (1 steht für Deaktivieren)
  - **Bit 3** – Aktivieren/deaktivieren der Schaltfläche **Schließen** in der Symbolleiste (1 steht für Deaktivieren)

Der Standardwert lautet 0 (alle Funktionen sind aktiviert). Wählen Sie beispielsweise den Wert 3, um die Schaltflächen **Abbrechen** und **Minimieren** zu deaktivieren und um die Schaltfläche **Schließen** aktiviert zu lassen.

- **DisplayShutdown** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 wird der Client-Benutzeroberfläche eine interaktive Schaltfläche hinzugefügt, über die der Benutzer das Zugriffsgerät herunterfahren kann. Dieselbe Schaltfläche wird auch mithilfe der Optionen **DisplayShutdown**, **DisplayRestart** und **DisplayLogoff** hinzugefügt. Wenn die Schaltfläche bereits durch Auswahl einer anderen Option angezeigt wird, wird die Option **Herunterfahren** zum Dropdown-Menü der Schaltfläche hinzugefügt. Nicht gültig für die Blade Workstation Client-Reihe und den Linux-Client. Der Standardwert lautet 0 (nicht anzeigen).
- **DisplayRestart** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 wird der Client-Benutzeroberfläche eine interaktive Schaltfläche hinzugefügt, über die der Benutzer das Zugriffsgerät neu starten kann. Dieselbe Schaltfläche wird auch mithilfe der Optionen **DisplayShutdown**, **DisplayRestart** und **DisplayLogoff** hinzugefügt. Wenn die Schaltfläche bereits durch Auswahl einer anderen Option angezeigt wird, wird die Option **Neustart** zum Dropdown-Menü der Schaltfläche hinzugefügt. Nicht gültig für die Blade Workstation Client-Reihe und den Linux-Client. Der Standardwert lautet 0 (nicht anzeigen).
- **DisplayLogoff** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 wird der Client-Benutzeroberfläche eine interaktive Schaltfläche hinzugefügt, über die der Benutzer das Zugriffsgerät abmelden kann. Dieselbe Schaltfläche wird auch mithilfe der Optionen **DisplayShutdown**, **DisplayRestart** und **DisplayLogoff** hinzugefügt. Wenn die Schaltfläche bereits durch Auswahl einer anderen Option angezeigt wird, wird die Option **Abmelden** zum Dropdown-Menü der Schaltfläche hinzugefügt. Nicht gültig für die Blade Workstation Client-Reihe und den Linux-Client. Der Standardwert lautet 0 (nicht anzeigen).
- **DefaultSessionAction** – Ganzzahlwert, 0, 1 oder 2. Beim Wert 0 ist die Standard-Sitzungsaktion (Anklicken der Schaltfläche ohne Erweitern der Dropdown-Liste) für die Schaltfläche „Herunterfahren“. Bei Auswahl des Werts 1 ist die Standardaktion „Neustart“. Bei Auswahl des Werts 2 ist die Standardaktion „Abmelden“. Wenn nur eine Aktion aktiviert ist, ist diese die Standardaktion und die Einstellung wird ignoriert. Wenn der Wert einer Aktion entspricht, die nicht aktiviert ist, ist keine Standardaktion verfügbar. Nicht gültig für die Blade Workstation Client-Reihe und den Linux-Client. Der Standardwert lautet 0.

## Richtlinieneinträge


Durch manuelle Bearbeitung der .SAM-Datei können Sie Richtlinieneinträge festlegen. Diese Einstellungen müssen sich in einem Richtlinienabschnitt der .SAM-Datei befinden, beispielsweise [Local Area Network] oder [saved settings]. Diese Werte geben nur die Standardeinstellungen für die Benutzeroberfläche an. Werte, die der Benutzer in der Benutzeroberfläche ändert, sind wirksam.

- **Protocol** – Ganzzahlwert, 0, 1 oder 3. Gibt das für die Verbindung zu verwendende Protokoll an. RDP entspricht dem Wert 1, RGS dem Wert 3. Der Wert 0 (automatisch) verwendet automatisch erkannte Einstellungen, wobei RGS gegenüber RDP bevorzugt wird. Der Standardwert lautet 0.
- **Mute** – 0 oder 1. Wenn der Wert 0 lautet, ist Audio für diese Verbindung aktiviert. Bei Auswahl des Werts 1 ist Audio deaktiviert. Der Standardwert lautet 0.
- **SoundQuality** – Ganzzahlwert, 1, 2, oder 3. Wählen Sie 1 für die niedrigste und 3 für die höchste Tonqualität aus. Dieser Wert wird nur für RGS-Verbindungen unterstützt. Der Standardwert lautet 2.
- **SoundStereo** – 0 oder 1. Bei Auswahl des Werts 1 wird Stereo-Ton unterstützt. Beim Wert 0 wird Mono-Ton wiedergegeben. Dieser Wert wird nur für RGS-Verbindungen unterstützt. Der Standardwert lautet 1.
- **BordersEnabled** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 werden normale Fensterränder verwendet. 0 = keine Ränder. Dieser Wert wird nur für RGS-Verbindungen unterstützt. Der Standardwert lautet 1.
- **WindowSnapEnabled** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 kann das Sitzungsfenster beim Verschieben am Bildschirmrand ausgerichtet werden. Dieser Wert wird nur für RGS-Verbindungen unterstützt. Der Standardwert lautet 1.
- **AudioFollowsFocus** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 0 ist der Ton aller Sitzungen zu hören. Bei Auswahl des Werts 1 ist nur der Ton der Sitzung mit dem Fokus zu hören. Dieser Wert wird nur für RGS-Verbindungen unterstützt. Der Standardwert lautet 0.
- **MicrophoneEnabled** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 wird die analoge Mikrofoneingabe vom Zugriffsgerät an RGS-Sitzungen gesendet. Dieser Wert wird nur für RGS-Verbindungen unterstützt. Er wird von RDP-Sitzungen ignoriert. Für die Nutzung dieser Funktion wird RGS 5.1.3 oder höher benötigt. Der Standardwert lautet 0.
- **KeyRepeatEnabled** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 wird die Unterdrückung von Tastenwiederholungen deaktiviert. Diese Funktion ist in RGS normalerweise erforderlich, damit Tasten in Tastenkombinationen nicht wiederholt werden, wenn sie gedrückt gehalten werden. Dieser Wert wird nur für RGS-Verbindungen unterstützt. Der Standardwert lautet 0.
- **MapUSB** – Ganzzahlwert, 0 oder 1. Die Auswahl des Werts ermöglicht die USB-Umleitung. Dieser Wert wird nur für RGS-Verbindungen unterstützt. Bei RGS 5.1.3 oder höher können Sie USB-Geräte über die HP SAM Verbindungsleiste einer ausgewählten Sitzung neu zuweisen. Der Standardwert lautet 0.
- **ImageQuality** – Ganzzahlwert, 0 bis 100. Legt die Bildqualität fest. 0 = niedrigste Qualität, minimale Nutzung der Netzwerkbandbreite. 100 = höchste Qualität, maximale Nutzung der Netzwerkbandbreite. Dieser Wert wird nur für RGS-Verbindungen unterstützt. Der Standardwert lautet 65.

- **Compression** – 0 oder 1. Bei Auswahl des Werts 1 ist die RDP-Komprimierung aktiviert. Dieser Wert wird nur für RDP-Verbindungen unterstützt. Der Standardwert lautet 1.
- **Wallpaper** – 0 oder 1. Bei Auswahl des Werts 1 wird das Hintergrundbild des Remote-Desktops angezeigt. Dieser Wert wird nur für RDP-Verbindungen unterstützt. Der Standardwert lautet 1.
- **Connbar** – 0 oder 1. Bei Auswahl des Werts 1 wird oben im Fenster eine kleine Leiste angezeigt. Mit diesem Fenster kann der Benutzer den Bildschirm im Vollbildmodus minimieren. Dieser Wert wird nur für RDP-Verbindungen unterstützt. Der Standardwert lautet 1.
- **FullDrag** – 0 oder 1. Bei Auswahl des Werts 1 werden die Fensterinhalte angezeigt, wenn das Fenster gezogen wird. Dieser Wert wird nur für RDP-Verbindungen unterstützt. Der Standardwert lautet 1.
- **Themes** – 0 oder 1. Bei Auswahl des Werts 1 werden Windows XP-Themen in der Sitzung angezeigt. Dieser Wert wird nur für RDP-Verbindungen unterstützt. Der Standardwert lautet 1.
- **Animation** – 0 oder 1. Bei Auswahl des Werts 1 wird die Menü-Animation in der Sitzung angezeigt. Dieser Wert wird nur für RDP-Verbindungen unterstützt. Der Standardwert lautet 1.
- **Caching** – 0 oder 1. Bei Auswahl des Werts 1 ist die RDP-Bitmap-Cachespeicherung aktiviert. Dieser Wert wird nur für RDP-Verbindungen unterstützt. Der Standardwert lautet 0.
- **AutoReconnect** – 0 oder 1. Bei Auswahl des Werts 1 ist die RDP-Neuverbindung aktiviert. Nicht empfohlen für eine HP SAM Lösung. Dieser Wert wird nur für RDP-Verbindungen unterstützt. Der Standardwert lautet 0.
- **MapDrives** – 0 oder 1. Bei Auswahl des Werts 1 werden lokale Laufwerke für die Remote-Sitzung zugänglich gemacht. Dieser Wert wird nur für RDP-Verbindungen unterstützt. Der Standardwert lautet 0.
- **MapPorts** – 0 oder 1. Bei Auswahl des Werts 1 werden serielle Anschlüsse für die Remote-Sitzung zugänglich gemacht. Dieser Wert wird nur für RDP-Verbindungen unterstützt. Der Standardwert lautet 0.
- **MapPrinters** – 0 oder 1. Ist der Wert 1 angegeben, werden lokale Drucker für die Remote-Sitzung zur Verfügung gestellt. Dieser Wert wird nur bei RDP-Verbindungen unterstützt. Der Standardwert lautet 1 für Windows und wird von den Linux-Client- und Blade-Workstation-Client-Serien nicht unterstützt.
- **MapSmartcards** – 0 oder 1. Bei Auswahl des Werts 1 werden lokale Smart Cards für die Remote-Sitzung zugänglich gemacht. Dieser Wert wird nur für RDP-Verbindungen unterstützt. Der Standardwert lautet 1 beim Windows XPe-Client und 0 beim Linux-Client und der Blade Workstation Client-Reihe.
- **ColorDepth** – Ganzzahlwert, 8, 16, 24 oder 32. Die Farbtiefe für die RDP-Sitzung. Dieser Wert wird nur für RDP-Verbindungen unterstützt. Der Standardwert lautet 24 (Bit), bei Linux kann er jedoch je nach Grafikfunktionalität des Zugriffsgeräts niedriger liegen. 32-Bit-Farbe gilt nur für Windows.
- **FullScreen** – 0 oder 1. Bei Auswahl des Werts 1 wird eine Vollbild-Sitzung erzeugt. Der Standardwert lautet 1.
- **Keys** – Ganzzahlwert, 0, 1 oder 2. Gibt an, wie bestimmte Tastenkombinationen (z. B. Alt + Tab) in einer RDP-Sitzung behandelt werden sollen. Wenn der Wert 0 ausgewählt ist, werden die Tastenkombinationen auf dem lokalen Rechner behandelt. Wenn der Wert 1 ausgewählt ist, werden die Tastenkombinationen auf dem Remote-Rechner behandelt. Wenn der Wert 2

ausgewählt ist, werden die Tasten auf dem Remote-Rechner in einer Vollbild-Sitzung behandelt. Dieser Wert wird nur für RDP-Verbindungen unterstützt. Der Standardwert lautet 2.

- **Height** – Ganzzahlwert. Zusammen mit der Option **Width** wird die Größe des Fensters bestimmt. Der Standardwert lautet 600.
- **Width** – Ganzzahlwert. Zusammen mit der Option **Height** wird die Größe des Fensters bestimmt. Der Standardwert lautet 800.
- **RgsWarningTimeout** – Ganzzahlwert. Der Timeout in Millisekunden, der zum Ermitteln einer Netzwerkstörung und zur Benachrichtigung des Benutzers verwendet wird. Weitere Informationen finden Sie unter `rgreceiver.network.timeout.warning` in der RGS-Dokumentation. Der Standardwert ist der Benutzeroberflächen-Standardwert von 2.000 Millisekunden (2 Sekunden). Die Benutzeroberfläche zeigt diesen Wert in Sekunden an. Dieser Wert wird nur für RGS-Verbindungen unterstützt.
- **RgsErrorTimeout** – Ganzzahlwert. Der Timeout in Millisekunden, der zum Ermitteln und Trennen einer inaktiven Verbindung verwendet wird. Weitere Informationen finden Sie unter `rgreceiver.network.timeout.error` in der RGS-Dokumentation. Der Standardwert ist der Benutzeroberflächen-Standardwert von 30.000 Millisekunden (30 Sekunden). Die Benutzeroberfläche zeigt diesen Wert in Sekunden an. Dieser Wert wird nur für RGS-Verbindungen unterstützt.
- **RgsDialogTimeout** – Ganzzahlwert. Der Timeout in Millisekunden, der für die Anzeige von und das Warten auf Antworten von Eingabedialogen wie dem Autorisierungsdialog oder dem PAM-Authentifizierungsdialog verwendet wird. Weitere Informationen finden Sie unter `rgreceiver.network.timeout.dialog` in der RGS-Dokumentation. Der Standardwert ist der Benutzeroberflächen-Standardwert von 15.000 Millisekunden (15 Sekunden). Die Benutzeroberfläche zeigt diesen Wert in Sekunden an. Dieser Wert wird nur für RGS-Verbindungen unterstützt.
- **ClearType** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 wird die Unterstützung für die Schriftartglättung in einer RDP6-Sitzung aktiviert. Diese Option wird für RDP5, RGS und `rdesktop` ignoriert. Mit dem Wert 0 wird die Unterstützung deaktiviert. Der Standardwert lautet 0.
- **ComposedUI** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts wird die Unterstützung für die Vista Aero-Oberfläche (Desktop-Effekt) aktiviert. Für diese Option ist RDP6 erforderlich, für RDP5 und RGS wird sie ignoriert. Zusätzlich müssen einige Hardware- und Betriebssystemanforderungen erfüllt werden, bevor die Vista Aero-Oberfläche angezeigt werden kann. Mit dem Wert 0 wird die Unterstützung deaktiviert. Der Standardwert lautet 1.
- **Autosize** – Ganzzahl, 0 oder 1. Bei Auswahl des Werts 1 wird die RDP-Sitzung automatisch angepasst, wenn das Fenster, in dem sie ausgeführt wird, verkleinert oder vergrößert wird. Bei Auswahl des Werts 0 ist die maximale Fenstergröße die der Remote-Sitzung. Beim Verkleinern des Fensters werden Bildlaufleisten angezeigt. Dieser Wert wird für RGS und `rdesktop` ignoriert und ist nur in einer Sitzung in einem Fenster gültig. Der Standardwert lautet 0.
- **MapClipboard** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 wird die Zwischenablage für Remote-Sitzungen zugänglich gemacht und bietet begrenzte Funktionen zum Kopieren und Einfügen von Inhalten vom lokalen Rechner in die Remote-Sitzung und umgekehrt. Diese Option wird für RGS-Versionen vor 5.2 und RDP5 ignoriert. Beim Wert 0 wird die Funktion deaktiviert. Der Standardwert lautet 1.

 **HINWEIS:** Die Aktivierung oder Deaktivierung der Zwischenablage in der HP SAM Client-Benutzeroberfläche wirkt sich auf alle Sitzungen aus, die über den betreffenden Client verbunden sind.

Die Einstellung für die Zwischenablage kann über HP SAM Richtlinien erzwungen werden. Wenn die Richtlinien Rollen zugeordnet sind und ein Benutzer mehrere Sitzungen gleichzeitig geöffnet hat, kann das Kopieren und Einfügen in einigen Sitzungen zulässig sein, in anderen dagegen nicht.

- **NetworkAuthentication** – Ganzzahlwert, 0, 1 oder 2. Beim Wert 1 gibt der RDP-Client beim Verbinden mit einer Ressource, die nicht authentifiziert werden kann, eine Warnung aus. Beim Wert 2 verweigert der RDP-Client die Verbindung mit einer nicht authentifizierten Ressource. Beim Wert 0 wird die Verbindung unabhängig vom Authentifizierungsstatus hergestellt. Für diese Einstellung ist RDP6 erforderlich, für RDP5 oder RGS wird sie ignoriert. Der Standardwert lautet 0.
- **MapDrivesList** – Zeichenfolgenwert, nur bei RDP6 oder höher. Dieses Feld ist nur gültig, wenn für **MapDrives** der Wert 1 festgelegt wurde. Mit dieser Einstellung kann gesteuert werden, welche logischen Geräte für die Remote-Sitzung verfügbar gemacht werden. Die Liste entspricht dem Format der RDP-Konfigurationsdatei und sieht folgendermaßen aus:

```
MapDrivesList=c;;d;;e;;DrivesDynamic
```

In diesem Beispiel werden die Laufwerke c:, d: und e: neben den Laufwerken zur Verfügung gestellt, die nach dem Einrichten der Sitzung verbunden werden (DrivesDynamic).

- **Span** – Ganzzahlwert, 0 oder 1. Bei Auswahl des Werts 1 wird festgelegt, dass die Sitzung alle verfügbaren Monitore einbeziehen soll (im Rahmen der von dem verwendeten Protokoll vorgegebenen Beschränkungen). Für diese Einstellung ist RDP6 oder RGS erforderlich, für RDP5 wird sie ignoriert. Der Standardwert für diese Option lautet 0 (Sitzung wird nur auf einem Monitor angezeigt). Zusätzlich gelten die folgenden Einschränkungen für RDP6:
  - Die kombinierte Monitorauflösung kann nicht mehr als 4096 x 2048 Pixel betragen.
  - Alle Monitore müssen die gleiche Auflösung verwenden.
  - Alle Monitore müssen nebeneinander aufgestellt sein.
- **MatchClientDisplays** – Ganzzahlwert, 0 oder 1. Wenn dieser Parameter auf den Wert 1 gesetzt wird, kann RGS die Sender-Anzeigen den Client-Anzeigegeräten zuordnen. RGS-Sitzungen müssen an den physischen Anzeigebegrenzungen auf dem Client-Desktop ausgerichtet werden, damit gültige Bildschirmauflösungen auf dem Sender festgelegt werden können. Verwenden Sie diese Funktion für Clients mit mehreren Anzeigen, die auf Sendern mit mehreren physischen Bildschirmen zum Einsatz kommen. Sender, die für die Verwendung einer einzigen logischen Anzeige konfiguriert sind, bewirken, dass RGS eine einzige Anzeige statt mehrerer Anzeigen festlegt. RGS 5.1.3 oder höher ist erforderlich. Der Standardwert lautet 0.

## Globale und lokale Client-Konfigurationsdateien

Diese Funktion ermöglicht Administratoren das 'Sperrern' bestimmter Optionen, während andere Optionen weiterhin von Benutzern geändert werden können.

Es gibt drei Dateiebenen:

- Global: hprdc\_admin.sam
- Lokal: hprdc\_accessdevice.sam
- Persönlich: hprdc.sam


Prioritätsreihenfolge:

- Die persönliche Datei wird zuerst gelesen.
  - XPe: Beliebige Position im Dateisystem (Doppelklicken auf „hprdc.sam“)
  - XPe-Suchpositionen in dieser Reihenfolge – sobald eine persönliche Datei gefunden wurde, wird die Suche gestoppt:
    - %AppData%; Standardpfad unter XP: C:\Dokumente und Einstellungen\<<Benutzername>\Anwendungsdaten\hprdc.sam. Standardpfad unter Vista oder Windows 7: C:\Benutzer\<<Benutzername>\AppData\Roaming\hprdc.sam
    - Installationsverzeichnis; Standardpfad: C:\Programme\Hewlett-Packard\HP Session Allocation Client\hprdc.sam
    - \$SystemRoot%; Standardpfad: C:\windows\
  - Speicherort der Betriebssystemdatei des Workstation Clients:
    - /root/user/hprdc.sam
  - Linux-Client:
    - /root/hprdc.sam für den Root-Benutzer
    - /home/<Benutzername>/hprdc.sam für andere Benutzer
- Parameter in der lokalen Datei setzen die persönlichen Parameter außer Kraft.
  - Speicherort unter XP ist das Installationsverzeichnis. Standardpfad: C:\Programme\Hewlett-Packard\HP Session Allocation Client\hprdc\_accessdevice.sam
  - Speicherort der Betriebssystemdatei des Workstation Clients: /opt/hpsam/hprdc\_accessdevice.sam (/root/writable/opt/hpsam/hprdc\_accessdevice.sam)
  - Linux-Client:
    - /opt/hpsam/hprdc\_accessdevice.sam
- Parameter in der globalen Datei setzen die persönlichen und lokalen Parameter außer Kraft.
  - Speicherort unter XP ist das Installationsverzeichnis. Standardpfad: C:\Programme\Hewlett-Packard\HP Session Allocation Client\hprdc\_admin.sam
  - Speicherort der Betriebssystemdatei des Workstation Clients: /opt/hpsam/hprdc\_admin.sam (/root/writable/opt/hpsam/hprdc\_admin.sam)
  - Linux-Client:
    - /opt/hpsam/hprdc\_admin.sam

## Banner für rechtliche Hinweise

Vor der Anmeldung kann so ein Haftungsausschluss angezeigt werden. Geben Sie der Datei den Namen Haftungsausschluss.<Dateityp>, und kopieren Sie die Datei in das entsprechende Verzeichnis (erstellen Sie den Ordner ggf. selbst). Dies sind die Standardpfade:

- **Client-Zugriffsggerät:** Nach der Installation des Banners für rechtliche Hinweise auf einem Zugriffsgerät wird das Banner nur auf diesem Zugriffsgerät angezeigt. Geben Sie der Datei den Namen Haftungsausschluss.<Dateityp>, und kopieren Sie die Datei in das folgende Verzeichnis auf dem Zugriffsgerät (erstellen Sie den Ordner ggf. selbst):
  - **Windows:** C:\Programme\Hewlett-Packard\HP Session Allocation Client\\${LANG}\Haftungsausschluss.<Dateityp>
  - **Betriebssystem des Workstation Clients:** /root/writable/opt/hpsam/site/\${LANG}/Haftungsausschluss.<Dateityp>
  - **Linux:** /opt/hpsam/site/\${LANG}/Haftungsausschluss.<Dateityp>
- **Web-Client:** Durch die Installation eines Rechtshinweis-Banners auf dem HP SAM-Webserver wird das Banner für alle Benutzer angezeigt, die sich über den Web-Client verbinden. Benennen Sie die Datei als disclaimer.<file type> und kopieren Sie sie in das folgende Verzeichnis (erstellen Sie gegebenenfalls den Ordner) **auf dem HP SAM-Server:**
  - **Webclient:** C:\Programme\hewlett-packard\SAM\webclient\images\\${LANG}\Haftungsausschluss.<Dateityp>

 **HINWEIS:** **Windows:** Ersetzen Sie \${LANG} durch den entsprechenden Ordernamen für die gewünschte Sprache: EN für Englisch, JP für Japanisch, FR für Französisch, DE für Deutsch, KO für Koreanisch oder CN für vereinfachtes Chinesisch).


**Linux-Client und Workstation Client-Betriebssystem:** Ersetzen Sie \${LANG} durch einen Ordernamen, der genau dem (bei der Installation oder später) ausgewählten Tastatur-/Gebietsschema entspricht. Für US-Englisch lautet das korrekte Gebietsschema en\_US.UTF-8. Die Ordernamen für andere Tastatur-/Gebietsschemas finden Sie in der nachstehenden Tabelle. Bei der Workstation Client-Reihe wird dies durch die Tabelle /etc/kbd\_lang.table gesteuert und im Dialogfeld „Info“ angezeigt, das Sie durch Klicken mit der rechten Maustaste auf dem Desktop aufrufen können.

fr_BE.UTF-8	Französisch (Belgien) – Français (Belgique)
en_CA.UTF-8	Französisch (Kanada) – Français Canadien
zh_CN.UTF-8	Chinesisch (vereinfacht)
zh_TW.UTF-8	Chinesisch (traditionell)
da_DK.UTF-8	Dänisch – Dansk
nl_NL.UTF-8	Niederländisch – Nederlands
en_US.UTF-8	Englisch, international
en_GB.UTF-8	Englisch (Großbritannien)
en_GB.UTF-8	Englisch (Großbritannien, erweitert)
en_US.UTF-8	Englisch (USA)

fi_FI.UTF-8	Finnisch – Suomi
fr_FR.UTF-8	Französisch – Français
de_DE.UTF-8	Deutsch
it_IT.UTF-8	Italienisch – Italiano
ja_JP.UTF-8	Japanisch
ko_KR.UTF-8	Koreanisch
nb_NO.UTF-8	Norwegisch – Norsk
pt_PT.UTF-8	Portugiesisch – Português
pt_BR.UTF-8	Portugiesisch (Brasilien) – Português do Brasil
es_ES.UTF-8	Spanisch – Español
es_MX.UTF-8	Spanisch (Lateinamerika) – América Latina
sv_SE.UTF-8	Schwedisch – Svenska
de_CH.UTF-8	Swiss-German - Deutsch (Schweiz)
tr_TR.UTF-8	Türkisch – Türkçe

Die folgenden Dateitypen werden unterstützt:

- JPG
- GIF
- BMP

 **HINWEIS:** Diese Funktion wird standardmäßig aktiviert, wenn die Datei mit dem Haftungsausschluss an der richtigen Position gefunden wird.

## Bereitstellen des HP SAM Registrierungsdienstes auf allen HP SAM Rechnerressourcen

Bei einem Einsatz auf einer großen Zahl von Rechnern empfiehlt HP, ein Softwaretool wie HP Rapid Deployment Pack zu verwenden.

1. Installieren Sie den Dienst auf allen Rechnerressourcen.
2. Erstellen Sie die Konfigurationsdatei für den HP SAM Registrierungsdienst (hpevent.cfg) auf einem einzelnen Blade, und speichern Sie diese Datei als später zu verwendende Vorlage.
3. Starten Sie den Dienst auf einer einzelnen Rechnerressource bzw. starten Sie ihn dort neu, und überprüfen Sie, ob sich die Rechnerressource automatisch beim HP SAM-Webserver registriert.
4. Legen Sie die Konfigurationsdatei des HP SAM Registrierungsdienstes (hpevent.cfg) auf allen Rechnerressourcen ab, und starten Sie den Dienst auf diesen Einheiten.




# Bereitstellen der HP SAM Client-Software auf allen HP SAM Zugriffsgeräten

Für die Bereitstellung des Internet-Explorer-basierten HP SAM-Clients müssen Sie Ihrer Benutzer anweisen, die HP SAM-Server-Website(s) aufzurufen, die Sie eingerichtet haben.

Wenn das Zugriffsgerät zum ersten Mal auf den HP SAM Server zugreift, muss es zwei ActiveX-Steuererelemente installieren (HP SAM Web Client Utility Class und Microsoft RDP Client Control). Der Installationsort für diese Steuererelemente ist der Ordner **%SystemRoot%\Downloaded Program Files\**.

---


 **HINWEIS:** Verwenden Sie das Installationsprogramm für die Webclient-Steuererelemente aus dem HP SAM SoftPak, damit Sie keine Steuererelemente automatisch über den Browser herunterladen und installieren müssen. Dies ist nützlich, wenn das Zugriffsgerät so gesperrt ist, dass der Benutzer keine ActiveX-Steuererelemente automatisch über den Browser installieren darf.

---

Der Windows-basierte HP SAM Client kann für die Zugriffsgeräte auf unterschiedliche Weise bereitgestellt werden. Es folgen zwei Beispiele.

- Verwenden Sie Softwarebereitstellungstools wie HP Rapid Deployment Pack.
  - a. Installieren Sie den HP SAM Client auf den Zugriffsgeräten.
  - b. Aktualisieren Sie die Datei „hprdc.sam“ des Clients, um eine Verbindung zum HP SAM Server herzustellen, und nehmen Sie die gewünschten Einstellungen vor (siehe Schritte zur Anpassung des jeweiligen HP SAM Clienttyps).
- Stellen Sie die Installationsdatei für den Windows-basierten HP SAM-Client auf einer Website oder auf einem Dateifreigabeportal bereit. Wenn Sie eine hprdc.sam-Datei für Ihre Umgebung erstellt haben, sollten Sie diese Datei ebenfalls dort bereitstellen. Weisen Sie die Benutzer anschließend zu folgendem Vorgehen an:
  - a. die Client-Software herunterzuladen und zu installieren und
  - b. die Konfigurationsdatei (hprdc.sam) auf dem Desktop abzulegen und
  - c. die HP SAM Datei durch Doppelklicken zu starten.

---

 **HINWEIS:** Wenn eine Firewall installiert ist, müssen Sie diese durch entsprechende Änderungen für den HP SAM Client durchgängig machen. Nehmen Sie diese Änderungen nicht auf der Portebene, sondern auf der Anwendungsebene vor.

---

---

# 4 Verwaltung

## Anmelden

Geben Sie in der Adresszeile in Internet Explorer den Namen des HP SAM-Webservers ein, gefolgt von dem Ausdruck „/manage“ am Ende der URL (Beispiel: `http://HPSAMservername/manage`). Verwenden Sie „https:“, sofern die HP SAM-Verwaltungskonsole so konfiguriert wurde, dass SSL erforderlich ist.

Wenn SSL konfiguriert ist und eine Sicherheitsmeldung zum Zertifikat angezeigt wird, klicken Sie auf **Ja**.

Sobald die Anmeldeseite angezeigt wird, geben Sie Ihren Benutzernamen und Ihr Passwort ein und klicken Sie auf die Schaltfläche **Sign In (Anmelden)**. Sie haben zwei Möglichkeiten für die Eingabe Ihres Benutzernamens. Sie können ihn als `domain\benutzername` eingeben oder Sie können Ihren User Principal Name (UPN) eingeben (`ihrname@ihrefirma.com`).

## Allgemeine Navigation und Aufbau der Benutzeroberfläche

Die HP SAM-Verwaltungskonsole enthält Registerkarten und Hyperlinks für die Navigation. Auf einigen Registerkarten gibt es zudem einen Bereich mit einer Filteroption. Der Hauptarbeitsbereich bzw. die Ergebnisliste befindet sich unten auf der Seite.

### Anzeigen von mehr (oder weniger) Elementen pro Seite

Das System zeigt standardmäßig nur eine bestimmte Anzahl von Elementen pro Seite an. Sie können diese Anzahl ändern, indem Sie im Feld **Anzeigen** einen neuen Wert (10, 25, 50, 100, 250 oder 500) auswählen. Die Seite wird sofort unter Berücksichtigung der neuen Einstellung aktualisiert.

### Verschieben von Spalten

Das System zeigt das Ergebnisdatenraster auf eine bestimmte Weise an. Sie können Spalten verschieben, indem Sie die Spaltenüberschriften an einen geeigneten Ort im Gitter ziehen.

### Sortieren der Ergebnisliste

Ergebnisraster können nach jeder der angezeigten Spalten sortiert werden. Klicken Sie auf den entsprechenden Spaltenkopf, um nach der betreffenden Spalte zu sortieren. Klicken Sie auf den gleichen Spaltenkopf, um zwischen ab- und aufsteigender Sortierung umzuschalten.

## Auswählen von mehr als einem Element

Die obere linke Seite des Ergebnisrasters enthält ein Kontrollkästchen.

- Wenn Sie alle Elemente auf allen Seiten und nicht nur auf der angezeigten Seite auswählen möchten, aktivieren Sie dieses Kontrollkästchen.
- Wenn Sie alle Felder auf allen Seiten und nicht nur auf der angezeigten Seite deaktivieren möchten, deaktivieren Sie dieses Kontrollkästchen.

## Verwalten der HP SAM Administratorzugangsliste


Der Domänenadministrator, die Domänenbenutzer in der Administratorgruppe auf dem Domänencontroller und die Domänenbenutzer in der lokalen Administratorgruppe des HP SAM Servers sind automatisch Mitglieder der HP SAM Administratorgruppe. Informationen zum Hinzufügen eines weiteren Benutzers zur HP SAM Administratorgruppe finden Sie unter [„So weisen Sie Attribute zu“ auf Seite 66](#).

## Hinzufügen einzelner Benutzer zur Gruppe der HP SAM Administratoren

Wenn Sie nur wenige Benutzer hinzufügen, fügen Sie die Namen der Gruppe der HP SAM Administratoren direkt hinzu.

1. Rufen Sie die Seite **Neue Benutzer hinzufügen** auf.
2. Wählen Sie für **Suchen nach** die Einstellung **Benutzer** aus.
3. Wenn Sie einen Filter auf eine bestimmte Domäne einstellen möchten, wählen Sie in der Liste **Domänenname** die Domäne aus, oder wählen Sie **Globaler Katalog** für alle Domänen im selben Active Directory-Bereich, in dem sich auch der HP SAM Server befindet, aus.
4. Geben Sie einen oder mehrere der in den folgenden Beispielen dargestellten Parameter ein:
  - a. **Nachname**: Bei der Eingabe von Zeichen wird eine Suche nach Nachnamen ausgeführt.
  - b. **Vorname**: Nach einem Komma eingegebene Zeichen leiten eine Suche nach Vornamen ein. Durch die Eingabe eines Leerzeichens können Sie gleichzeitig nach Vornamen und Nachnamen suchen. Zeichen vor dem Leerzeichen leiten eine Suche nach Vornamen ein. Zeichen nach dem Leerzeichen leiten eine Suche nach Nachnamen ein.
  - c. **UPN-Name**: Die Eingabe eines Namens mit einem at-Zeichen (@) startet eine Suche nach UPN-Name (z. B. peter.meier@).


---

 **HINWEIS:** Die Ergebnisse werden bei der Eingabe angezeigt.

---

5. Klicken Sie auf **Hinzufügen**, um der Liste hervorgehobene Benutzer hinzuzufügen.
6. Wählen Sie in der Liste die Benutzer aus, die HP SAM hinzugefügt werden sollen.
7. Klicken Sie auf **Speichern**.

---

 **HINWEIS:** Nach dem Klicken auf **Speichern** können Sie Benutzerattribute, z. B. Administratorgruppen, festlegen. Sie haben auch die Möglichkeit, dedizierte Ressourcen automatisch zuweisen zu lassen. Wenn ein Benutzer bereits in HP SAM aufgenommen wurde, werden seine Attribute an die hier vorgenommenen Einstellungen angepasst.


---

## Hinzufügen von Sicherheitsgruppen oder organisatorischen Einheiten zur HP SAM Administratorgruppe


So fügen Sie viele Benutzer hinzu:

1. Nutzen Sie Active Directory-Dienste durch Hinzufügen der Namen im Active Directory unter einer Sicherheitsgruppe oder einer organisatorischen Einheit.
2. Rufen Sie die Seite **Neue Benutzer hinzufügen** auf.
3. Fügen Sie die Sicherheitsgruppe oder organisatorische Einheit direkt zur HP SAM Administratorgruppe hinzu.
  - a. Wählen Sie unter **Suchen nach** die Optionen **Organisatorische Einheiten** oder **Sicherheitsgruppen** aus.
  - b. Wenn Sie einen Filter auf eine bestimmte Domäne einstellen möchten, wählen Sie in der Liste **Domänenname** die Domäne aus, oder wählen Sie **Globaler Katalog** für alle Domänen im selben Active Directory-Bereich aus, in dem sich auch der HP SAM Server befindet.
  - c. Durch die Eingabe von Zeichen in das Suchfeld können Sie nach Gruppen suchen. Die Ergebnisse werden bei der Eingabe angezeigt. Sie können eine Gruppe hervorheben und über die Schaltfläche **Anzeigen** die Benutzer anzeigen, die direkte Mitglieder der Gruppe sind.
  - d. Klicken Sie auf **Hinzufügen**, um der Liste hervorgehobene Gruppen hinzuzufügen.
  - e. Wählen Sie in der Liste die Gruppen aus, die HP SAM hinzugefügt werden sollen.
  - f. Klicken Sie auf **Speichern**.

---

 **HINWEIS:** Nach dem Klicken auf **Speichern** können Sie SG- oder OU-Attribute, z. B. Administratorgruppen, festlegen. Wenn eine SG oder OU bereits in HP SAM aufgenommen wurde, werden ihre Attribute an die hier vorgenommenen Einstellungen angepasst.

---

 **HINWEIS:** Wenn Sie später Änderungen vornehmen möchten, gehen Sie zu Active Directory, und fügen Sie diesen Gruppen Benutzer hinzu, oder entfernen Sie Benutzer aus diesen Gruppen.

Sie müssen die Gruppen nicht erneut in HP SAM hinzufügen.

---

## Entfernen von Benutzern oder Gruppen aus der HP SAM Administratorgruppe

Sie können Benutzer aus der HP SAM Administratorliste entfernen. Rufen Sie dazu **Benutzer und Rollen > Benutzer verwalten** auf.

1. Wählen Sie im Bereich **Filteroptionen** den Eintrag [Administrator] in der Liste **Rolle** aus. Die Namen von Administratorgruppen stehen in eckigen Klammern, z. B. [Administratorgruppe].
2. Klicken Sie auf **Suchen**.

3. Aktivieren Sie das Kontrollkästchen neben den gewünschten Namen.
4. Wenn Sie Benutzer oder Gruppen unwiderruflich aus dem System löschen möchten, wählen Sie in der Liste **Operation** die Option **Löschen** aus, und klicken Sie auf **Los**.
5. Wenn Sie Benutzer oder Gruppen aus der HP SAM Administratorgruppe entfernen möchten, ohne sie aus dem System zu löschen, führen Sie die folgenden Schritte aus:
  - a. Wählen Sie in der Liste **Operation** die Option **Attribute zuweisen** aus, und klicken Sie anschließend auf die Schaltfläche **Los**.
  - b. Wählen Sie neben der Administratorgruppe **<Leer>** aus (oder löschen Sie den Inhalt).
  - c. Klicken Sie zum Speichern der Änderungen auf **Speichern**.

# Registerkarten in der HP SAM-Verwaltungskonsole

## Registerkarte „Home“

Wenn Sie sich bei HP SAM anmelden, wird als Startseite standardmäßig die Seite „Home“ angezeigt. HP SAM zeigt als Überblick für den Administrator eine Momentaufnahme über den aktuellen Status der Ressourcen an, gruppiert nach Rollen.

## Registerkarte „Benutzer und Rollen“


Auf der Registerkarte **Benutzer und Rollen** können Rollen und die Benutzerzugriffsliste verwaltet werden.

### Verwalten von Ressourcenrollen

Es werden alle Rollen angezeigt, die von Rechnerressourcen bei deren Selbstregistrierung oder über die Schaltfläche **Erstellen** erstellt wurden.

- Spalte **Rolle**: Eine Liste aller Rollen.


---

 **HINWEIS:** Rollennamen sind auf 128 Zeichen begrenzt. Wenn Sie für einen Rollennamen in einer Ressourcenkonfigurationsdatei mehr als 128 Zeichen eingeben, funktioniert der Name korrekt, wird jedoch auf 128 Zeichen gekürzt.

---

- Spalte **Systemgruppe**: Zeigt die zu den einzelnen Rollen gehörenden Systemgruppen an.
- Spalte **Beschreibung**: Sie können die Beschreibung jeder Rolle ändern, wenn aus dem Namen selbst die Rolle nicht eindeutig hervorgeht oder wenn Sie die Rolle von anderen Rollen unterscheiden möchten. Der Rollename und die Beschreibung werden dem Benutzer auf dem Zugriffsgerät während des Herstellens der Verbindung angezeigt, falls der Benutzer Zugriffsrechte für mehrere Rollen besitzt.
- Spalte **Richtlinie**: Standardmäßig werden die HP SAM Clienteneinstellungen der globalen Richtlinie zugewiesen. Alle erzwungenen Verbindungseinstellungen der globalen Richtlinie (sofern vorhanden) werden auf alle Benutzer angewendet.

---

 **HINWEIS:** Wenn Sie die globale Richtlinie durch eine andere Richtlinie außer Kraft setzen möchten, müssen Sie zuerst die Richtlinie auf der Registerkarte **Richtlinien** erstellen und dann hier die Rolle zur Verwendung der entsprechenden Richtlinie erneut zuweisen.

---

- Spalte **Aktiviert**:
  - Ist diese Spalte aktiviert, kann die Rolle zugeordnet werden.
  - Ist sie nicht aktiviert, steht im Geltungsbereich dieser Rolle kein Blade für Benutzerverbindungen über HP SAM zur Verfügung.
  - Sie können die Einstellung ändern. Klicken Sie dazu auf den Link für die Rolle, wählen Sie im Dialog das Kontrollkästchen aus, oder heben Sie dessen Auswahl auf, und klicken Sie dann auf **Speichern**.
  - Bei aufgehobener Auswahl des Kontrollkästchens **Aktiviert**:
    - Neue Benutzerverbindungsanfragen für diese Rolle werden vom HP SAM-Webserver verweigert.

- Aktuell aktive Verbindungen bleiben bestehen.

- Nicht verbundenen Benutzern wird nicht gestattet, für ihre getrennten Sitzungen erneut eine Verbindung herzustellen.

- Spalte **Öffentlich**:
  - Ist die Spalte aktiviert, steht die Rolle allen Benutzern in Active Directory zur Verfügung.
  - Ist die Spalte nicht aktiviert, steht die Rolle nur den Benutzern in der Zugriffsliste der betreffenden Rolle zur Verfügung.
  - Sie können die Einstellung ändern. Klicken Sie dazu auf den Link für die Rolle, wählen Sie im Dialog das Kontrollkästchen aus, oder heben Sie dessen Auswahl auf, und klicken Sie dann auf **Speichern**.
- Spalte **Zugriffsbeschränkung**: In dieser Spalte wird eine Zusammenfassung der Ressourcenreservierungen angezeigt, die der Rolle hinzugefügt wurden.
- Schaltfläche **Erstellen**: Über diese Schaltfläche können Sie eine neue Rolle erstellen, die Sie Ressourcen zuweisen können.
- Schaltfläche **Löschen**: Über diese Schaltfläche können Sie ausgewählte Rollen löschen.

## Verwalten von Systemgruppen


Der HP SAM Administrator oder Domänenadministrator verfügt über umfassende Berechtigungen für alle Systemgruppen auf dem HP SAM Server. Mithilfe von Systemgruppen können HP SAM Administratoren, die über volle Rechte verfügen, Objekte (Ressourcen, Benutzer usw.) einschränken oder verbergen, die von anderen Administratoren angezeigt und verwaltet werden dürfen:

- Clients
- Ressourcen
- Benutzer, organisatorische Einheiten (OUs), Sicherheitsgruppen (SGs)
- Rollen
- Monitorlayout-IDs
- Richtlinien
- Protokolle
- Berichte

Der HP SAM Administrator oder Domänenadministrator erstellt auch die administrativen Gruppen.

- Durch Zuweisung von Administratorgruppen können eine oder mehrere Systemgruppen gesteuert werden.
- Die in den einzelnen Administratorgruppen enthaltenen Benutzer können alle Assets in den erkannten Systemgruppen steuern.
- Administratoren können nur die Assets sehen, die mit den von ihnen gesteuerten Systemgruppen verknüpft sind.

---

 **HINWEIS:** Der HP SAM Administrator oder Domänenadministrator verfügt über umfassende Berechtigungen für alle Systemgruppen auf dem HP SAM Server.


---

- Spalte **Systemgruppe**: Eine Liste aller Systemgruppen.
- Spalte **Beschreibung**: Sie können die Beschreibung für jede Systemgruppe ändern, wenn der Name selbst keine eindeutige Erklärung bietet, oder wenn Sie die Gruppe von anderen Systemgruppen stärker abgrenzen möchten.
- Schaltfläche **Erstellen**: Über diese Schaltfläche können Sie eine neue Systemgruppe erstellen.

Sie können Systemgruppen auch löschen. Wählen Sie dazu die betreffende Gruppe aus, und klicken Sie auf **Löschen**.

## Administrative Berechtigungen verwalten

---

 **HINWEIS:** Für folgende Aktionen benötigen Sie vollständige HP SAM Administratorrechte:

- Erstellen, Ändern oder Löschen von Administratorgruppen
- Zuweisen von Benutzern zu Administratorgruppen


Die folgenden Benutzer verfügen über diese Rechte:

- HP SAM Serveradministratoren
- Domänenadministratoren
- Domänenbenutzer, die zur Administratorgruppe „Administrator“ in HP SAM gehören

---

Passen Sie in diesem Fenster die Rechte für verschiedene Stufen von Administratorzugriffsrechten an. Nachdem Sie die Administratorstufen erstellt haben, müssen Sie die Benutzer der erstellten Administratorgruppe hinzufügen, um ihnen Benutzerzugriff zu erteilen.

---

 **HINWEIS:** Wenn Sie einen Benutzer mehreren Administratorgruppen zuweisen, die über verschiedene Berechtigungen verfügen, erhält der Benutzer alle Rechte der zugewiesenen Administratorgruppen.

---

So erstellen Sie eine neue Gruppe mit administrativen Rechten:

1. Klicken Sie auf **Erstellen**.
2. Geben Sie im Feld **Gruppenname** einen Namen für die Administratorgruppe ein.
3. Geben Sie im Feld **Beschreibung** eine Beschreibung für die Gruppe ein.
4. Wählen Sie in den Feldern unter **Systemgruppenzuweisung** die Systemgruppe(n) aus, die mit der neuen Administratorgruppe verknüpft werden soll(en).
5. Wählen Sie in der Liste **Kategorie** die Kategorie aus, für die Sie die spezifischen Berechtigungsebenen angeben möchten.
6. Wählen Sie im Bereich **Berechtigungen** die Berechtigungen aus, die für diese Kategorie bei dieser speziellen Administratorgruppe zugelassen sein sollen.
7. Wiederholen Sie die Schritte 5 und 6 für jede Kategorie.
8. Klicken Sie auf **Speichern**.



So nehmen Sie Änderungen an einer Administratorgruppe vor:

1. Wählen Sie die Gruppe, die Sie ändern möchten, durch Klicken auf den Gruppennamen-Hyperlink aus.
2. Nehmen Sie die erforderlichen Änderungen vor.
3. Um Werte der verschiedenen Kategorien zu ändern, wählen Sie eine Kategorie aus der Liste **Kategorie** aus und nehmen im Bereich **Berechtigungen** die gewünschten Berechtigungsänderungen vor. Wiederholen Sie diesen Vorgang für jede Kategorie, in der Sie Änderungen vornehmen möchten.
4. Klicken Sie auf **Speichern**.

So löschen Sie eine Administratorgruppe:

1. Wählen Sie die Gruppe oder Gruppen aus, die Sie löschen möchten. Sie können mit diesem Verfahren mehr als eine Gruppe löschen.
2. Klicken Sie auf **Löschen**, und bestätigen Sie mit **OK**.

## Benutzer verwalten

Standardmäßig werden in den Suchergebnissen alle Benutzer, Sicherheitsgruppen und organisatorischen Einheiten aufgeführt.

- **Suchen nach: Organisatorischen Einheiten, Sicherheitsgruppen, Benutzer** – Wählen Sie aus, welche Gruppen durchsucht werden sollen.
- **Filteroptionen:** Mithilfe der Filteroptionen können Sie die Anzahl der in der Liste angezeigten Benutzer verringern. Die Filteroption basiert auf „UND“-Kombinationen. Je mehr Felder Sie angeben, desto stärker wird das Suchergebnis eingegrenzt.
  - **Name** – Geben Sie den Namen ein, nach dem gesucht werden soll.
  - **Rolle** – Wählen Sie die Rolle aus, nach der gesucht werden soll. Namen in eckigen Klammern([ ]) sind Administratorgruppen, z. B. [Administrator]. Namen ohne Klammern sind Ressourcenrollen.
  - **Systemgruppe** – Zeigen Sie die Benutzer oder Gruppen an, die zu einer bestimmten Systemgruppe gehören.
  - **Vorname** – Geben Sie einen Vornamen ein, nach dem gesucht werden soll.
  - **Nachname** – Geben Sie einen Nachnamen ein, nach dem gesucht werden soll.
  - **Domänenname** – Geben Sie eine Domäne ein, nach der gesucht werden soll.

## Operation

So führen Sie eine der folgenden Aktionen aus:


1. Wählen Sie die entsprechenden Benutzer aus.
2. Wählen Sie die auszuführende Aktion aus der Liste **Operation** aus.
3. Klicken Sie auf die Schaltfläche **Los**.

## So weisen Sie Attribute zu

Auf dieser Seite können Sie die einem Benutzer zugewiesenen Rollen und Systemgruppen ändern, eine Richtlinie zuweisen und einem Benutzer eine Administratorgruppe zuweisen.

So weisen Sie einem Benutzer Attribute zu:

1. Geben Sie die entsprechenden Filteroptionen ein (filtern Sie beispielsweise die Rolle aus der Liste aus).
2. Klicken Sie auf **Suchen**.
3. Wählen Sie das Kontrollkästchen neben dem/den gewünschten Namen aus.
4. Wählen Sie in der Liste **Operation** den Eintrag **Attribute zuweisen** aus, und klicken Sie dann auf **Los**, um das Fenster „Benutzer zu Richtlinie/Rolle zuweisen“ zu öffnen.
5. Wenn Sie einem Benutzer eine Richtlinie zuweisen möchten, wählen Sie eine Richtlinie aus der Liste **Richtlinie** aus.
6. Wenn Sie den Benutzer einer Administratorgruppe zuweisen möchten, wählen Sie eine Gruppe aus der Liste **Administratorgruppe** aus.


 **HINWEIS:** Administratorgruppen sind nur für Sicherheitsgruppen und Benutzerkonten verfügbar.

7. Doppelklicken Sie auf die Systemgruppen, oder verwenden Sie die Pfeile zwischen den Feldern **Verfügbar** und **Ausgewählt**, um die Systemgruppen zu verschieben. Verschieben Sie alle Systemgruppen, die Sie dem ausgewählten Benutzer zuweisen möchten, in das Feld **Ausgewählt**.
8. Doppelklicken Sie auf die Rollen, oder benutzen Sie die Pfeile zwischen den Feldern **Verfügbar** und **Ausgewählt**, um die Rollen zu verschieben. Fügen Sie alle Rollen, die Sie dem ausgewählten Benutzer zuweisen möchten, in das Feld **Ausgewählt** ein.
9. Klicken Sie zum Speichern der Änderungen auf **Speichern**.

## So weisen Sie Ressourcen zu

Über diese Option können Sie eine bestimmte Ressource (z. B. einen Blade-PC) einem Benutzer zuweisen. Sie können auch einer dedizierten Ressource eine Reserveressource und der Ressource einen Anzeigenamen zuweisen. Für die Zuweisung von Ressourcen können Sie eine der folgenden drei Methoden wählen:

- Wählen Sie einen einzelnen Benutzer aus, und weisen Sie ihm manuell Ressourcen zu.
- Wählen Sie einen oder mehrere Benutzer aus, und lassen Sie deren Attribute und Ressourcen auf der Grundlage eines einzigen Vorlagenbenutzers automatisch zuweisen.
- Wählen Sie einen oder mehrere Benutzer und eine Rolle aus, und lassen Sie jedem Benutzer aus der Rolle automatisch Blades zuweisen.

 **HINWEIS:** Einem Vorlagenbenutzer muss ein statisch zugewiesenes Blade in einer Rolle zugeordnet sein, und die Rolle muss genügend verfügbare Ressourcen für die Benutzer während der automatischen Zuweisung statischer Ressourcen enthalten.

Wenn sich ein Blade-PC in einer dynamischen Rolle befindet und als dedizierte Ressource erneut einem Benutzer zugewiesen wird, kann dieser Blade nicht mehr einem anderen Benutzer in dynamischer Rolle zugewiesen werden, auch wenn der aktuelle Status **Verfügbar** lautet. Mit Ausnahme des Vorlagenbenutzers empfiehlt es sich, dedizierte Ressourcen nicht als dynamische Rolle zuzuweisen, damit die **verfügbaren** und **verwendeten** Ressourcen korrekt verfolgt werden können.

## So weisen Sie Ressourcen manuell zu

1. Klicken Sie auf **Benutzer verwalten**.
2. Suchen Sie den Benutzer in der HP SAM Datenbank.
3. Aktivieren Sie das Kontrollkästchen neben dem entsprechenden Namen.

 **HINWEIS:** Beim manuellen Zuweisen von Ressourcen dürfen Sie nur einen Namen auswählen.

4. Wählen Sie im Feld **Operationen** die Operation **Ressourcen zuweisen** aus, und klicken Sie dann auf die Schaltfläche **Los**, um das Fenster **Ressource Benutzer(n) zuweisen** zu öffnen.
5. Wählen Sie **Ressourcen manuell zuweisen** aus, und klicken Sie auf **Weiter**.
6. Wenn Sie dem Benutzer eine spezielle Ressource zuweisen möchten:
  - a. Klicken Sie auf **Hinzufügen**.
  - b. Geben Sie die IP-Adresse oder den Hostnamen der Ressource ein.
  - c. Klicken Sie auf **Suchen**, um nach zuweisbaren Ressourcen zu suchen.
  - d. Wählen Sie eine Ressource aus der Liste aus.
  - e. Klicken Sie auf **Speichern**, um die Ressourcenzuweisung zu ändern.
  - f. Wiederholen Sie die Schritte a bis e für jede weitere Ressource, die Sie dem Benutzer zuweisen möchten.
7. Wenn Sie den Anzeigenamen der Ressource ändern möchten, klicken Sie auf den Link in der Spalte **Anzeigename**, und geben Sie dann im Fenster „Anzeigename aktualisieren“ einen neuen Anzeigenamen für die Ressource ein.

Standardmäßig entspricht der Anzeigename dem Hostnamen der Ressource.
8. Wenn Sie eine Sicherung für die dedizierte Ressource zuweisen möchten, klicken Sie in der Spalte **Sicherung** entweder auf **Rolle** oder **Ressource** für den jeweiligen Benutzer.

So wählen Sie eine Rolle aus:

  - ▲ Wählen Sie eine Rolle aus, die Sie dem Benutzer als Sicherung zuweisen möchten, und klicken Sie dann auf **Speichern**.


So wählen Sie eine Ressource aus:

- a. Geben Sie die IP-Adresse oder den Hostnamen der Sicherungsressource ein, und klicken Sie dann auf **Suchen**.
  - b. Wählen Sie die Ressource aus, die als Sicherung dienen soll, und klicken Sie auf **Speichern**.
9. Klicken Sie zum Löschen des gesamten Inhalts dieser Zeile (dedizierte Ressourcen, Sicherungsrollen und Sicherungsressourcen) in der Spalte **Operation** auf **Entfernen**.
10. So entfernen Sie nur die Sicherungsressource oder -rolle:
- a. Klicken Sie in der Spalte **Sicherung** auf die Sicherungsrolle oder -ressource.
  - b. Wenn Sie eine Rolle entfernen, klicken Sie auf die Schaltfläche **Rolle**, und deaktivieren Sie das Kontrollkästchen der Rolle, die Sie entfernen möchten.
  - c. Klicken Sie auf **Speichern**.
  - d. Wenn Sie eine Ressource entfernen, klicken Sie auf die Schaltfläche **Ressource**, anschließend auf **Suchen**, und deaktivieren Sie das Kontrollkästchen der Ressource, die Sie entfernen möchten.
  - e. Klicken Sie auf **Speichern**.
11. Klicken Sie auf **Schließen**.

### So lassen sich Ressourcen automatisch über Vorlagenbenutzer zuweisen

1. Klicken Sie auf **Benutzer verwalten**.
2. Suchen Sie nach Benutzern.
3. Aktivieren Sie die Kontrollkästchen neben den entsprechenden Namen.


---

 **HINWEIS:** Es können mehrere Benutzer ausgewählt werden.

---

4. Wählen Sie aus der Liste **Operation** den Eintrag **Ressourcen zuweisen** aus, und klicken Sie auf **Los**.
5. Wählen Sie **Ressourcen über Vorlagenbenutzer zuweisen** aus.
6. Wählen Sie den Vorlagenbenutzer aus der Liste aus.
7. Klicken Sie auf **Weiter**.

---

 **HINWEIS:** Wenn Sie versuchen, Ressourcen einem Benutzer zuzuweisen, der bereits über Ressourcen verfügt, oder wenn die primären Rollen nicht über genügend Ressourcen verfügen, wird eine entsprechende Meldung angezeigt.

---


Dem Vorlagenbenutzer muss mindestens eine dedizierte Ressource zugeordnet sein, die in einer Rolle enthalten ist. Bei der Zuweisung von dedizierten Ressourcen zu mehreren Benutzern werden nur primäre Rollen berücksichtigt. Den ausgewählten Benutzern werden aus freien Ressourcen in dieser Rolle dedizierte Ressourcen zugewiesen. Den ausgewählten Benutzern werden zudem dieselben Rollen, Systemgruppen und Richtlinien wie dem Vorlagenbenutzer zugewiesen. Den ausgewählten Benutzern wird keine auf dem Vorlagenbenutzer basierende Administratorgruppe zugewiesen.

---

## So lassen sich Ressourcen automatisch über eine Rolle zuweisen

1. Klicken Sie auf **Benutzer verwalten**.
2. Suchen Sie nach Benutzern.
3. Aktivieren Sie die Kontrollkästchen neben den entsprechenden Namen.


---

 **HINWEIS:** Es können mehrere Benutzer ausgewählt werden.

---

4. Wählen Sie aus der Liste **Operation** den Eintrag **Ressourcen zuweisen** aus, und klicken Sie auf **Los**.
5. Wählen Sie **Ressourcen über Rolle zuweisen** aus.
6. Wählen Sie die Rolle aus der Liste aus.
7. Klicken Sie auf **Weiter**.

---


 **HINWEIS:** Wenn die Rolle nicht über genügend Ressourcen verfügt, wird eine entsprechende Meldung angezeigt.

Bei der Zuweisung von dedizierten Ressourcen zu mehreren Benutzern werden nur primäre Rollen berücksichtigt.

---

## So weisen Sie dem Benutzer ein Monitorlayout zu und konfigurieren es


---

 **HINWEIS:** Sie sollten das Monitorlayout erstellen, bevor Sie es dem Benutzer zuweisen. Siehe [„Verwalten des Monitorlayouts“ auf Seite 75](#).

---

1. Aktivieren Sie das Kontrollkästchen neben dem entsprechenden Namen.
2. Wählen Sie in der Liste **Operation** den Eintrag **Monitorlayouts zuweisen** aus, und klicken Sie dann auf die Schaltfläche **Los**, um das Fenster **Monitorlayout für <Benutzername>** zu öffnen, das die Monitorlayouts enthält, die dem ausgewählten Benutzer zugewiesen sind.
3. Klicken Sie auf **Hinzufügen**.
4. Wählen Sie das hinzuzufügende Monitorlayout aus der Liste der Monitorlayout-IDs aus.
5. Aktivieren Sie das Kontrollkästchen neben den Rechnerressourcen und Rollen, die dem Monitorlayout zugewiesen werden sollen.
6. Geben Sie die neue horizontale und vertikale Auflösung sowie den horizontalen und vertikalen Offset ein.

---

 **HINWEIS:** Wenn Sie keine Angaben zu Auflösung und Offset machen, werden die Standardparameter des Systems angewendet.

---

7. Wählen Sie die allgemeine Richtlinie aus. Diese gibt an, welche Sitzungsrichtlinie zu verwenden ist, wenn alle Sitzungen verbunden sind.
8. Wählen Sie „USB-Voreinstellung“ aus. Dies ist die Sitzung, die von RGS standardmäßig für USB-Geräte verwendet werden soll, die mit dem Zugriffsgerät verbunden sind.
9. Klicken Sie auf **Speichern**.

## So ändern Sie die Monitorlayout-Konfiguration für die Benutzer

1. Aktivieren Sie das Kontrollkästchen neben dem entsprechenden Namen.
2. Wählen Sie in der Liste **Operation** den Eintrag **Monitorlayouts zuweisen** aus, und klicken Sie dann auf die Schaltfläche **Los**, um das Fenster **Monitorlayout für <Benutzername>** zu öffnen, das die Monitorlayouts enthält, die dem ausgewählten Benutzer zugewiesen sind.
3. Klicken Sie auf den Link in der Spalte **Monitor Layout ID**.
4. Geben Sie die neue horizontale und vertikale Auflösung, den horizontalen und vertikalen Offset, die allgemeine Richtlinie und die USB-Voreinstellung an.
5. Klicken Sie auf **Speichern**.

## So löschen Sie eine Monitorlayout-ID für den Benutzer

1. Aktivieren Sie das Kontrollkästchen neben dem entsprechenden Namen.
2. Wählen Sie in der Liste **Operation** den Eintrag **Monitorlayouts zuweisen** aus, und klicken Sie dann auf die Schaltfläche **Los**, um das Fenster **Monitorlayout für <Benutzername>** zu öffnen, das die Monitorlayouts enthält, die dem ausgewählten Benutzer zugewiesen sind.
3. Klicken Sie in der Spalte **Operation** auf **Entfernen**.

## So löschen Sie einen Benutzer

Löscht einen Benutzer aus dem System.

So löschen Sie einen Benutzer:

1. Wählen Sie das Kontrollkästchen neben dem/den gewünschten Namen aus.
2. Wählen Sie in der Liste **Operation** die Option **Löschen** aus, und klicken Sie dann auf die Schaltfläche **Los**.


## Hinzufügen neuer Benutzer

Für alle Rollen, die nicht öffentlich sind, müssen die Benutzer in der HP SAM-Zugangsliste aufgeführt sein, um eine Rechnerressource (z. B. einen Blade-PC) von der betreffenden Rolle anfordern zu können. Sie können den Benutzer als Einzelbenutzer hinzufügen, als Mitglied einer Sicherheitsgruppe oder als Mitglied einer Organisationseinheit. Wenn das System nach den hinzugefügten Benutzerkonten sucht, verwendet es dabei die HP SAM-Webserverdomain und/oder andere Active-Directory-Server, die sich in derselben Gesamtstruktur befinden wie in den **System Settings (Systemeinstellungen)** > auf der Registerkarte **Active Directory** konfiguriert.

## So gewähren Sie einzelnen Benutzern Zugang

1. Rufen Sie die Seite **Neue Benutzer hinzufügen** auf.
2. Wählen Sie für **Suchen nach** die Einstellung **Benutzer** aus.
3. Wenn Sie einen Filter auf eine bestimmte Domäne einstellen möchten, wählen Sie in der Liste **Domänennamen** die Domäne aus, oder wählen Sie **Globaler Katalog** für alle Domänen im selben Active Directory-Bereich aus, in dem sich auch der HP SAM Server befindet.


---

 **HINWEIS:** Mit der Option Searching by Global Catalog (Globalen Katalog durchsuchen) werden alle Benutzer von externen Domains angezeigt. Benutzer von anderen Domains können mit der Option Global Catalog (Globaler Katalog) zu HP SAM hinzugefügt werden; allerdings können sie sich möglicherweise nicht anmelden, wenn die Einstellung **External (Extern)** auf der Seite **Active Directory** in der Registerkarte **System Settings (Systemeinstellungen)** nicht gewählt wurde.

---

4. Geben Sie, wie in den folgenden Beispielen gezeigt, einen oder mehrere Parameter ein:
  - a. **Nachname:** Bei der Eingabe von Zeichen wird eine Suche nach Nachnamen ausgeführt.
  - b. **Vorname:** Nach einem Komma eingegebene Zeichen leiten eine Suche nach Vornamen ein. Durch die Eingabe eines Leerzeichens können Sie gleichzeitig nach Vornamen und Nachnamen suchen. Zeichen vor dem Leerzeichen leiten eine Suche nach Vornamen ein. Zeichen nach dem Leerzeichen leiten eine Suche nach Nachnamen ein.
  - c. **UPN-Name:** Die Eingabe eines Namens mit einem at-Zeichen (@) startet eine Suche nach UPN-Name (z. B. peter.meier@).

---

 **HINWEIS:** Die Ergebnisse werden bei der Eingabe angezeigt.

---


5. Klicken Sie auf **Hinzufügen**, um der Liste hervorgehobene Benutzer hinzuzufügen.
6. Wählen Sie in der Liste die Benutzer aus, die HP SAM hinzugefügt werden sollen.
7. Klicken Sie auf **Speichern**.

## So gewähren Sie Sicherheitsgruppen oder organisatorischen Einheiten Zugang

Zum Hinzufügen zahlreicher Benutzer können Sie die Active-Directory-Dienste nutzen und die Benutzernamen im Active Directory als Mitglieder einer Sicherheitsgruppe oder Organisationseinheit hinzufügen. Fügen Sie anschließend die Sicherheitsgruppe bzw. Organisationseinheit direkt in die Zugangsliste für HP SAM-Rollen ein. Sie können die Zugangsliste ändern: Rufen Sie das Active Directory auf und fügen Sie Benutzer dort hinzu bzw. entfernen Sie sie dort, anstatt auf der HP SAM-Verwaltungskonsole.

1. Rufen Sie die Seite **Neue Benutzer hinzufügen** auf.
2. Wählen Sie für **Suchen nach** die Einstellung „Organisatorische Einheiten“ oder „Sicherheitsgruppen“ aus.
3. Wenn Sie nach einer bestimmten Domäne filtern möchten, wählen Sie in der Liste **Domänenname** die Domäne aus, oder wählen Sie **Globaler Katalog** für alle Domänen im selben Active Directory-Bereich aus, in dem sich auch der HP SAM Server befindet, aus.
4. Geben Sie den Namen der organisatorischen Einheit oder Sicherheitsgruppe ein.

---

 **HINWEIS:** Durch die Eingabe von Zeichen in das Suchfeld können Sie nach Gruppen suchen. Die Ergebnisse werden bei der Eingabe angezeigt.

---

5. Klicken Sie auf **Hinzufügen**, um der Liste hervorgehobene Gruppen hinzuzufügen.
6. Wählen Sie in der Liste die Gruppen aus, die HP SAM hinzugefügt werden sollen.
7. Klicken Sie auf **Speichern**.

## Registerkarte „Ressourcen“

In den folgenden Abschnitten wird erklärt, welche Optionen auf der Registerkarte **Ressourcen** zur Verfügung stehen.

### Verwalten von Ressourcen


Die Suche zeigt standardmäßig alle Rechnerressourcen (z. B. Blade-PCs) an. Mithilfe der Filteroptionen können Sie die Anzahl der in der Liste angezeigten Ressourcen verringern. Die Filteroption basiert auf „UND“-Kombinationen. Je mehr Felder Sie angeben, desto stärker wird das Suchergebnis eingegrenzt. Folgende Filteroptionen sind verfügbar:

- **IP-Adresse/Hostname** – Ressourcen anzeigen, deren IP-Adresse oder Hostname mit den eingegebenen Daten übereinstimmen (oder einen Bereich oder eine Gruppe von Rechnerressourcen, die mit den Angaben übereinstimmen).
- **Dedizierte Ressource** – Suche auf Ressourcen begrenzen, die als dedizierte Ressourcen zugewiesen wurden.
- **Aktiviert** – Ressourcen anzeigen, die nur manuell aktiviert oder deaktiviert werden können.
- **Rolle** – Ressourcen anzeigen, die zu einer speziellen Rolle gehören.
- **Systemgruppe** – Ressourcen anzeigen, die zu einer bestimmten Systemgruppe gehören.
- **Verfügbar** – Ressourcen anzeigen, die zugeordnet werden können (keine verbundenen Benutzer).
- **Nicht verbunden** – Ressourcen anzeigen, die über nicht verbundene Benutzer verfügen.
- **In Gebrauch** – Ressourcen anzeigen, die über gerade aktiv verbundene Benutzer verfügen.
- **Offline** – Ressourcen anzeigen, die nicht für die Zuordnung zur Verfügung stehen, weil der Registrierungsdienst nicht reagiert (Dienst funktioniert nicht richtig, Hardware wurde ausgeschaltet usw.).

### Die Funktion „Automatisch aktualisieren“

Nachdem eine Suche durchgeführt und eine Ressourcenliste angezeigt wurde, stehen folgende Funktionen zur Verfügung:

**Auto Refresh (seconds) (Automatische Aktualisierung (Sekunden))** – Mit dieser Funktion lässt sich die Webseite –mit der Registerkarte **Resource (Ressource)** automatisch aktualisieren. Die Liste mit Rechnerressourcen wird dadurch von der Datenbank mit den neuesten Informationen abgerufen.


 **HINWEIS:** Wenn diese Option aktiviert ist, wird das Zeitlimit der HP SAM-Verwaltungskonsole außer Kraft gesetzt, und Sie werden von der HP SAM-Verwaltungskonsole nicht abgemeldet. Dies könnte allerdings aus sicherheitstechnischen Gründen bedenklich sein, insbesondere wenn die Sitzung an einem öffentlichen Endgerät stattfindet und der Benutzer vergisst, den Browser zu schließen oder sich abzumelden.

Zum Aktivieren dieser Funktion setzen Sie den Wert auf 5, 15, 30 oder 60 Sekunden, zum Deaktivieren der Funktion setzen Sie den Wert auf **Aus**. Klicken Sie anschließend auf **Übernehmen**. Die Einstellung wird sofort wirksam.




## Anzeigen von Detailinformationen

Um einzelne Informationen über eine Ressource anzuzeigen, klicken Sie auf das Vergrößerungsglas in der Spalte **Details**.

 **HINWEIS:** Um anzuzeigen, wer gerade mit einer Rechnerressource verbunden bzw. nicht verbunden ist, bewegen Sie den Mauszeiger langsam über das Symbol unter der Spalte **Status**. Das mit dem Blade verknüpfte Benutzerkonto wird angezeigt.

## Operationen

 **HINWEIS:** Für manche der unten aufgeführten Operationen, beispielsweise **Abmelden**, **Neustart** und **Herunterfahren**, muss das HP SAM Dienstkonto über Administratorrechte auf der Rechnerressource (z. B. einem Blade-PC) verfügen.

So führen Sie die unten aufgeführten Operationen aus:

1. Wählen Sie die entsprechende(n) Ressource(n) aus.
2. Wählen Sie die auszuführende Aufgabe aus der Liste **Operation** aus.
3. Klicken Sie auf die Schaltfläche **Los**.

## Operationen

- **Löschen** – Ressource aus dem System löschen. Auf diese Weise können Sie die Datenbank bereinigen. Sie können eine Rechnerressource nur dann löschen, wenn ihr Status **Offline** lautet.
- **Deaktivieren** – Weitere Zuordnungen der Ressource verhindern. Bei „In Verwendung“ ist die aktuelle Benutzersitzung nicht betroffen. Bei „Getrennt“ kann der Benutzer sich nicht mehr bei der Rechnerressource anmelden.
- **Aktivieren** – Ressource zur Zuordnung zulassen.
- **Benutzer abmelden** – Abmelden des aktuellen Benutzers von der Ressource erzwingen.
- **Neustart** – Ressource neu starten.
- **Nachricht senden** – Textnachricht (Pop-up-Nachricht) an den Benutzer der Ressource senden.  
Wird für Linux-Ressourcen nicht unterstützt.
- **Herunterfahren** – Ressource herunterfahren.


 **HINWEIS:** Seit SAM 3.2 werden die Vorgänge Abmelden, Neustarten und Herunterfahren jetzt für Linux-Ressourcen unterstützt. Um diese Funktion zu aktivieren, muss ein Zertifikat von der Domain-Zertifizierungsstelle auf der HP SAM-Website in IIS installiert sein.

- **Synchronize (Synchronisieren)** – Sendet eine Anfrage direkt an die Ressource, damit diese ihren aktuellen Status zurücksendet. Unter normalen Umständen ist dies nicht nötig, weil der Registrierungsdienst den Status der Ressource zurücksendet, sobald sich eine Statusänderung ergibt (Einschalten, Ausschalten, Benutzeranmeldung, Benutzertrennung und Benutzerabmeldung). Dies ist nützlich, wenn die Netzwerkverbindung zwischen der Ressource und dem HP SAM-Server vorübergehend unterbrochen war, weil so der aktuelle Status der Ressource abgefragt werden kann.
- **Rollen zuweisen** – Der Ressource neue Rollen zuweisen. Diese Einstellung setzt die Konfigurationsdatei für die Ressource außer Kraft.

Wenn Sie diese Option auswählen, wird das Fenster für die Ressourcen-Rollen-Zuweisung geöffnet. Verwenden Sie dieses Fenster, um primäre und alternative Rollen für die Ressource auszuwählen.

Sie können in diesem Fenster auch neue Rollen erzeugen.

---

 **HINWEIS:** Nach der Zuweisung zu Rollen mithilfe der HP SAM-Verwaltungskonsole werden etwaige Änderungen der Rollen in der Konfigurationsdatei ignoriert. Um die Einstellung mithilfe der Konfigurationsdatei wieder rückgängig zu machen, löschen Sie die Ressource aus der Datenbank und führen Sie einen Neustart der Rechnerressource durch.

---

- **Systemgruppen zuweisen** – Der Ressource neue Systemgruppen zuweisen.


## Ansicht anpassen

In diesem Fenster können Sie die Spalten für die Ressourcen anpassen, die im Fenster „Ressourcen verwalten“ angezeigt werden. Sie können dazu die Pfeiltasten verwenden oder auf die Objekte in den Feldern „Verfügbar“ und „Ausgewählt“ doppelklicken, um diese zu verschieben. Mit dem einfachen Pfeil können Sie das ausgewählte Objekt, mit dem Doppelpfeil alle Objekte in der Liste verschieben. Sie können mindestens drei und maximal sechs Spalten anzeigen.

## Verwalten von Zugriffsgeräten

### So fügen Sie manuell ein Zugriffsgerät hinzu

---

 **HINWEIS:** Der Windows-basierte Client, der Blade Workstation Client und der Linux-Client registrieren Zugriffsgeräte beim Herstellen einer Verbindung zum HP SAM Server automatisch. Dem XP Embedded-Betriebssystemabbild fehlt es auf einigen Thin Client-Zugriffsgeräten an der dazu benötigten Unterstützung. Befolgen Sie für diese Systeme die Anweisungen im Ordner CIMWIN32, der im Ordner AddOns des HP SAM SoftPaq enthalten ist.


---

1. Klicken Sie auf **Erstellen**.
2. Geben Sie die Seriennummer und einen Anzeigenamen ein.
3. Sie können die **Systemgruppen** auswählen, auf die dieses Gerät Zugriff haben wird.
4. Sie können ein Monitorlayout auswählen.
5. Klicken Sie auf **Speichern**.

### So ändern Sie ein Zugriffsgerät

1. Geben Sie einen oder mehrere Parameter ein, und klicken Sie auf **Suchen**, oder klicken Sie direkt auf **Suchen**, um alle registrierten Zugriffsgeräte anzuzeigen.
2. So ändern Sie die Einstellungen des Zugriffsgeräts:
  - a. Klicken Sie auf den Link mit der **Seriennummer**, und ändern Sie dann im Dialog die entsprechenden Einstellungen des Zugriffsgeräts.
  - b. Klicken Sie auf **Speichern**.

## So löschen Sie ein Zugriffsgerät

 **HINWEIS:** Ein Zugriffsgerät, das gerade verwendet wird, kann nicht gelöscht werden.

1. Geben Sie einen oder mehrere Parameter ein, und klicken Sie auf **Suchen**, oder klicken Sie direkt auf **Suchen**, um alle registrierten Zugriffsgeräte anzuzeigen.
2. Aktivieren Sie das Kontrollkästchen neben dem entsprechenden Zugriffsgerät.
3. Klicken Sie auf **Löschen** und anschließend auf **OK**.

## Verwalten des Monitorlayouts

In diesem Bereich können Sie ein neues Layout erstellen oder ein bestehendes Layout ändern oder löschen.

### So erstellen Sie ein Monitorlayout

1. Klicken Sie auf **Erstellen**.
2. Geben Sie die Monitorlayout-ID ein.
3. Geben Sie eine Beschreibung für das Layout ein.
4. Wählen Sie die mit diesem Monitorlayout verknüpften **Systemgruppen** aus.
5. Klicken Sie auf **Speichern**, um die neue Layout-ID hinzuzufügen.

### So ändern Sie ein Monitorlayout


1. Klicken Sie auf den Link in der Spalte „Monitorlayout-ID“, und ändern Sie dann die entsprechenden Einstellungen, um den Namen, die Beschreibung oder die Systemgruppe des Monitorlayouts zu ändern.
2. Klicken Sie auf **Speichern**, um die Monitorlayout-ID zu ändern.

### So löschen Sie ein Monitorlayout

1. Aktivieren Sie das Kontrollkästchen neben dem entsprechenden Monitorlayout.
2. Markieren Sie **Löschen**, und klicken Sie dann auf **OK**.

## Verwalten von Rechenzentren

Rechenzentren in HP SAM zählen zu den Gehäusegruppen. Rechenzentren dienen nur zur Speicherung von Gehäusepasswörtern, um die Funktion zu aktivieren, mit der Benutzer Blade-PCs über die HP SAM Verbindungsleiste aus- und wieder einschalten können.

 **HINWEIS:** Für die HP BladeSystem PC-Gehäuse muss Integrated Administrator (IA) Software der Version 4.20 oder höher verwendet werden. Standardmäßig weist die IA-Software ein deaktiviertes Konto mit dem Namen **SAM** auf. Sie müssen das Konto **SAM** aktivieren und ein Passwort erstellen, damit die Option für das Ausschalten und erneute Einschalten funktioniert.

Das IA-Passwort für das integrierte **SAM**-Konto muss in HP SAM auf der Seite „Rechenzentren verwalten“ gespeichert sein.

Die Blade-Energieverwaltung in Gehäusen der C-Klasse (Blade Workstations) wird nicht unterstützt.

## So erstellen Sie ein Rechenzentrum

1. Klicken Sie auf **Erstellen**.
2. Geben Sie den Namen des Rechenzentrums und das Gehäusepasswort ein.
3. Klicken Sie auf **Speichern**.

## So ändern Sie ein Rechenzentrum

1. Klicken Sie auf einen Link in der Spalte **Rechenzentrum**.
2. Ändern Sie den Namen des Rechenzentrums und/oder das Passwort.
3. Klicken Sie auf **Speichern**.

## So fügen Sie einem Rechenzentrum Gehäuse hinzu

1. Aktivieren Sie das Kontrollkästchen für das entsprechende Rechenzentrum.
2. Wählen Sie aus der Liste **Operation** den Eintrag **Gehäuse anzeigen** aus, und klicken Sie auf **Los**.
3. Klicken Sie auf **Hinzufügen**.
4. Geben Sie Suchbegriffe (optional) ein, und klicken Sie dann auf **Suchen**.
5. Aktivieren Sie die Kontrollkästchen für die hinzuzufügenden Gehäuse, und klicken Sie dann auf **Speichern**.
6. Klicken Sie auf **Schließen**.

## So löschen Sie Gehäuse aus einem Rechenzentrum

1. Aktivieren Sie das Kontrollkästchen für das entsprechende Rechenzentrum.
2. Wählen Sie aus der Liste **Operation** den Eintrag **Gehäuse anzeigen** aus, und klicken Sie auf **Los**.
3. Aktivieren Sie die Kontrollkästchen für die zu löschenden Gehäuse.
4. Klicken Sie auf **Löschen**.
5. Klicken Sie auf **Schließen**.

## So löschen Sie ein Rechenzentrum

1. Aktivieren Sie das Kontrollkästchen für das entsprechende Rechenzentrum oder die Rechenzentren.
2. Wählen Sie aus der Liste **Operation** den Eintrag **Löschen** aus, und klicken Sie auf **Los**.
3. Klicken Sie auf **OK**.

## Registerkarte „Richtlinien“

Über die Richtlinienverwaltung kann der Administrator die vom Benutzer gewählten Einstellungen für den HP SAM Client außer Kraft setzen. Im Allgemeinen wird dem Benutzer die flexible clientseitige

Anpassung der Verbindungseinstellungen gestattet. Für bestimmte Einstellungen, die der Benutzer stets zum Herstellen der Verbindung benötigt, kann der Administrator über die Registerkarte **Richtlinien** erzwungene Einstellungen definieren.

Die HP SAM Hierarchie-Richtlinie umfasst 5 Ebenen:

- Global
- Rolle
- OU (organisatorische Einheit)
- Sicherheitsgruppe
- Benutzer

Die einem Benutzer zugewiesenen Richtlinieneinstellungen haben Vorrang vor Richtlinieneinstellungen, die einer Sicherheitsgruppe zugeordnet sind, usw. bis zum Anfang der Liste.

**Schritte:**

1. Erzeugen oder aktualisieren Sie die Richtlinie auf der Registerkarte **Richtlinien**. Um eine bereits bestehende Richtlinie zu aktualisieren, klicken Sie auf den Richtliniennamen-Hyperlink.
2. Weisen Sie die Richtlinie:
  - einer Rolle zu (**Benutzer und Rollen > Ressourcenrollen verwalten**)
  - einem Benutzer, einer organisatorischen Einheit oder einer Sicherheitsgruppe zu (**Benutzer und Rollen > Benutzer verwalten**)

HP SAM erstellt stets die globale Policy. Diese Policy gilt für alle Benutzerverbindungen, sofern sie nicht von anderen Polycys außer Kraft gesetzt wird. Als Standardeinstellung ist das Feld Auto Reconnect (Automatisch neu verbinden) deaktiviert. Dadurch wird sichergestellt, dass nicht mehrere Benutzer gleichzeitig versuchen sich bei demselben Blade anzumelden. Wenn ein Netzwerkfehler oder Ähnliches auftritt, kann es sein, dass der Benutzer unwissentlich von der betreffenden Ressource abgemeldet wurde. Dies hängt von den Netzwerkeinstellungen und den AD-Gruppen-Policy-Einstellungen ab. HP SAM kann die betreffende Rechnerressource einem anderen Benutzer zuweisen. Wenn die Funktion zum automatischen Wiederverbinden aktiviert ist, wird der ursprüngliche Benutzer wieder mit derselben Rechnerressource verbunden, die anderenfalls möglicherweise einer anderen Person zugewiesen worden wäre. Wenn dies nicht von Bedeutung ist, können einen anderen geeigneten Wert für die Funktion zum automatischen Wiederverbinden festlegen.

**Tabelle 4-1 Beispiel für eine effektive hierarchische Richtlinie**

Parameter	Global	Rolle	OU	SG1	SG2	Benutzer	Effektiv
P1	<b>ON</b>	Nicht zugewiesen	Nicht zugewiesen	Nicht zugewiesen	Nicht zugewiesen	Nicht zugewiesen	ON
<sup>1</sup> P2	ON	<b>OFF</b>	Nicht zugewiesen	Nicht zugewiesen	Nicht zugewiesen	Nicht zugewiesen	OFF
P3	ON	OFF	ON	<b>OFF</b>	Nicht zugewiesen	Nicht zugewiesen	OFF
<sup>2</sup> P4	<b>ON/No Overrides Allowed</b>	OFF	Nicht zugewiesen	Nicht zugewiesen	Nicht zugewiesen	Nicht zugewiesen	ON

**Tabelle 4-1 Beispiel für eine effektive hierarchische Richtlinie (Fortsetzung)**

Parameter	Global	Rolle	OU	SG1	SG2	Benutzer	Effektiv
P5	<b>ON/No Overrides Allowed</b>	OFF/No Overrides Allowed	Nicht zugewiesen	Nicht zugewiesen	Nicht zugewiesen	Nicht zugewiesen	ON
<sup>3</sup> P6	ON	OFF	ON	<b>OFF</b>	ON	Nicht zugewiesen	OFF


- Die Reihenfolge der Richtlinienzuweisung lautet **Benutzer (höchste Ebene) > Sicherheitsgruppe > OU > Rolle > Globale Richtlinie (niedrigste Ebene)**. Einzelne Parameter, die auf der Benutzerebene zugewiesen wurden, setzen Parameter der Gruppenebene außer Kraft usw. Hinweis: Parameter P2 ist auf der globalen Ebene auf ON gesetzt, dies wird jedoch durch die Einstellung OFF der höheren Rollenebene außer Kraft gesetzt, sodass die effektive Einstellung OFF lautet.
- No Overrides Allowed** (Kein Außerkraftsetzen möglich) kann auf jeder Ebene eingestellt werden, um ein Außerkraftsetzen von Einstellungen durch höhere Ebenen zu vermeiden. Hinweis: Die Einstellung ON bei „No Overrides allowed“ für Parameter P4 auf der niedrigsten Ebene „Global“ setzt die Einstellung OFF der höheren Ebene „Rolle“ außer Kraft. Diese Option hat keinen Einfluss darauf, ob die geltende Einstellung für den Benutzer erzwungen wird. Die geltende Einstellung wird immer erzwungen.
- Auf der Sicherheitsgruppen-Ebene überprüft HP SAM alle Sicherheitsgruppen in alphanumerischer Reihenfolge und verwendet im Bedarfsfall die Richtlinie der ersten gefundenen Sicherheitsgruppe. Sicherheitsgruppe 1 ist die erste gefundene Sicherheitsgruppe, sodass auch bei Parameter P6 die effektive Einstellung OFF lautet und die Einstellung ON der Sicherheitsgruppe 2 ignoriert wird.

Die Option **No Overrides Allowed** wird für eine Einstellung aktiviert, um zu verhindern, dass die Übernahme anderer Richtlinien die Einstellung außer Kraft setzt.

## Erstellen oder Aktualisieren einer Richtlinie

Klicken Sie zum Erstellen einer neuen Richtlinie auf die Schaltfläche **Erstellen**, und geben Sie den Namen der neuen Richtlinie ein. Zum Aktualisieren oder Bearbeiten einer bestehenden Richtlinie klicken Sie auf den Hyperlink des Richtliniennamens. Wenn das Fenster „Richtlinie aktualisieren“ angezeigt wird, geben Sie die gewünschten Werte in die Felder ein oder lassen Sie diese frei, um einen Wert zu übernehmen.

Wenn Sie Richtlinien aktualisieren oder erstellen, können Sie alle verfügbaren Richtlinien anzeigen oder gültige Eigenschaften für RGS oder RDP angeben. Wählen Sie in der Liste **Eigenschaften anzeigen** entweder **ALL**, **RDP5**, **RDP6** oder **RGS** aus, um die aktiven Werte auf dem Bildschirm zu bestimmen.


 **HINWEIS:** Weitere Informationen zu RGS finden Sie in der Dokumentation über Ihre Remote Graphics Software.

## Effektive Richtlinie anzeigen

Mit dieser Funktion können Sie die gültige Richtlinie für einen bestimmten Benutzer anzeigen. Siehe [Tabelle 4-1, „Beispiel für eine effektive hierarchische Richtlinie“, auf Seite 77](#).

- Klicken Sie auf **Effektive Richtlinie anzeigen**.
- Geben Sie den UPN-Namen des Benutzers ein.
- Klicken Sie auf **Los**.

Die Richtlinienhierarchie für den Benutzer wird angezeigt.

 **HINWEIS:** Sie können auch eine Rolle für den Benutzer auswählen, um die effektive Richtlinie basierend auf dieser Rolle anzuzeigen, da diese je nach Rolle des Benutzers unterschiedlich sein kann.

## Registerkarte „Systemeinstellungen“

Mit dieser Registerkarte kann der Administrator einstellen, wie sich der HP SAM Server verhält.

### Allgemein

Auf dieser Seite kann der Administrator die Einstellungen für das gesamte System definieren. Nehmen Sie die gewünschte(n) Veränderung(en) vor, und klicken Sie zum Übernehmen auf „Speichern“.

- **Neue Rolleneinstellungen** – Wenn eine neue Rolle erstellt wird (die Rechnerressource registriert sich selbstständig bei einer neuen Rolle im System), werden die Markierungen entsprechend dem zugewiesenen Wert gesetzt.
  - **Aktiviert** – Ist diese Option bei der Erstellung einer neuen Rolle ausgewählt, wird das Flag „Rolle aktiviert“ markiert, d. h. die Rolle kann sofort zugeordnet werden.
  - **Öffentlich** – Ist diese Option bei der Erstellung einer neuen Rolle ausgewählt, wird das Flag „Öffentlich“ markiert, d. h. für die Rolle ist keine Einschränkung der Benutzerzugriffsrechte erforderlich.
- **Neue Ressourceneinstellungen** – Wenn eine neue Rechnerressource sich selbst registriert, wird sie vom System umgehend für die Zuordnung aktiviert oder deaktiviert.
- **Synchronisierung der Zeitzone** – Wenn diese Option ausgewählt ist, wird die Zeitzoneneinstellung auf der Rechnerressource mit der des Zugriffsgeräts des Benutzers synchronisiert.
- **Protokoll** – Bei Auswahl dieser Option, sammelt das System Prüfprotokolldaten. Sie können die Prüfprotokolldaten über die Registerkarte „Protokoll“ anzeigen lassen.




**HINWEIS:** Durch Protokolldaten kann die Größe der HP SAM Datenbank schnell und deutlich zunehmen. Wenn die Protokollierung aktiviert ist, sollten Sie möglichst einen Protokollwartungsplan festlegen. Siehe [„Planung der Protokollbereinigungsprüfung“ auf Seite 85.](#)

- **Verlauf** – Bei Auswahl dieser Option erfasst und archiviert das System historische Daten für Berichte für einen in der Liste **Rohdaten aufbewahren für** ausgewählten Zeitraum. Über diese Option können Sie die Größe der Verlaufsdatenbank begrenzen. Bei Microsoft 2005 oder 2008 Express Edition ist die Datenbankgröße auf 4 GB begrenzt. Ältere Daten, die außerhalb des in der Liste **Rohdaten aufbewahren für** ausgewählten Zeitraums liegen, werden pro Tag in einem Eintrag zusammengefasst. Auf der Registerkarte **Berichte** können Sie historische Daten einsehen.
- **Vor Zuweisung authentifizieren** – Bei Auswahl dieser Option authentifiziert HP SAM die Passwörter des Benutzers mit AD, bevor es ihm eine Ressource zuweist. Dies kann in sicherheitssensiblen Umgebungen wünschenswert sein. Bei aktivierter Option **Abgelaufenes Passwort zulassen** sorgt HP SAM dafür, dass Benutzer mit abgelaufenen Passwörtern den Ressourcen zugeordnet bleiben, sodass sie das Passwort im Betriebssystem der Ressource ändern können.
- **Erneute Versuche der Synchronisierungsabfrage** – Die Anzahl der Wiederholungsläufe, die das System ausführt, bevor es die Ressourcen als „offline“ markiert.
- **Synchronisierungszeit zwischen erneuten Versuchen** – Die Anzahl von Sekunden, die das System zwischen den einzelnen Wiederholungsläufen für die Synchronisierungsoperation wartet.



- **Zeitbegrenzung für die Benutzeranmeldung** – Die Anzahl an Sekunden, die ein Benutzer zum Anmelden zur Verfügung hat. Die Ressource wird während dieses Zeitraums keinem anderen Benutzer zugewiesen. Wenn die Zeit abläuft, bevor die Anmeldung erfolgt ist, wird die Rechnerressource wieder in der Liste verfügbarer Ressourcen angezeigt.
- **Timeout für Zugriffsbeschränkungswarnung** – Dauer in Sekunden während der dem Benutzer vor der erzwungenen Abmeldung durch die Zugriffsbeschränkungsfunktion ein entsprechender Warndialog angezeigt wird.
- **Automatische Verbindung für mehrere Sitzungen** – Wenn diese Option aktiviert ist, kann das System den Benutzer automatisch mit allen Ressourcen des gewählten Typs verbinden, die diesem Benutzer zugewiesen sind, sofern sich der Benutzer über ein Zugriffsgerät ohne zugewiesene Monitorlayout-ID angemeldet hat. Zur Auswahl stehen:
  - Dedizierte Ressourcen
  - Öffentliche Rollen
  - Nicht öffentliche Rollen
- **Client-Ressourcennetzwerk** – Sie können angeben, welche Methode verwendet werden soll, wenn das Zugriffsgerät eine Verbindung zur Rechnerressource herstellt.
  - **Host-Name** – Wenn diese Option ausgewählt ist, übermittelt das System dem Zugriffsgerät den **Computernamen** der Ressource, um eine Verbindung aufzubauen, und stützt sich auf den DNS-Server, um den Namen an die entsprechende IP-Adresse weiterzuleiten.
  - **IP-Adresse** – Wenn diese Option ausgewählt wird, gibt das System die IP-Adresse der Rechnerressource zum Herstellen einer Verbindung an das Zugriffsgerät des Benutzers weiter. Wenn die Rechnerressource über mehr als eine Netzwerkkarte verfügt, müssen Sie eine Option auswählen.
    - **Gemeldetes Subnetz** – Das Subnetz, bei dem sich die Rechnerressource registriert hat und über das sie mit HP SAM kommuniziert hat.
    - **Angegebenes Subnetz** – Wenn sowohl der HP SAM Server als auch die Rechnerressource je über zwei NIC-Karten verfügen und über zwei unabhängige Subnetze kommunizieren, muss angegeben werden, über welches Subnetz das Zugriffsgerät eine Verbindungsanfrage stellen soll.

---

 **HINWEIS:** HP SAM erlaubt nur die Eingabe eines Subnetzbereichs. Wenn die Netzwerkumgebung komplex ist, müssen Sie anstelle der IP-Adresse den Hostnamen eingeben.

---

## Web-Client


Auf dieser Seite kann der Administrator die Einstellungen für den Web-Client festlegen. Führen Sie die gewünschten Änderungen durch und klicken Sie auf **Save (Speichern)**, damit die Änderungen wirksam werden.

- **Zugriff aktivieren** – Wählen Sie diese Option aus, um Benutzern die Möglichkeit zu geben, eine Desktop-Sitzung über den Internet Explorer-basierten Client anzufordern.
- **Cookies** – Wählen Sie **Benutzerauswahl** aus, damit der Benutzer die Wahl hat, den Benutzernamen, die Domäne und die Client-Einstellungen auf den Browser-Cookies des Zugriffsgeräts zu speichern. Wenn Sie Sicherheitsbedenken haben (z. B. öffentlicher Terminalzugriff), wählen Sie die Option **Nicht erlauben** aus, damit die Informationen nicht gespeichert werden und der Benutzer bei jeder Anmeldung den Benutzernamen und die Domäne eingeben muss.
- **Domänenfeld anzeigen** – Wählen Sie **Aktiviert** aus, um das Domäneneingabefeld anzuzeigen, in dem Benutzer eine Domäne angeben können. Ist diese Option nicht ausgewählt, müssen die Benutzer einen Namen im UPN-Format eingeben.
- **Show password field (Passwortfeld anzeigen)** – Wählen Sie **Enabled (Aktiviert)**, um das Feld **Password (Passwort)** auf dem Bildschirm des Web-Clients anzuzeigen.
- **Show configuration options (Konfigurationsoptionen anzeigen)** – Wählen Sie **Enabled (Aktiviert)**, um den Konfigurationslink auf dem Bildschirm des Web-Clients anzuzeigen.
- **Show resolution selection (Ausgewählte Auflösung anzeigen)** – Wählen Sie **Enabled (Aktiviert)**, um die gewählte Auflösung auf dem Bildschirm des Web-Clients anzuzeigen.
- **Default Domain (Standard-Domain)** – Geben Sie die Standard-Domain für die Anmeldung beim Web-Client ein.

- **Banner text (Banner-Text)** – Wählen Sie die Sprache aus und geben Sie die entsprechende Meldung in das Feld ein, um die benutzerdefinierbare Meldung zu ändern, die für den Benutzer auf der HP SAM-Web-Client-Seite angezeigt wird.
- **Smart Card**
  - **Smart card login (Smartcard-Anmeldung)** – Wählen Sie den Wert für die gewünschte Art der Anmeldung aus.
    - **Disallowed (Nicht erlaubt)** – Wählen Sie diese Option, um die Anmeldung mit Smartcard zu deaktivieren. Nur die herkömmlichen Felder für die Zugangsdaten werden angezeigt.
    - **Optional** – Wählen Sie diese Option, wenn die Anmeldung über die Smartcard optional sein soll. Alle Anmeldefelder werden angezeigt.
    - **Required (Obligatorisch)** – Wählen Sie diese Option, wenn die Anmeldung über die Smartcard obligatorisch sein soll. Nur die Zugangsdaten für die Smartcard werden angezeigt.
  - **User name field (Benutzernamenfeld)** – Wählen Sie den geeigneten Wert für das Feld auf dem Zertifikat aus, das den Anmeldenamen des Benutzers enthält.
    - **Email (E-Mail)** – Wählen Sie, ob HP SAM im E-Mail-Feld auf dem Zertifikat nach dem Anmeldenamen suchen soll. Die in diesem Feld gefundenen Daten müssen mit dem UPN-Namen des Benutzers übereinstimmen.
    - **UPN** – Wählen Sie, ob HP SAM im UPN-Feld auf dem Zertifikat nach dem Anmeldenamen suchen soll.
  - **Automatisches Verbinden** – Wählen Sie **Aktiviert** aus, damit der Client automatisch eine Verbindung herstellt, wenn der Benutzer die Smart Card einschiebt.
  - **Cryptographic Service Providers (CSP)** – Geben Sie den Namen des CSP ein, der die Smartcard-Lösung unterstützt, die Sie bei der Konfiguration der Smartcard-Anmeldung ausgewählt haben. Dieser Wert stellt den Identifizierer des zu verwendenden Cryptographic Service Providers (CSP) dar. Führen Sie anhand der Schaltflächen **Create (Erstellen)**, **Edit (Bearbeiten)** oder **Delete (Löschen)** die geeignete Aktion für diesen Wert durch.


## Active Directory

Auf dieser Seite wird die Verbindung des Systems zu Active Directory-Diensten definiert, über die Benutzerkontoinformationen abgerufen werden.

- **Extern** – Wählen Sie diese Option aus, um alle Domänen zu durchsuchen.
- 
-  **HINWEIS:** Wenn Sie dieses Feld deaktivieren, können Benutzer in anderen Domains dennoch angezeigt werden, wenn Sie die Seite Add New Users (Neue Benutzer hinzufügen) in der HP SAM-Verwaltungskonsole durchsuchen. Allerdings wird HP SAM diesen Benutzern keine Ressourcen mehr zuweisen, wenn sich diese über den HP SAM-Client anmelden.
- 
- **Server Query Time Limit (Zeitlimit Serveranfrage)** – Geben Sie den Wert für die Zeitlimitüberschreitung ein. HP SAM wartet dann bis zum Zeitlimit, wenn der Active-Directory-Server Kontoinformationen extrahiert. Der HP SAM-Webserver ruft die Benutzerkontendaten ab, wenn diese innerhalb dieses eingestellten Zeitlimits vom Active Directory zurückgegeben werden.

Erhöhen Sie den Wert nur, wenn Sie auf der HP SAM-Verwaltungskonsole auf der Seite Add New User (Neuen Benutzer hinzufügen) dazu angeleitet wurden.

## Automatische Planungen

 **HINWEIS:** Diese Planungen befinden sich jetzt nicht mehr im oberen Menü, sondern auf der Seite **Automatische Planungen**.

---

### Planung der Ressourcensynchronisierung

Um die Synchronisierung zum Erfassen der Offline-Ressourcen zeitlich zu planen, stellen Sie den Timer wie unten beschrieben ein, und klicken Sie auf **Erstellen** oder **Aktualisieren**. Bei normalem Betrieb der Ressourcen ist dies in der Regel nicht nötig. Wenn Sie lieber regelmäßig Rückmeldungen über die Ressourcen erhalten möchten, setzen Sie die Synchronisierung in regelmäßigen Intervallen (z. B. täglich um Mitternacht) an.

- **Automatische Ereignisplanung** – Markieren Sie zum Einschalten dieser Option das Kästchen **Aktiviert**.
- **Geplantes Startdatum** – Wählen Sie das Startdatum für das Ereignis aus.
- **Geplante Zeit** – Wählen Sie die Uhrzeit aus, zu der die Synchronisierungsoperation durchgeführt werden soll. Aktivieren Sie so viele Zeitpunkte wie nötig.
- **Geplanter Tag** – Wählen Sie eine der folgenden Optionen aus:
  - **Täglich** – Geben Sie die Anzahl der Tage ein, nach denen das Ereignis erneut auftreten soll.
  - **Wöchentlich** – Geben Sie die Anzahl der Wochen ein, nach denen das Ereignis erneut auftreten soll, und den/die Wochentag(e).

Um die Synchronisierung manuell auszuführen, klicken Sie auf die Registerkarte **Ressourcen**, suchen und öffnen Sie die Ressourcenliste, und wählen Sie die zu synchronisierenden Ressourcen aus. Wählen Sie aus der Liste **Operation** die Option **Synchronisieren** aus.

### Planung der Protokollbereinigungsprüfung


Um die Durchführung einer Datenbankbereinigung zeitlich zu planen, stellen Sie den Timer wie unten beschrieben ein, und klicken Sie auf **Erstellen** oder **Aktualisieren**. Führen Sie diese Operation aus, um die Verwaltbarkeit der Datenbank zu gewährleisten und die Beeinträchtigung der Leistung von HP SAM auf ein Minimum zu begrenzen.


- **Automatische Ereignisplanung** – Markieren Sie zum Einschalten dieser Option das Kästchen **Aktiviert**.
- **Geplantes Startdatum** – Wählen Sie das Startdatum für das Ereignis aus.
- **Geplante Zeit** – Wählen Sie die Uhrzeit aus, zu der die Synchronisierungsoperation durchgeführt werden soll. Aktivieren Sie so viele Zeitpunkte wie nötig.

- **Geplanter Tag** – Wählen Sie eine der folgenden Optionen aus:
  - **Täglich** – Geben Sie die Anzahl der Tage ein, nach denen das Ereignis erneut auftreten soll.
  - **Wöchentlich** – Geben Sie die Anzahl der Wochen ein, nach denen das Ereignis erneut auftreten soll und den/die Wochentag(e).
- **Optionen löschen**
  - **Einträge löschen, die älter sind als** – Geben Sie den Zeitraum an (in Tagen), für den Einträge gespeichert bleiben, bevor sie gelöscht werden.
  - **Typen löschen** – Markieren Sie zum Löschen **Information, Warnung** und/oder **Fehler**.
  - **Ohne Speichern löschen** – Wählen Sie diese Option aus, wenn die Daten dauerhaft gelöscht werden sollen.
  - **Als CSV-Datei speichern und dann löschen** – Wählen Sie diese Option aus, wenn Sie die Daten vor dem dauerhaften Löschen in einer externen Textdatei speichern möchten.
    - Geben Sie den Dateipfad an, unter dem die CSV-Datei gespeichert werden soll.

## Log Off User from Resource Scheduler (Benutzer vom Ressourcenplaner abmelden)

Um die erzwungene Abmeldung von Benutzern bei ihren Ressourcen zeitlich zu planen, stellen Sie den Timer wie unten beschrieben ein, und klicken Sie auf **Erstellen** oder **Aktualisieren**.

 **HINWEIS:** Ein Zertifikat von der Domain-Zertifizierungsstelle muss auf der HP SAM-Website in IIS installiert sein, damit diese Funktion funktioniert.

- **Automatische Ereignisplanung** – Markieren Sie zum Einschalten dieser Option das Kästchen **Aktiviert**.
  - **Geplantes Startdatum** – Wählen Sie das Startdatum für das Ereignis aus.
  - **Geplante Zeit** – Wählen Sie die Uhrzeit aus, zu der die Abmeldeoperation durchgeführt werden soll. Aktivieren Sie so viele Zeitpunkte wie nötig.
-  **HINWEIS:** Die hier festgelegte Zeit ist die Zeit für den HP SAM Server. Wenn sich die Ressourcen in einer anderen Zeitzone als der HP SAM Server befinden, müssen Sie diese Zeitangabe entsprechend anpassen.
- **Geplanter Tag** – Wählen Sie eine der folgenden Optionen aus:
    - **Täglich** – Geben Sie die Anzahl der Tage ein, nach denen das Ereignis erneut auftreten soll.
    - **Wöchentlich** – Geben Sie die Anzahl der Wochen ein, nach denen das Ereignis erneut auftreten soll und den/die Wochentag(e).
  - **Rollen** – Übertragen Sie Rollen aus dem linken Feld in das rechte Feld, damit Benutzer, denen Ressourcen aus dieser Rolle zugeordnet sind, zu den angegebenen Zeiten automatisch abgemeldet werden.

## Lizenzen

Standardmäßig (d. h., wenn kein Lizenzschlüssel angegeben wurde) können Sie bis zu 30 Ressourcen ausführen (z. B. Blade-PCs). Dies dient nur zu Testzwecken. In Produktionsumgebungen müssen auch

bei weniger als 30 Ressourcen Lizenzen für alle Ressourcen erworben werden. Es gibt kein Ablaufdatum für diese Testsoftware.


Die HP SAM-Lizenzierung erfolgt je Ressource, nicht je Benutzer. In einer Umgebung, in der 300 Benutzer 100 Ressourcen gemeinsam nutzen, sind beispielsweise nur 100 lizenzierte Arbeitsplätze erforderlich. Wenn die Zahl der Ressourcen die Zahl der lizenzierten Arbeitsplätze überschreitet, wird auf der HP SAM-Verwaltungskonsole ein orangefarbenes Warnbanner angezeigt. Unter diesen Umständen gehen keine Funktionalitäten verloren. Die HP SAM-Lizenzen sind flexible Lizenzen, die nicht an eine bestimmte Ressource gebunden sind.

Die Lizenzschlüssel für HP SAM sind mit einer bestimmten Anzahl Arbeitsplätze (Ressourcen), einer Versionsnummer und ggf. einem Ablaufdatum für die Software Assurance (SA) kodiert. Diese Informationen können auf der Seite Licensing (Lizenz) nachgesehen werden, die in diesem Abschnitt beschrieben wird. Die Versionsnummer legt fest, für welche HP SAM-Hauptversion die Lizenz gelten soll. Ein Lizenzschlüssel mit Version 2 bedeutet beispielsweise, dass der Schlüssel für HP SAM Version 2.x erstellt wurde. Diese Lizenz kann zur Lizenzierung von Ressourcen in einer beliebigen 2.x-Version von HP SAM verwendet werden. Die Lizenz läuft niemals ab, solange die Version 2.x verwendet wird.

Um das obige Beispiel weiter fortzuführen, wenn für HP SAM ein Upgrade auf eine Version 3.x durchgeführt wird, funktioniert die Version-2-Lizenz weiterhin mit jeder beliebigen SAM-Version, deren Gültigkeitsdatum (dieses wird oben in der HP SAM-Verwaltungskonsole angezeigt) vor dem SA-Ablaufdatum liegt. Wenn Sie eine Version von SAM installieren, deren Gültigkeitsdatum nach dem SA-Ablaufdatum liegt, verlieren die entsprechenden Lizenzen ihre Gültigkeit. Dies kann dazu führen, dass ein orangefarbenes Warnbanner angezeigt wird, in dem Sie darauf hingewiesen werden, dass Sie mehr Ressourcen als Lizenzen haben. Selbst in dieser Situation gehen keine Funktionalitäten verloren. Der Kunde muss dann Lizenzen für Version 3 kaufen oder eine ältere Version von HP SAM weiterbenutzen.

Klicken Sie auf die Schaltfläche **Neuen Schlüssel eingeben**, um HP SAM einen neuen Schlüssel hinzuzufügen. Nach dieser Eingabe zeigt das System die auf diesem Schlüssel kodierte Information an. Wenn Sie den Schlüssel aus dem System löschen möchten, aktivieren Sie den/die entsprechenden Schlüssel, und klicken Sie dann auf **Löschen**.

---

 **HINWEIS:** Damit der Lizenzschlüssel für HP SAM erfolgreich angegeben werden kann, muss das HP SAM Dienstkonto zur lokalen Administratorgruppe des Servers gehören.

---

Wenn eine Lizenznachricht auf der HP SAM-Verwaltungskonsole angezeigt wird, sollten Sie jeweils diesen Bereich aufrufen, um die Einzelheiten der Lizenzmeldung zu studieren.

## Registerkarte „Berichte“

---

 **HINWEIS:** Sie müssen unter **Systemeinstellungen > Allgemein** die Verlaufsaufzeichnung aktivieren, um Berichte erstellen zu können.

---

Administratoren können nur die Berichte sehen, die mit den von ihnen gesteuerten Systemgruppen verknüpft sind.

---

HP SAM verfügt über drei Berichtstypen:

- **Bericht zum Ressourcenkapazitätsverbrauch** – Diesem Bericht können Sie die Spitzenauslastung der Ressource in Prozent entnehmen und die Prozentwerte markieren, die einen bestimmten Schwellenwert übersteigen.
- **Trendbericht zum Ressourcenkapazitätsverbrauch** – Dieser Bericht enthält die aufgezeichneten Spitzenauslastungswerte der Ressource über einen bestimmten Zeitraum.
- **Ressourcennutzungsbericht** – Diesem Bericht können Sie den aktuellen Status der Ressourcennutzung entnehmen. Dieser Bericht wird auch auf der Hauptregisterkarte **Home** veröffentlicht.

## Bericht zum Ressourcenkapazitätsverbrauch

Wählen Sie die Filter- und Anzeigeeoptionen aus, und klicken Sie auf die Schaltfläche **Bericht erzeugen**.

### Filter

- **Zeitraumen (Von/Bis)** – Grenzen Sie die angezeigten Daten auf den Zeitraum ein, der Sie interessiert.
- **Rolle aktiviert** – Grenzen Sie die Daten auf alle aktivierten Rollen (**Ja**) bzw. alle deaktivierten Rollen (**Nein**) ein, oder ignorieren Sie diese Markierung durch Auswahl von **Beide**.
- **Öffentliche Rolle** – Grenzen Sie die Daten auf Rollen ohne Zugangsbeschränkung für Benutzer (**Ja**) bzw. Rollen mit Zugangsbeschränkung (**Nein**) ein, oder ignorieren Sie diese Markierung durch Auswahl von **Beide**.
- **Rollen** – Zeigen Sie nur Daten zu den ausgewählten Rollen an. Wenn Sie diese Option wählen, grenzt das System die Auswahl anhand der zuvor von Ihnen gewählten Auswahloptionen ein.

### Anzeigeeoptionen


- **Schwellenwertprozentsätze** – In diesem Bericht können Sie Daten markieren, wenn sie den hier eingegebenen Wert überschreiten.
  - **Mindestens verfügbar** – Wenn die Daten den hier eingegebenen Wert unterschreiten, werden sie im Bericht automatisch markiert.
  - **Maximum verbraucht** – Wenn die Daten den hier eingegebenen Wert überschreiten, werden sie im Bericht automatisch markiert.
- **In neuem Fenster öffnen** – Bei Auswahl dieser Option werden die Ergebnisdaten in einem neuen Browser-Fenster angezeigt.

### Ausgabebericht

- **Rollename** – Name der Rolle
- **Mindestens verfügbar %** – Für den ausgewählten Zeitraum wird der Spitzenwert des verfügbaren Minimums angezeigt. Dieser Wert gibt an, dass der Prozentsatz der Rechnerressourcen, die noch zugeordnet werden können, auf den angegebenen niedrigsten Wert abgesunken ist.



- **Mindestens verfügbar** – Dieser Wert stellt eine Ergänzung zu dem o. a. Prozentsatz dar und gibt im Einzelnen an, wie viele Ressourcen innerhalb der Rolle noch zur Verfügung stehen.
- **Maximum verbraucht %** – Dieser Wert gibt den höchsten Prozentsatz an Ressourcen an, die im ausgewählten Zeitraum genutzt wurden.
- **Maximum verbraucht** – Dieser Wert stellt eine Ergänzung zu dem o. a. Prozentsatz dar und gibt im Einzelnen an, wie viele Ressourcen innerhalb der Rolle genutzt wurden.
- **Keine Ressourcen mehr** – Dieser Wert gibt für den ausgewählten Zeitraum an, wie oft das System eine Situation festgestellt hat, in der keine Rechnerressourcen zur Ausführung der Verbindungsanfrage verfügbar waren.

 **HINWEIS:** In der Regel sollte das verbrauchte Maximum das Gegenteil des verfügbaren Minimums sein. Dies gilt nicht, wenn die Rechnerressource mehreren Rollen zugeordnet ist. Die Ressource wird in diesem Fall mehrmals gezählt, einmal pro zugewiesener Rolle. Wenn die Rechnerressource deaktiviert ist, wird sie bei der Angabe der Gesamtzahl nicht berücksichtigt.

## Trendbericht zum Ressourcenkapazitätsverbrauch

Wählen Sie die Filter- und Anzeigeeoptionen aus, und klicken Sie auf die Schaltfläche **Bericht erzeugen**.

### Filter

- **Zeitraumen (Von/Bis)** – Grenzen Sie die angezeigten Daten auf den Zeitraum ein, der Sie interessiert.
- **Rolle aktiviert** – Grenzen Sie die Daten auf alle aktivierten Rollen (**Ja**) bzw. alle deaktivierten Rollen (**Nein**) ein, oder ignorieren Sie diese Markierung durch Auswahl von **Beide**.
- **Öffentliche Rolle** – Grenzen Sie die Daten auf Rollen ohne Zugangsbeschränkung für Benutzer (**Ja**) bzw. Rollen mit Zugangsbeschränkung (**Nein**) ein, oder ignorieren Sie diese Markierung durch Auswahl von **Beide**.
- **Rollen** – Zeigen Sie nur Daten zu den ausgewählten Rollen an. Wenn Sie diese Option wählen, grenzt das System die Auswahl anhand der zuvor von Ihnen gewählten Auswahloptionen ein.

### Anzeigeeoptionen

- **Schwellenwertprozentsätze** – In diesem Bericht können Sie Daten markieren, wenn sie den hier eingegebenen Wert überschreiten.
  - **Mindestens verfügbar** – Wenn die Daten den hier eingegebenen Wert unterschreiten, werden sie im Bericht automatisch markiert.
  - **Maximum verbraucht** – Wenn die Daten den hier eingegebenen Wert überschreiten, werden sie im Bericht automatisch markiert.
- **Zeitintervall** – Daten werden in einem Maßstab aufgezeichnet, der auf Stunde, Tag, Woche oder Monat beruht.

- **Rohdaten einbeziehen** – Wenn auch die Rohdaten in den Bericht mit aufgenommen werden sollen, aktivieren Sie das Feld **Rohdaten einbeziehen**.
- **In neuem Fenster öffnen** – Bei Auswahl dieser Option werden die Ergebnisdaten in einem neuen Browser-Fenster angezeigt.

## Ausgabebericht

- **Diagramme für Mindestkapazität und maximale Kapazität** – Diese Diagramme zeigen die Mindestanzahl an Blade-PCs, die in dem angegebenen Zeitraum zur Verfügung standen, und die Höchstanzahl der benutzten Blade-PCs an. Im Allgemeinen sollte die Summe dieser Werte 100 % ergeben. Wenn ein Blade-PC jedoch mehrere Rollen unterstützt, dann lassen sich die Werte nicht auf diese Weise addieren, da die Nutzung eines Blade-PCs in einer Rolle gleichzeitig das verfügbare Minimum in der anderen Rolle herabsetzt.
- **Zeitintervall** – Das Zeitintervall, für das der Bericht erstellt wurde. Ausschlaggebend für diesen Wert ist die Auswahl unter **Anzeigeoptionen: Zeitintervall**.
- **Datum** – Das Datum des Berichts.
- **Rollename** – Der Name der Rolle.
- **Mindestens verfügbar %** – Für den ausgewählten Zeitraum wird der Spitzenwert des verfügbaren Minimums angezeigt. Dieser Wert gibt an, dass der Prozentsatz der Rechnerressourcen, die noch zugeordnet werden können, auf den angegebenen niedrigsten Wert abgesunken ist.
- **Mindestens verfügbar** – Dieser Wert stellt eine Ergänzung zu dem o. a. Prozentsatz dar und gibt im Einzelnen an, wie viele Ressourcen innerhalb der Rolle noch zur Verfügung stehen.
- **Maximum verbraucht %** – Dieser Wert gibt den höchsten Prozentsatz an Ressourcen an, die im ausgewählten Zeitraum genutzt wurden.
- **Maximum verbraucht** – Dieser Wert stellt eine Ergänzung zu dem o. a. Prozentsatz dar und gibt im Einzelnen an, wie viele Ressourcen innerhalb der Rolle genutzt wurden.
- **Keine Ressourcen mehr** – Dieser Wert gibt für den ausgewählten Zeitraum an, wie oft das System eine Situation festgestellt hat, in der nicht genügend Rechnerressourcen zur Ausführung von Verbindungsanfragen verfügbar waren.

## Ressourcennutzungsbericht

Wählen Sie die Filter- und Anzeigeoptionen aus, und klicken Sie auf die Schaltfläche **Bericht erzeugen**.

### Filter

- **Gesamtzahl der Ressourcen** – Der physische Zählvorgang beruht auf den einzelnen physischen Ressourcen (d. h. nur primäre Rolle). Der logische Zählvorgang ergibt höhere Zahlen, da eine Rechnerressource mehrmals gezählt wird, wenn sie mehreren Rollen zugewiesen wurde.
- **Rolle aktiviert** – Grenzen Sie die Daten auf alle aktivierten Rollen (**Ja**) oder alle deaktivierten Rollen (**Nein**) ein, oder ignorieren Sie diese Markierung durch Auswahl von **Beide**.

- **Öffentliche Rolle** – Grenzen Sie die Daten auf Rollen ohne Zugangsbeschränkung für Benutzer (**Ja**) oder Rollen mit Zugangsbeschränkung (**Nein**) ein, oder ignorieren Sie diese Markierung durch Auswahl von **Beide**.
- **Rollen** – Zeigen Sie nur Daten zu den ausgewählten Rollen an. Wenn Sie diese Option wählen, grenzt das System die Auswahl anhand der zuvor von Ihnen gewählten Auswahloptionen ein.


## Anzeigeoptionen

- **In neuem Fenster öffnen** – Bei Auswahl dieser Option werden die Ergebnisdaten in einem neuen Browser-Fenster angezeigt.

## Ausgabebericht

- **Rollenname** – Name der Rolle
- **Offline** – Anzahl der Rechnerressourcen, die offline sind
- **Deaktiviert** – Anzahl der manuell deaktivierten Rechnerressourcen
- **Verfügbar** – Anzahl der verfügbaren Rechnerressourcen
- **Getrennt** – Anzahl der Rechnerressourcen mit Benutzern, die nicht mit der Sitzung verbunden sind
- **In Verwendung** – Anzahl der Rechnerressourcen mit Benutzern, die diese gerade aktiv nutzen
- **Gesamtzahl** – Anzahl der Rechnerressourcen, die offline sind, zur Verfügung stehen, nicht verbunden und in Verwendung sind

## Registerkarte „Protokoll“

 **HINWEIS:** Administratoren können nur die Protokolleinträge sehen, die mit den von ihnen gesteuerten Systemgruppen verknüpft sind.

Zum Anzeigen von Verlaufsaktivitäten des Systems stellen Sie die Filteroptionen entsprechend ein, um den anzuzeigenden Inhalt einzuschränken, und klicken Sie dann auf **Suchen**.

### Filter


- **Kategorie** – Standardeinstellung für die Suche ist **alle**. Sie können die Auswahl aber auch auf eine der unten genannten Kategorien einschränken.
  - **Sicherheit** – Nur Daten zu sicherheitsbezogenen Ereignissen anzeigen.
  - **Usage Activities (Nutzungsaktivitäten)** – Engen Sie die Daten so ein, dass nur Daten zu den Benutzerverbindungen, -trennungen und -abmeldungen angezeigt werden.
  - **Administrationstätigkeiten** – Nur Daten zu Administrationstätigkeiten anzeigen.
- **Typ** – Zum Eingrenzen der Daten auf die Ereignisebene. Zur Auswahl stehen die Optionen **Information**, **Warnung** und **Fehler**.
- **Beschreibung** – Ereignisse suchen, für die das Feld **Beschreibung** Text enthält.
- **Zeitrahmen** – Datenanzeige auf die eingegebenen Daten beschränken.
- **Systemgruppen** – Datenanzeige auf die ausgewählten Systemgruppen beschränken.

Sie können folgende vier Operationen ausführen:

- **Ausgewählte speichern**
- **Gesamtes Protokoll speichern**
- **Ausgewählte löschen**
- **Gesamtes Protokoll löschen**

## Einrichten der Smartcard-Anmeldung auf dem Zugangsgerät

---

 **HINWEIS:** RGS 5.1.3 oder höher ist für die Anmeldung mit RGS mithilfe von Smartcards erforderlich. Die Anmeldung mit SmartCard funktioniert nicht, wenn RGS Single Sign-on aktiviert ist. Sie müssen Easy Login auf dem RGS-Sender aktivieren und den USB auf dem RGS-Empfänger auf **Remote and Local (Remote und Lokal)** oder **Remote** einstellen. Treiber für das Smartcard-Lesegerät sind sowohl auf der Ressource als auch auf dem Zugangsgerät erforderlich.

---


Lesen Sie dieses White Paper zur Konfiguration der Smart Card auf der Rechnerressource, bevor Sie versuchen, die folgenden Schritte auszuführen: *Implementing ActivIdentity Smart Cards for Use with HP Compaq t5720 Thin Clients and HP Blade PCs* unter [http://h20000.www2.hp.com/bc/docs/support/SupportManual/c01153197/c01153197.pdf?jumpid=reg\\_R1002\\_USEN](http://h20000.www2.hp.com/bc/docs/support/SupportManual/c01153197/c01153197.pdf?jumpid=reg_R1002_USEN).

Sie müssen die Smart Card erfolgreich auf der Rechnerressource konfiguriert haben, bevor Sie versuchen, sie auf dem Zugriffsgerät zu konfigurieren:

Gehen Sie folgendermaßen vor, um den HP SAM-Client für die Anmeldung mit Smartcard zu aktivieren.

1. Schließen Sie das Smart Card-Lesegerät an das Zugriffsgerät an.
2. Installieren Sie den Treiber des Smart Card-Lesegeräts auf dem Zugriffsgerät.
3. Installieren Sie die Smart Card-CSP-Software (Kryptographiedienstanbieter-Software), die Ihre Smart Card-Lösung unterstützt, auf dem Zugriffsgerät. Diese Software ist erforderlich, um den Inhalt der Smart Card zu lesen.
4. Installieren Sie die HP SAM Client-Software auf dem Zugriffsgerät.
5. Wenn Sie einen Internet-Explorer-basierten Client verwenden, konfigurieren Sie den Client auf der HP SAM-Verwaltungskonsole unter **System Settings (Systemeinstellungen) > Web Client (Web-Client) > Smartcard cryptographic service providers (CSP) (Cryptographic Service Providers (CSP) für Smartcard)**. Für weitere Informationen siehe [„Web-Client“ auf Seite 82](#).

---

 **HINWEIS:** Wenn Sie den Client so konfigurieren, dass er das Feld „UPN“ oder „E-Mail“ aus dem Zertifikat des Benutzers liest, müssen die in diesen Feldern gelesenen Daten mit dem UPN-Namen des Benutzers übereinstimmen.

---

6. Wenn Sie den XPe-Client verwenden, müssen Sie die CSP-Zeichenfolge in der .SAM-Datei angeben. Weitere Informationen hierzu finden Sie unter [„Smart Card-Einstellungen“ auf Seite 47](#).

7. Wenn Sie möchten, dass das System den HP SAM Client automatisch startet, wenn ein Benutzer eine Smart Card einsetzt, lesen Sie die Schritte a und b. (**HINWEIS:** Schritt a ist die Standardeinstellung.)
  - a. Bearbeiten Sie für den Windows-basierten Client (Standardeinstellung) die Datei 'scwatch.cfg' folgendermaßen:
 

```
[scwatch]

Action=c:\Program Files\Hewlett-Packard\HP Session
Allocation Client\hprdcw32.exe

ActionDir=c:\Program Files\Hewlett-Packard\HP Session
Allocation Client\


– oder –
```
  - b. Bearbeiten Sie bei Verwendung eines Internet Explorer-basierten Clients die Datei 'scwatch.cfg' folgendermaßen:
 

```
Action=c:\Program Files\internet explorer\iexplore.exe http://HP SAMServername
```
8. Starten Sie den Dienst wie folgt:
  - a. Klicken Sie auf **Start > Systemsteuerung > Verwaltung > Dienste**.
  - b. Klicken Sie mit der rechten Maustaste auf **HP Smart Card-Monitordienst**.
  - c. Wählen Sie **Start** aus.

Weitere Informationen über die HP SAM Smart Card-Einstellungen finden Sie unter [„Smart Card-Einstellungen“ auf Seite 47](#).

Anschließend können Sie die Smartcard-bezogenen Einstellungen im Web-Client konfigurieren. Rufen Sie von der HP SAM-Verwaltungskonsole aus **System Settings (Systemeinstellungen) > Web Client (Web-Client)** auf.

---

 **HINWEIS:** Die CAC ist ein äußerst sicherer Smart Card-Typ, der vom Militär eingesetzt wird. Ihr Verhalten in HP SAM entspricht dem typischer Smart Cards. HP SAM greift außer auf das Zertifikat, das zur Feststellung der Benutzerberechtigung erforderlich ist, auf keine weiteren Daten auf der CAC zu.

---

## Konfigurieren von Sitzungszeitbeschränkungen für Remote-Sitzungen

Mit HP CCI Session Timers können Administratoren die automatische Trennung oder Abmeldung von Remote-Sitzungen nach einer bestimmten Zeitspanne steuern. Die integrierten Sitzungs-Timer bieten die Möglichkeit, sowohl RGS- als auch RDP-Sitzungen zu steuern. Sie können Zeitbeschränkungen für **aktive Sitzungen**, **aktive Sitzungen im Leerlauf** und **getrennte Sitzungen** konfigurieren und außerdem die CPU-Überwachung für **aktive Sitzungen im Leerlauf** und für **getrennte Sitzungen** konfigurieren. Dadurch wird die Trennung oder Abmeldung verhindert, wenn die CPU-Auslastung über einem konfigurierbaren Schwellenwert bleibt. Dies ist nützlich, um sicherzustellen, dass Verbindungen nicht abgemeldet werden, während beispielsweise wichtige Berechnungen laufen.

Die Sitzungs-Timer bestehen aus zwei Hauptelementen:

- Einem Dienstprogramm (HPCCIST.EXE und zugehörige Dateien), das zusammen mit dem HP SAM Registrierungsdienst auf der Ressource installiert wird. HPCCIST.EXE ist so konfiguriert, dass das Dienstprogramm zusammen mit Windows gestartet, jedoch nur dann weiter ausgeführt wird, wenn eine Richtlinie festgelegt ist, die dies verlangt.
- Eine administrative Vorlage für Active Directory-Gruppenrichtlinien, über die Sie HP CCI Session Timers aktivieren können. Die administrative Vorlage (HPCCIST.ADM) befindet sich im Ordner C:\Windows\inf (sofern Windows im Ordner C:\Windows installiert ist).


So importieren Sie die Sitzungs-Timer in das Dienstprogramm „Gruppenrichtlinienverwaltung“ auf dem Domänencontroller:

1. Kopieren Sie die Datei HPCCIST.ADM auf den Domänencontroller.
2. Erstellen Sie in der Gruppenrichtlinienverwaltung auf dem Domänencontroller ein Gruppenrichtlinienobjekt (GPO).
  - ▲ Klicken Sie mit der rechten Maustaste auf **Gruppenrichtlinienobjekte**, und wählen Sie **Neu** aus.
3. Klicken Sie mit der rechten Maustaste auf das **GPO**, wählen Sie **Bearbeiten** aus, und bearbeiten Sie das GPO.
4. Klicken Sie mit der rechten Maustaste auf **Administrative Vorlagen**.
5. Klicken Sie auf **Hinzufügen**, und navigieren Sie zu **HPCCIST.ADM**.
6. Klicken Sie auf das neue GPO, und ziehen Sie es in Ihre OU (die Ihre Ressourcen enthält), um eine Verknüpfung zu erstellen.
7. Klicken Sie mit der rechten Maustaste auf das **GPO**, wählen Sie **Bearbeiten** aus, und bearbeiten Sie das GPO, um die Parameter für HP Sitzungs-Timer festzulegen.

Unter Windows 2003 Server befinden sich die Richtlinien für HP Sitzungs-Timer unter **Computerkonfiguration > Administrative Vorlagen > HP Client Consolidated Infrastructure**.

Unter Windows 2008 Server befinden sich die Richtlinien für HP Sitzungs-Timer unter **Computerkonfiguration > Richtlinien/Administrative Vorlagen > Klassische administrative Vorlagen > HP Client Consolidated Infrastructure**.

---

 **HINWEIS:** Für Benutzer können Sie diese Richtlinie auch unter **Benutzerkonfiguration** festlegen. Wenn widersprüchliche Richtlinien sowohl Computern als auch Benutzern zugewiesen sind, gilt die den Computern zugewiesene Richtlinie.

---

Nachdem die administrative Vorlage in das Dienstprogramm „Gruppenrichtlinienverwaltung“ auf dem Domänencontroller importiert wurde, stehen drei neue Richtlinien zur Verfügung:

- **Emulate Terminal Services Session Time Limits** (Sitzungszeitbeschränkungen von Terminaldiensten emulieren) – Diese Richtlinie steuert, ob die HP Sitzungs-Timer-Dienstprogramme die Gruppenrichtlinien der Microsoft Sitzungs-Timer emulieren. Dies ist für Ressourcen nützlich, auf denen Windows XP Pro mit Service Pack 2 oder niedriger läuft. Die Microsoft Sitzungs-Timer (für aktive Sitzungen, aktive Sitzungen im Leerlauf und getrennte Sitzungen) funktionieren sonst nicht mit diesen XP Versionen. Wenn diese Emulation aktiviert ist, funktionieren diese Richtlinien. Wenn auf der Ressource XP Pro mit Service Pack 3, Vista oder Windows 7 installiert ist, wird diese Emulation nicht benötigt.
- **Set CPU utilization time limit for active but idle remote sessions (Zeitlimit für Prozessorlast für aktive, aber im Leerlauf befindliche Remote-Sitzungen festlegen)** – Mit dieser Policy kann der Administrator festlegen, wie viel Zeit ohne Benutzereingabe (über Tastatur oder Maus) vergehen soll, bis der Systemstatus als Leerlauf gilt. An diesem Punkt wird durch einen anderen (vom Administrator festgelegten) Zeitraum definiert, wie lange die Prozessorlast auf dem System unter eine ebenfalls konfigurierte Schwelle fallen muss, bis der Benutzer getrennt oder abgemeldet wird (die Einstellungen werden jeweils vom Administrator vorgenommen). Der Administrator kann diese Einstellungen weiter feinabstimmen, indem er festlegt, wie viel Prozent des fraglichen Zeitraums die Prozessorlast unterhalb der Schwelle liegen muss, damit die Trennung oder Abmeldung veranlasst wird. Dies ist nützlich, weil dadurch eine begrenzte Menge an Prozessorlastspitzen zugelassen wird, das System aber dennoch irgendwann getrennt oder der Benutzer abgemeldet wird.
- **CPU-Auslastungszeitbeschränkung für getrennte Remote-Sitzungen festlegen** – Mit dieser Richtlinie kann der Administrator, ähnlich wie bei der vorangehenden, eine Zeitspanne festlegen, nach deren Ablauf die Sitzung getrennt wird. Wenn die CPU-Auslastung für diesen Zeitraum unter dem gewählten Schwellenwert bleibt, wird der Benutzer von der Ressource abgemeldet, sodass diese für andere Benutzer verfügbar wird.

Ausführliche Informationen zu diesen Einstellungen erhalten Sie, wenn Sie die Richtlinie im Dienstprogramm **Gruppenrichtlinienverwaltung** öffnen und dann auf die Registerkarte **Erklären** klicken.

Wenn der HP SAM Administrator keinen Zugriff auf den Domänencontroller hat, kann die Richtlinie stattdessen auf den einzelnen Ressourcen angewendet werden.

## Sitzungszeitgeber für Linux

HP SAM-Sitzungszeitgeber für Linux wurden hinzugefügt, um Administratoren von Linux-Ressourcen ähnliche Funktionalitäten zu ermöglichen, wie sie es früher nur für Windows-Ressourcen gab. Mit dem Zeitgeber können Benutzer getrennt oder abgemeldet werden, wenn sie über einen bestimmten Zeitraum angemeldet, angemeldet im Leerlauf oder getrennt gewesen sind. Bei dieser Funktion kann auch die Prozessorlast mit konfigurierbaren Schwellenwerten mitkonfiguriert werden.

Die Session-Timer für Linux sind als Datei im RPM-Format in einem herunterladbaren SAM-Paket enthalten. Nach dem Kopieren der RPM-Datei auf eine Linux-basierte Ressource kann sie mit folgendem Befehl installiert werden: `rpm -ivh <hpst-Datei>.rpm` (Beispiel: `rpm -ivh hpst-1.0.0-1.x86_64.rpm`).

Die diversen Sitzungszeitgebertypen (siehe Beschreibung unten) und ihre Optionen werden innerhalb der Konfigurationsdatei (`/etc/hpstd.conf`) auf jeder Ressource festgelegt. Damit diese Einstellungen wirksam werden, geben Sie den Befehl `/opt/hpstd/sbin/hpstd -reload` ein, nachdem Sie die Einstellungen in

der Konfigurationsdatei geändert haben. Die Zeitgeber für den Status Active (Aktiv) und Active But Idle (Aktiv, aber im Leerlauf) trennen den Benutzer, wenn der Zeitgeber ausgelöst wird. Die Zeitgeber für Disconnect Session (Sitzung trennen) melden den Benutzer von der betreffenden Ressource ab, wenn sie ausgelöst werden. Alle Zeitgeber funktionieren nur, wenn sie über das HP RGS-Protokoll verbunden sind. Sie eignen sich nicht für den Gebrauch mit Ressourcen, auf denen die Anmeldung lokal erfolgen soll.

Die folgenden Timertypen stehen zur Verfügung:

- Aktive Sitzungen – Ermöglicht dem Administrator, das Trennen der Verbindung zu erzwingen, wenn für die angegebene Zeitdauer eine Verbindung zum Benutzer bestand.
- Aktive Sitzungen im Leerlauf – Ermöglicht dem Administrator, das Trennen der Verbindung zu erzwingen, wenn eine Verbindung zum Benutzer besteht und für die angegebene Zeitdauer keine Aktivitäten erkennbar waren (d. h. keine Aktivitäten mit der Maus oder der Tastatur).
- Getrennte Sitzungen – Ermöglicht dem Administrator, eine Abmeldung zu erzwingen, sobald die angegebene Zeitdauer nach dem Trennen der Verbindung durch den Benutzer (manuell, über Timer oder Netzwerkunterbrechung) abgelaufen ist.
- Disconnected Sessions CPU Low (Sitzungen wegen geringer Prozessorlast getrennt) – Funktioniert wie der Zeitgeber Disconnected Sessions (Sitzungen trennen); allerdings wird der Benutzer nicht abgemeldet, solange die Prozessoraktivität oberhalb des angegebenen Schwellenwertes liegt. Dieser Zeitgeber ist hilfreich, weil dadurch die Abmeldung eines getrennten Benutzers verhindert wird, der noch prozessorintensive Aufgaben ausführt.
- Disconnected Sessions CPU High (Sitzungen wegen hoher Prozessorlast getrennt) – Dieser Zeitgeber funktioniert wie der Zeitgeber oben, außer dass er die Abmeldung erzwingt, wenn die Prozessoraktivität oberhalb des angegebenen Schwellenwertes liegt. Dadurch sollen Ressourcen frei gemacht werden, die möglicherweise in einer Endlosschleife festhängen.

Auf der Hilfeseite (man hpstd) finden Sie detaillierte Informationen und weitere Optionen.

## Ressourcenreservierungen (auch bekannt als Zugriffsbeschränkungen)

Über diese Funktion kann der Administrator festlegen, wann und von welchem Ort Benutzer auf Ressourcen zugreifen können. Sie ermöglicht auch die bedarfsgerechte Freisetzung von Ressourcen für andere Benutzer.

Durch Rolleneinstellungen kann der Administrator jetzt die Tageszeit und die Wochentage für den Quell-IP-Adressbereich angeben. Benutzer, denen eine bestimmte Rolle zugewiesen wurde, erhalten eine Ressource innerhalb dieser Rolle dann nur an dem bestimmten Tag während des angegebenen Zeitraums. In diesem Fall wird der Benutzer direkt zu einer Ressource in dieser Rolle geleitet, obwohl ihm viele andere Rollen zugeordnet sind. Bei diesem Vorgang wird kein Dialog für die Rollenauswahl angezeigt. Außerhalb des IP-Adressbereichs und des Zeitfensters wird dem Benutzer der Zugriff auf die Rolle verweigert. Jeder Rolle können zahlreiche solcher Reservierungen zugewiesen werden.

Standardmäßig wird der Benutzer am Ende des reservierten Zeitraums von der Ressource abgemeldet. Die Option **Allow time extension (Zeitverlängerung zulassen)** kann so eingestellt werden, dass ein Benutzer über den Ablauf der derzeitigen reservierten Ressourcenzeit hinaus angemeldet bleiben kann. Der Benutzer kann solange angemeldet bleiben, bis ein anderer Ressourcenreservierungszeitraum für dieselbe Rolle beginnt (oder um Mitternacht, wenn keine anderen




Reservierungen eingestellt sind). Ein Dialog warnt den Benutzer, bevor die Abmeldung erfolgt. Die Vorlaufzeit für diese Warnmeldung kann in den System Settings (Systemeinstellungen) auf der Seite General (Allgemein) der HP SAM-Verwaltungskonsole konfiguriert werden.

Beispielsweise kann eine Schule durch die Verwendung von Ressourcenreservierungen sicherstellen, dass den Schülern jeder Klasse eine Ressource von der richtigen Rolle bereitgestellt wird, und dafür sorgen, dass die Ressourcen innerhalb derselben Rolle rechtzeitig für einen später abgehaltenen Unterricht freigegeben werden. Der Administrator kann eine Reservierung für die Rolle **Mathematikklasse** einrichten und dazu den IP-Adressbereich eines bestimmten Unterrichtsraums und den Tag einschließlich der Uhrzeit angeben, an dem der Mathematikunterricht stattfindet. Ein Schüler, der sich am richtigen Tag und zur richtigen Uhrzeit an einem Computer in diesem Unterrichtsraum anmeldet, erhält eine Ressource aus der Rolle **Mathematikklasse**, ohne eine bestimmte Rolle auswählen zu müssen. Er kann diese Ressource bis zum Unterrichtsende nutzen. Eine weitere für die Rolle **Mathematikklasse** eingerichtete Reservierung kann für dieselbe(n) Ressource(n) gelten, die zu einem späteren Zeitpunkt einer anderen Mathematikklasse in einem anderen Raum bereitgestellt werden. Durch die automatische Abmeldung ist sichergestellt, dass die Ressourcen den Schülern der späteren Mathematikklasse zur Verfügung stehen.

Wenn sich der HP SAM Server und die Zugriffsgeräte in unterschiedlichen Zeitzonen befinden, gelten die im Rahmen der Ressourcenreservierung festgelegten Uhrzeiten für das Zugriffsgerät und nicht für den Server. Beispielsweise befindet sich der HP SAM Server in der Zeitzone Central Standard Time, und für die Reservierung wurde als Uhrzeit 16:00 Uhr angegeben. Dies entspricht der Uhrzeit 16:00 Uhr des in der Zeitzone Pacific Standard Time befindlichen Zugriffsgeräts (obwohl das Betriebssystem des HP SAM Servers 18:00 Uhr als Uhrzeit anzeigt.) Sie müssen sich also vergewissern, dass auf allen beteiligten Systemen die korrekten Uhrzeiten und Zeitzonen eingestellt sind.

Die Zeit für die automatische Abmeldung wird der Ressource bei der Benutzeranmeldung zugewiesen. Diese Zeit wird nicht aktualisiert, wenn die Reservierungen später auf dem Server aktualisiert werden. Ist ein Benutzer beispielsweise während einer Reservierung angemeldet, die von 14 bis 15 Uhr festgelegt wurde und für die die Option **Allow time extensions (Zeitverlängerungen zulassen)** aktiviert wurde und ist die nächste Reservierung für 17 bis 18 Uhr festgelegt, so wird der Benutzer um 17 Uhr von der Ressource abgemeldet. Wenn der HP SAM-Administrator nach der Anmeldung des Benutzers für den ersten Reservierungszeitraum eine neue Reservierung einrichtet, die bereits um 16 Uhr beginnt, so wird der Benutzer dennoch erst um 17 Uhr abgemeldet. Mit den Funktionen des Logoff Scheduler (Abmeldeplaners, [„Log Off User from Resource Scheduler \(Benutzer vom Ressourcenplaner abmelden\)“](#) auf Seite 86) kann eine Abmeldezeit kurz vor 16 Uhr eingestellt werden, um sicherzustellen, dass die Ressourcen für die neu eingerichtete Reservierung auch frei sind. Ein manueller oder programmierter Synchronisierungsvorgang hat keinerlei Auswirkungen auf die Reservierungen von Ressourcen.

 **HINWEIS:** Diese Funktion wird nur für Ressourcen unterstützt, auf denen ein Windows Betriebssystem installiert ist.

Während der Verwendung dieser Funktion dürfen keine Ressourcen genutzt werden, die mehreren Rollen zugewiesen sind. Dies kann dazu führen, dass keine automatische Abmeldung erfolgt, wenn die Ressource für eine Reservierung benötigt wird, die für eine der anderen Rollen der Ressource erstellt wurde.

Mit zwei anderen Funktionen von HP SAM lässt sich die Anzeige des Rollenauswahldialogs für Benutzer umgehen, denen mehrere Rollen zugeordnet sind: **Monitorlayouts** und **Automatische Verbindung für mehrere Sitzungen**. Bei einem Konflikt hat **Monitorlayouts** Vorrang vor der Funktion **Ressourcenreservierungen**, die wiederum Vorrang vor der Funktion **Automatische Verbindung für mehrere Sitzungen** hat.

## Vor Zuweisung authentifizieren

Die Aktivierung dieser Funktion verbessert die Sicherheit. Der Benutzer wird aufgefordert, zur Authentifizierung durch Active Directory seinen Benutzernamen und sein Passwort am HP SAM Client einzugeben. Erst dann wird ihm eine Ressource zugeteilt oder eine Liste der Rollen und Ressourcen angezeigt. Dadurch ist nun auch ausgeschlossen, dass ein Benutzer von Active Directory gesperrt wird, weil er bei dem Versuch, gleichzeitig eine Verbindung zu mehreren Ressourcen herzustellen, ein falsches Passwort eingegeben hat. Diese Funktion ist standardmäßig deaktiviert.


Im deaktivierten Zustand entspricht das Verhalten dieser Funktion dem Verhalten früherer Versionen von HP SAM, bei denen die Passwortauthentifizierung erst bei der Anmeldung beim Ressourcenbetriebssystem erfolgt.

Zur Aktivierung dieser Funktion sind folgende Konfigurationseinstellungen vorzunehmen:

- Aktivieren Sie **Authentication before Allocation (Vor Zuweisung authentifizieren)** auf der Seite General (Allgemein) in den System Settings (Systemeinstellungen) der HP SAM-Verwaltungskonsole.
- Versichern Sie sich, dass ein Zertifikat von der Domain-Zertifizierungsstelle auf der HP SAM-Website in IIS auf dem HP SAM-Server installiert ist.
- Über die HP SAM Client-Konfigurationsdatei muss auf allen Zugriffsgeräten die folgende Option aktiviert sein: `AuthenticateBeforeAllocation=1`.
- Für den Web-Client ist kein Setup erforderlich, aber der Benutzer muss die URL mit `https` eingeben anstatt mit `http` (Beispiel: `https://samserver`).
- Stellen Sie sicher, dass die Kommunikation zwischen dem Zugriffsgerät und dem HP SAM Server via SSL (normalerweise Port 443) nicht von einer Firewall blockiert wird.

Über die Einstellung **Abgelaufenes Passwort zulassen** in den Systemeinstellungen kann der HP SAM Administrator Benutzern mit abgelaufenen Passwörtern die Weiterarbeit ermöglichen, damit Sie das Passwort im Betriebssystem der Ressource ändern können.

---

 **HINWEIS:** Wenn diese Funktion aktiviert ist, können keine Versionen des HP SAM Clients vor HP SAM 2.3 verwendet werden.

Diese Funktion ist nicht mit der Single-Sign-On-Anmeldung über eine Smart Card kompatibel und muss vor der Verwendung von Smart Cards deaktiviert werden.

---


# A Firewall-Regeln

In diesem Anhang finden Sie eine Auflistung der Regeln, die für die Kommunikation zwischen den verschiedenen Komponenten erforderlich sind. Die Werte in Klammern stellen Anschlüsse dar. BELIEBIG steht für einen beliebigen Anschluss auf dieser Komponente.

## Webserver

- Eingehend:
  - Von Clients (TCP/ALLE) zum Webserver (TCP/80-HTTP)
  - Von Clients (TCP/ALLE) zum Webserver (TCP/443-HTTPS)
  - Von Blades (TCP/ALLE) zum Webserver (TCP/80-HTTP)
  - Von admin\_workstation (TCP/ALLE) zum Webserver (TCP/443-HTTPS)
  - Von Ressourcen (UDP/47777) zum Webserver (UDP/47777-Benutzerdefiniert)
- Abgehend:
  - Vom Webserver (TCP/ALLE) zu SQL\_Server (TCP/1433-MSSQL)
  - Vom Webserver (TCP/ALLE) zu den Ressourcen (TCP/139-RPC)
  - Vom Webserver (UDP/47777) zu den Ressourcen (UDP/47777-Benutzerdefiniert)

## Clients

- Eingehend:
  - Keine
- Abgehend:
  - Von Clients (ALLE) zum Webserver (TCP/80-HTTP)
  - Von Clients (BELIEBIG) zu Ressourcen (TCP/80–3389-RDP)
  - Von Clients (BELIEBIG) zu Ressourcen (TCP/42966–RGS)
  -  **HINWEIS:** Der Standard-RGS-Port ist TCP/42966; allerdings kann diese Einstellung in RGS 5.3 und höher geändert werden. Für nähere Informationen wird auf die RGS-Dokumentation verwiesen.
  - Von Clients (ALLE) zum Webserver (TCP/443-HTTPS)

## Ressourcen

- Eingehend:
  - Vom Webserver (UDP/47777) zu den Ressourcen (UDP/47777-Benutzerdefiniert)
  - Vom Webserver (TCP/ALLE) zu den Ressourcen (TCP/139-RPC)
  - Von Clients (TCP/BELIEBIG) zu Ressourcen (TCP/3389-RDP)
  - Von Clients (TCP/BELIEBIG) zu Ressourcen (TCP/42966-RGS)
- 📄 **HINWEIS:** Der Standard-RGS-Port ist TCP/42966; allerdings kann diese Einstellung in RGS 5.3 und höher geändert werden. Für nähere Informationen wird auf die RGS-Dokumentation verwiesen.
- Abgehend:
  - Von Ressourcen (TCP/ALLE) zum Webserver (TCP/80-HTTP)
  - Von Ressourcen (UDP/47777) zum Webserver (UDP/47777)

## SQL-Server

(nur wenn die Ausführung nicht auf demselben Rechner erfolgt wie dem Webserver)

- Eingehend:
  - Vom Webserver (TCP/ALLE) zu SQL\_Server (TCP/1433)
- Abgehend:
  - Keine

# B Häufig gestellte Fragen (FAQ)

Frage	Antwort
Warum müssen manche Benutzer auf dem HP SAM Client eine Rolle oder Ressource auswählen und andere nicht?	Benutzer mit mehreren Rollen, müssen für die Verbindung eine Rolle auswählen. Benutzern mit nur einer Rolle wird dieser Bildschirm nicht angezeigt. Ein Benutzer, dem nur eine dedizierte Ressource zugewiesen wurde, muss keine Rolle auswählen. Bei der Verwendung von Monitorlayout-IDs, automatischen Verbindungen für mehrere Sitzungen oder Ressourcenreservierungen wird der Benutzer ebenfalls nicht zur Auswahl einer Rolle oder Ressource aufgefordert.
Kann der Benutzer vom selben Client-Zugriffsgerät aus Verbindungen zu mehreren Rechnerressourcen herstellen?	Ja. Wenn dem Benutzer mehrere Ressourcen zugewiesen wurden, kann er auch eine Verbindung zu diesen herstellen. Wenn der Benutzer über mehrere Rollen verfügt, kann er über jede Rolle eine Verbindung zu einer Ressource herstellen.
Warum ist mein Blade als offline gekennzeichnet, obwohl ich über die Remotedesktopverbindung eine Verbindung zu ihm herstellen kann?	Überprüfen Sie die Firewall-Einstellungen auf der Rechnerressource, um sicherzustellen, dass der HP SAM Port (47777) eine eingehende Verbindung zulässt.
Mein Benutzer kann keine Verbindung zu einer Rechnerressource auf dem Browser-basierten Web-Client herstellen. Wie kommt das?	Überprüfen Sie, ob der Server in Betrieb ist und ob Ihre Firewall-Einstellung Port 3389 für IEXPLORE.EXE zulässt.
Warum wechselt mein Client nicht zum Failover-Server in meiner Liste?	Vergewissern Sie sich, dass Ihre .SAM-Datei die Einstellung FAILOVER=1 enthält
Warum werden meine Benutzer bei jedem Auftreten eines Netzwerkfehlers aufgefordert, die Verbindung über den HP SAM Client erneut herzustellen?	Die Einstellung Auto-Reconnect (Automatisch wiederverbinden) ist ausgeschaltet ( <b>OFF (AUS)</b> ). Wenn Ihr Netzwerk so konfiguriert ist, dass die Benutzer abgemeldet werden, wenn sie getrennt werden oder das Zeitlimit überschritten ist, wird der Benutzer bei jeder Netzwerkunterbrechung, durch die der Benutzer getrennt wird oder ein Zeitlimit überschreitet, ebenfalls abgemeldet. Ein anderer Benutzer könnte sich dann verbinden. Wenn die Einstellung Auto-Reconnect (Automatisch wiederverbinden) eingestellt ist ( <b>On (Ein)</b> ), kann sich der ursprüngliche Benutzer in einem solchen Fall automatisch wiederverbinden und der neue Benutzer wird abgewiesen. HP empfiehlt, Auto-Reconnect (Automatisch wiederverbinden) auszuschalten ( <b>OFF (AUS)</b> ).
Warum sind meine Einstellungen nicht wirksam, wenn ich sie auf der Clientseite vornehme?	Die Einstellungen auf der Clientseite sind möglicherweise von den erzwungenen Einstellungen auf dem HP SAM Server in der Registerkarte <b>Richtlinie</b> außer Kraft gesetzt worden. Außerdem werden Einstellungen ignoriert, die für das verwendete Protokoll nicht gültig sind.

Frage	Antwort
<p>Warum muss mein Benutzer das Passwort bei jeder Anmeldung bei einer Rechnerressource zweimal eingeben?</p>	<p>Dies darf eigentlich nicht vorkommen. Die Active-Directory-Policy verlangt, dass sich der Benutzer interaktiv auf dem Blade anmeldet. Deaktivieren Sie diese Policy, oder entfernen Sie das <b>Password (Passwort)</b>-Feld vom HP SAM-Client, indem Sie in der .SAM-Datei den Wert PasswordEnable=0 konfigurieren. Eine andere Ursache könnte auch die Verwendung von RGS im Easy-Login- oder Standardmodus sein.</p>
<p>Bei der Installation des Upgrades für den Registrierungsdienst tritt ein Fehler auf.</p>	<p>Prüfen Sie, ob das Ereignisprotokoll geöffnet ist. Wenn ja, müssen Sie das Protokoll schließen, damit das Programm die alte ausführbare Datei löschen und durch die neue ersetzen kann.</p>
<p>Wie aktiviere ich HP Sygate Security Agent auf dem Windows XP Embedded-basierten Thin Client für die HP SAM Clients?</p>	<p>Rufen Sie die erweiterten Regeln für den HP Sygate Security Agent auf und erstellen Sie eine neue Regel für HP SAM. Fügen Sie IEXPLORE.EXE und/oder hprdcw32.exe auf der Registerkarte <b>Application (Anwendung)</b> hinzu. Wählen Sie auf der Registerkarte <b>Ports and Protocol (Ports und Protokoll)</b> das Protokoll <b>TCP</b> und geben Sie 80,443,3389,42966 in die Remote-Port-Zeile ein, wenn beide Clients funktionieren sollen. Anderenfalls versichern Sie sich, dass für <b>IEXPLORE</b> der Port 3389 gewählt ist. Sie können einen der Ports 80, 443, 3389 oder 42966 für den Windows-basierten Client festlegen oder gar keinen Port angeben (<b>All (Alle)</b>). Für erweiterte Methoden wie ein Altiris-Skript können Sie das Skript hier in ähnlicher Weise erstellen oder mit dem Tool HP Sygate Security Agent Policy Editor arbeiten (dieses können Sie als SoftPac von der HP-Website herunterladen).</p>
<p>Ich kann die japanischen Zeichen nicht auf dem Web-Client anzeigen.</p>	<p>Prüfen Sie, ob auf dem Zugriffsgerät japanische Fonts installiert sind.</p>
<p>Kann ich den HP SAM Server über einen anderen Browser, z. B. Opera oder Firefox, verwalten?</p>	<p>Nein, diese Browser werden nicht unterstützt.</p>

---

**Frage**

Wie kann ich als http- und als https-Port für den HP SAM-Webserver andere Werte als die Standardwerte 80 und 443 festlegen?

**Antwort**

Nachdem Sie den gewünschten Wert (TCP- und/oder SSL-Ports) im Internet Information Services (IIS) Manager geändert haben, ändern Sie die CONNECTION.CONFIG-Datei. Diese befindet sich auf dem HP SAM-Webserver im Stammordner des HP SAM-Installationsverzeichnis (normalerweise: c:\Programme\Hewlett-Packard\HP SAM). Bearbeiten Sie die Datei mit dem Editor. Ändern Sie die folgenden drei Zeilen:

```
<!-- add key="ClientServiceURL" value="http://samservername:80" /-->
```

```
<!--add key="ResourceServiceURL" value="http://samservername:80" /-->
```

```
<!--add key="AdministrativeConsoleURL" value="http://samservername:80" /-->
```

In:

```
<add key="ClientServiceURL" value="http://sam_server_name:port_number" />
```

```
<add key="ResourceServiceURL" value="http://sam_server_name:port_number" />
```

```
<add key="AdministrativeConsoleURL" value="http://sam_server_name:port_number"/>
```

Dabei ist `sam_server_name` der Name des HP SAM Servers und der `http-Port` entspricht dem Wert `port_number`, der in IIS Manager festgelegt wurde (nicht der Wert des SSL-Ports).

Wenn Sie nur den Wert des *SSL-Ports* in IIS Manager ändern, müssen Sie dennoch die Datei CONNECTION.CONFIG wie oben beschrieben ändern. Verwenden Sie in keiner der obigen Zeilen die Schreibweise HTTPS.

Wenn Sie den *TCP-Port* ändern, müssen Sie die Konfigurationsdatei vom HP SAM-Registrierungsdienst `hpevent.cfg` auf allen Rechnerressourcen aktualisieren, damit der neuer `http-Port` für den Webserver verwendet wird (Beispiel: *IhrHPSAMservername:8080*). Außerdem müssen Sie alle Zugangsgeräte aktualisieren, damit sie denselben `http-Port` verwenden.

**HINWEIS:** Sie müssen auch die Firewall-Ausnahmen entsprechend aktualisieren.

---

Frage	Antwort
<p>Wie lege ich für den HP SAM Datagramm-Kommunikationsanschluss einen anderen Wert als den Standardwert 47777 fest?</p>	<p>Ändern Sie die Datei <b>connection.config</b>. Diese befindet sich auf dem HP SAM-Webserver im HP SAM-Installationsverzeichnis (normalerweise handelt es sich um den Pfad c:\Programme\Hewlett-Packard\HP SAM). Bearbeiten Sie die Datei mit dem Editor. Fügen Sie diese Zeile in den Abschnitt <b>appSettings</b> ein:</p> <pre data-bbox="855 422 1321 447">&lt;add key="ProtocolChannel" Value="port number"/&gt;</pre> <p>Im obigen Codeausschnitt gibt <i>port number</i> (Anschlussnummer) den neuen HP SAM Datagramm-Kommunikationsanschluss an, den Sie nutzen möchten.</p> <p>Sie müssen den HP Session Allocation Management Service auf dem HP SAM-Webserver beenden und neu starten. Sie müssen außerdem den HP SAM-Registrierungsdienst in der hpevent.cfg-Datei auf allen Rechnerressourcen aktualisieren, damit sie denselben HP SAM-Datagramm-Kommunikationsport verwenden. Führen Sie anschließend einen Neustart des HP SAM-Registrierungsdienstes auf allen Rechnerressourcen durch. Aktualisieren Sie ebenfalls die entsprechenden Firewall-Regeln auf dem HP SAM-Webserver und den Rechnerressourcen.</p>
<p>Kann ich Doppelbyte-Zeichen im Benutzernamen verwenden?</p>	<p>Nein. HP SAM unterstützt nur Einzelbyte-Zeichen.</p>
<p>Ich erhalte Warnmeldungen, wenn ich in einer asiatischen Sprache mit Doppelbyte-Zeichensatz (DBCS) auf der HP SAM-Verwaltungskonsole arbeite und numerische Werte in die Registerkarte <b>System Settings (Systemeinstellungen)</b> eingebe.</p>	<p>Die HP SAM-Verwaltungskonsole nimmt nur Einzelbyte-Zahlen als Werte an.</p>
<p>Warum sehe ich manchmal Liniendiagramme im Resource Capacity Consumption Report (Ressourcenauslastungsbericht) in der HP SAM-Verwaltungskonsole und manchmal nicht?</p>	<p>Versichern Sie sich, dass die Browsersprache, in der Sie den Bericht anzeigen, mit der Sprache des Betriebssystems vom HP SAM-Webserver übereinstimmt. Beispiel: Wenn Sie die HP SAM-Verwaltungskonsole auf Deutsch anzeigen, muss die Sprache des Betriebssystems für den HP SAM-Webserver ebenfalls Deutsch sein.</p>
<p>Das Internet Explorer-Fenster „AutoVervollständigen“ verdeckt das HP SAM Suchfenster „Neue Benutzer hinzufügen“. Wie kann ich meine Suchergebnisse sehen?</p>	<p>Deaktivieren Sie die Funktion „AutoVervollständigen“ von Internet Explorer für Formularfelder:</p> <ol data-bbox="855 1381 1410 1591" style="list-style-type: none"> <li>1. Klicken Sie in der Menüleiste von Internet Explorer auf <b>Extras</b>.</li> <li>2. Wählen Sie unter „Internetoptionen“ die Registerkarte <b>Inhalte</b> aus, und klicken Sie auf <b>AutoVervollständigen</b>.</li> <li>3. Deaktivieren Sie das Kontrollkästchen <b>Formulare</b>.</li> </ol>
<p>Ich habe einen Benutzer als HP SAM-Administrator hinzugefügt, aber diese Kollegin kann sich nicht bei der HP SAM-Verwaltungskonsole anmelden.</p>	<p>Vergewissern Sie sich, dass in der Administratoren-Gruppenrichtlinie die lokale Anmeldung zugelassen ist. Dies gilt für Benutzer, die nicht zur lokalen Serveradministratorgruppe, jedoch zur HP SAM Administratorgruppe gehören.</p> <p>Computerkonfiguration\Lokale Richtlinien\Zuweisen von Benutzerrechten\Lokal anmelden zulassen</p>



---

<b>Frage</b>	<b>Antwort</b>
Ich sehe eine allgemeine Fehlermeldung der HP SAM-Verwaltungskonsole – wie kann ich genauere Informationen über den Fehler erhalten?	Aus Sicherheitsgründen können Details zu manchen Fehlerarten nicht remote angezeigt werden. Wenn Sie den Fehler direkt auf dem HP SAM reproduzieren, können Sie die Details und einen Stack-Trace anzeigen, aus denen Sie ggf. die Ursache des Fehlers ersehen können. Diese Informationen können auch vom Supportpersonal benötigt werden, um das Problem zu diagnostizieren.

---

Frage	Antwort
<p>Die Benutzer erhalten die Meldung <b>All resources are currently in use. Please try again later. (Alle Ressourcen sind derzeit besetzt. Bitte versuchen Sie es später erneut.)</b>, aber auf der HP SAM-Verwaltungskonsole sieht es so aus, als gäbe es noch freie Ressourcen. Was sind die möglichen Ursachen hierfür?</p>	<p>Aktualisieren Sie zunächst die Ressourcenliste in der HP SAM-Verwaltungskonsole und prüfen Sie, ob Ressourcen in der Rolle (bzw. reservierten Ressource) verfügbar sind, auf die der Benutzer zuzugreifen versucht. Wenn keine Ressourcen als <b>Available (Verfügbar)</b> angezeigt werden, führen Sie einen Synchronisierungsvorgang auf allen Ressourcen durch, um sicherzustellen, dass ihr Status aktuell ist. Wenn dann immer noch keine Ressourcen als <b>Available (Verfügbar)</b> angezeigt werden, ist die Meldung richtig, und weitere Ressourcen können zum Pool hinzugefügt werden, oder mithilfe der HP SAM-Sitzungszeitgeber können im Leerlauf befindliche Ressourcen frei gemacht werden.</p> <p>Wenn Ressourcen als <b>Verfügbar</b> angezeigt werden, aber Benutzer weiterhin diese Meldung erhalten, ziehen Sie die folgenden Ursachen in Betracht:</p> <ul style="list-style-type: none"> <li>• Einige Ressourcen sind in HP SAM als deaktiviert markiert.</li> <li>• Einige Ressourcen sind einem Benutzer als dedizierte Ressource zugewiesen. Überprüfen Sie auf der Seite „Benutzer verwalten“, ob diese Ressourcen als dedizierte Ressourcen für Benutzer angezeigt werden.</li> </ul> <p><b>HINWEIS:</b> Wenn eine Ressource in einer Rolle enthalten und außerdem für einen Benutzer dediziert ist, wird sie nie einem Benutzer zugewiesen, der eine Ressource anfordert, die diese Rolle verwendet. In anderen Worten ist sie nur für diesen Benutzer allein dediziert.</p> <ul style="list-style-type: none"> <li>• Einige Ressourcen sind möglicherweise vorübergehend reserviert. Wenn HP SAM eine Ressource zu einem Benutzer zuweist, reserviert das Programm die Ressource für den betreffenden Benutzer für einen bestimmten Zeitraum (standardmäßig 3 Minuten), um dem Benutzer Zeit für die Anmeldung zu geben. Während dieser Zeit wird die Ressource in HP SAM als <b>Available (Verfügbar)</b> angezeigt, obwohl kein Benutzer angemeldet ist; sie kann jedoch nicht einem anderen Benutzer zugewiesen werden.</li> </ul> <p><b>HINWEIS:</b> Dieses Szenario kann häufiger auftreten, wenn diese Zeitdauer erhöht wird. Dieser Wert wird über die Option „Zeitlimit für Benutzeranmeldung“ unter "Einstellungen   Allgemein" festgelegt.</p> <ul style="list-style-type: none"> <li>• Überprüfen Sie, ob der HP Session Allocation Management Service auf dem HP SAM-Server ausgeführt wird. Normalerweise gehen Ressourcen vom Netz, wenn sich Benutzer anzumelden versuchen, ohne dass dieser Dienst ausgeführt wird.</li> <li>• Überprüfen Sie, ob der HP SAM-Kommunikationsport (UDP 47777, standardmäßig) nicht durch eine Firewall blockiert ist. Dies ist der Port, über den der HP SAM-Registrierungsdienst und der HP SAM-Server den Blade-Status kommunizieren. Normalerweise gehen Ressourcen vom Netz, wenn Benutzer sich anzumelden versuchen und dieser Port blockiert ist.</li> <li>• Überprüfen Sie, ob die Ressourcen das gewünschte Protokoll in der HP SAM-Verwaltungskonsole ausweisen. Beispiel: Wenn die HP SAM-Clients so konfiguriert sind, dass die Verbindung NUR über RGS aufgebaut werden kann, dann werden Ressourcen, die als <b>Available (Verfügbar)</b> angezeigt werden, die jedoch nicht das</li> </ul>

---

<b>Frage</b>	<b>Antwort</b>
Warum wird einem Benutzer, dessen Sicherheitsgruppe HP SAM aus einer untergeordneten Domäne hinzugefügt wurde, die Fehlermeldung „Ihr Konto konnte keinen vorhandenen Benutzerrollen zugewiesen werden“ angezeigt?	Dieser Fehler kann auftreten, wenn der Benutzer bei der Anmeldung bei HP SAM seinen Benutzernamen im Format UPN (Benutzer@Domäne.dom) eingibt. Bei Verwendung des UPN-Formats prüft HP SAM den globalen Katalog auf Gruppenmitgliedschaften in Active Directory. Lokale und globale Sicherheitsgruppen werden dabei nicht angezeigt. Der Administrator kann in diesem Fall entweder die Sicherheitsgruppe in eine universale Sicherheitsgruppe ändern oder den Benutzer anweisen, bei der Anmeldung nicht das UPN-Format zu verwenden.
Ich habe meine HP SAM Datenbank von einer Bandsicherung wiederhergestellt, nachdem der HP SAM SQL-Server nach einem unerwarteten Ausfall wiederhergestellt wurde. Genügt eine Synchronisierung, um den aktuellen Status aller Rechnerressourcen abzurufen?	Das hängt davon ab, wann die Datenbanksicherung durchgeführt wurde. Neue Rechnerressourcen wurden möglicherweise registriert, nachdem die letzte Sicherung durchgeführt wurde. Ist dies der Fall, so sind die betreffenden Rechnerressourcen in den Sicherungsdaten nicht vorhanden. Der Synchronisierungsvorgang funktioniert nur auf Rechnerressourcen, die dem System bekannt sind. Wenn der Status der betreffenden Rechnerressourcen offline, getrennt oder online war, als der SQL-Server ausfiel, dann müssen Sie die betreffenden Rechnerressourcen suchen und wieder zum HP SAM-System hinzufügen. Dazu müssen Sie den Registrierungsdienst auf den betreffenden Geräten beenden und neu starten. Wenn Sie nicht sicher sind, beenden Sie den Registrierungsdienst auf allen Rechnerressourcen und starten Sie ihn wieder neu. Diese Aktion hat keine Auswirkungen auf aktuelle Benutzer, die die Rechnerressourcen aktiv benutzen.

---

---

## C Registrierungsdienst – Fehlercodes

Im Folgenden ist eine Liste mit möglichen Fehlern aufgeführt, die der Registrierungsdienst in das Ereignisprotokoll auf der Rechnerressource schreiben könnte. Wenn Sie ein Problem auf dem Blade feststellen, notieren Sie sich den Fehlercode und wenden Sie sich an das Support-Team.

BC0001–Interner Fehler beim Zugriff auf WMI. Wenden Sie sich an Ihr HP SAM Support-Team.

BC0002–Interner Fehler beim Zugriff auf WMI. Wenden Sie sich an Ihr HP SAM Support-Team.

BC0003–Interner Fehler verhinderte die Erzeugung von Threads, im Allgemeinen aufgrund eines geringen Arbeitsspeichers. Schließen Sie andere Anwendungen oder erweitern Sie den verfügbaren Speicher.

BC0005–Interner Fehler. Wenden Sie sich an Ihr HP SAM Support-Team.

BC0006–Interner Fehler, im Allgemeinen aufgrund von Problemen im Zusammenhang mit einem geringen Arbeitsspeicher. Schließen Sie andere Anwendungen oder erweitern Sie den verfügbaren Speicher.

BC0007–Aktualisierungs-Thread konnte nicht erzeugt werden. Interner Fehler, möglicherweise aufgrund eines geringen Arbeitsspeichers. Schließen Sie andere Anwendungen, oder erweitern Sie den verfügbaren Speicher.

BC0008–Dienst konnte nicht gestartet werden (OpenSCManager()-Fehler). Stellen Sie sicher, dass der Dienst über das Zugriffsgerätekonto mit ausreichenden Berechtigungen zum Starten/Anhalten des Dienstes ausgeführt wird.

BC0009–Dienst konnte nicht gestartet werden (OpenService()-Fehler). Stellen Sie sicher, dass der Dienst über das Zugriffsgerätekonto mit ausreichenden Berechtigungen zum Starten/Anhalten des Dienstes ausgeführt wird.

BC0010–Dienst konnte nicht gestartet werden (StartService()-Fehler). Stellen Sie sicher, dass der Dienst über das Zugriffsgerätekonto mit ausreichenden Berechtigungen zum Starten/Anhalten des Dienstes ausgeführt wird.

BC0011–Dienst konnte nicht gestartet werden (Statusüberprüfungsfehler). Stellen Sie sicher, dass der Dienst über das Zugriffsgerätekonto mit ausreichenden Berechtigungen zum Starten/Anhalten des Dienstes ausgeführt wird.

BC0012–Interner Fehler beim Einrichten des Dienstes. Stellen Sie sicher, dass der Dienst über das Zugriffsgerätekonto mit ausreichenden Berechtigungen zum Starten/Anhalten des Dienstes ausgeführt wird.

BC0013–Dienstkonfigurationsdatei (Tattoo) konnte nicht gefunden werden. Den Listenordner, in dem angegeben ist, wo die CFG-Datei gespeichert werden muss, damit der Dienst Lesezugriff darauf hat, finden Sie im Abschnitt über die Registrierungsdienst-Installation weiter oben.

BC0014–Gateway-Abschnitt in der Konfigurationsdatei konnte nicht gefunden werden. Hinweise, wie der korrekte Inhalt der CFG-Datei erstellt wird, finden Sie im Abschnitt über die Registrierungsdienst-Installation weiter oben.

BC0015–Interner Programmfehler. Wenden Sie sich an Ihr HP SAM Support-Team.

BC0016–Interner Programmfehler. Wenden Sie sich an Ihr HP SAM Support-Team.

BC0017–Interner Programmfehler. Wenden Sie sich an Ihr HP SAM Support-Team.

BC0018–Interner Programmfehler. Wenden Sie sich an Ihr HP SAM Support-Team.

BC0020–Speicherzuordnungsfehler. Schließen Sie andere Anwendungen, oder erhöhen Sie den verfügbaren Speicher.

BC0021–Speicherzuordnungsfehler. Schließen Sie andere Anwendungen, oder erhöhen Sie den verfügbaren Speicher.

BC0022–Speicherzuordnungsfehler. Schließen Sie andere Anwendungen, oder erhöhen Sie den verfügbaren Speicher.

BC0023–Interner Fehler. Wenden Sie sich an Ihr HP SAM Support-Team.

BC0024–Interner Fehler. Wenden Sie sich an Ihr HP SAM Support-Team.

BC0025–Interner Fehler. Wenden Sie sich an Ihr HP SAM Support-Team.

BC0026–Kommunikationsfehler mit dem Subsystem „Terminaldienste“. Wenden Sie sich an Ihr HP SAM Support-Team.

BC0028–UDP-Server-Port konnte nicht eingerichtet werden. Überprüfen Sie, ob ein anderes Programm bereits denselben UDP-Port nutzt (in der Regel ist die Standardeinstellung Port 47777).

BC0029–Vom Netzwerk konnten keine UDP-Daten empfangen werden (recvfrom() failed). Überprüfen Sie Ihre Netzwerk- und/oder Firewall-Einstellungen.

BC0030–Keine Reaktion des Servers auf „SYNC“-Aufforderung (Synchronisieren). Das kann dazu führen, dass der Computer während der Synchronisierung als „offline“ markiert wird. Überprüfen Sie Ihre Netzwerk- und/oder Firewall-Einstellungen.

BC0032–Keine Reaktion des Servers auf „PRECONNECT“-Aufforderung (Herstellen einer Verbindung vor dem Aufbauen einer Verbindung zum Server). Das kann dazu führen, dass der Computer bei der Zuordnung ausgelassen wird. Überprüfen Sie Ihre Netzwerk- und/oder Firewall-Einstellungen.

BC0035—No gateway/web server defined (Kein Gateway/Webserver definiert). Oben im Abschnitt über die Installation des Registrierungsdienstes sehen Sie, wie Sie den Inhalt der CFG-Datei richtig erstellen können.

BC0036—Failed to connect to gateway/web server (Verbindung zum Gateway/Webserver fehlgeschlagen). Oben im Abschnitt über die Installation des Registrierungsdienstes erhalten Sie Informationen darüber, wie Sie den Inhalt der CFG-Datei richtig erstellen können. Achten Sie darauf, dass der Servername richtig angegeben und dass der Server unter dem Namen erreichbar ist.

BC0037—Failed to connect to gateway/web server (Verbindung zum Gateway/Webserver fehlgeschlagen). Oben im Abschnitt über die Installation des Registrierungsdienstes erhalten Sie Informationen darüber, wie Sie den Inhalt der CFG-Datei richtig erstellen können. Achten Sie darauf, dass der Servername richtig angegeben und dass der Server unter dem Namen erreichbar ist.

BC0038–Japanischer Support wurde angefragt, aber die Datei dsvc0411.dll, die den japanischen Support enthält, ist nicht vorhanden. Installieren Sie die Datei noch einmal.

BC0039–Interner Fehler. Wenden Sie sich an Ihr HP SAM Support-Team.

BC0040–Interner Fehler beim Zugriff auf WMI. Wenden Sie sich an Ihr HP SAM Support-Team.

BC0041–Interner Fehler. Es konnte keine Verbindung zu WMI hergestellt werden. Wenden Sie sich an Ihr HP SAM Support-Team.

BC0042–Interner Fehler. Wenden Sie sich an Ihr HP SAM Support-Team.

BC0043–Win32\_SystemEnclosure-WMI-Klasse konnte nicht gelesen werden. Wenden Sie sich an Ihr HP SAM Support-Team.

BC0044–Win32\_ComputerSystem-WMI-Klasse konnte nicht gelesen werden. Wenden Sie sich an Ihr HP SAM Support-Team.

BC0045–Win32\_BaseBoard-WMI-Klasse konnte nicht gelesen werden. Wenden Sie sich an Ihr HP SAM Support-Team.

BC0046–Win32\_NetworkAdapterConfiguration-WMI-Klasse konnte nicht gelesen werden. Wenden Sie sich an Ihr HP SAM Support-Team.

BC0047–Win32\_NetworkAdapterConfiguration-WMI-Klasse konnte nicht gelesen werden. Wenden Sie sich an Ihr HP SAM Support-Team.

BC0048–Eine spezifische WMI-Eigenschaft konnte nicht abgefragt werden. Wenden Sie sich an Ihr HP SAM Support-Team.

BC0049–Ein WMI-Ereignis konnte nicht registriert werden. Wenden Sie sich an Ihr HP SAM Support-Team.

BC0050–Problem beim Zugriff auf WMI, möglicherweise in Zusammenhang mit einem fehlenden QFE, das im MS KB-Artikel 828653 dokumentiert ist.

BC0100–Timer konnte nicht eingestellt werden. BC0006–Interner Fehler, möglicherweise aufgrund eines geringen Arbeitsspeichers. Schließen Sie andere Anwendungen, oder erweitern Sie den verfügbaren Speicher.

BC0101–Gateway/HP SAM Server wurde in der Konfigurationsdatei nicht gefunden. Lesen Sie im Abschnitt oben zur Installation des Registrierungsdienstes nach, wie die korrekten CFG-Dateiinhalte zu erstellen sind. Vergewissern Sie sich, dass der Servername korrekt ist.

BC0104–Eigenschaften für Sound-UDP-Socket konnten nicht eingestellt werden. Wenden Sie sich an Ihr HP SAM Support-Team.

BC0105–(Warnung) Diese Ressource hat keine definierten Rollen. Ohne eine Rolle kann eine Rechnerressource nicht zugeordnet werden.

BC0106–(Warnung) Interner Dienstfehler bei der Kommunikation mit dem SCM. Kann die Art und Weise beeinträchtigen, wie der Service Control Manager (Dienstkontrollmanager) bestimmt, ob der Dienst gestartet oder angehalten wird. Wenden Sie sich an Ihr HP SAM Support-Team.

BC0107–Timer konnte nicht eingestellt werden. Interner Fehler, möglicherweise aufgrund zu geringen Arbeitsspeichers. Schließen Sie andere Anwendungen, oder erweitern Sie den verfügbaren Speicher.

BC0108–Timer konnte nicht eingestellt werden. Interner Fehler, möglicherweise aufgrund zu geringen Arbeitsspeichers. Schließen Sie andere Anwendungen, oder erweitern Sie den verfügbaren Speicher.

BC0110–Zeitzone-Information konnte nicht synchronisiert werden. Wenden Sie sich an Ihr HP SAM Support-Team.

BC0111–Zeitzone-Information konnte nicht synchronisiert werden. Wenden Sie sich an Ihr HP SAM Support-Team.

BC0200–(Information) Dienst wurde gestartet.

BC0201–(Information) Dienst wurde angehalten.

---

## D Glossar

**Zugriffsggerät** – Ein Gerät, z. B. ein Thin Client, das auf HP SAM zugreift, um eine Verbindung mit Rechnerressourcen herzustellen.

**Active Directory** – Ein Microsoft Windows-Verzeichnisdienst, der die Informationen und Einstellungen eines Unternehmens in einer zentralen und organisierten Datenbank speichert, auf die zugegriffen werden kann. Active Directory gibt den Administratoren die Möglichkeit, für ein ganzes Unternehmen Richtlinien zuzuweisen, Programme zu implementieren und kritische Aktualisierungen vorzunehmen.

**Administrator Group (Administratorgruppe)** – Eine Gruppe, der Sie Benutzer zuweisen können, um den Zugriff zu bestimmten Funktionen in der HP SAM-Verwaltungskonsole zu gewähren oder zu widerrufen.

**Systemgruppe** – Eine Gruppe aus Zugriffsgeräten, Benutzern, Rechnerressourcen, Rollen, Monitorlayout-IDs, Richtlinien, Protokollen und Berichten, die von einer Administratorgruppe gesteuert wird.

**Client** – Ein Zugangsggerät, das Anfragen an den HP SAM-Webserver sendet, um eine verfügbare Rechnerressource zu ermitteln, mit der es sich verbinden kann.

**CSP** – Cryptographic Service Provider (Kryptographiedienstleister). Eine Software-Bibliothek, die hardware- und softwarebasierte Datenverschlüsselungs- und Datenentschlüsselungsdienste ausführt.

**Rechnerressource** – Eine Desktop-Sitzung; eine Rechnerressource, z. B. ein Blade-PC oder eine Blade Workstation, oder eine virtuelle Maschine.

**Rechenzentrum** – Eine Gehäusegruppe in HP SAM, die das Speichern von Gehäusepasswörtern (für die clientseitige Funktion zum Aus- und Wiedereinschalten erforderlich) ermöglicht.

**Dedizierte Ressource** – Bestimmte Rechnerressource(n), die einem Benutzer zugewiesen ist/sind. Auch als statische Zuweisung bezeichnet.

**Beschreibung (Blade)** – Im Allgemeinen vom Blade-Hersteller für den Blade-PC erstellt. Sie kann auf Wunsch verändert werden.

**Follow-Me-Roaming** – Darüber kann der Benutzer mit verschiedenen Zugriffsgeräten an verschiedenen Orten eine Verbindung zur selben Sitzung herstellen, bzw. erneut herstellen.

**Gateway** – Siehe Webserver.

**Globale Richtlinie** – Mit dieser Richtlinie wird die Verbindungsumgebung aller Benutzer eingestellt. Sie kann durch Gruppen- oder Einzelrichtlinienzuweisung aufgehoben werden.

**Gruppenrichtlinie** – Mit dieser Richtlinie wird die Verbindungsumgebung für eine Gruppe von Benutzern eingestellt. Diese Richtlinie hebt die globale Richtlinie auf, kann jedoch selbst durch Einzelrichtlinienzuweisung außer Kraft gesetzt werden.

**Einzelrichtlinie** – Mit dieser Richtlinie wird die Verbindungsumgebung für einen speziellen Benutzer festgelegt. Diese Richtlinienzuweisung hebt die Gruppenrichtlinie auf, die wiederum die Regeln der globalen Richtlinie außer Kraft setzt.

**Monitorlayout-ID** – Identifikationsname für eine Sammlung von Einstellungen, die die Abbildung mehrerer Sitzungen auf dem Bildschirm eines Zugriffsgeräts steuert, sowie für andere zugehörige Einstellungen.

**OU** – Organisatorische Einheit

**Richtlinie** – Eine Richtlinie definiert die Einstellungen, die der HP SAM Server für die Benutzer erzwingt. Sie bestimmt das Erscheinungsbild des Desktops, der Taskleiste, der Befehlseingabe, Verfügbarkeit von Ton usw. Es gibt fünf Richtlinienebenen: Global, Rolle, OU, SG, Benutzer (Benutzereinstellungen setzen SG-Einstellungen außer Kraft usw.).

**Öffentliche Rolle** – Eine öffentliche Rolle ist allen Benutzern im Active Directory zugänglich.

**Registrierungsdienst** – Auch als Blade Service bezeichnet. Ein Service, der auf den Rechnerressourcen läuft und den Status der Ressourcen an den HP SAM Server zurückmeldet.

**Ressource** – Ein verwalteter Computer innerhalb von HP SAM, der einem Client zwecks Anmeldung über RGS oder RDP bereitgestellt werden kann. Auch Rechnerressource oder Desktop-Sitzung genannt. Bei einer Ressource kann es sich um einen Blade-PC, eine Blade Workstation oder eine virtuelle Maschine handeln.

**RDP** – Microsoft Remote Desktop Protocol. Ein Multikanal-Protokoll, das dem Benutzer ermöglicht, sich mit einem Computer zu verbinden, auf dem Microsoft Terminal Services ausgeführt werden.

**RGS** – HP Remote Graphics Software (RGS) ist ein Kommunikationsprotokoll ähnlich dem Microsoft Remote Desktop Protocol (RDP), das es Benutzern ermöglicht, über ein Standard-Computernetzwerk eine Verbindung zum Desktop eines Remote-Computers herzustellen. Zusätzlich verfügt RGS über erweiterte Grafikfunktionen, die eine bessere Videowiedergabe ermöglichen. Mit HP SAM können Sie entweder RGS oder RDP für die Kommunikation verwenden.

**Roaming-Profil** – Sammlung von Benutzereinstellungen im Active Directory, die nahtlos von verschiedenen Rechnerressourcen gemeinsam genutzt werden können. Es ermöglicht Benutzern, bei Verbindungen zu verschiedenen Rechnerressourcen dieselbe gewohnte Oberfläche zu verwenden.

**Rolle** – Eine Rolle ist eine Gruppe von Benutzern und eine Gruppe von Rechnerressourcen, die das Zuweisen von Benutzern zu den entsprechenden Ressourcen ermöglicht.

**HP SAM** – HP Session Allocation Manager. Das in diesem Dokument beschriebene Softwaresystem.

**Sitzungspersistenz** – Möglichkeit des Benutzers, eine Verbindung zur aktuellen Sitzung herzustellen, ohne sich abmelden zu müssen.

**SG** – Sicherheitsgruppe

**Smart Card** – Eine Karte im Taschenformat mit integrierten Schaltkreisen zur Bereitstellung von Sicherheitsdiensten, die z. B. die sichere Passwortspeicherung ermöglichen.

**UPN** – Hauptname des Benutzers (User Principal Name). Ein Anzeigenname im Format einer E-Mail-Adresse.

**Web server (Webserver)** – Die HP SAM-Komponente, die für die Verwaltung des Rechnerressourcenpools, die Bereitstellung einer Benutzeroberfläche für die Verwaltung und die Bereitstellung von Rechnerressourcen-Vermittlungsdiensten für die Clients zuständig ist. Auf der Softwareebene setzt sich der Webserver aus einem IIS-Webserver und einer SQL-Datenbank zusammen, die auf demselben physischen Server angesiedelt sein können, aber nicht müssen.



# Index

## A

Active Directory 26, 83  
ActiveX-Steuerelemente 38  
Administrativ  
    Berechtigungen 64  
    erforderliche Rechte zur  
    Installation 26  
Administrator  
    Zugang, gewähren 31  
    Zugangsliste 59  
Aktualisieren, Richtlinie 78  
Allgemein 80  
Ändern  
    Monitorlayout 75  
    Monitorlayout-Konfiguration  
    70  
    Rechenzentrum 76  
    Zugriffsgesamt 74  
Ändern eines Monitorlayouts 75  
Anforderungen  
    Blade Workstation Client 25  
    Desktop- oder Notebook-PC  
    24  
    Domänenumgebung 16  
    Hardware und Software 13  
    mobiler Thin Client 24  
    Personal Workstation Client  
    25  
    Registrierungsdienst 23  
    SQL-Server 16  
    Thin Client 24  
    Webserver 16  
    Zugriffsgesamt 23  
Animation 51  
Anmelden 58  
Anpassen  
    Administrative Berechtigungen  
    64  
Ansicht anpassen 74  
Anzahl, HP SAM Server 15  
Anzeigen von Elementen pro  
    Seite 58  
Architekturempfehlungen 13  
AssetGroup=AssetGroupList 44

AssetGroupList 35  
Attribute, zuweisen 66  
AudioFollowsFocus 50  
Auswahl einer Rolle,  
    Anforderung 101  
Autodial 43  
Automatisch aktualisieren 72  
Automatische Planungen 85  
Automatisches Verbinden (Feld)  
    83  
AutoReconnect 51  
Autosize 52  
**B**  
Backup  
    Server 34  
Banner 48  
Banner für rechtliche Hinweise 55  
Benutzer  
    Entfernen aus der  
    Administratorgruppe 60  
    hinzufügen 70  
    Löschen 70  
    Oberfläche 58  
    Oberflächeneinstellungen 47  
    verwalten 65  
Benutzerdefinition  
    HP Blade Workstation Client  
    40  
    RHEL-Client 42  
    Windows-basierter Client 39  
Benutzernamenfeld 83  
Benutzer vom Ressourcenplaner  
    abmelden 86  
Bereitstellen  
    HP SAM Client-Software 57  
Bereitstellung  
    Registrierungsdienst 56  
Berichte  
    Ressourcenkapazitätsverbrauch  
    h 88  
    Ressourcennutzung 90  
    Trendbericht zum  
    Ressourcenkapazitätsverbrauch  
    h 89

Bericht zum  
    Ressourcenkapazitätsverbrauch  
    88  
Beschränkungen, Zugriff 96  
Blade, offline 101  
Blade Workstation Client  
    Hardwareanforderungen 25  
    Softwareanforderungen 25  
BordersEnabled 50  
Browser, andere 102  
**C**  
Caching 51  
ClearType 52  
Client  
    Firewall-Regeln 99  
    Konfigurationseinstellungen 43  
    Software, Bereitstellen 57  
Client-Ressourcennetzwerk (Feld)  
    81  
ColorDepth 51  
ComposedUI 52  
Compression 51  
Connbar 51  
ConnectionBar.AutoHideTimeout  
    45  
ConnectionBar.Enable 44  
ConnectionBar.EnableAddNew  
    44  
ConnectionBar.EnableCloseAll 44  
ConnectionBar.EnableContextMen  
    u 45  
ConnectionBar.EnableDisconnectIns  
    tance 45  
ConnectionBar.EnableReconnectAl  
    l 44  
ConnectionBar.EnableSave 45  
ConnectionBar.FollowMouse 44  
ConnectionBar.HideTimingFactor  
    45  
ConnectionBar.Location 44  
ConnectionBar.SessionWindow.En  
    ableIdentify 45  
ConnectionBar.ShowDelay 45

ConnectionBar.ShowHardReboot 46  
ConnectionBar.ShowLogoff 46  
ConnectionBar.ShowOnDisconnect 45  
ConnectionBar.ShowReboot 46  
ConnectionBar.ShowTimingFactor 45  
Cookies (Feld) 82

## D

Datenbank, Empfehlungen für SQL 13  
Datenbanken, mehrere SQL 16  
Debug 44  
dedizierte Ressource, Einrichtung 10  
DefaultDomain 43  
DefaultInsecurePassword 43  
DefaultMonitorLayoutID 44  
DefaultPolicy 43  
DefaultSessionAction 49  
DefaultUsername 43  
Desktop- oder Notebook-PC  
  Hardwareanforderungen 24  
  Softwareanforderungen 24  
Diagramme 90  
Diagramm für maximale Kapazität 90  
Diagramm für Mindestkapazität 90  
Dienstkonto 26  
DisclaimerDisplay.Timeout 45  
DisplayLogoff 49  
DisplayRestart 49  
DisplayShutdown 49  
DnsDomain 35  
Domänenfeld anzeigen (Feld) 82  
Domänenumgebung 16  
Doppelbytezeichen, Verwendung 104  
Dynamisch  
  Ressource einrichten 9  
  Verbindung 3

## E

Einrichten  
  dynamische Ressource 9  
Einrichtung  
  dedizierte Ressource 10

HP SAM 8  
  statische Ressource 10  
Einstellungen  
  Benutzeroberfläche 47  
  HP SAM konfigurieren 31  
  Smart Card 47  
  Web-Client 82  
Einzelheiten anzeigen 73  
Empfehlungen für die Architektur 13  
EnableDomain 48  
EnableOptionsButton 48  
EnablePassword 48  
EnablePublicRoles 44  
EnableServer 48  
Entfernen  
  Benutzer 70  
  Benutzer aus der Administratorgruppe 60  
  Monitorlayout 75  
  Monitorlayout-ID 70  
  Reserveressourcen 66  
  Ressourcen 66  
  Zugriffsggerät 75  
erstellen  
  Registrierungsdienst-Konfigurationsdatei 33  
Erstellen  
  Dienstkonto 26  
  Monitorlayout 75  
  Richtlinie 78

## F

Failover  
  Rechnerressourcen 66  
  Server 34, 101  
Feld „Banner text (Banner-Text)“ 83  
Feld „Cryptographic Service Provider (CSP)“ 83  
Feld „Default Domain (Standard-Domain)“ 82  
Feld „Show configuration options (Konfigurationsoptionen anzeigen)“ 82  
Feld „Show resolution selection (Ausgewählte Auflösung anzeigen)“ 82  
Firewall 26, 30, 38

Firewall-Regeln  
  Clients 99  
  Ressourcen 100  
  SQL-Server 100  
  Webserver 99  
FullDrag 51  
FullScreen 51

## G

Gateways 43  
Gehäuse aus Rechenzentren löschen 76  
Globale und lokale Client-Konfigurationsdateien 53  
Größenbestimmung, Server 13

## H

Hardware  
  Anforderungen 13  
  SQL-Anforderungen 18  
Häufige Aufgaben 8  
Häufig gestellte Fragen (FAQ) 101  
Height 52  
Hierarchische Richtlinie, Tabelle 77  
Hinzufügen  
  Benutzer 70  
  Benutzer zur Administratorgruppe 59  
  Gehäuse zu Rechenzentren 76  
  Monitorlayout 75  
  organisatorische Einheiten zur Administratorrolle 60  
  Sicherheitsgruppen zur Administratorrolle 60  
  Zugriffsggerät, manuell 74  
HP Blade Workstation Client 40  
HP Remote Graphics Software 3, 4  
HP SAM  
  ActiveX-Steuerelemente 38  
  Client-Software, installieren 37  
  Client-Vergleichstabelle 37  
  Datagramm-Kommunikationsanschluss, Wert ändern 104  
  Datenbankwiederherstellung 107  
  Einrichtung 8

- Hardwareanforderungen für Webserver 16
- häufige Aufgaben 8
- Installieren 27
- Merkmale 2
- Registrierungsdienst-Anforderungen 23
- Softwareanforderungen für Webserver 17
- SQL-Datenbank, Hardwareanforderungen 18
- SQL-Datenbank, Softwareanforderungen 22
- Überblick 4
- HP Sygate Security Agent, aktivieren 102
- HP ThinPro GT-Client 41

## I

- ImageQuality 50
- Installation
  - Administratorrechte 26
  - Fehler 102
  - HP Blade Workstation Client-Reihe 40
  - HP SAM SQL-Software 28
  - HP SAM Webserver 28
  - HP ThinPro GT-Client 41
  - Internet Explorer-basierter Client 38
  - neu 27
  - Reihenfolge 27
  - Upgrade 27
  - Windows-basierter Client 39
- Installieren
  - HP SAM Client-Software 37
  - HP SAM Registrierungsdienst 32
  - HP SAM Registrierungsdienst-Software 32
  - RHEL-Client 42
- Internet Explorer-basierter Client 38
- IP-Adressenliste 30

## J

- Japanische Zeichen 102

## K

- keine Verbindung 101
- KeyRepeatEnabled 50

- Keys 51
- KioskMode 49
- Kommunikationsanschluss, Wert ändern 104
- Komponenten, Software 7
- Konfiguration
  - Datei 33
  - Einstellungen 43
  - Firewall 26, 30
  - HP SAM Systemeinstellungen 31
  - Optionen 43
  - Sitzungszeitbeschränkungen 93
  - Smartcard-Anmeldung 92
  - SSL 32
- Konto, Dienst 26

## L

- Liniendiagramme, Verfügbarkeit 104
- Linux, Sitzungszeitgeber 95
- Linux-basierter Client 40
- Lizenzen 86
- Löschen
  - Benutzer 70
  - Benutzer aus der Administratorgruppe 60
  - Monitorlayout 75
  - Monitorlayout-ID 70
  - Rechenzentrum 76
  - Reserveressourcen 66
  - Ressourcen 66
  - Zugriffsgert 75

## M

- MapClipboard 52
- MapDrives 51
- MapDrivesList 53
- MapPorts 51
- MapPrinters 51
- MapSmartcards 51
- MapUSB 50
- MatchClientDisplays 53
- Mehrere Elemente auswählen 59
- Merkmale 2
- MicrophoneEnabled 50
- Microsoft Remote Desktop Protocol 3, 4

- Mobiler Thin Client
  - Hardwareanforderungen 24
  - Softwareanforderungen 24
- Monitorlayout
  - ändern 75
  - Ändern der Konfiguration 70
  - Entfernen der ID 70
  - erstellen 75
  - konfigurieren 11
  - Löschen 75
  - Zuweisen 69
- Mute 50

## N

- Navigation, HP SAM-Verwaltungskonsole 58
- NetworkAuthentication 53
- Netzwerkfehler, neu verbinden 101
- Neue Funktionen
  - Ressourcenreservierungen 96
  - Vor Zuweisung
    - authentifizieren 98
    - Zugriffsbeschränkungen 96
- Neue Ressourceneinstellungen (Feld) 80
- Neue Rolleneinstellungen (Feld) 80
- Neuverbinden nach Netzwerkfehler 101

## O

- Offline-Blade 101
- Operation 73
- Optimale Vorgehensweisen 13
- Organisatorischen Einheiten
  - Zugang gewähren 71

## P

- Passwort, zweimal anmelden 102
- Personal Workstation Client
  - Hardwareanforderungen 25
  - Softwareanforderungen 25
- Planung der Prüfprotokollbereinigung 85
- Planung der Ressourcensynchronisierung 85
- Port-Wert 80 und 443, ändern 103
- Protocol 50

- R**
- RDC-Einstellungen, nicht wirksam 101
- RDP 3, 4
- Rechenzentren
  - Ändern 76
  - Erstellen 76
  - Gehäuse hinzufügen 76
  - Gehäuse löschen 76
  - Löschen 76
  - Regionalisierung 15
  - verwalten 75
- Rechenzentrum erstellen 76
- Referenzsuche (Feld) 83
- Regel
  - Einträge 50
  - hierarchisch, Tabelle 77
- Regionalisierung von Rechenzentren 15
- Registerkarten
  - Benutzer und Rollen 62
  - Berichte 87
  - Home 62
  - Protokoll 91
  - Ressourcen 72
  - Richtlinien 76
  - Systemeinstellungen 80
  - Verwaltungskonsole 62
- Registerkarte „Benutzer und Rollen“ 62
- Registerkarte „Berichte“ 87
- Registerkarte „Home“ 62
- Registerkarte „Protokoll“ 91
- Registerkarte „Ressourcen“ 72
- Registerkarte „Richtlinien“ 76
- Registerkarte „Systemeinstellungen“ 80
- Registrierungsdienst
  - Fehlercodes 108
  - Hardwareanforderungen 23
  - Implementierung auf allen Blades 56
  - Installation, Fehler 102
  - Installieren 32
  - Konfigurationsdatei 33
  - Konfigurationsdateiname 33
  - Softwareanforderungen 23
  - Software installieren 32
  - Software validieren 32
- starten 36
- testen 36
- Reihenfolge der Installation 27
- Remote Desktop Protocol 3, 4
- Remote Graphics Software 3, 4, 7
- Reserve
  - Rechnerressourcen 66
  - Ressourcen, entfernen 66
  - Ressourcen, zuweisen 66
- ResetAfterSession 44
- Resolutions 45
- Ressourcen
  - Entfernen 66
  - Zuweisen 66
  - zuweisen über Rolle 69
  - zuweisen über Vorlagenbenutzer 68
- Ressourcen, manuell zuweisen 67
- Ressourcen-Firewall-Regeln 100
- Ressourcennutzungsbericht 90
- Ressourcenreservierungen 96
- Ressourcenrollen verwalten 62
- RGS 3, 4, 7
- RgsDialogTimeout 52
- RgsErrorTimeout 52
- RgsWarningTimeout 52
- RHEL-Client 42
- Richtlinie
  - effektiv, anzeigen 78
  - erstellen oder aktualisieren 78
- Richtlinien 43
- RolesList 35
- Rolle, Zuweisen von Ressourcen 69
- S**
- Serveranzahl 15
- Servergröße bestimmen 13
- ServicePort 35
- ShowVersion 48
- Sicherheit
  - Aktivierung 102
  - Sicherheitsgruppen Zugang gewähren 71
- Sicherung
  - Server 101
- Sitzungszeitbeschränkungen konfigurieren 93
- Sitzungszeitgeber für Linux 95
- Smartcard
  - Anmeldung 92
- Smart Card
  - Einstellungen 47
- SmartCardAlways 47
- Smartcard-Anmeldeliste 83
- SmartCardAutoDisconnect 47
- SmartcardCSP 47
- Smartcard Requires Click 47
- SmartCardUidOid 47
- SmartCardUidType 47
- Software
  - Bereitstellen, Client 57
  - Komponenten 7
- Softwareanforderungen
  - Blade Workstation Client 25
  - Desktop- oder Notebook-PC 24
  - mobiler Thin Client 24
  - Personal Workstation Client 25
  - Registrierungsdienst 23
  - SQL 22
  - Thin Client 24
  - Webserver 17
- Sortieren 58
- SoundQuality 50
- SoundStereo 50
- Spalten 58
- Span 53
- SQL
  - Datenbankempfehlungen 13
  - Datenbank-
    - Hardwareanforderungen 18
    - Datenbank-
      - Softwareanforderungen 22
      - mehrere Datenbanken 16
  - SQL-Server-Firewall-Regeln 100
  - SSL konfigurieren 32
  - Standardwert für http-Port, ändern 103
  - Standardwert für https-Port, ändern 103
  - Starten des
    - Registrierungsdienstes 36
  - Statische Ressource, Einrichtung 10
  - Statische Verbindung 3
  - Systemgruppen, verwalten 63

## T

Testen des Registrierungsdienstes  
36  
Themes 51  
Thin Client  
Hardwareanforderungen 24  
Softwareanforderungen 24  
Thin Client, mobil  
Hardwareanforderungen 24  
Softwareanforderungen 24  
Titlebar Text 48  
Trendbericht zum  
Ressourcenkapazitätsverbrauch  
89

## U

Überblick, HP SAM 4  
UILanguage 48  
UiMode 47  
Umgebung,  
Domänenanforderungen 16  
Upgrade-Installation 27  
URL, Internet Explorer-basierter  
Client 38  
User Sign-in Time Out 81

## V

Validieren, HP SAM  
Registrierungsdienst-Software 32  
Verbindung, keine 101  
Vergleichen von Clients, Tabelle  
37  
Verlauf (Feld) 80  
Verschieben von Spalten 58  
Verwalten  
Administrative Berechtigungen  
64  
Administratorzugangsliste 59  
HP SAM Benutzer 65  
Ressourcenrollen 62  
Systemgruppen 63  
Zugriffsgeräte 74  
Verwalten von Ressourcen 72  
Verwaltung  
Konsole-Registerkarten 62  
Vorgehensweisen, optimale 13  
Vorlagenbenutzer, Ressourcen  
zuweisen 68  
Vor Zuweisung authentifizieren  
98

## W

Wallpaper 51  
Web-Client 82  
Webserver  
Firewall-Regeln 99  
Hardwareanforderungen 16  
Softwareanforderungen 17  
WebServerList 34  
Width 52  
Wiederherstellung, HP SAM  
Datenbank 107  
Windows-basierter Client 39  
WindowSnapEnabled 50

## Z

Zugang gewähren  
Benutzern 70  
Sicherheitsgruppen 71  
Zugangsliste 59  
Zugriff aktivieren (Feld) 82  
Zugriffsbeschränkungen 96  
Zugriffsgerät  
ändern 74  
Anforderungen 23  
Löschen 75  
manuell hinzufügen 74  
Zugriffsgeräte verwalten 74  
Zuweisen  
Attribute 66  
Monitorlayout 69  
Reserveressourcen 66  
Ressourcen 66  
Ressourcen über Rolle 69  
Ressourcen über  
Vorlagenbenutzer 68  
Zuweisen von Ressourcen  
manuell 67