Integriertes Managementmodul II

Benutzerhandbuch

Integriertes Managementmodul II

Benutzerhandbuch

Dritte Ausgabe (Juli 2013)

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Integrated Management Module II, User's Guide,
IBM Teilenummer 47C9203,
herausgegeben von International Business Machines Corporation, USA

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
TSC Germany
Kst. 2877
Juli 2013

Inhaltsverzeichnis

Tabellen

Kapitel 1. Einführung

Beim Serviceprozessor "Integrated Management Module II" (IMM2) handelt es sich um die zweite Generation des Serviceprozessors "Integrated Management Module" (IMM), bei dem die Serviceprozessor-Funktionalität sowie die Super E/A-, die Videocontroller- und die Remote-Presence-Funktion auf einem einzigen Chip auf der Systemplatine vereint sind. Wie schon das IMM bietet das IMM2 einige Verbesserungen gegenüber den kombinierten Funktionalitäten des Baseboard Management Controller (BMC) und des Remote Supervisor Adapter II, darunter die folgenden Funktionen:

- Auswahl zwischen einer dedizierten oder einer gemeinsam genutzten Ethernet-Verbindung für das Systemmanagement.
- Eine gemeinsame IP-Adresse für IPMI (Intelligent Platform Management Interface) und die Serviceprozessorschnittstelle. Diese Funktion ist nicht auf Blade-Servern von IBM® BladeCenter ausführbar.
- Embedded Dynamic System Analysis (DSA).
- Ferne Konfiguration mit dem Dienstprogramm für erweiterte Einstellungen (Advanced Settings Utility - ASU). Diese Funktion ist nicht auf Blade-Servern von IBM BladeCenter ausführbar.
- Die Möglichkeit für Anwendungen und Tools, zwischen Inband- oder Außerbandzugriff auf das IMM2 zu wählen. Auf Blade-Servern von IBM BladeCenter wird nur die Inbandverbindung zum IMM2 unterstützt.
- Erweiterte Remote-Presence-Funktion. Diese Funktion ist nicht auf Blade-Servern von IBM BladeCenter ausführbar.

Anmerkungen:

- Auf Blade-Servern von IBM BladeCenter und auf manchen System x-Servern ist kein dedizierter Systemmanagement-Netzanschluss verfügbar; für diese Server steht lediglich die Einstellung *shared* (gemeinsam genutzt) zur Verfügung.
- Bei Blade-Servern von IBM BladeCenter ist das erweiterte Managementmodul von IBM BladeCenter das primäre Managementmodul für Systemmanagementfunktionen und für KVM-Multiplexing (Keyboard/Video/Mouse - Tastatur/Bildschirm/Maus).

Die IBM System x® Server-Firmware ist die IBM Implementierung der UEFI (Unified Extensible Firmware Interface). Es ersetzt bei Servern von IBM System x und in Blade-Servern von IBM BladeCenter das BIOS (Basic Input/Output System). Das BIOS war der Standardfirmwarecode, der die grundlegenden Hardwareoperationen, wie z. B. Interaktionen mit Diskettenlaufwerken, Festplattenlaufwerken und der Tastatur, steuerte. Die Server-Firmware von IBM System x bietet mehrere zusätzliche Funktionen, die im BIOS nicht zur Verfügung stehen, einschließlich Kompatibilität mit UEFI 2.3, iSCSI-Kompatibilität, Active Energy Manager-Technologie und erweiterter Zuverlässigkeits- und Servicekompetenzen. Das Konfigurationsdienstprogramm bietet Serverinformationen, Serverkonfiguration und Anpassungskompatibilität sowie die Möglichkeit, die Bootreihenfolge festzulegen.

Anmerkungen:

- In diesem Dokument wird die Server-Firmware von IBM System x oft als "Server-Firmware" und gelegentlich als "UEFI" bezeichnet.

- Die Server-Firmware von IBM System x ist mit Betriebssystemen ohne UEFI vollständig kompatibel.
- Weitere Informationen zur Verwendung der Server-Firmware von IBM System x finden Sie in der Dokumentation, die mit Ihrem IBM Server geliefert wurde.

In diesem Dokument wird erläutert, wie die Funktionen des IMM2 in einem IBM Server verwendet werden. Das IMM2 stellt mithilfe der Server-Firmware von IBM System x Systemverwaltungsfunktionen für System x, BladeCenter und IBM Flex System bereit.

Gehen Sie wie folgt vor, um zu prüfen, ob Firmwareaktualisierungen verfügbar sind.

Anmerkung: Beim ersten Zugriff auf das IBM Support Portal müssen Sie die Produktkategorie, die Produktfamilie und die Modellnummern Ihrer Speichersubsysteme auswählen. Wenn Sie das nächste Mal auf das IBM Support Portal zugreifen, werden die Produkte, die Sie beim ersten Mal ausgewählt haben, von der Website erneut geladen, sodass nur die Links für Ihre Produkte angezeigt werden. Um Ihre Produktliste zu ändern oder Elemente zu ihr hinzuzufügen, klicken Sie auf den Link **Manage my product lists** (Meine Produktlisten verwalten).

Die IBM Website wird in regelmäßigen Abständen aktualisiert. Die Vorgehensweisen zum Bestimmen der Firmware und der Dokumentation weicht möglicherweise geringfügig von den Beschreibungen im vorliegenden Dokument ab.

1. Wechseln Sie zu http://www.ibm.com/support/entry/portal.
2. Wählen Sie unter **Choose your products** (Produkt auswählen) die Option **Browse for a product** (Nach Produkt suchen) aus und erweitern Sie **Hardware**.
3. Klicken Sie je nach Servertyp auf **Systems** > **System x** oder auf **Systems** > **BladeCenter** und wählen Sie das Feld für Ihre(n) Server aus.
4. Klicken Sie unter **Choose your task** (Task auswählen) auf **Downloads**.
5. Klicken Sie unter **See your results** (Ergebnisse anzeigen) auf **View your page** (Ihre Seite anzeigen).
6. Klicken Sie im Feld "Flashes & Alerts" auf den Link für den betreffenden Download oder klicken Sie auf **More results**, um weitere Links anzuzeigen.

Funktionen von "IMM2 Basic Level", "IMM2 Standard Level" und "IMM2 Advanced Level"

Zusammen mit dem IMM2 werden die Funktionalitätsebenen "Basic Level", "Standard Level" und "Advanced Level" angeboten. Weitere Informationen zu der auf Ihrem IBM-Server installierten IMM2-Version finden Sie in der Dokumentation für Ihren Server. Alle Versionen bieten folgende Funktionen:

- Fernzugriff und Fernverwaltung Ihres Servers rund um die Uhr
- Fernverwaltung unabhängig vom Status des verwalteten Servers
- Fernsteuerung der Hardware und der Betriebssysteme

Zusätzlich unterstützen die Versionen "Standard Level" und "Advanced Level" die webbasierte Verwaltung mit Standard-Web-Browsern.

Anmerkung: Manche Funktionen gelten möglicherweise nicht für IBM BladeCenter-Blade-Server.

Im Folgenden sind die allgemeinen Funktionen des IMM2 aufgeführt:

Funktionen von "IMM2 Basic Level"

Im Folgenden sind die Funktionen vom Typ "IMM2 Basic Level" aufgeführt:

- IPMI 2.0 Interface (IPMI-2.0-Schnittstelle)
- Thermal Monitoring (Temperaturüberwachung)
- Fan Control (Lüftersteuerung)
- LED Management (Anzeigenverwaltung)
- Server Power/Reset Control (Steuerung von Einschalten/Zurücksetzen des Servers)
- Sensor Monitoring (Sensorüberwachung)
- IPMI Platform Event Trap Alerting (Trap-Alerts für IPMI-Plattformereignisse)
- IPMI Serial over LAN

Funktionen von "IMM2 Standard Level"

Im Folgenden finden sind die Funktionen von "IMM2 Standard Level" aufgeführt:

- Alle Funktionen von "IMM2 Basic Level"
- Webbasierte Verwaltung mithilfe von Standard-Web-Browsern
- SNMPv1- und SNMPv3-Schnittstellen
- Telnet- und SSH-Befehlszeilenschnittstelle (CLI)
- Zeitgesteuertes Ein-/Ausschalten und Neustarten des Servers
- Ereignisse in Klarschrift und Prüfprotokollaufzeichnung
- Anzeige des Systemzustands
- Betriebssystemladeprogramm- und Betriebssystem-Watchdogs
- LDAP-Authentifizierung und -Berechtigung
- Meldung von Alertausgaben in Form von SNMP-Trap, E-Mail, syslog und CIM
- NTP-Taktgebersynchronisation
- Serielle Konsolenumleitung über Telnet/SSH

Funktionen von "IMM2 Advanced Level"

Im Folgenden sind die Funktionen für "IMM2 Advanced Level" aufgeführt:

- Alle Funktionen von "IMM2 Basic Level" und "IMM2 Standard Level"
- Remote Presence-Java- und ActivX-Clients:
  - Remote Keyboard, Video, and Mouse Support (Unterstützung für ferne Tastatur, Anzeige und Maus)
  - Remote Media (Ferne Datenträger)
  - Remote Disk on Card (Ferne Kartendatenträger)
- Failure Screen Capture for Operating System hangs (Fehleranzeigenerfassung für Betriebssystemblockierungen)

Funktionsverbesserungen beim IMM2

Im Folgenden sind die im Vergleich zu den IMM-Funktionen verbesserten IMM2-Funktionen aufgeführt:

- Sicherheit (vertrauenswürdiger Serviceprozessor):
  - Sicheres Booten
  - Signierte Aktualisierungen
  - IMM2-Core-Root zur Überprüfung der Vertrauenswürdigkeit
  - TPM (Trusted Platform Module)

- Neues, bei IBM System x konsistentes Web-GUI-Design
- Verbesserte Remote-Presence-Bildschirmauflösung und -Farbpalette
- Remote-Presence-Client von ActiveX
- Auf USB 2.0 aktualisierte Ethernet-over-USB-Schnittstelle
- Syslog-Alertausgabe
- Nach Konfigurationsänderungen kein Zurücksetzen des IMM2 erforderlich

Upgrade für IMM2 durchführen

Wenn Ihr IBM Server über die IMM2-Firmwarefunktion der Stufe "Basic Level" oder "Standard Level" verfügt, können Sie möglicherweise ein Upgrade für die IMM2-Funktionen auf Ihrem Server durchführen. Weitere Informationen zu den verfügbaren Upgradestufen und wie Sie sie bestellen können, finden Sie in Kapitel 7, „Features on Demand", auf Seite 143.

IMM2 zusammen mit dem erweiterten BladeCenter-Managementmodul verwenden

Das erweiterte BladeCenter-Managementmodul ist die Systemmanagement-Standardschnittstelle für IBM BladeCenter-Produkte. Obwohl das IMM2 nun in einigen IBM Blade-Servern enthalten ist, bleibt das erweiterte Managementmodul das Managementmodul für Systemmanagementfunktionen und KVM-Multiplexing (Keyboard/Video/Mouse - Tastatur/Bildschirm/Maus) für IBM BladeCenter-Produkte einschließlich IBM Blade-Server.

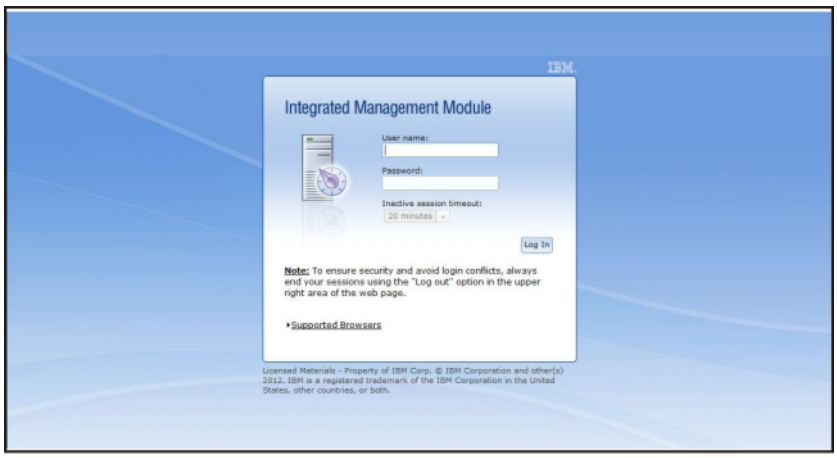
Auf IBM BladeCenter-Blade-Servern gibt es keinen externen Netzzugriff auf das IMM2 und zur fernen Verwaltung von Blade-Servern von IBM BladeCenter muss das erweiterte Managementmodul verwendet werden. Das IMM2 ersetzt die Funktionalität des BMC und der cKVM-Erweiterungskarte (cKVM - Concurrent Keyboard, Video and Mouse) in früheren IBM Blade-Server-Produkten.

Voraussetzungen - Web-Browser und Betriebssystem

Für die IMM2-Webschnittstelle sind das Java™-Plug-in ab Version 1.5 (für die Remote-Presence-Funktion) und einer der folgenden Web-Browser erforderlich:

- Microsoft Internet Explorer Version 7 oder 8
- Mozilla Firefox ab Version 3.5

Wenn Sie neuere Microsoft Internet Explorer-Versionen verwenden, wird empfohlen, dass Sie die Kompatibilitätsansicht im Internet Explorer zum Anzeigen der IMM2-Webseiten verwenden. Die oben aufgelisteten Browser stellen die aktuell von der IMM2-Firmware unterstützen Browser dar. Die IMM2-Firmware kann in regelmäßigen Abständen erweitert werden, um Unterstützung für andere Browser bereitzustellen. Die Liste der Browser, die von der aktuell auf dem System ausgeführten IMM2-Firmwareversion unterstützt werden, finden Sie in der Liste "Supported Browsers" (Unterstützte Browser) auf der IMM2-Anmeldeseite. In der folgenden Abbildung ist die IMM2-Anmeldeanzeige dargestellt.



Die folgenden Serverbetriebssysteme bieten USB-Unterstützung, die für die Remote-Presence-Funktion erforderlich ist:

- Microsoft Windows Server 2008
- Microsoft Windows Server 2003
- Red Hat Enterprise Linux, Version 4.0 und 5.0
- SUSE Linux Version 10.0
- Novell NetWare 6.5

Im Zwischenspeicher Ihres Internet-Browsers werden Informationen zu Webseiten, die Sie besuchen, gespeichert, damit diese zukünftig schneller geladen werden können. Nach einer Flashaktualisierung der IMM2-Firmware verwendet Ihr Browser möglicherweise weiterhin die Informationen aus seinem Zwischenspeicher, anstatt sie aus dem IMM2 abzurufen. Nach Aktualisierung der IMM2-Firmware wird empfohlen, dass Sie den Browser-Zwischenspeicher leeren, um sicherzustellen, dass Webseiten, die durch IMM2 bereitgestellt werden, ordnungsgemäß angezeigt werden.

Bemerkungen in diesem Buch

In dieser Dokumentation werden die folgenden Bemerkungen verwendet:

- **Anmerkung:** Diese Bemerkungen enthalten wichtige Tipps, Anleitungen oder Ratschläge.
- **Wichtig:** Diese Bemerkungen enthalten Informationen oder Ratschläge, die Ihnen helfen, schwierige oder problematische Situationen zu vermeiden.
- **Achtung:** Diese Bemerkungen weisen auf die Gefahr der Beschädigung von Programmen, Einheiten oder Daten hin. Eine Bemerkung vom Typ "Achtung" befindet sich direkt vor der Anweisung oder der Beschreibung der Situation, die diese Beschädigung bewirken könnte.

Kapitel 2. IMM2-Webschnittstelle öffnen und verwenden

Wichtig: Dieser Abschnitt gilt nicht für IBM BladeCenter und IBM Blade-Server. Obwohl das IMM2 in einigen IBM BladeCenter-Produkten und IBM Blade-Servern standardmäßig enthalten ist, bleibt das erweiterte IBM BladeCenter-Managementmodul das primäre Managementmodul für Systemmanagementfunktionen und KVM-Multiplexing (Keyboard/Video/Mouse - Tastatur/Bildschirm/Maus) für IBM BladeCenter-Produkte einschließlich IBM Blade-Server. Benutzer, die die IMM2-Einstellungen auf Blade-Servern konfigurieren möchten, sollten das Dienstprogramm für erweiterte Einstellungen (Advanced Settings Utility - ASU) auf dem Blade-Server zum Ausführen dieser Aktionen verwenden.

Das IMM2 kombiniert Serviceprozessorfunktionen, einen Videocontroller und eine Remote-Presence-Funktion (wenn ein optionaler Virtual Media Key installiert ist) in einem einzigen Chip. Für einen Fernzugriff auf das IMM2 mithilfe der IMM2-Webschnittstelle müssen Sie sich zuerst anmelden. In diesem Kapitel werden das Anmeldeverfahren und die Aktionen beschrieben, die Sie über die IMM2-Webschnittstelle ausführen können.

Zugriff auf die IMM2-Webschnittstelle

Das IMM2 unterstützt eine statische IPv4-Adressierung wie auch eine DHCP-IPv4-Adressierung. Die standardmäßig dem IMM2 zugewiesene statische IPv4-Adresse lautet 192.168.70.125. Das IMM2 ist anfangs so konfiguriert, dass es versucht, eine Adresse von einem DHCP-Server abzurufen. Ist dies nicht möglich, verwendet es die statische IPv4-Adresse.

Das IMM2 unterstützt auch IPv6, aber es verfügt standardmäßig nicht über eine festgelegte statische IPv6-IP-Adresse. Beim Erstzugriff auf das IMM2 in einer IPv6-Umgebung können Sie entweder die IPv4-IP-Adresse oder die lokale IPv6-Verbindungsadresse verwenden. Das IMM2 generiert eine eindeutige lokale IPv6-Verbindungsadresse, die in der IMM2-Webschnittstelle auf der Seite "Network Interfaces" (Netzschnittstellen) angezeigt wird. Die lokale IPv6-Verbindungsadresse weist dabei dasselbe Format auf, das im folgenden Beispiel dargestellt ist.

```
fe80::21a:64ff:fee6:4d5
```

Beim Zugriff auf das IMM2 sind die folgenden IPv6-Bedingungen als Standardwerte definiert:

- Die automatische IPv6-Adressenkonfiguration ist aktiviert.
- Die statische IPv6-IP-Adressenkonfiguration ist inaktiviert.
- DHCPv6 ist aktiviert.
- Die statusunabhängige automatische Konfiguration ist aktiviert.

Das IMM2 ermöglicht die Auswahl einer dedizierten Systemmanagement-Netzverbindung (falls vorhanden) oder einer Netzverbindung, die gemeinsam mit dem Server verwendet wird. Die Standardverbindung für in einem Gehäuserahmen installierte Server und Turmserver verwendet den dedizierten Systemmanagement-Netzanschluss.

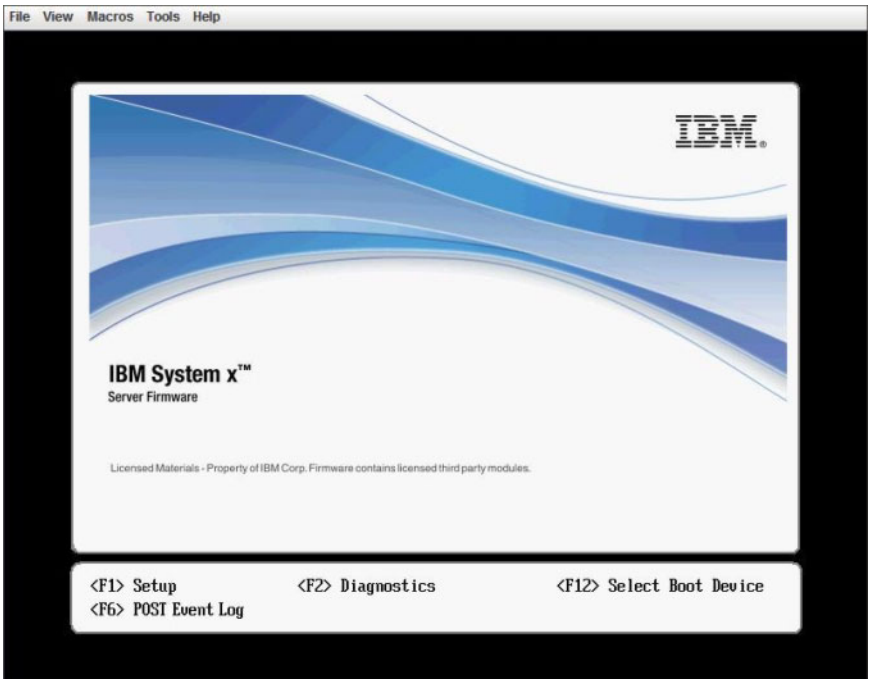
Anmerkung: Möglicherweise verfügt Ihr Server über keinen dedizierten Systemmanagement-Netzanschluss. Wenn auf Ihrer Hardware kein dedizierter Netzanschluss vorhanden ist, ist die Einstellung *shared* (freigegeben) die einzig verfügbare IMM2-Einstellung.

IMM2-Netzverbindung mit dem Konfigurationsdienstprogramm der Server-Firmware für IBM System x einrichten

Nachdem Sie den Server gestartet haben, können Sie über das Konfigurationsdienstprogramm eine IMM2-Netzverbindung auswählen. Der Server mit der IMM2-Hardware muss mit einem DHCP-Server verbunden sein oder das Servernetz muss so konfiguriert sein, dass es die statische IP-Adresse des IMM2 verwendet. Gehen Sie wie folgt vor, um die IMM2-Netzverbindung über das Konfigurationsdienstprogramm herzustellen:

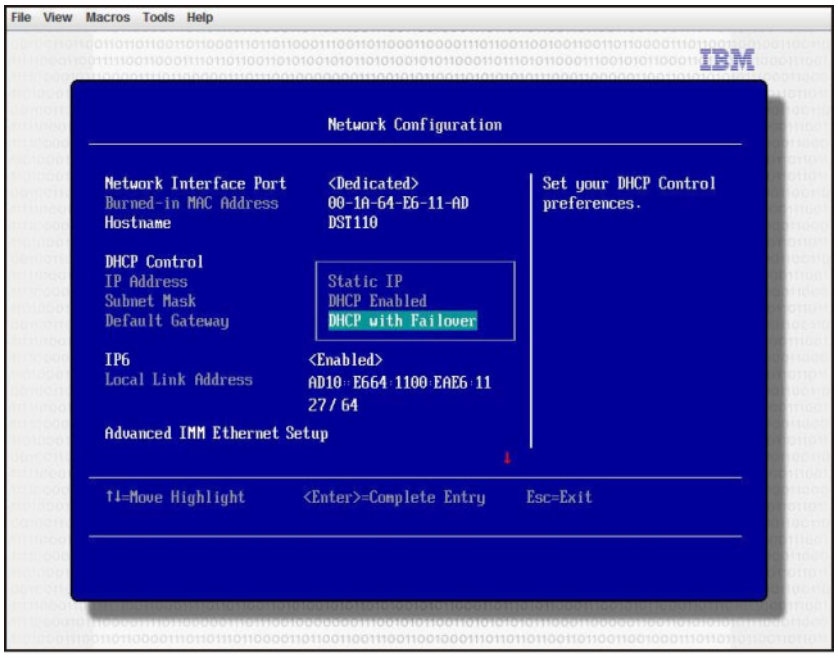
1. Schalten Sie den Server ein. Die Eingangsanzeige der Server-Firmware für IBM System x wird angezeigt.

   Anmerkung: Der Netzschalter wird etwa 90 Sekunden nach dem Anschließen des Servers an die Wechselstromversorgung aktiviert.



2. Wenn die Aufforderung `<F1> Setup` (F1 für Konfiguration) angezeigt wird, drücken Sie die Taste F1. Wenn Sie sowohl ein Startkennwort als auch ein Administratorkennwort festgelegt haben, müssen Sie das Administratorkennwort eingeben, um auf das vollständige Menü des Konfigurationsdienstprogramms zugreifen zu können.
3. Wählen Sie im Hauptmenü des Konfigurationsdienstprogramms **System Settings** (Systemeinstellungen) aus.
4. Wählen Sie in der nächsten Anzeige die Option **Integrated Management Module** aus.
5. Wählen Sie in der nächsten Anzeige die Option **Network Configuration** (Netzkonfiguration) aus.
6. Markieren Sie **DHCP Control**. Im Feld **DHCP Control** stehen drei IMM2-Netzverbindungen zur Auswahl:

- Static IP (Statisches IP)
- DHCP Enabled (DHCP aktiviert)
- DHCP with Failover (default) (DHCP mit Funktionsübernahme (Standard))



7. Wählen Sie eine der Netzverbindungen aus.
8. Wenn Sie sich dafür entscheiden, eine statische IP-Adresse zu verwenden, müssen Sie die IP-Adresse, die Teilnetzmaske und das Standard-Gateway angeben.
9. Sie können das Konfigurationsdienstprogramm auch dazu verwenden, eine dedizierte Netzverbindung (wenn Ihr Server einen dedizierten Netzanschluss hat) oder eine gemeinsam genutzte IMM2-Netzverbindung auszuwählen.

   Anmerkungen:

   - Möglicherweise verfügt Ihr Server über keinen dedizierten Systemmanagement-Netzanschluss. Wenn auf Ihrer Hardware kein dedizierter Netzanschluss vorhanden ist, ist die Einstellung *Shared* (Gemeinsam genutzt) die einzige verfügbare IMM2-Einstellung. Wählen Sie auf der Anzeige **Network Configuration** im Feld **Network Interface Port** (Netzschnittstellenport) **Dedicated** (dediziert) (falls zutreffend) oder **Shared** (gemeinsam genutzt) aus.
   - Informationen dazu, wo sich auf Ihrem Server die vom IMM2 genutzten Ethernet-Anschlüsse befinden, finden Sie in der Dokumentation zum Server.
10. Blättern Sie abwärts und wählen Sie **Save Network Settings** (Netzeinstellungen speichern) aus.
11. Beenden Sie das Konfigurationsdienstprogramm.

Anmerkungen:

- Sie müssen etwa eine Minute warten, bis die Änderungen wirksam werden und die Server-Firmware wieder funktioniert.
- Sie können die IMM2-Netzverbindung auch über die IMM2-Webschnittstelle oder die Befehlszeilenschnittstelle konfigurieren. In der IMM2-Webschnittstelle werden die Netzverbindungen auf der Seite **Network Protocol Properties** (Netzprotokolleigenschaften) konfiguriert (Wählen Sie **Network** (Netz) im Menü **IMM Management** (IMM-Verwaltung) aus). In der IMM2-Befehlszeilenschnittstelle werden die Netzverbindungen mit mehreren Befehlen konfiguriert, je nach der Konfiguration Ihrer Installation.

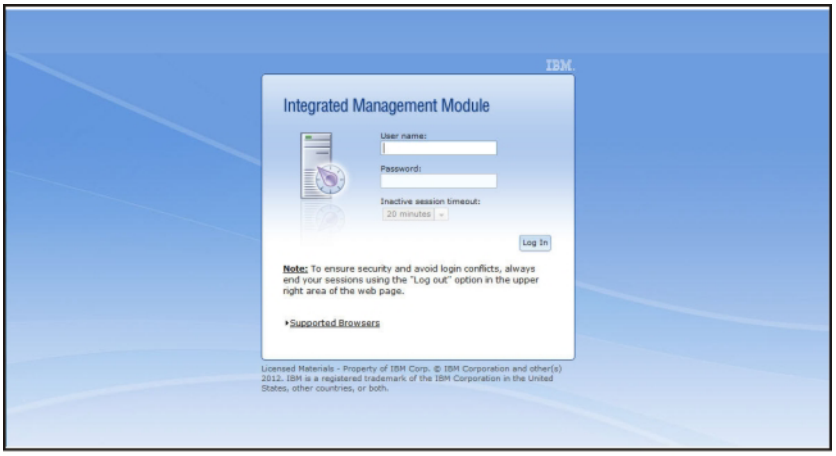
Am IMM2 anmelden

Wichtig: Das IMM2 ist anfangs auf den Benutzernamen `USERID` und das Kennwort `PASSW0RD` (mit einer Null anstelle des Buchstabens "O") eingestellt. Bei dieser Standard-Benutzereinstellung haben nur Administratoren Zugriff. Ändern Sie für größere Sicherheit diesen Benutzernamen und das zugehörige Kennwort bei der Erstkonfiguration.

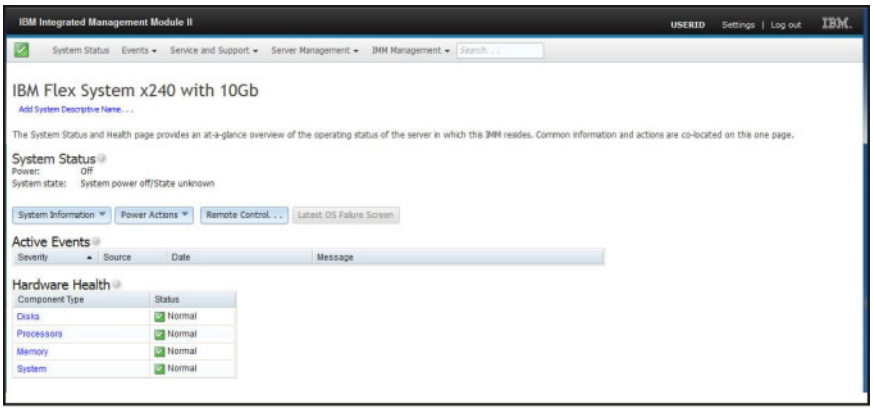
Gehen Sie wie folgt vor, um über die IMM2-Webschnittstelle Zugriff auf das IMM2 zu erhalten:

1. Öffnen Sie einen Web-Browser. Geben Sie im Adress- oder URL-Feld die IP-Adresse oder den Hostnamen des IMM2 ein, mit dem Sie eine Verbindung herstellen möchten.
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort in das Fenster "IMM2 Login" (Anmeldung am IMM2) ein. Wenn Sie das IMM2 zum ersten Mal verwenden, können Sie Ihren Benutzernamen und Ihr Kennwort von Ihrem Systemadministrator anfordern. Alle Anmeldeversuche werden im Ereignisprotokoll dokumentiert. Je nachdem, wie Ihr Systemadministrator die Benutzer-ID konfiguriert hat, müssen Sie möglicherweise ein neues Kennwort eingeben.

   Das Fenster "Login" (Anmeldung) ist in der folgenden Abbildung dargestellt.



3. Klicken Sie auf **Log in** (Anmelden), um die Sitzung zu starten. Im Browser wird die Seite "System Status" (Systemstatus) geöffnet, wie in der folgenden Abbildung dargestellt. Auf dieser Seite erhalten Sie einen schnellen Überblick über den Serverstatus und eine Zusammenfassung des Serverzustands.



Beschreibungen der Aktionen, die Sie über die Registerkarten oben in der IMM2-Webschnittstelle ausführen können, finden Sie im Abschnitt „Beschreibungen der IMM2-Aktionen".

Beschreibungen der IMM2-Aktionen

Navigieren Sie zum Anfang des IMM2-Fensters, um mit dem IMM2 Aktivitäten durchzuführen. In der Titelleiste wird der angemeldete Benutzername angegeben. Über die Titelleiste können Sie **Settings** (Einstellungen) für die Aktualisierungsfrequenz der Statusanzeige sowie eine benutzerdefinierte Übergriffsnachricht konfigurieren und sich über die Option **Log out** (Abmeldung) von der Webschnittstelle des IMM2 abmelden. Unter der Titelleiste befinden sich Registerkarten, über die Sie Zugang zu unterschiedlichen in Tabelle 1 aufgeführten IMM2-Funktionen bekommen.

Tabelle 1. IMM2-Aktionen

Registerkarte	Auswahl	Beschreibung
System Status (Systemstatus)		Auf der Systemstatusseite können Sie Informationen zu Systemstatus, aktiven Systemereignissen und Hardwarezustand anzeigen. Sie bietet Quick Links zu den Systeminformationen, Serverstromversorgungsaktionen und Fernsteuerungsfunktionen der Registerkarte "Server Management" und ermöglicht es Ihnen, ein Bild von der Erfassung der letzten Anzeige bei einem Systemabsturz anzuzeigen. In den Abschnitten „Registerkarte "System Status"" auf Seite 21 und „Systemstatus anzeigen" auf Seite 97 finden Sie weitere Informationen.

Tabelle 1. IMM2-Aktionen (Forts.)

Registerkarte	Auswahl	Beschreibung
Events (Ereignisse)	Event Log (Ereignisprotokoll)	Auf der Ereignisprotokollseite werden Einträge angezeigt, die derzeit im IMM2-Ereignisprotokoll gespeichert sind. Das Protokoll enthält eine Textbeschreibung von gemeldeten Systemereignissen, einschließlich Informationen über sämtliche Fernzugriffsversuche und Konfigurationsänderungen. Alle Ereignisse im Protokoll bekommen mithilfe der Datums- und Uhrzeiteinstellungen des IMM2 eine Zeitmarke. Manche Ereignisse lösen auch Alerts aus, wenn sie entsprechend konfiguriert wurden. Sie können Ereignisse im Ereignisprotokoll sortieren und filtern und sie in eine Textdatei exportieren. Weitere Informationen finden Sie in den Abschnitten „Registerkarte "Events" (Ereignisse)" auf Seite 27 und „Ereignisprotokoll verwalten" auf Seite 127.
	Event Recipients (Ereignis-empfänger)	Auf der Seite "Event Recipients" können Sie festlegen, wer bei Systemereignissen benachrichtigt werden soll. Sie können jeden Empfänger konfigurieren und Einstellungen verwalten, die für alle Ereignisempfänger gelten. Sie können außerdem ein Testereignis generieren, um zu überprüfen, ob die Benachrichtigungsfunktion funktioniert. Weitere Informationen finden Sie in den Abschnitten „Event Recipients (Ereignisempfänger)" auf Seite 30 und „Benachrichtigung zu Systemereignissen" auf Seite 129.
Service and Support (Service und Unterstützung)	Download Service Data (Servicedaten herunterladen)	Die Seite "Download Service Data" erstellt eine komprimierte Datei mit Informationen, die vom IBM Support dazu verwendet werden kann, Ihnen zu helfen. Weitere Informationen finden Sie in den Abschnitten „Download Service Data (Servicedaten herunterladen)" auf Seite 32 und „Informationen für Service und Support erfassen" auf Seite 135.

Tabelle 1. IMM2-Aktionen (Forts.)

Registerkarte	Auswahl	Beschreibung
Server Management (Serververwaltung)	Server Firmware (Server-Firmware)	Die Seite "Server Firmware" gibt Firmwareversionen an und ermöglicht es Ihnen, die IMM2-Firmware, Server-Firmware und DSA-Firmware zu aktualisieren. Weitere Informationen finden Sie in den Abschnitten „Server Firmware (Server-Firmware)" auf Seite 34 und „Server-Firmware aktualisieren" auf Seite 122.
	Remote Control (Fernsteuerung)	Über die Seite "Remote Control" können Sie den Server auf Betriebssystemebene steuern. Sie bietet den Zugriff auf die Funktionalität für ferne Datenträger und ferne Konsolen. Sie können die Serverkonsole über Ihren Computer anzeigen und bedienen und eines der Plattenlaufwerke des Computers, z. B. das CD-ROM-Laufwerk oder das Diskettenlaufwerk, an den Server anhängen. Wenn Sie einen Datenträger angehängt haben, können Sie ihn für einen Neustart des Servers sowie für die Aktualisierung der Firmware auf dem Server verwenden. Das angehängte Laufwerk wird als an den Server angeschlossenes USB-Plattenlaufwerk angezeigt. Weitere Informationen finden Sie in den Abschnitten „Remote Control (Fernsteuerung)" auf Seite 39 und „Remote-Presence- und Fernsteuerungsfunktionen" auf Seite 107.
	Server Properties (Servereigenschaften)	Die Seite "Server Properties" ermöglicht den Zugriff auf unterschiedliche Eigenschaften, Statusbedingungen und Einstellungen Ihres Servers. Die folgenden Optionen sind von der Seite "Server Properties" verfügbar: • Auf der Registerkarte "General Settings" werden Informationen angezeigt, die das System für Vorgänge sowie für Supportmitarbeiter kenntlich macht. • Auf der Registerkarte "LEDs" wird der Status aller Systemanzeigen angezeigt. Über sie können Sie auch den Zustand der Positionsanzeige ändern. • Auf der Registerkarte "Hardware Information" werden elementare Produktdaten (VPD - Vital Product Data) zum Server angezeigt. Das IMM2 erfasst Serverinformationen, Serverkomponentenangaben und Netzhardwareinformationen. • Auf der Registerkarte "Environmentals" werden Informationen zur Spannung und Temperatur für den Server und seine Komponenten angezeigt. • Auf der Registerkarte "Hardware Activity" wird ein Verlauf der Komponenten von durch den Kundendienst austauschbaren Funktionseinheiten (FRU - Field Replaceable Unit) angezeigt, die zum System hinzugefügt oder daraus entfernt worden sind. Weitere Informationen finden Sie im Abschnitt „Server Properties (Servereigenschaften)" auf Seite 44.
	Server Power Actions (Serverstromversorgungsaktionen)	Über die Seite "Server Power Actions" kann die Stromversorgung des Servers vollständig ferngesteuert werden. Dies umfasst Aktionen zum Einschalten, Ausschalten und für den Neustart. Weitere Informationen finden Sie in den Abschnitten „Server Power Actions (Serverstromversorgungsaktionen)" auf Seite 49 und „Stromversorgungsstatus des Servers steuern" auf Seite 106.
	Disks (Platten)	Auf der Seite "Hard Disks" (Festplatten) wird der Status von Festplattenlaufwerken im Server angezeigt. Sie können auf den Namen eines Laufwerks klicken, um aktive Ereignisse für das Festplattenlaufwerk anzuzeigen. Weitere Informationen finden Sie im Abschnitt „Disks (Platten)" auf Seite 49.
	Memory (Speicher)	Auf der Seite "Memory" werden die im System verfügbaren Speichermodule sowie deren Status, Typ und Kapazität angezeigt. Sie können auf einen Modulnamen klicken, um ein Ereignis und zusätzliche Hardwareinformationen für das Speichermodul anzuzeigen. Wenn Sie ein Dual Inline Memory Module (DIMM) entfernen oder ersetzen, muss der Server danach mindestens einmal eingeschaltet werden, um die korrekten Speicherdaten anzuzeigen. Weitere Informationen finden Sie im Abschnitt „Memory (Speicher)" auf Seite 50.

Tabelle 1. IMM2-Aktionen (Forts.)

Registerkarte	Auswahl	Beschreibung
Server Management (Serververwaltung) *(Fortsetzung)*	Processors (Prozessoren)	Auf der Seite für CPUs werden die Mikroprozessoren im System samt deren Status und Taktgeschwindigkeit angezeigt. Sie können auf den Namen eines Mikroprozessors klicken, um Ereignisse und weitere Hardwareinformationen für den Mikroprozessor anzuzeigen. Weitere Informationen finden Sie im Abschnitt „Processors (Prozessoren)" auf Seite 51.
	Server Timeouts (Serverzeitlimits)	Über die Seite "Server Timeouts" können Sie zur Erkennung von und zum Wiederherstellen nach aufgetretenen Blockierungen des Servers Startzeitlimits für den Server verwalten. Weitere Informationen finden Sie in den Abschnitten „Server Timeouts (Serverzeitlimits)" auf Seite 52 und „Serverzeitlimits festlegen" auf Seite 58.
	PXE Network Boot (PXE-Netzboot)	Auf der Seite "PXE Network Boot" können Sie die Startreihenfolge (Bootreihenfolge) des Host-Servers für den nächsten Neustart ändern, um einen PXE/DHCP-Netzwerkstart (Preboot Execution Environment/Dynamic Host Configuration Protocol) zu versuchen. Die Host-Startreihenfolge wird nur geändert, wenn für den Host kein privilegierter Zugriffsschutz (Privileged Access Protection, PAP) festgelegt ist. Weitere Informationen finden Sie in den Abschnitten „PXE Network Boot (PXE-Netzboot)" auf Seite 52 und „PXE-Netzboot einrichten" auf Seite 121.
	Latest OS Failure Screen (Letzte Betriebssystem-Fehleranzeige)	Auf der Seite "Latest OS Failure Screen" wird (falls vorhanden) eine Anzeige des letzten Betriebssystemfehlers auf dem Server angezeigt. Damit Ihr IMM2 Anzeigen von Betriebssystemfehlern aufzeichnen kann, muss der Watchdog Ihres Betriebssystems aktiviert sein. Weitere Informationen finden Sie in den Abschnitten „Latest OS Failure Screen (Letzte Betriebssystem-Fehleranzeige)" auf Seite 53 und „Daten der letzten Betriebssystem-Fehleranzeige erfassen" auf Seite 136.
	Power Management (Stromverbrauchssteuerung)	Über die Seite "Server Power Management" können Sie die Richtlinien zum Stromverbrauch und die Hardware verwalten. Hier befindet sich auch das Verlaufsprotokoll zur Stromverbrauchsmenge des Servers. Weitere Informationen finden Sie im Abschnitt „Serverstromversorgung verwalten" auf Seite 137.
IMM Management (IMM-Verwaltung) *(Fortsetzung auf der nächsten Seite)*	IMM Properties (IMM-Eigenschaften)	Die Seite "IMM Properties" ermöglicht den Zugriff auf unterschiedliche Eigenschaften und Einstellungen Ihres IMM2. Die folgenden Optionen sind von der Seite "IMM Properties" verfügbar: • Die Registerkarte "Firmware" enthält einen Link zum Abschnitt "Server Firmware" des Bereichs "Server Management". • Auf der Registerkarte "IMM Date and Time Settings" können Sie die Einstellung für Datum und Uhrzeit beim IMM2 anzeigen und konfigurieren. • Auf der Registerkarte "Serial Port" werden die IMM2-Einstellungen für den seriellen Anschluss konfiguriert. Diese Einstellungen schließen die von der Umleitungsfunktion des seriellen Anschlusses verwendete Baudrate des seriellen Anschlusses sowie die Schlüsselfolge zum Wechseln zwischen dem Modus zur seriellen Umleitung und dem CLI-Modus ein. Weitere Informationen finden Sie in Kapitel 4, „IMM2 konfigurieren", auf Seite 55.
	Users (Benutzer)	Auf der Seite "Users" werden die Anmeldeprofile und die allgemeinen Anmeldeeinstellungen für das IMM2 konfiguriert. Sie können auch Benutzerkonten anzeigen, die derzeit am IMM2 angemeldet sind. Die globalen Anmeldeeinstellungen umfassen das Aktivieren der LDAP-Serverauthentifizierung (Lightweight Directory Access Protocol), das Festlegen des Inaktivitätszeitlimits für das Web und das Anpassen der Einstellungen für die Accountsicherheit. Weitere Informationen finden Sie im Abschnitt „Benutzerkonten konfigurieren" auf Seite 63.

Tabelle 1. IMM2-Aktionen (Forts.)

Registerkarte	Auswahl	Beschreibung
IMM Management (IMM-Verwaltung) *(Fortsetzung)*	Network (Netz)	Die Seite "Network Protocol Properties" (Netzprotokolleigenschaften) ermöglicht den Zugriff auf Netzwerkeigenschaften, Statusangaben und Einstellungen Ihres IMM2: • Auf der Registerkarte "Ethernet" können Sie verwalten, wie das IMM2 über Ethernet kommuniziert. • Auf der Registerkarte "SNMP" werden die SNMPv1- und SNMPv3-Agenten konfiguriert. • Auf der Registerkarte "DNS" werden die DNS-Server konfiguriert, mit denen das IMM2 interagiert. • Auf der Registerkarte "DDNS" wird das Dynamic Domain Name System für das IMM2 aktiviert oder inaktiviert und konfiguriert. • Auf der Registerkarte "SMTP" werden SMTP-Serverinformationen für Alerts konfiguriert, die per E-Mail gesendet werden. • Auf der Registerkarte "LDAP" wird die Benutzerauthentifizierung für die Verwendung mit einem oder mehreren LDAP-Servern konfiguriert. • Auf der Registerkarte "Telnet" wird der Telnet-Zugriff auf das IMM2 verwaltet. • Über die Registerkarte "USB" wird die USB-Schnittstelle für die In-band-Kommunikation zwischen dem Server und dem IMM2 gesteuert. Diese Einstellungen haben keine Auswirkungen auf die USB-Fernsteuerungsfunktionen (Tastatur, Maus und Massenspeicher). • Auf der Registerkarte "Port Assignments" können Sie die Portnummern ändern, die von einigen Services auf dem IMM2 verwendet werden. Weitere Informationen finden Sie im Abschnitt „Netzprotokolle konfigurieren" auf Seite 72.
	Security (Sicherheit)	Die Seite "IMM Security" ermöglicht den Zugriff auf Sicherheitseigenschaften, Statusangaben und Einstellungen Ihres IMM2: • Auf der Registerkarte "HTTPS Server" können Sie den HTTPS-Server aktivieren oder inaktivieren und seine Zertifikate verwalten. • Auf der Registerkarte "CIM Over HTTPS" können Sie CIM over HTTPS aktivieren oder inaktivieren und die zugehörigen Zertifikate verwalten. • Auf der Registerkarte "LDAP Client" können Sie die LDAP-Sicherheit aktivieren oder inaktivieren und ihre Zertifikate verwalten. • Auf der Registerkarte "SSH Server" können Sie den SSH-Server aktivieren oder inaktivieren und seine Zertifikate verwalten. Weitere Informationen finden Sie im Abschnitt „Sicherheitseinstellungen konfigurieren" auf Seite 86.
	IMM Configuration (IMM-Konfiguration)	Auf der Seite "IMM Configuration" wird eine Zusammenfassung der aktuellen Einstellungen für die IMM2-Konfiguration angezeigt. Weitere Informationen finden Sie im Abschnitt „IMM-Konfiguration wiederherstellen und ändern" auf Seite 94.
	Restart IMM (IMM erneut starten)	Über die Seite "Restart IMM" können Sie das IMM2 zurücksetzen. Weitere Informationen finden Sie im Abschnitt „IMM2 erneut starten" auf Seite 94.
	Reset IMM to factory defaults... (IMM auf werkseitige Voreinstellungen zurücksetzen)	Über die Seite "Reset IMM to factory defaults..." können Sie die Konfiguration des IMM2 auf die werkseitigen Voreinstellungen zurücksetzen. Weitere Informationen finden Sie im Abschnitt „IMM2 auf die werkseitigen Voreinstellungen zurücksetzen" auf Seite 95. **Achtung:** Wenn Sie auf **Reset IMM to factory defaults...** klicken, gehen alle Änderungen, die Sie am IMM2 vorgenommen haben, verloren.
	Activation Key Management (Aktivierungsschlüsselverwaltung)	Auf der Seite "Activation Key Management" können Sie Aktivierungsschlüssel für optionale FoD-Funktionen (Features on Demand) des IMM2 oder des Servers verwalten. Weitere Informationen finden Sie im Abschnitt „Aktivierungsschlüsselverwaltung" auf Seite 96.

Kapitel 3. Übersicht über die IMM2-Webbenutzerschnittstelle

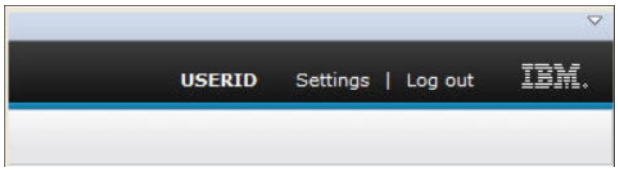
Dieses Kapitel enthält eine Übersicht der Funktionen der IMM2-Webbenutzerschnittstelle und ihre Verwendung.

Wichtig: Dieser Abschnitt gilt nicht für IBM BladeCenter und IBM Blade-Server. Obwohl das IMM2 in einigen IBM BladeCenter-Produkten und IBM Blade-Servern standardmäßig enthalten ist, bleibt das erweiterte IBM BladeCenter-Managementmodul das primäre Managementmodul für Systemmanagementfunktionen. Benutzer, die die IMM2-Einstellungen auf Blade-Servern konfigurieren möchten, sollten das Dienstprogramm für erweiterte Einstellungen (Advanced Settings Utility - ASU) auf dem Blade-Server zum Ausführen dieser Aktionen verwenden.

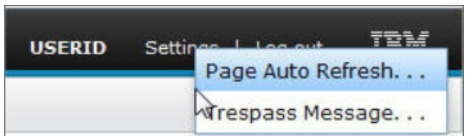
Websitzungseinstellungen

Dieser Abschnitt enthält Informationen zu den Einstellungen für die Hauptseite der Webschnittstellensitzung.

Auf der IMM2-Hauptseite werden Menüoptionen im oberen rechten Bereich der Webseite angezeigt. Mithilfe dieser Menüoptionen können Sie das Aktualisierungsverhalten der Webseite sowie die Nachricht, die einem Benutzer beim Eingeben des Berechtigungsnachweises zur Anmeldung angezeigt wird, konfigurieren. In der folgenden Abbildung werden die Menüoptionen im oberen rechten Bereich der Webseite dargestellt.

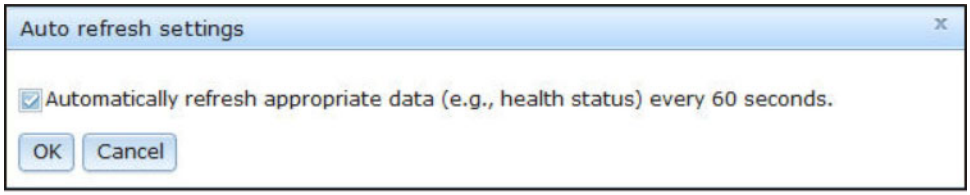


Klicken Sie auf die Menüoption **Settings** (Einstellungen). Die folgenden Menüoptionen werden angezeigt:



Page Auto Refresh

Verwenden Sie die Option **Page Auto Refresh** (Seite automatisch aktualisieren) unter der Menüoption "Settings" (Einstellungen) im oberen rechten Bereich der Websitzungsseite, um festzulegen, dass der Seiteninhalt alle 60 Sekunden automatisch aktualisiert wird. Um festzulegen, dass der Seiteninhalt alle 60 Sekunden aktualisiert wird, wählen Sie das Kontrollkästchen **Automatically refresh appropriate data...** (Entsprechende Daten automatisch aktualisieren) aus und klicken Sie auf **OK**. Um die automatische Aktualisierung der Seite zu inaktivieren, wählen Sie das Kontrollkästchen ab und klicken Sie auf **OK**. In der folgenden Abbildung ist das Fenster "Auto refresh settings" (Einstellungen für automatische Aktualisierung) dargestellt.



Manche IMM2-Webseiten werden automatisch aktualisiert, auch wenn das Kontrollkästchen zur automatischen Aktualisierung nicht ausgewählt ist. Folgende IMM2-Webseiten werden automatisch aktualisiert:

- **System Status** (Systemstatus):

  Der Systemstatus und der Stromversorgungsstatus werden automatisch alle drei Sekunden aktualisiert.
- **Server Power Actions** (Serverstromversorgungsaktionen, auf der Registerkarte "Server Management" (Serververwaltung)**:**

  Der Stromversorgungsstatus wird automatisch alle drei Sekunden aktualisiert.
- **Remote Control** (Fernsteuerung, auf der Registerkarte "Server Management"**:**

  Die Schaltflächen zur Option "Start remote control..." (Fernsteuerung starten) werden automatisch jede Sekunde aktualisiert. Die Tabelle "Session List" (Sitzungsliste) wird alle 60 Sekunden aktualisiert.

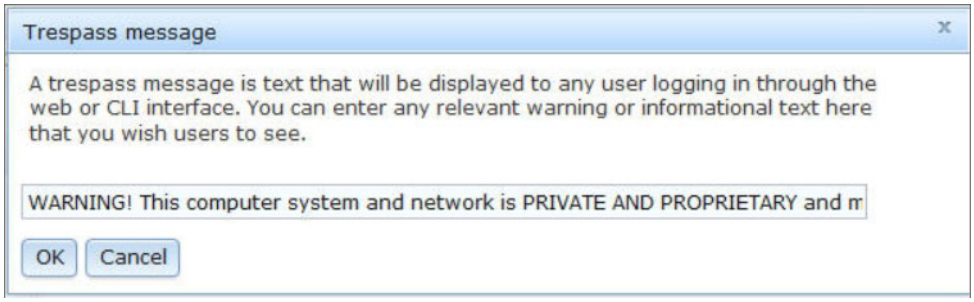
Anmerkungen:

- Wenn Sie über Ihren Web-Browser zu einer Webseite wechseln, die automatisch aktualisiert wird, wird Ihre Websitzung nicht automatisch durch das Inaktivitätszeitlimit beendet.
- Wenn Sie über die Seite mit den Optionen für die Fernsteuerung unter "Server Management" eine Anforderung an einen Fernsteuerungsbenutzer senden, läuft das Zeitlimit für Ihre Websitzung unabhängig davon, von welcher Webseite aus Sie navigieren, nicht ab, bis eine Antwort vom Fernsteuerungsbenutzer empfangen wird oder bis das Zeitlimit für den Fernsteuerungsbenutzer abläuft. Wenn die Verarbeitung der Anforderung durch den Fernsteuerungsbenutzer abgeschlossen wurde, wird die Funktion für das Inaktivitätszeitlimit wieder aktiv.

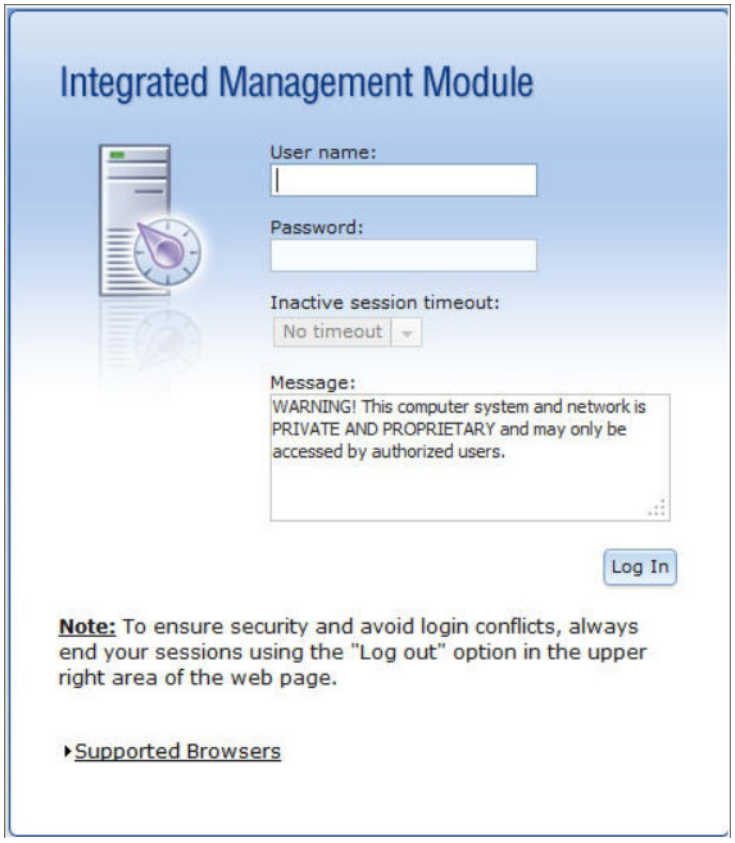
  Anmerkung: Die vorherige Anmerkung gilt für alle Webseiten.
- Die IMM2-Firmware unterstützt bis zu sechs gleichzeitige Websitzungen. Um Sitzungen für andere Benutzer freizugeben, melden Sie sich von der Websitzung ab, wenn Sie fertig sind, anstatt darauf zu warten, dass Ihre Sitzung durch das Inaktivitätszeitlimit automatisch geschlossen wird. Wenn Sie den Browser verlassen, während Sie sich auf einer IMM2-Webseite befinden, die automatisch aktualisiert wird, wird Ihre Websitzung nicht automatisch aufgrund von Inaktivität geschlossen.

Trespass Message

Verwenden Sie die Option **Trespass Message** (Übertretungsnachricht) unter der Menüoption "Settings" (Einstellungen) im oberen rechten Bereich der Websitzungsseite, um eine Nachricht zu konfigurieren, die angezeigt werden soll, wenn sich ein Benutzer beim IMM2-Server anmeldet. Die folgende Anzeige erscheint, wenn Sie die Option "Trespass Message" auswählen. Geben Sie den Nachrichtentext, der dem Benutzer angezeigt werden soll, im vorgesehenen Feld ein und klicken Sie auf **OK**.



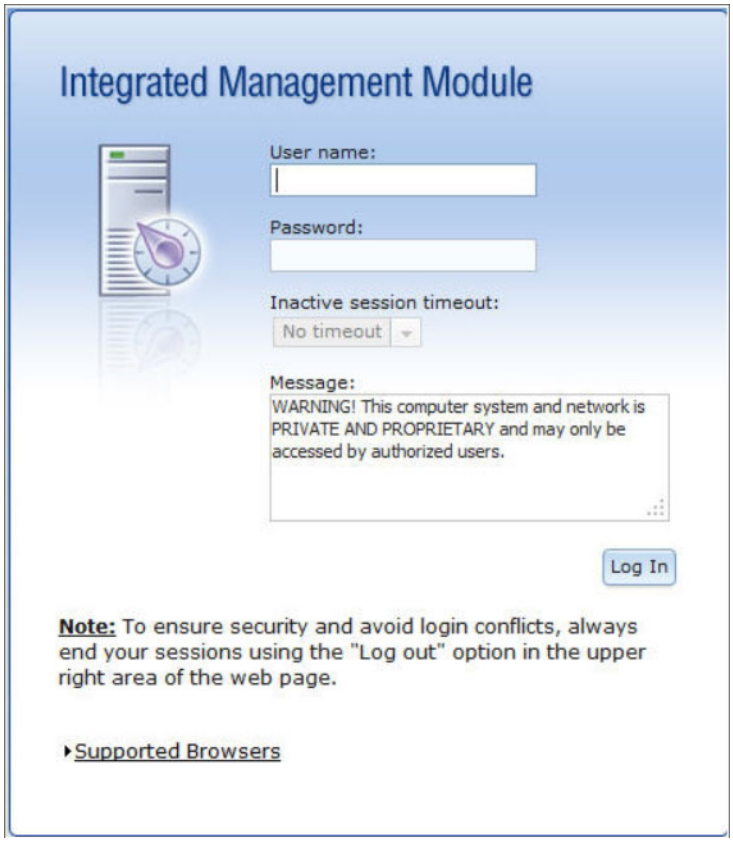
Der Nachrichtentext wird im Nachrichtenbereich der IMM2-Anmeldeseite angezeigt, wenn sich ein Benutzer anmeldet, wie in der folgenden Abbildung dargestellt.



Abmelden

Um unbefugten Zugriff zu verhindern, melden Sie sich von der IMM2-Websitzung ab, wenn Sie Ihre Arbeit beendet haben, und schließen Sie alle anderen IMM2-Web-Browser-Fenster, die Sie möglicherweise geöffnet haben, manuell.

Um sich von der Websitzung abzumelden, klicken Sie oben rechts auf der Webseite auf **Log out** (Abmelden). Das Fenster "Login" (Anmeldung) wird angezeigt.

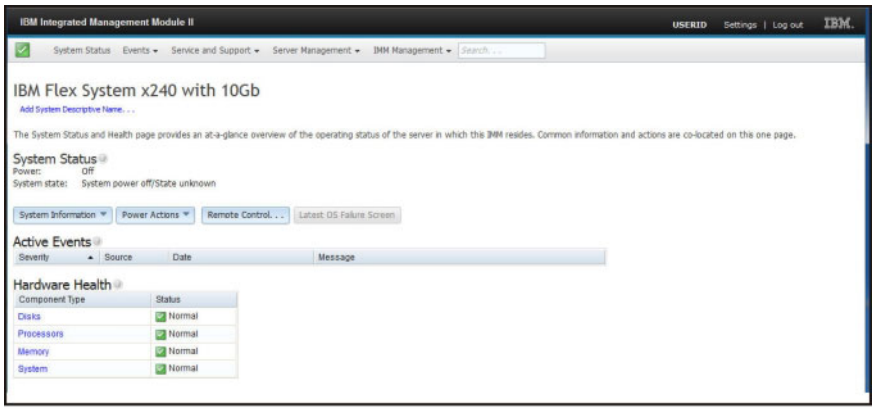


Anmerkung: Die IMM2-Firmware unterstützt bis zu sechs gleichzeitige Websitzungen. Um Sitzungen für andere Benutzer freizugeben, melden Sie sich von einer Websitzung ab, wenn Sie Ihre Arbeit beendet haben, anstatt darauf zu warten, dass die Sitzung nach dem Inaktivitätszeitlimit automatisch geschlossen wird. Wenn Sie das Browserfenster geöffnet lassen, während Sie eine IMM2-Webseite anzeigen, die automatisch aktualisiert wird, wird Ihre Websitzung nicht automatisch aufgrund von Inaktivität geschlossen.

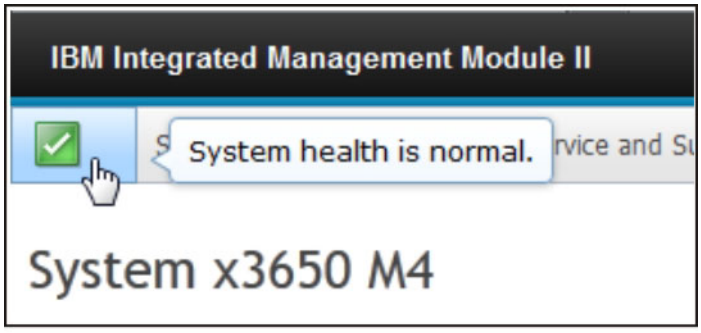
Registerkarte "System Status"

Dieser Abschnitt enthält Informationen zur Verwendung der Optionen auf der Registerkarte "System Status" (Systemstatus) in der IMM2-Webbenutzerschnittstelle.

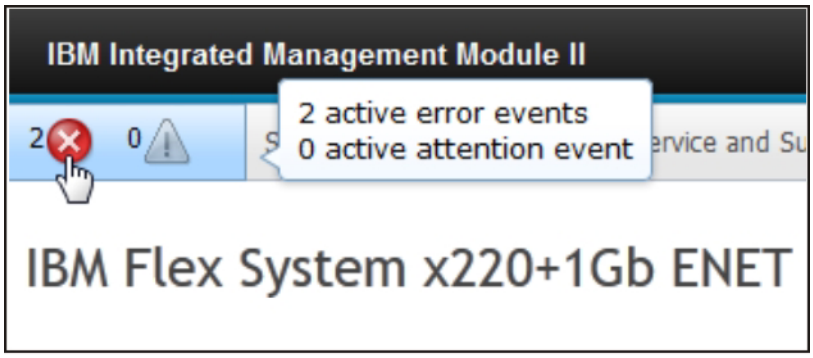
Die Seite "System Status" wird angezeigt, wenn Sie sich bei der IMM2-Webbenutzerschnittstelle angemeldet haben oder wenn Sie auf die Registerkarte "System Status" klicken. Auf der Seite "System Status" können Sie den Systemstatus, aktive Systemereignisse und Informationen zum Hardwarezustand anzeigen. Die folgende Anzeige wird geöffnet, wenn Sie auf die Registerkarte "System Status" klicken oder sich bei der IMM2-Webschnittstelle anmelden.



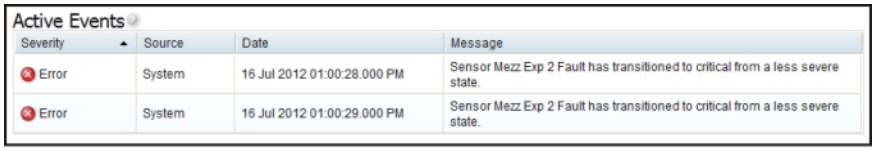
Sie können auf das grüne Symbol (mit dem Häkchen) in der oberen linken Ecke der Seite klicken, um eine kurze Übersicht über den Serverstatus zu erhalten. Ein Häkchen gibt an, dass der Server sich im Normalbetrieb befindet.



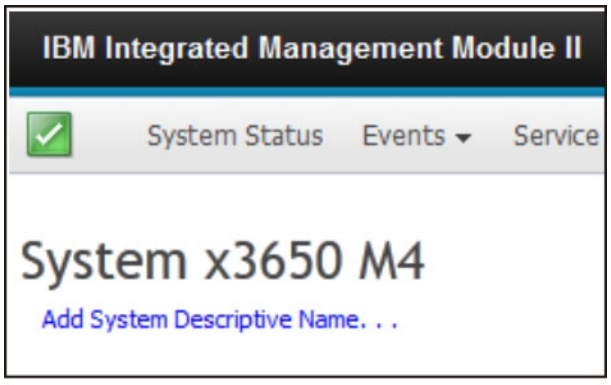
Wenn ein roter Kreis oder ein gelbes Dreieck angezeigt wird, bedeutet dies, dass eine Fehler- oder Warnbedingung vorliegt, wie in der folgenden Abbildung dargestellt.



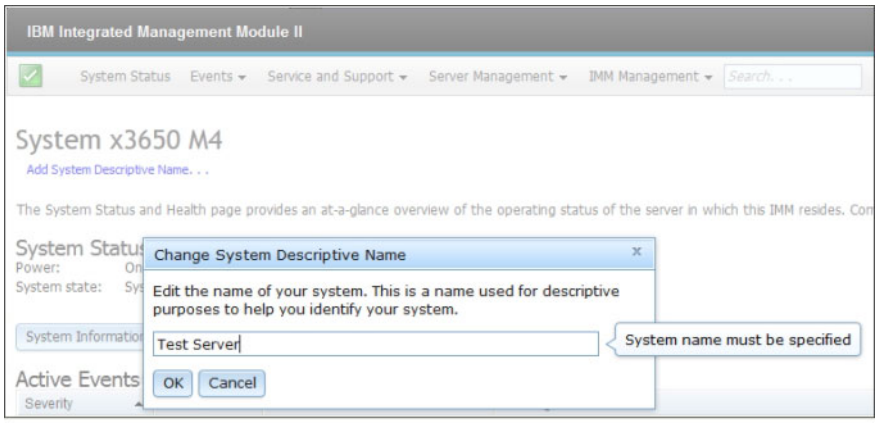
Das Symbol mit dem roten Kreis gibt an, dass auf dem Server eine Fehlerbedingung vorliegt. Das Symbol mit dem gelben Dreieck gibt an, dass eine Warnbedingung vorliegt. Wenn ein Symbol mit einem roten Kreis oder einem gelben Dreieck angezeigt wird, sind die Ereignisse, die der Bedingung zugeordnet sind, im Abschnitt "Active Events" (Aktive Ereignisse) auf der Seite "System Status" aufgeführt, wie in der folgenden Abbildung dargestellt.



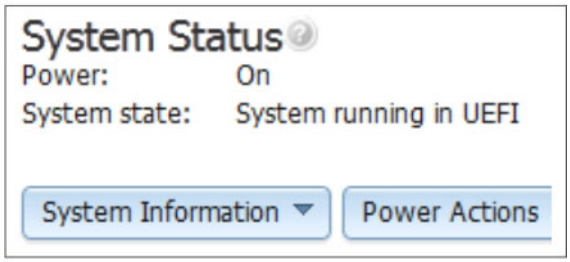
Sie können zum IMM2-Server einen beschreibenden Namen hinzufügen, damit Sie die einzelnen IMM2-Server voneinander unterscheiden können. Um dem IMM2-Server einen beschreibenden Namen zuzuordnen, klicken Sie auf den Link **Add System Descriptive Name...** (Beschreibenden Systemnamen hinzufügen) unter dem Namen des Serverprodukts.



Wenn Sie auf den Link **Add System Descriptive Name...** (Beschreibenden Systemnamen einfügen) klicken, wird das folgende Fenster angezeigt, in dem Sie einen Namen eingeben können, der dem IMM2-Server zugeordnet wird. Sie können den beschreibenden Systemnamen jederzeit ändern.



Der Abschnitt **System Status** auf der Seite "System Status" enthält Informationen zum Stromversorgungsstatus und zum Betriebsstatus des Servers. Angezeigt wird der Serverstatus zum Zeitpunkt des Öffnens der Seite "System Status" (wie in der folgenden Abbildung dargestellt).



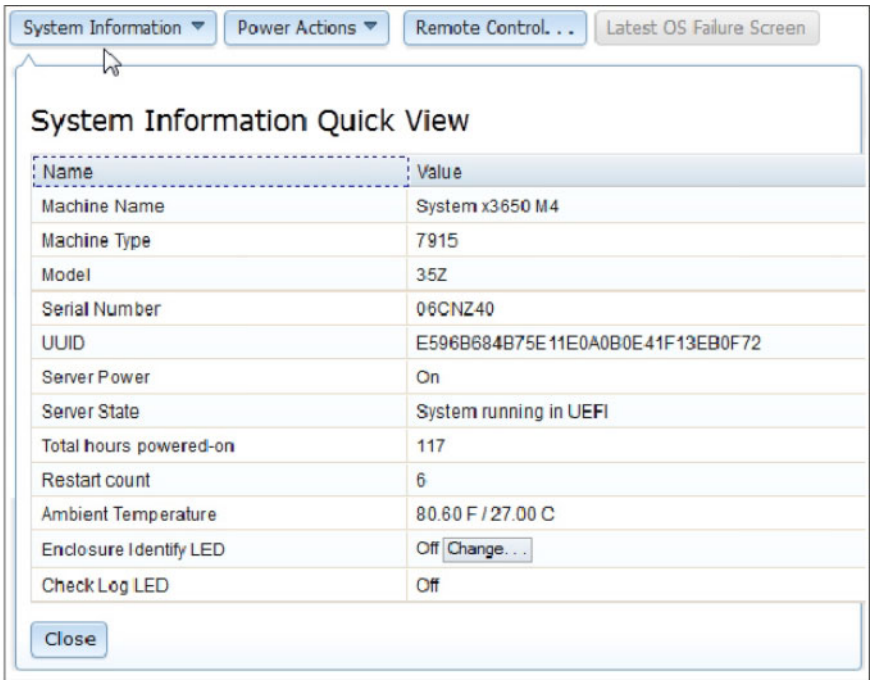
Der Server kann sich in einem der folgenden Status befinden:

Tabelle 2. Stromversorgungsstatus und Betriebsstatus des Servers

Serverstatus	**Beschreibung**
System power off/state unknown (Stromversorgung des Systems ausgeschaltet/Status unbekannt)	Der Server ist ausgeschaltet.
System on/starting UEFI (System eingeschaltet/UEFI wird gestartet)	Der Server ist eingeschaltet, aber die UEFI wird noch nicht ausgeführt.
System running in UEFI (System wird in UEFI ausgeführt)	Der Server ist eingeschaltet und die UEFI wird ausgeführt.
System stopped in UEFI (System wurde in UEFI gestoppt)	Der Server ist eingeschaltet; die UEFI hat einen Fehler erkannt und ihre Ausführung wurde beendet.
Booting OS or in unsupported OS (Betriebssystem wird gebootet oder es wird ein nicht unterstütztes Betriebssystem gebootet)	Der Server kann sich aus einem der folgenden Gründe in diesem Status befinden: • Das Ladeprogramm des Betriebssystems wurde gestartet, aber das Betriebssystem wird noch nicht ausgeführt. • Die Ethernet-over-USB-Schnittstelle des IMM2 ist inaktiviert. • Das Betriebssystem hat die Treiber, die die Ethernet-over-USB-Schnittstelle unterstützen, nicht geladen.
OS booted (Betriebssystem gebootet)	Das Serverbetriebssystem wird ausgeführt.
Suspend to RAM (Aussetzen in RAM)	Der Server wurde in den Bereitschafts- oder Ruhemodus versetzt.

Auf der Seite "System Status" werden außerdem die Registerkarten **System Information** (Systeminformationen), **Power Actions** (Stromversorgungsaktionen), **Remote Control** (Fernsteuerung) und **Latest OS Failure Screen** (Letzte Betriebssystem-Fehleranzeige) angezeigt.

Klicken Sie auf die Registerkarte **System Information**, um Informationen zum Server anzuzeigen.

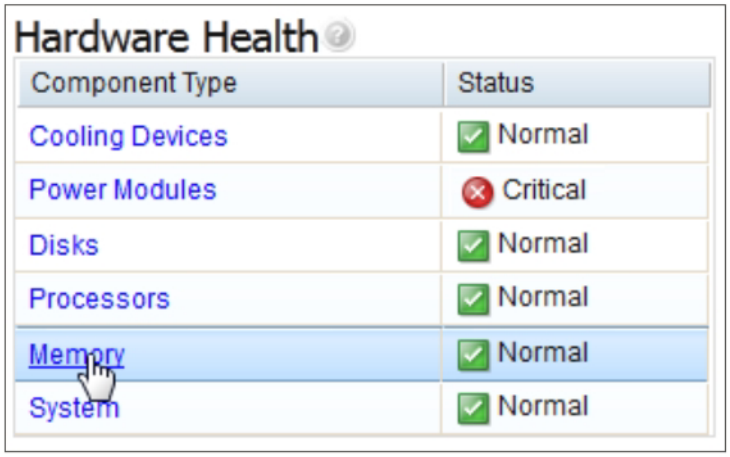


Klicken Sie auf die Registerkarte **Power Actions**, um die Aktionen anzuzeigen, die Sie zur vollständigen fernen Stromversorgungssteuerung des Servers über die Aktionen zum Einschalten, Ausschalten und Neustarten des Servers durchführen können. Details zur fernen Steuerung der Stromversorgung des Servers finden Sie unter „Stromversorgungsstatus des Servers steuern” auf Seite 106.

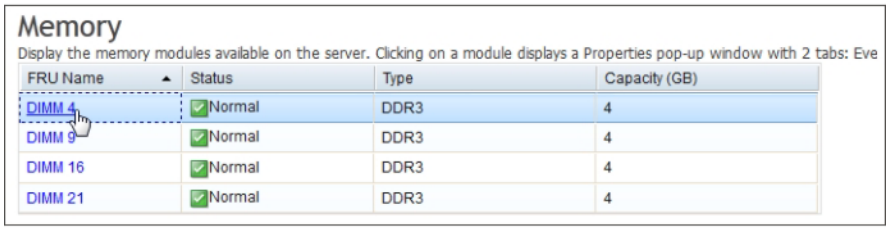
Klicken Sie auf die Registerkarte **Remote Control**, um Informationen zur Steuerung des Servers auf Betriebssystemebene zu erhalten. Unter „Remote-Presence- und Fernsteuerungsfunktionen” auf Seite 107 finden Sie Details zur Funktion "Remote Control".

Klicken Sie auf die Registerkarte **Latest OS Failure Screen**, um Informationen zum Erfassen der Daten der letzten Betriebssystem-Fehleranzeige zu erhalten. Details zur letzten Betriebssystem-Fehleranzeige finden Sie unter „Daten der letzten Betriebssystem-Fehleranzeige erfassen” auf Seite 136.

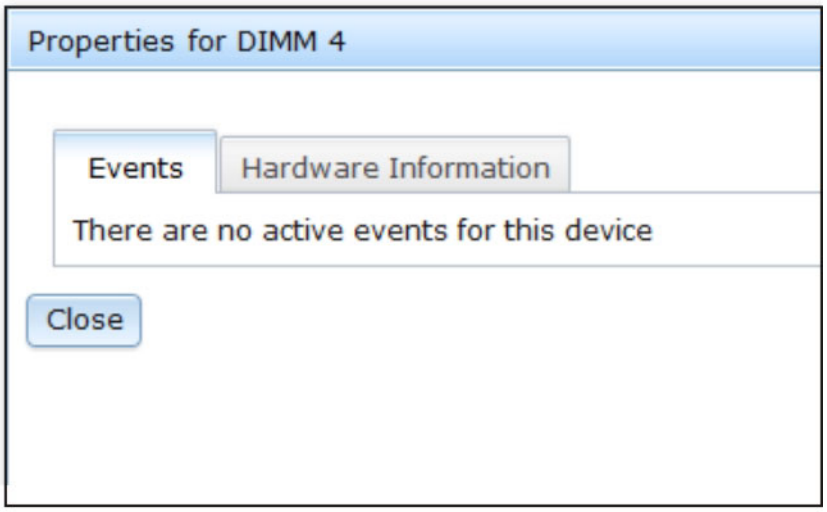
Im Abschnitt **Hardware Health** (Hardwarezustand) der Seite "System Status" befindet sich eine Tabelle mit einer Liste der überwachten Hardwarekomponenten und deren Status. In der Spalte "Component Type" (Komponententyp) der Tabelle wird möglicherweise der Zustand der Komponente mit dem kritischsten Zustand angezeigt. Ein Server kann z. B. über mehrere installierte Stromversorgungsmodule verfügen, die bis auf eines alle normal funktionieren. Der Status der Komponente "Power Modules" (Stromversorgungsmodule) wird dann aufgrund dieses einen Stromversorgungsmoduls als kritisch angezeigt (wie in der folgenden Abbildung dargestellt).



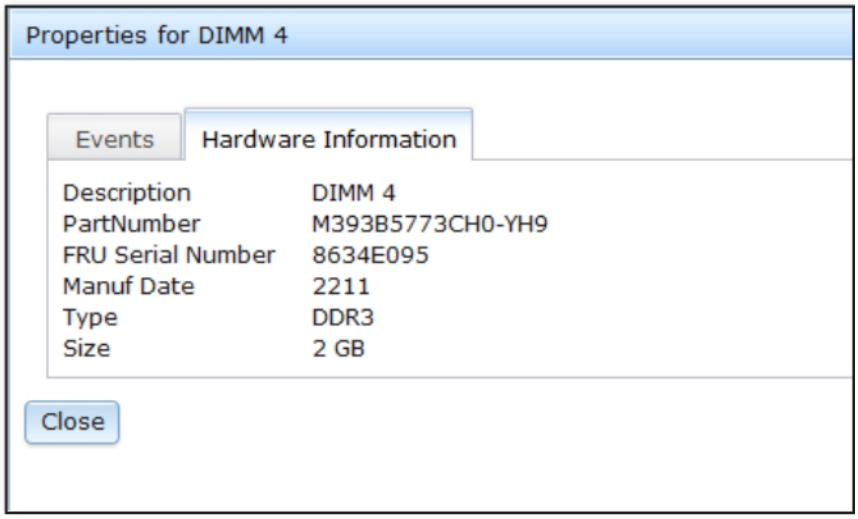
Bei jedem Komponententyp handelt es sich um einen Link, auf den Sie klicken können, um ausführlichere Informationen zu erhalten. Wenn Sie auf den Komponententyp klicken, wird eine Tabelle angezeigt, in der die Status der einzelnen Komponenten aufgeführt sind (wie in der folgenden Abbildung dargestellt).



Sie können auf eine Komponente in der Spalte "FRU Name" (Name der durch den Kundendienst austauschbaren Funktionseinheit) klicken, um zusätzliche Informationen zu dieser Komponente zu erhalten. Alle aktiven Ereignisse für die Komponente werden angezeigt.



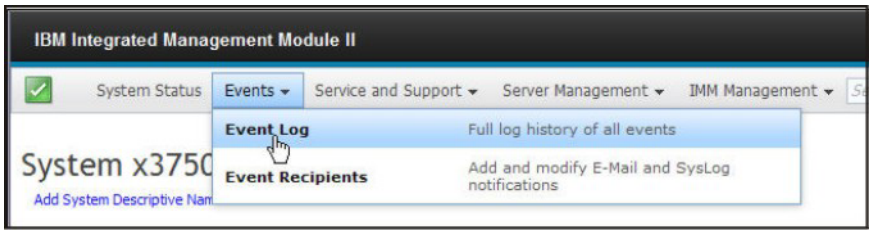
Klicken Sie auf die Registerkarte **Hardware Information** (Hardwareinformationen), um ausführliche Informationen zur Komponente anzuzeigen.



Registerkarte "Events" (Ereignisse)

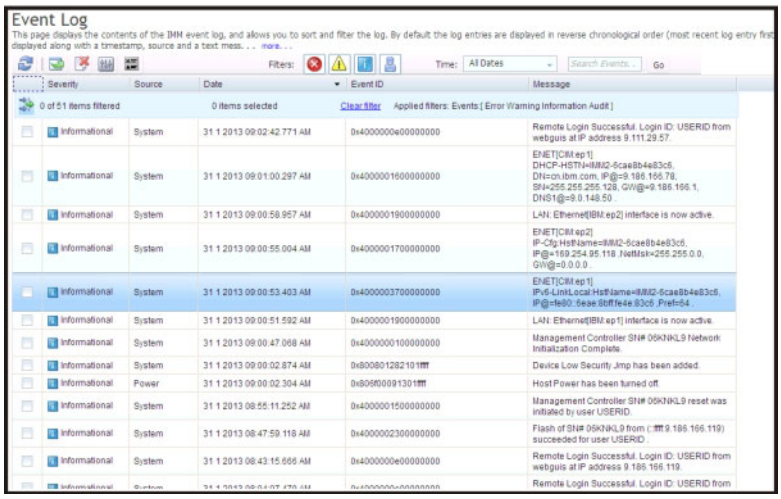
Dieser Abschnitt enthält Informationen zur Verwendung der Optionen auf der Registerkarte "Events" in der IMM2-Webbenutzerschnittstelle.

Die Optionen auf der Registerkarte **Events** ermöglichen Ihnen die Verwaltung des Ereignisprotokollverlaufs (Event Log) und der Ereignisempfänger (Event Recipients) für E-Mail- und syslog-Benachrichtigungen. In der folgenden Abbildung sind die Optionen auf der Registerkarte "Events" auf der IMM2-Webseite dargestellt.

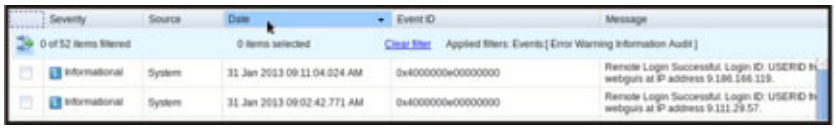


Event Log (Ereignisprotokoll)

Wählen Sie auf der Registerkarte "Events" (Ereignisse) die Option **Event Log** (Ereignisprotokoll) aus, um die Seite "Event Log" anzuzeigen. Auf der Seite "Event Log" wird der Schweregrad der Ereignisse angezeigt, die vom IMM2 gemeldet wurden, und Informationen zu allen Fernzugriffversuchen sowie zu allen Konfigurationsänderungen. Alle Ereignisse im Protokoll weisen eine Zeitmarke auf, die die IMM2-Einstellung für Datum und Uhrzeit verwendet. Einige Ereignisse generieren außerdem Alerts, falls dies auf der Seite "Event Recipients" (Ereignisempfänger) so konfiguriert wurde. Sie können Ereignisse im Ereignisprotokoll sortieren und filtern. In der folgenden Abbildung ist ein Beispiel für die Seite "Event log" dargestellt.

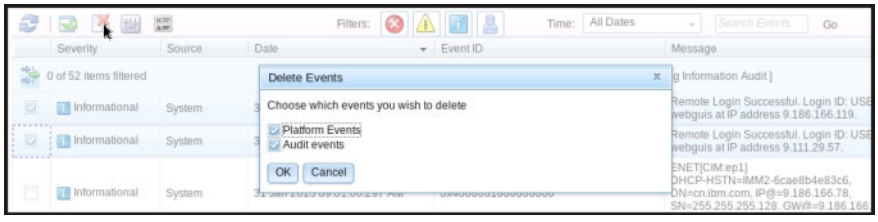


Um Ereignisse im Ereignisprotokoll zu sortieren und zu filtern, wählen Sie die entsprechende Spaltenüberschrift aus (wie in der folgenden Abbildung dargestellt).



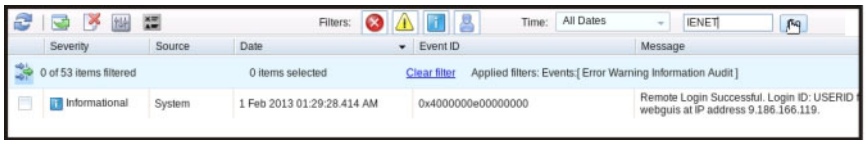
Sie können mithilfe der Schaltfläche **Export** alle oder ausgewählte Ereignisse aus dem Ereignisprotokoll speichern. Um bestimmte Ereignisse auszuwählen, wählen Sie auf der Hauptseite von "Event Log" ein oder mehr Ereignisse aus und klicken Sie mit der linken Maustaste auf die Schaltfläche **Export** (Exportieren) (wie in der folgenden Abbildung dargestellt).

Mit der Schaltfläche **Delete Events** (Ereignisse löschen) können Sie den Ereignistyp auswählen, den Sie löschen möchten (wie in der folgenden Abbildung dargestellt).

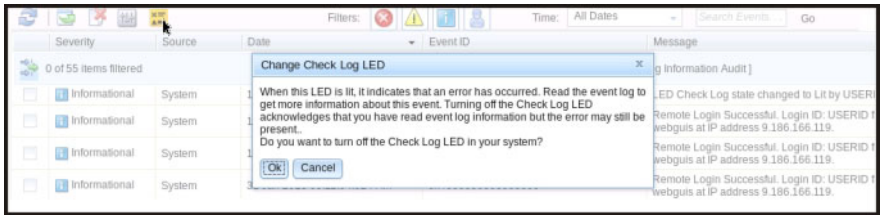


Um den Typ der Ereignisprotokolleinträge auszuwählen, den Sie anzeigen möchten, klicken Sie auf die entsprechende Schaltfläche (wie in der folgenden Abbildung dargestellt).

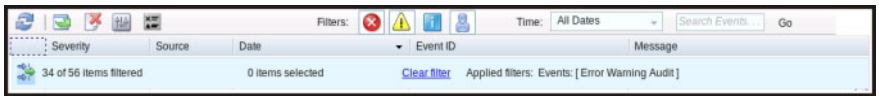
Um nach bestimmten Ereignistypen oder Suchbegriffen zu suchen, geben Sie den betreffenden Ereignistyp oder den Suchbegriff im Feld **Search Events** (Ereignisse suchen) ein. Klicken Sie dann auf **Go** (Start) (wie in der folgenden Abbildung dargestellt).



Um die Protokollprüfanzeige "Check Log LED" auszuschalten, wenn die Protokollprüfanzeige angeschaltet ist und die zugehörigen "Event Logs" (Ereignisprotokolle) ausgewählt wurden, klicken Sie auf die Schaltfläche **Check Log LED Status** (Status der Protokollprüfanzeige) (wie in der folgenden Abbildung dargestellt).

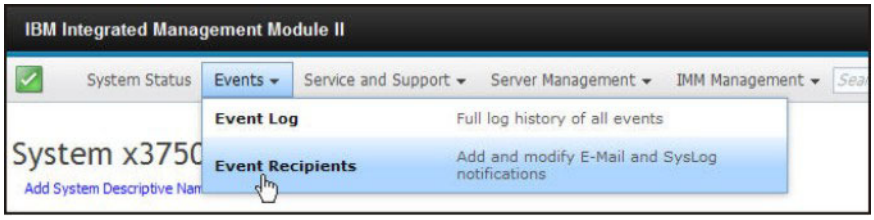


In der Symbolleiste "Event Log" (Ereignisprotokoll) können Sie auf jede beliebige Schaltfläche von **Filter Events** (Ereignisse filtern) klicken, um die Ereignisse auszuwählen, die angezeigt werden sollen. Um den Filter zu löschen und alle Ereignistypen anzuzeigen, klicken Sie auf den in der folgenden Abbildung dargestellten Link **Clear Filter** (Filter löschen).



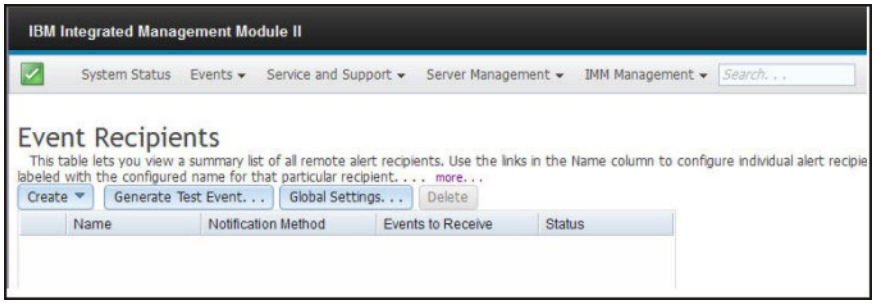
Event Recipients (Ereignisempfänger)

Mit der Option **Events Recipients** (Ereignisempfänger) auf der Registerkarte "Events" (Ereignisse) können Sie E-Mail- und syslog-Benachrichtigungen hinzufügen und ändern.



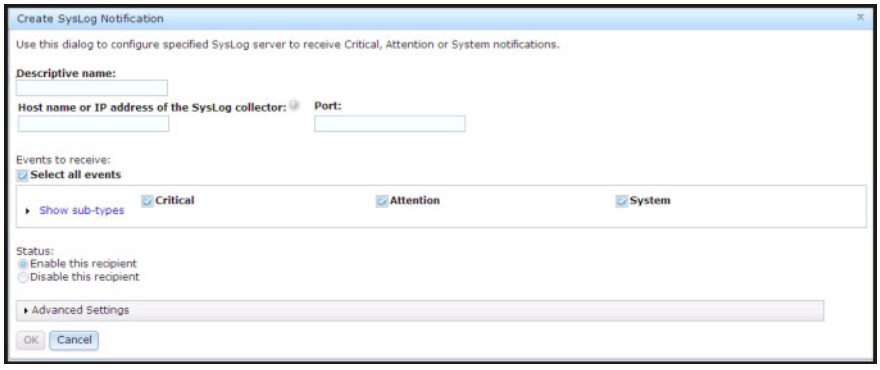
Mithilfe der Option "Event Recipients" können Sie die Empfänger von Benachrichtigungen über Systemereignisse verwalten. Sie können die einzelnen Empfänger konfigurieren und die Einstellungen verwalten, die für alle Ereignisempfänger gelten. Sie können auch ein Testereignis generieren, um die Benachrichtigungsfunktion zu überprüfen.

Klicken Sie auf die Schaltfläche **Create** (Erstellen), um E-Mail- und syslog-Benachrichtigungen zu erstellen.

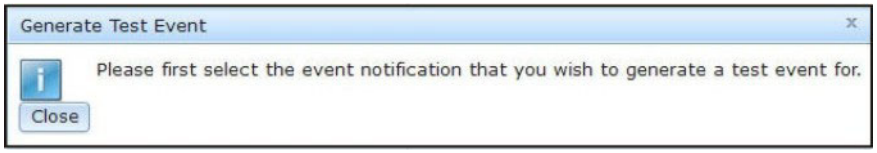


Wählen Sie die Option **Create E-mail Notification** (E-Mail-Benachrichtigung erstellen) aus, um eine Ziel-E-Mail-Adresse einzurichten und den Ereignistyp auszuwählen, für den Benachrichtigungen gesendet werden sollen. Außerdem können Sie auf **Advanced Settings** (Erweiterte Einstellungen) klicken, um die Startindexnummer auszuwählen. Um das Ereignisprotokoll in die E-Mail einzufügen, wählen Sie das Kontrollkästchen **Include the event log contents in the e-mail body** (Inhalt des Ereignisprotokolls in den Nachrichtentext der E-Mail einfügen) aus. In der folgenden Abbildung ist ein Beispiel für das Fenster "Create E-mail notification" dargestellt.

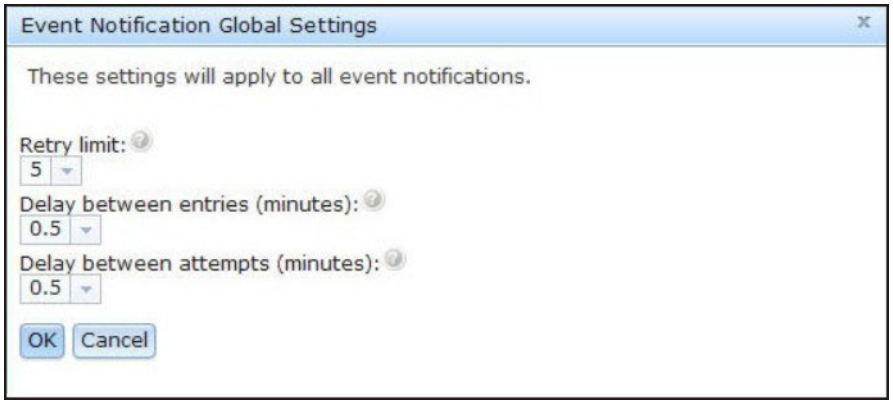
Wählen Sie die Option **Create SysLog Notification** (SysLog-Benachrichtigung erstellen) aus, um einen Hostnamen und eine IP-Adresse für den SysLog-Collector einzurichten und den Ereignistyp auszuwählen, für den Benachrichtigungen gesendet werden sollen. Außerdem können Sie auf **Advanced Settings** (Erweiterte Einstellungen) klicken, um die Startindexnummer auszuwählen. Sie können außerdem den Port auswählen, den Sie für diesen Benachrichtigungstyp verwenden möchten. In der folgenden Abbildung ist ein Beispiel für das Fenster "Create SysLog Notification" dargestellt.



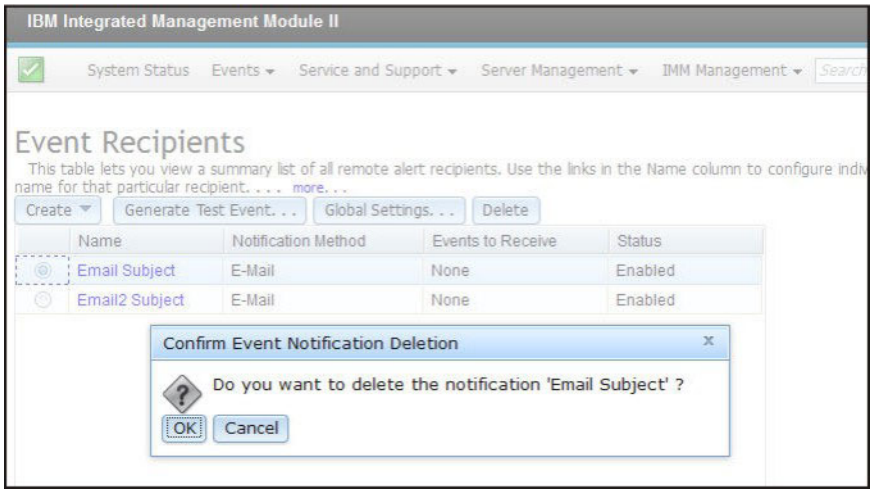
Wählen Sie die Schaltfläche **Generate Test Event** (Testereignis generieren) aus, um eine Test-E-Mail an das ausgewählte E-Mail-Ziel zu senden (wie in der folgenden Abbildung dargestellt).



Wählen Sie die Schaltfläche **Global Settings** (Globale Einstellungen) aus, um einen Grenzwert für die Wiederholungsversuche für Ereignisbenachrichtigungen, die Verzögerung (in Minuten) zwischen den Ereignisbenachrichtigungseinträgen und die Verzögerung (in Minuten) zwischen den Benachrichtigungsversuchen festzulegen (wie in der folgenden Abbildung dargestellt).



Wenn Sie ein Ziel für eine E-Mail- oder syslog-Benachrichtigung entfernen möchten, wählen Sie die Schaltfläche **Delete** (Löschen) aus. Das folgende Fenster wird geöffnet:

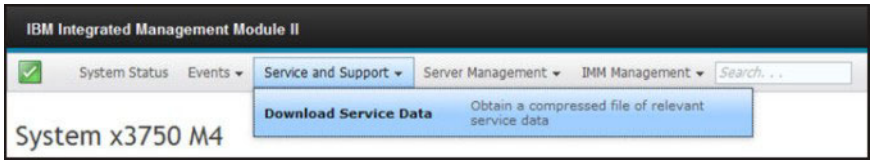


Registerkarte "Service and Support"

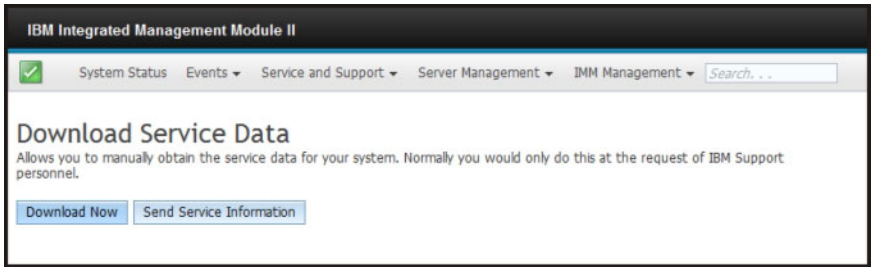
Dieser Abschnitt enthält Informationen zur Verwendung der Optionen auf der Registerkarte "Service and Support" der IMM2-Webbenutzerschnittstelle.

Download Service Data (Servicedaten herunterladen)

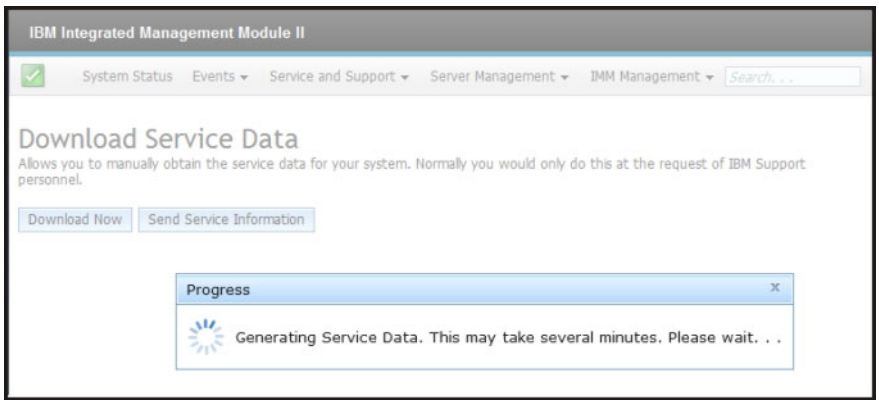
Verwenden Sie die Option **Download Service Data** (Servicedaten herunterladen) auf der Registerkarte "Service and Support" (Service und Unterstützung), um Informationen zu sammeln und eine komprimierte Datei über den Server zu erstellen, die Sie als Hilfestellung bei der Fehlerbestimmung an den IBM Support schicken können.



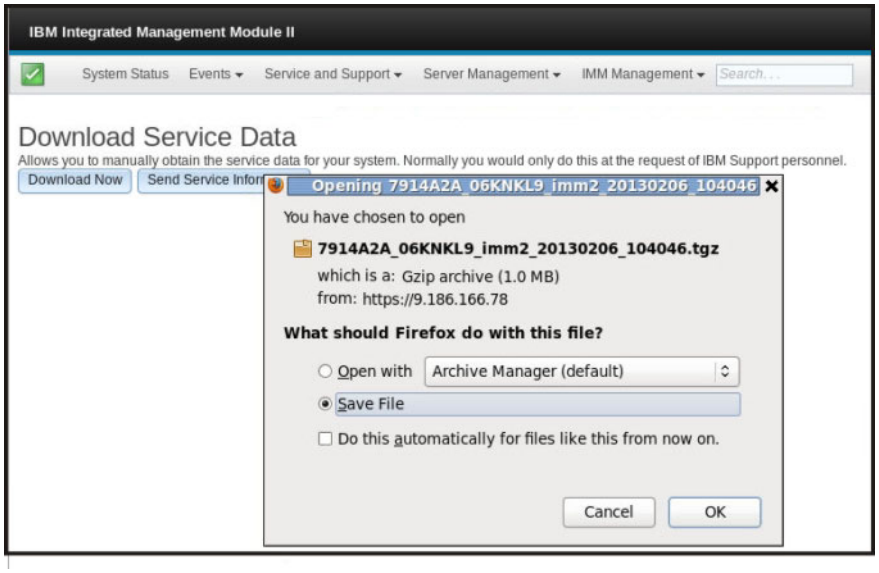
Klicken Sie auf die Schaltfläche **Download Now** (Jetzt herunterladen), um die Informationen zu Service und Support herunterzuladen (siehe folgende Abbildung).



Der Prozess zum Sammeln der Daten beginnt. Der Prozess generiert in ein paar Minuten die Servicedaten, die Sie dann in einer Datei speichern können. In einem Fortschrittsfenster wird angezeigt, dass die Daten generiert werden.



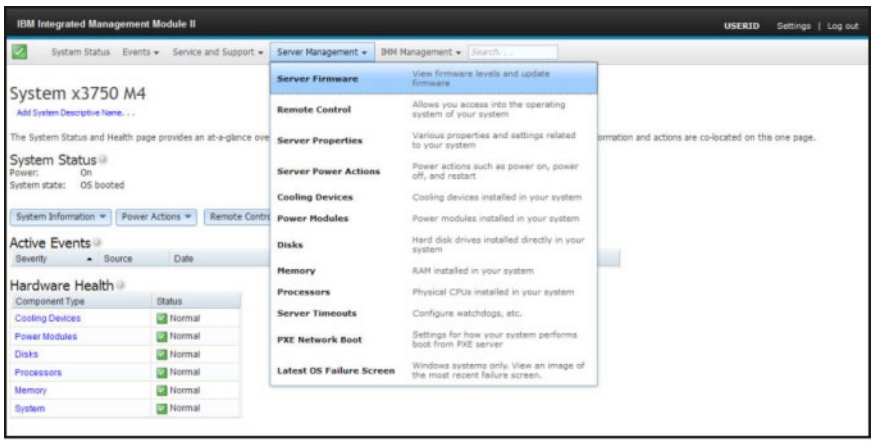
Wenn der Prozess abgeschlossen ist, wird das folgende Fenster angezeigt, das Sie auffordert anzugeben, auf welcher Position die generierte Datei gespeichert werden soll.



Registerkarte "Server Management" (Serververwaltung)

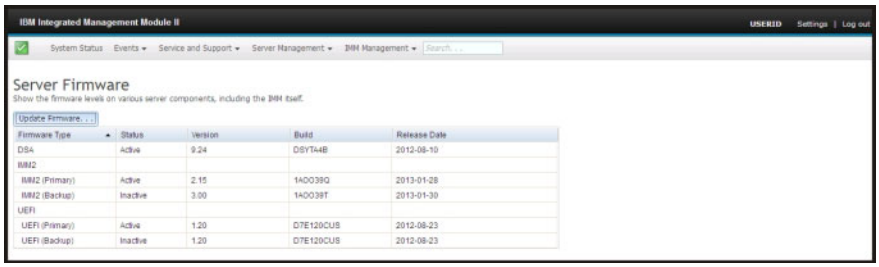
Dieser Abschnitt enthält Informationen zu den Optionen auf der Registerkarte "Server Management" (Serververwaltung) auf der Homepage der IMM2-Webbenutzerschnittstelle.

Mithilfe der Optionen auf der Registerkarte "Server Management" können Sie Informationen zum Status und zur Steuerung der Server-Firmware, zum Fernsteuerungszugriff, zum Status und zur Steuerung der Servereigenschaften, zu Serverstromversorgungsaktionen, zu Kühleinheiten, zu Stromversorgungsmodulen, zu Datenträgern, zum Speicher, zu Prozessoren, zu Zeitlimitüberschreitungen auf dem Server, zum PXE-Netzboot und zur letzten Betriebssystem-Fehleranzeige anzeigen (wie in der folgenden Abbildung dargestellt).



Server Firmware (Server-Firmware)

Wählen Sie die Option **Server Firmware** (Server-Firmware) auf der Registerkarte "Server Management" (Serververwaltung) aus, um die auf dem Server installierten Firmwareversionen anzuzeigen und Firmwareaktualisierungen anzuwenden. In der folgenden Anzeige werden die Server-Firmwareversionen angezeigt. Sie können über diese Anzeige die DSA-, IMM2- und UEFI-Firmware aktualisieren.



Der aktuelle Status und die aktuellen Versionen der IMM2-, UEFI- und DSA-Firmware werden angezeigt, einschließlich der primären Versionen und der Sicherungsversionen. Der Status der Firmware wird in drei Kategorien angegeben:

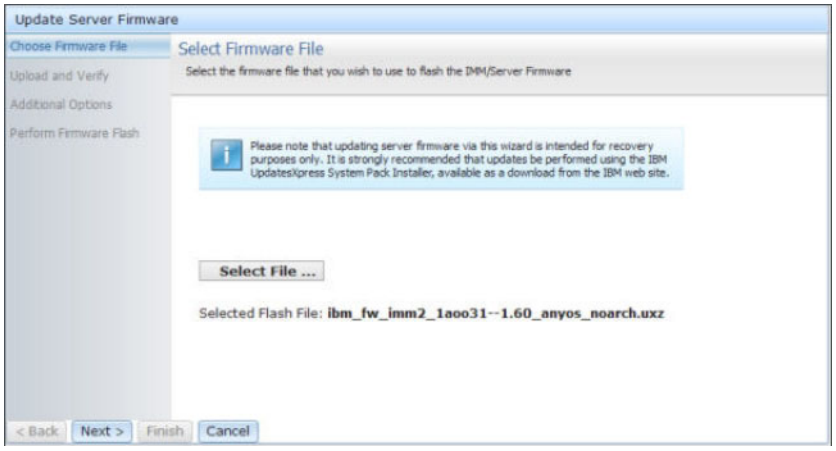
- **Active** (aktiv): Die Firmware ist aktiv.
- **Inactive** (inaktiv): Die Firmware ist inaktiv.
- **Pending** (anstehend): Die Firmware befindet sich im Wartestatus vor der Aktivierung.

Achtung: Die Installation der falschen Firmware könnte eine Serverstörung verursachen. Bevor Sie eine Firmware- oder Einheitentreiberaktualisierung installieren, lesen Sie alle Readme- und Änderungsprotokolldateien, die mit der heruntergeladenen Aktualisierung bereitgestellt werden. Diese Dateien enthalten wichtige Informationen zur Aktualisierung und zur Installationsprozedur der Aktualisierung, einschließlich Informationen zu besonderen Prozeduren bei der Aktualisierung von einer frühen Firmware- oder Einheitentreiberversion auf die neueste Version.

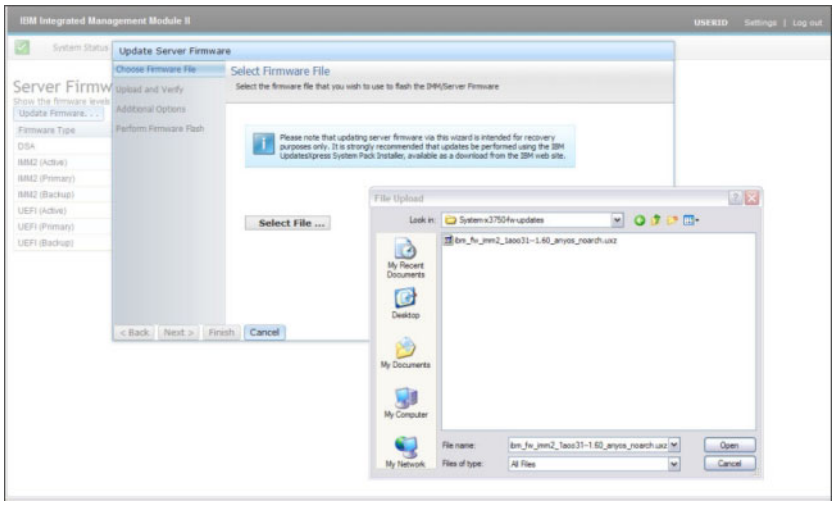
Um die Firmware zu aktualisieren, wählen Sie die Schaltfläche **Update Firmware...** (Firmware aktualisieren) aus. Das Fenster "Update Server Firmware" (Server-Firmware aktualisieren) wird angezeigt. Sie können auf **Cancel** (Abbrechen) klicken und zum vorherigen Fenster von "Server Firmware" zurückkehren, oder auf die

Schaltfläche **Select File...** (Datei auswählen) klicken, um die Firmwaredatei auszuwählen, die Sie für die Flashaktualisierung der Server-Firmware verwenden möchten.

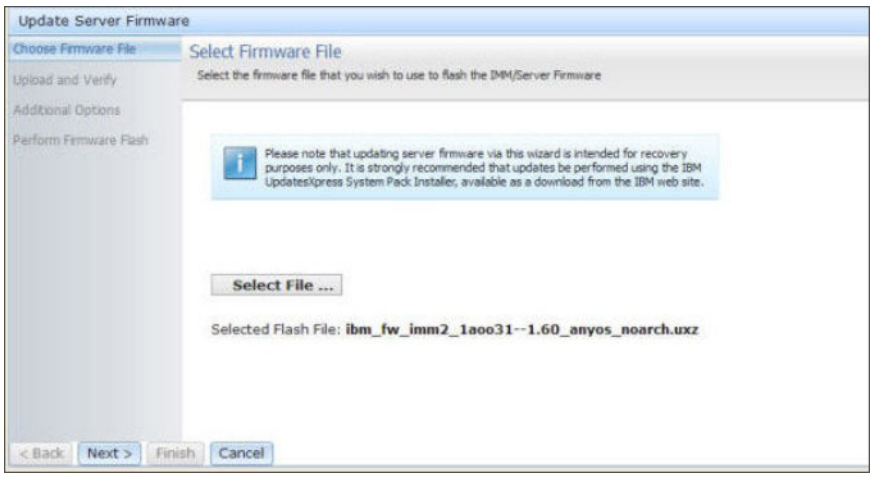
Anmerkung: Lesen Sie die in der Eingabeaufforderung angezeigte Warnung, bevor Sie auf die Schaltfläche **Select File...** (Datei auswählen) klicken.



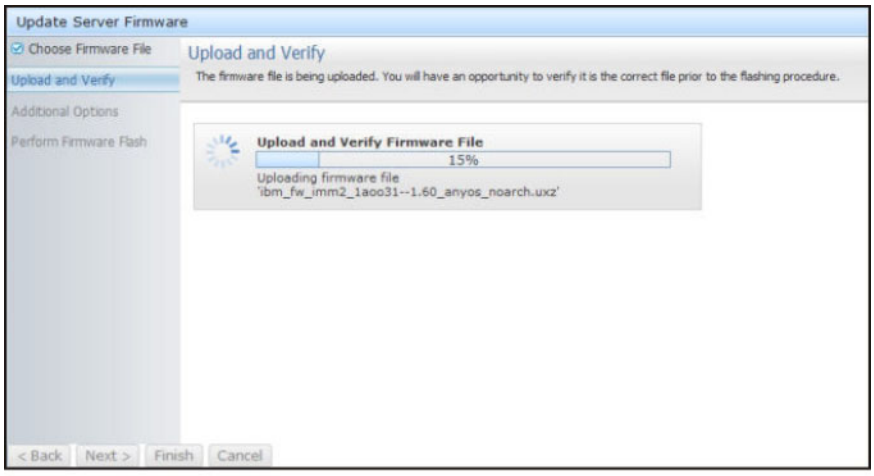
Wenn Sie auf die Schaltfläche **Select File...** klicken, wird das Fenster "File Upload" (Hochladen von Datei) angezeigt, in dem Sie nach der gewünschten Datei suchen können.



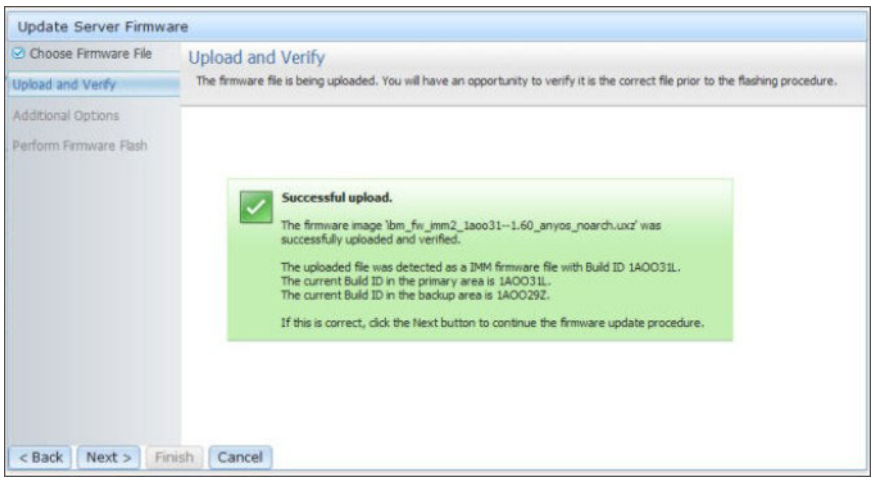
Klicken Sie, nachdem Sie zu der Datei navigiert sind, die Sie auswählen möchten, auf die Schaltfläche **Open** (Öffnen). Sie gelangen zurück zum Fenster "Update Server Firmware", in dem nun die ausgewählte Datei angezeigt wird (wie in der folgenden Abbildung dargestellt).



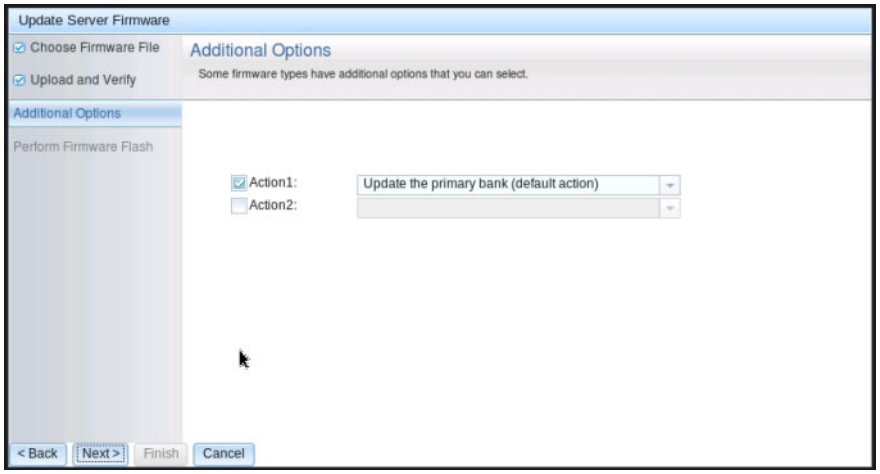
Klicken Sie auf die Schaltfläche **Next >** (Weiter), um den Upload- und Überprüfungsprozess für die ausgewählte Datei zu starten (wie in der folgenden Abbildung dargestellt). Eine Fortschrittsanzeige erscheint, während die Datei hochgeladen und überprüft wird.



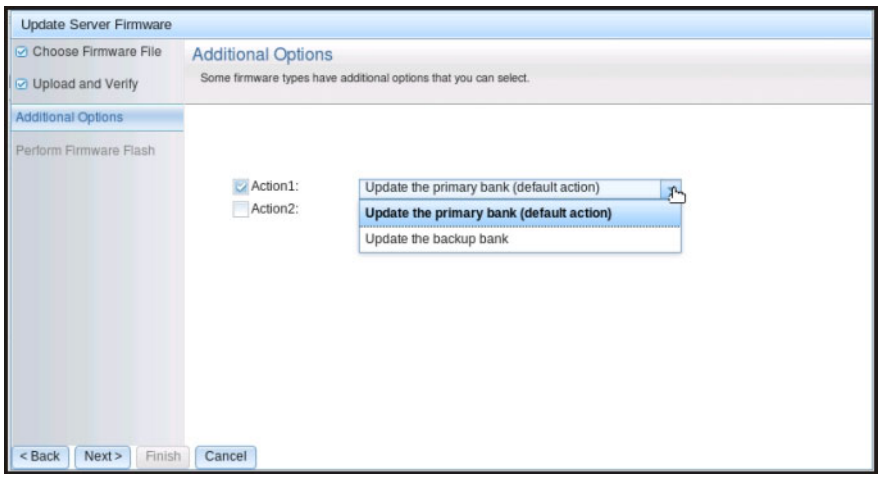
Ein Statusfenster wird angezeigt (wie in der folgenden Abbildung dargestellt), in dem Sie überprüfen können, ob es sich bei der ausgewählten zu aktualisierenden Datei um die richtige Datei handelt. Das Fenster enthält Informationen zum Typ der zu aktualisierenden Firmwaredatei, z. B. DSA, IMM2 oder UEFI. Wenn die Informationen richtig sind, klicken Sie auf die Schaltfläche **Next >**. Wenn Sie ausgewählte Optionen wieder abwählen möchten, klicken Sie auf die Schaltfläche **< Back** (Zurück).



Wenn Sie auf die Schaltfläche "Next >" klicken, wird eine Gruppe zusätzlicher Optionen angezeigt, wie in der folgenden Abbildung dargestellt.



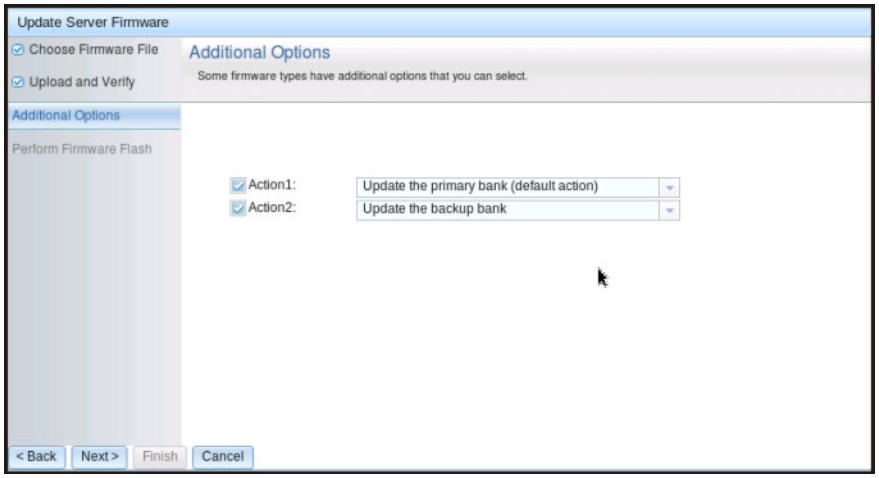
Im Dropdown-Menü neben **Action 1** (Aktion 1, wie in der folgenden Abbildung dargestellt) können Sie die Aktion **Update the primary bank (default action)** (primäre Speichergruppe aktualisieren (Standardaktion)) oder die Aktion **Update the backup bank** (Sicherungsspeichergruppe aktualisieren) auswählen.



Nachdem Sie eine Aktion ausgewählt haben, gelangen Sie zurück zum vorherigen Fenster. Hier können Sie durch Klicken auf das Kontrollkästchen **Action 2** weitere Aktionen ausführen.

Nachdem die ausgewählte Aktion geladen wurde, werden die ausgewählte Aktion und ein neues Dropdown-Menü **Action 2** (Aktion 2) angezeigt (wie in der folgenden Abbildung dargestellt).

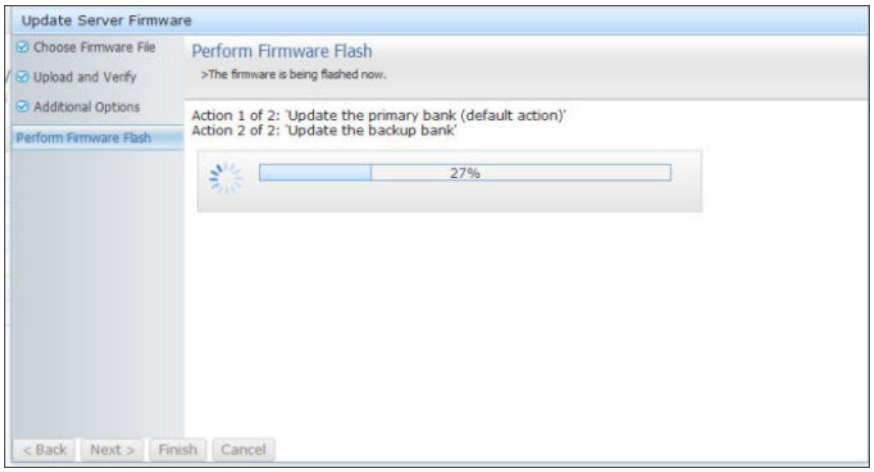
Anmerkung: Um eine Aktion zu inaktivieren, klicken Sie auf das Kontrollkästchen neben der zugehörigen Aktion.



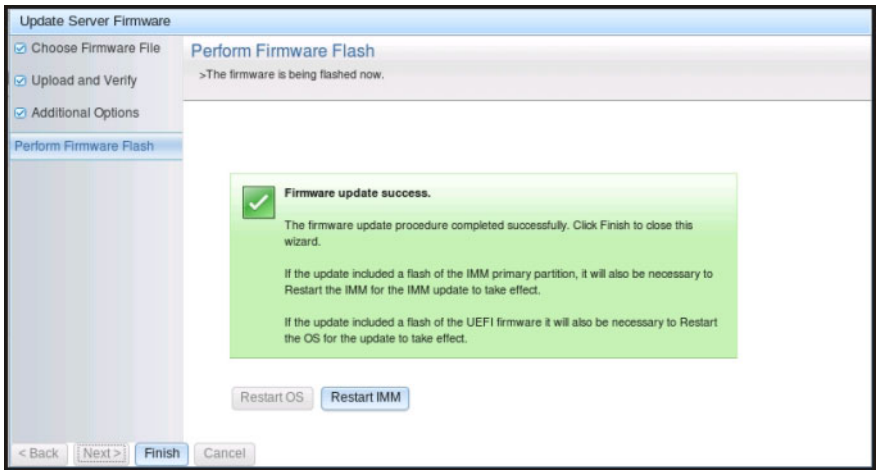
In der vorherigen Anzeige sehen Sie, dass für "Action 1" die primäre Speichergruppe zum Aktualisieren ausgewählt ist. Sie können auch auswählen, dass die Sicherungsspeichergruppe unter "Action 2" aktualisiert werden soll (wie im vorherigen Fenster dargestellt). Die primäre Speichergruppe und die Sicherungsspeichergruppe werden gleichzeitig aktualisiert, wenn Sie auf **Next >** klicken.

Anmerkung: "Action 1" muss sich von "Action 2" unterscheiden.

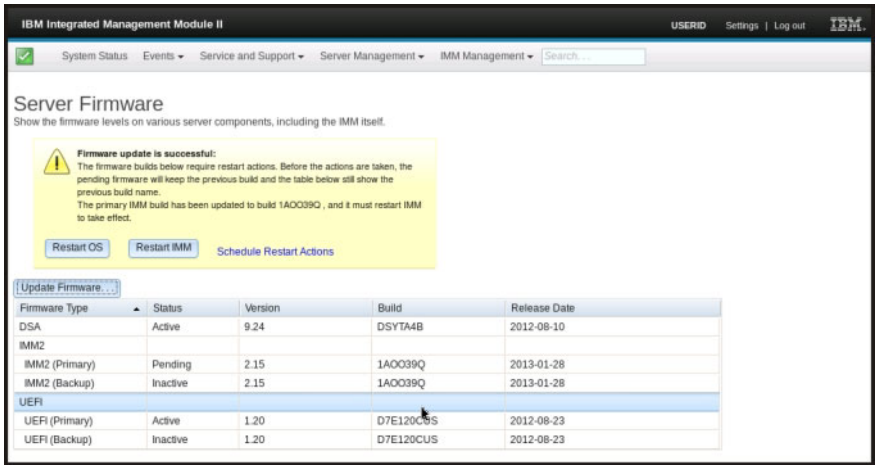
In einer Fortschrittsanzeige wird der Fortschritt der Firmwareaktualisierung angezeigt (wie in der folgenden Abbildung dargestellt).



Wenn die Firmwareaktualisierung erfolgreich abgeschlossen wurde, wird das folgende Fenster geöffnet. Wählen Sie die zugehörige Operation entsprechend den angezeigten Inhalten aus, um den Aktualisierungsprozess abzuschließen.



Wenn die primäre Firmwareaktualisierung nicht abgeschlossen wurde, wird das folgende Fenster geöffnet.



Remote Control (Fernsteuerung)

Dieser Abschnitt enthält Informationen zur Fernsteuerungsfunktion.

Der ActiveX-Client und der Java-Client sind grafische ferne Konsolen, mit denen Sie über Fernzugriff die Anzeige des Video Viewer des Servers sehen und über Tastatur und Maus des Clients damit interagieren können.

Anmerkungen:

- Der ActiveX-Client ist nur zusammen mit dem Internet Explorer-Browser verfügbar.
- Zur Verwendung des Java-Clients ist das Java-Plug-in ab Version 1.5 erforderlich.
- Der Java-Client ist mit IBM Java ab Version 6 SR9 FP2 kompatibel.

Die Fernsteuerungsfunktion besteht aus zwei separaten Fenstern:

- **Video Viewer** (Videoanzeigefunktion)

Im Fenster "Video Viewer" wird eine ferne Konsole für die Verwaltung ferner Systeme verwendet. Bei einer fernen Konsole handelt es sich um eine interaktive Anzeige der grafischen Benutzeroberfläche (GUI) des Servers, die auf Ihrem Computer angezeigt wird. Sie sehen auf Ihrem Bildschirm genau das, was auf der Serverkonsole angezeigt wird, und Sie können die Konsole per Tastatur und Maus steuern.

- **Virtual Media Session** (Sitzung mit virtuellen Datenträgern)

  Im Fenster "Virtual Media Session" werden alle Laufwerke auf dem Client angezeigt, die als ferne Laufwerke zugeordnet werden können. Außerdem können Sie ISO-Images und Imagedateien auf Disketten als virtuelle Laufwerke zuordnen. Jedes zugeordnete Laufwerk kann als schreibgeschützt gekennzeichnet werden. Die CD- und DVD-Laufwerke sowie die ISO-Images sind immer schreibgeschützt. Auf das Fenster "Virtual Media Session" wird über die Leiste des Menüs "Tools" (Werkzeuge) des Fensters "Video Viewer" zugegriffen.

  Anmerkungen:

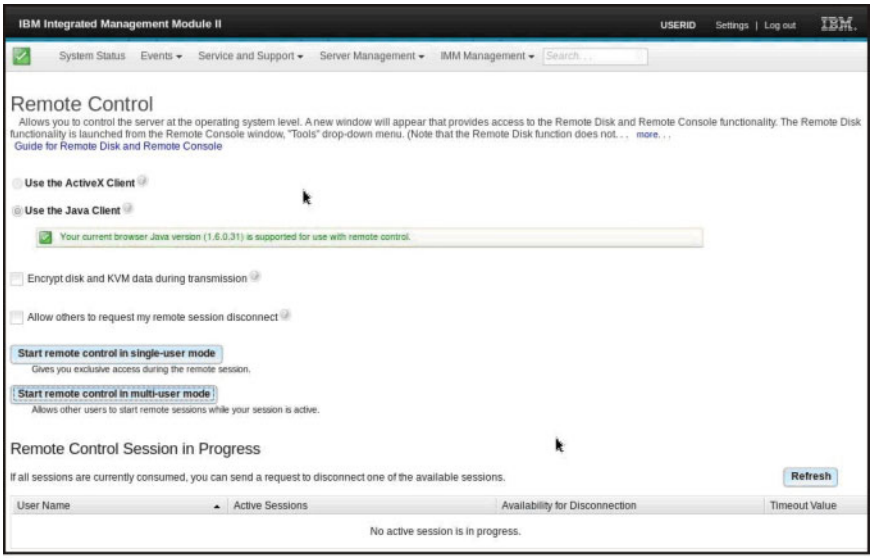
  – Die Sitzung mit fernen Datenträgern kann immer nur von einem Client für Fernsteuerungssitzungen verwendet werden.

  – Wenn der ActiveX-Client verwendet wird, wird ein übergeordnetes Fenster geöffnet. Dieses Fenster muss geöffnet bleiben, bis die ferne Sitzung abgeschlossen ist.

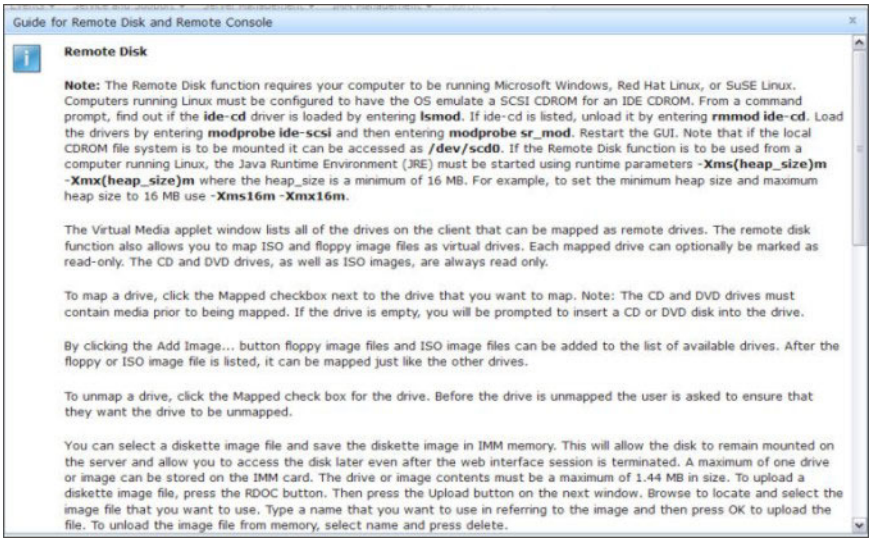
Gehen Sie wie folgt vor, um über Fernzugriff auf eine Serverkonsole zuzugreifen:

1. Melden Sie sich beim IMM2 an (weitere Informationen hierzu finden Sie unter „Am IMM2 anmelden" auf Seite 10).
2. Greifen Sie auf die Seite "Remote Control" (Fernsteuerung) zu, indem Sie eine der folgenden Menüoptionen auswählen:
   - Klicken Sie auf der Registerkarte "Server Management" auf **Remote Control**.
   - Klicken Sie auf der Seite "System Status" (Systemstatus) auf **Remote Control...**.

   Die Seite "Remote Control" wird geöffnet, wie in der folgenden Abbildung dargestellt.

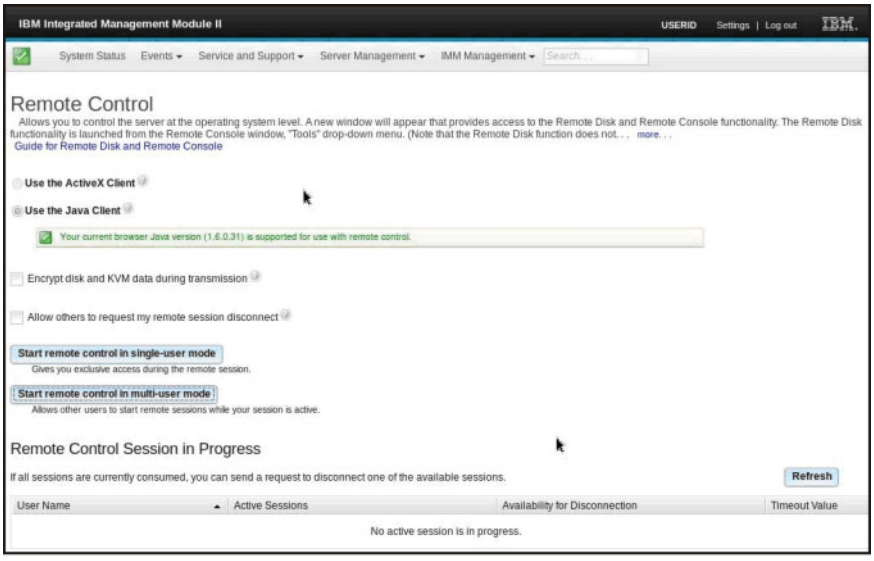


3. Sie können auf den Link **Guide for Remote Disk and Remote Console** (Anleitung für fernen Datenträger und ferne Konsole) klicken, um auf zusätzliche Informationen zuzugreifen. In der folgenden Abbildung ist das Fenster "Guide for Remote Disk and Remote Console" dargestellt.



   a. Klicken Sie auf **Close** (Schließen), um das Fenster "Guide for Remote Disk and Remote Console" zu verlassen.

4. Wählen Sie eine der folgenden Optionen der grafischen fernen Konsole aus:
   - Um den Internet Explorer als Browser zu verwenden, wählen Sie die Option **Use the ActiveX Client** (ActiveX-Client verwenden) aus.
   - Um den Java-Client zu verwenden, wählen Sie die Option **Use the Java Client** (Java-Client verwenden) aus, wie in der folgenden Abbildung dargestellt.

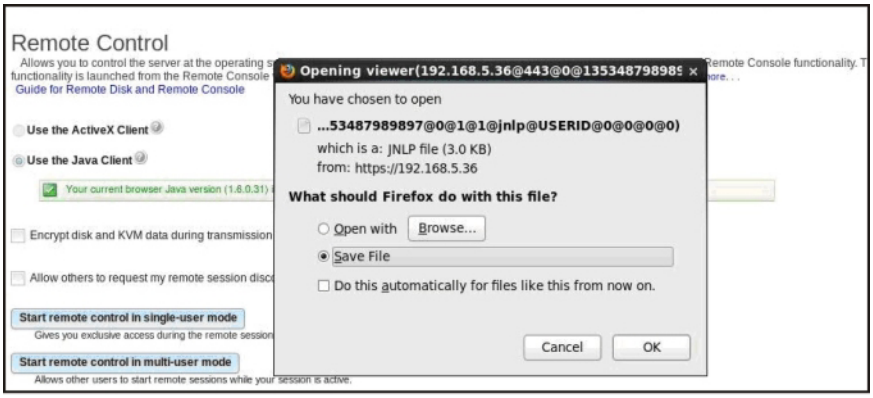


Anmerkungen:

- Wenn Sie nicht den Internet Explorer-Browser verwenden, kann nur der Java-Client ausgewählt werden.
- Der ActiveX-Client und der Java-Client verfügen über dieselbe Funktionalität.

- Es wird eine Statuszeile angezeigt, der Sie entnehmen können, ob Ihr Client unterstützt wird.

Das folgende Fenster wird geöffnet. Darin werden Informationen angezeigt, die der Browser (z. B. der Firefox-Browser) zum Öffnen der Viewer-Datei verwendet.

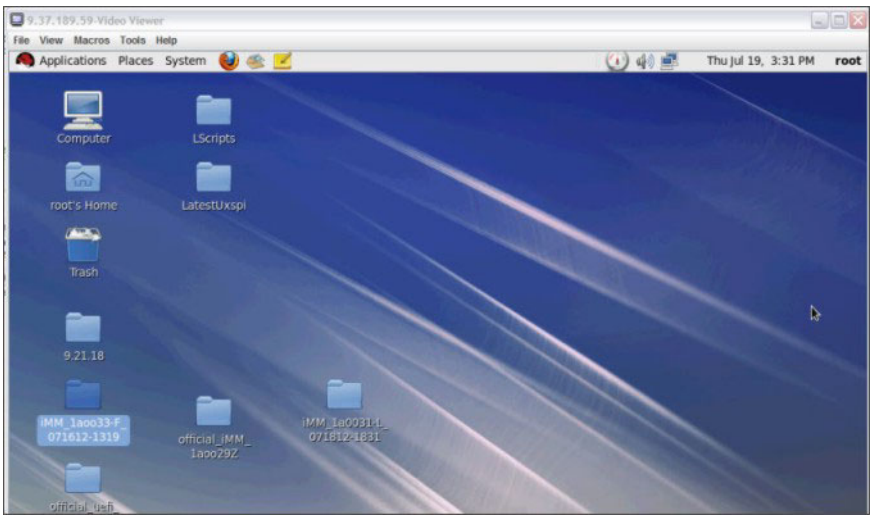


5. Nachdem der Browser die Viewer-Datei heruntergeladen und geöffnet hat, wird ein Bestätigungsfenster mit einer Warnung zur Überprüfung des Websitezertifikats angezeigt (wie in der folgenden Abbildung dargestellt). Klicken Sie auf **Yes**, um das Zertifikat zu akzeptieren.

6. Um den Server über Fernzugriff zu steuern, wählen Sie eine der folgenden Menüoptionen aus:
   - Um während der Sitzung über exklusiven Fernzugriff zu verfügen, klicken Sie auf **Start remote control in single User mode** (Fernsteuerung im Einzelbenutzermodus starten).
   - Um zuzulassen, dass während Ihrer Sitzung auch andere Personen Zugriff auf die ferne Konsole haben, klicken Sie auf **Start remote control in multi user mode** (Fernsteuerung im Mehrbenutzermodus starten).

     Anmerkung: Wenn vor dem Öffnen des Fensters "Video Viewer" das Kontrollkästchen **Encrypt disk and KVM data during transmission** (Datenträger- und KVM-Daten während der Übertragung verschlüsseln) ausgewählt wurde, werden die Datenträgerdaten während der Sitzung mit ADES verschlüsselt.

     Das Fenster "Video Viewer" wird geöffnet (wie in der folgenden Abbildung dargestellt). Das Fenster bietet Zugriff auf die Funktion "Remote Console".



7. Schließen Sie die Fenster "Video Viewer" und das Fenster "Virtual Media Session", wenn Sie mit dem Verwenden der Funktion "Remote Control" fertig sind.

Anmerkungen:

- Das Fenster "Video Viewer" schließt automatisch das Fenster "Virtual Media Session".
- Schließen Sie das Fenster "Virtual Media Session" *nicht*, wenn derzeit ein ferner Datenträger zugeordnet ist. Informationen zum Schließen und zum Trennen der Zuordnung eines fernen Datenträgers finden Sie im Abschnitt„Ferner Datenträger” auf Seite 119.
- Wenn beim Verwenden der Fernsteuerungsfunktion Probleme mit der Maus oder der Tastatur auftreten, finden Sie hierzu Hilfe auf der Seite "Remote Control" in der Webschnittstelle.
- Wenn Sie die ferne Konsole dazu verwenden, im Konfigurationsdienstprogramm Einstellungen des IMM2 zu ändern, kann es sein, dass der Server das IMM2 erneut startet. Die Verbindung zur fernen Konsole und die Anmeldesitzung werden abgebrochen. Nach einer kurzen Verzögerung können Sie sich mit einer neuen Sitzung erneut am IMM2 anmelden, die ferne Konsole erneut starten und das Konfigurationsdienstprogramm verlassen.

Wichtig: Das IMM2 verwendet ein Java-Applet oder ein ActiveX-Applet, um die Remote-Presence-Funktion auszuführen. Wenn das IMM2 auf die neueste Firmwareversion aktualisiert wird, werden auch das Java-Applet und das ActiveX-Applet auf die neueste Version aktualisiert. Java stellt zuvor verwendete Applets standardmäßig in den örtlichen Zwischenspeicher. Nach einer Flashaktualisierung der IMM2-Firmware ist das vom Server verwendete Java-Applet möglicherweise nicht auf dem neuesten Stand.

Um diesen Fehler zu beheben, inaktivieren Sie das Zwischenspeichern. Welche Methode verwendet wird, hängt von der Plattform und von der Java-Version ab. Die folgenden Schritte gelten für Oracle Java 1.5 unter Windows:

1. Klicken Sie auf **Start → Settings (Einstellungen) → Control Panel (Steuerkonsole)**.
2. Klicken Sie zweimal auf **Java Plug-in 1.5**. Das Fenster "Control Panel" des Java-Plug-in wird geöffnet.
3. Klicken Sie auf die Registerkarte **Cache** (Zwischenspeicher).
4. Wählen Sie eine der folgenden Optionen:

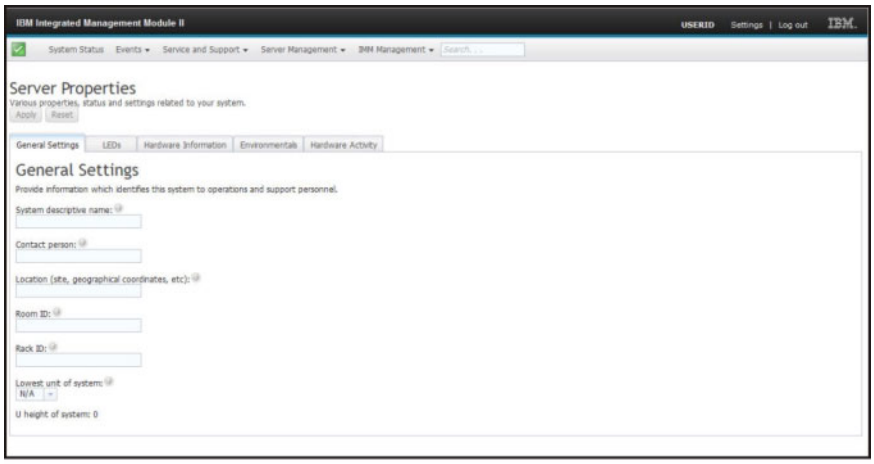
- Wählen Sie das Kontrollkästchen **Enable Caching** (Zwischenspeichern aktivieren) ab, damit die Java-Zwischenspeicherung immer inaktiviert ist.
- Klicken Sie auf **Clear Caching** (Zwischenspeichern abwählen). Wenn Sie diese Option wählen, müssen Sie nach jeder IMM2-Firmwareaktualisierung auf **Clear Caching** klicken.

Weitere Informationen zur Aktualisierung von IMM2-Firmware finden Sie im Abschnitt „Server-Firmware aktualisieren” auf Seite 122.

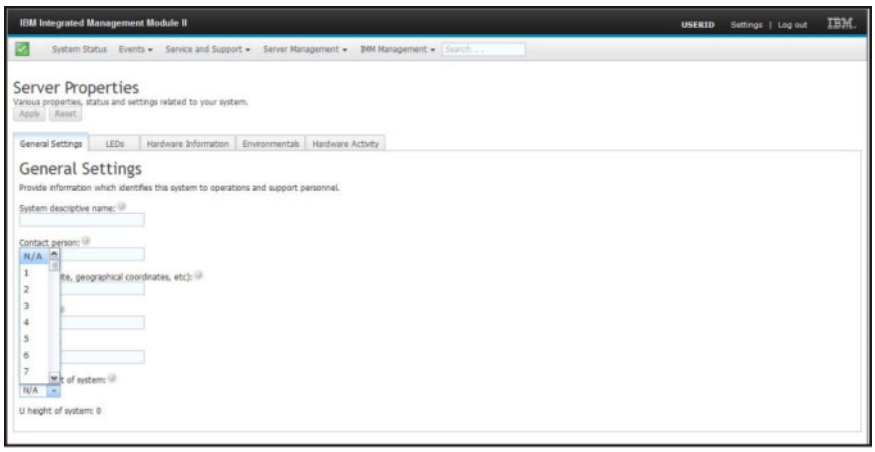
Weitere Informationen zum Verwenden der Fernsteuerungsfunktion finden Sie unter „Remote-Presence- und Fernsteuerungsfunktionen” auf Seite 107.

Server Properties (Servereigenschaften)

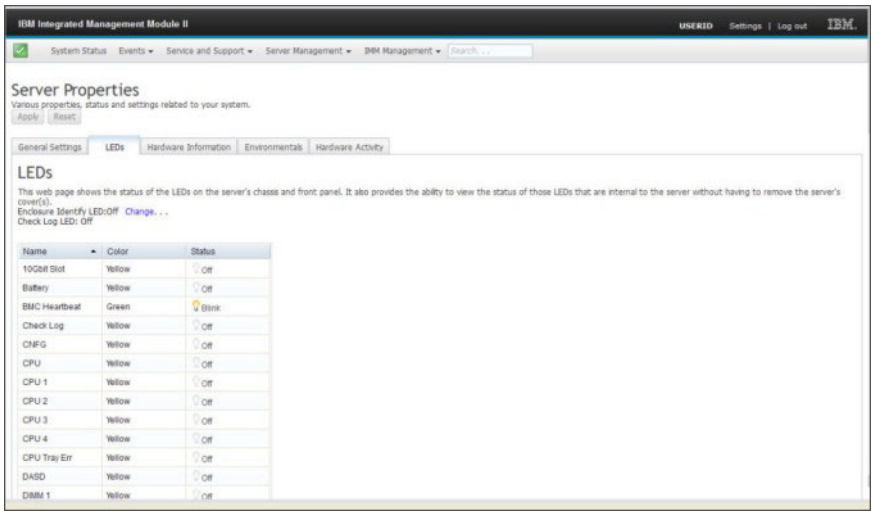
Wenn Sie die Option **Server Properties** (Servereigenschaften) auf der Registerkarte "Server Management" auswählen, wird das folgende Fenster angezeigt. Mit dieser Option können Sie verschiedene Parameter zur Identifizierung des Systems festlegen. Dazu gehören ein beschreibender Name, ein Ansprechpartner, ein Standort usw. Die Informationen, die Sie in diese Felder eingeben, werden wirksam, wenn Sie auf **Apply** (Übernehmen) klicken. Wenn Sie die Informationen löschen möchten, die seit dem letzten Übernehmen von Änderungen eingegeben wurden, klicken Sie auf **Reset** (Zurücksetzen).



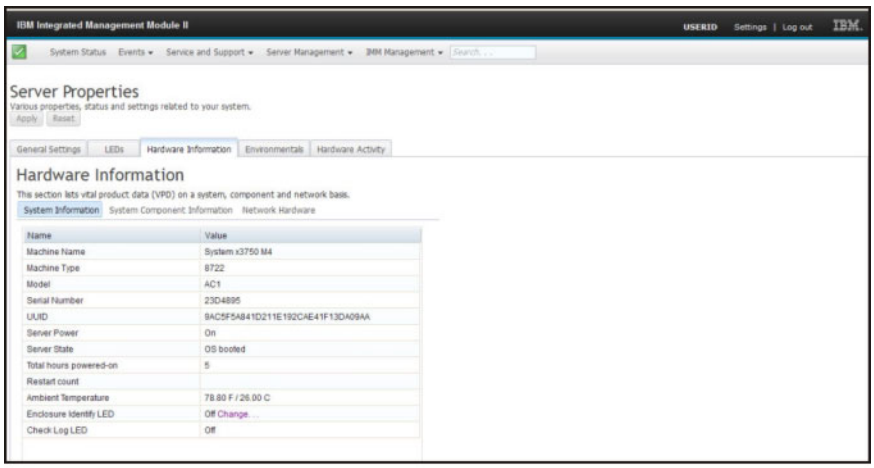
In der folgenden Abbildung können Sie die niedrigste Einheit des Systems (**Lowest unit of the system**) angeben. Für das Feld **Lowest unit of the system** ist eine Verbindung zum Managementmodul (z. B. Advanced Management Module oder CMM) erforderlich.



Um die Systemanzeigen anzuzeigen, klicken Sie auf die Registerkarte **LED**. Das folgende Fenster wird geöffnet.

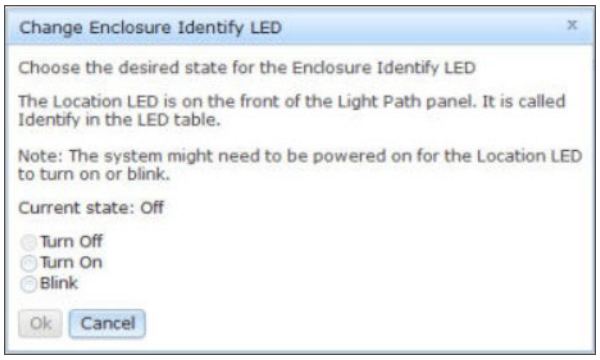


Um Informationen zum System, zu Systemkomponenten und zur Netzhardware anzuzeigen, klicken Sie auf die Registerkarte **Hardware Information** (Hardware-Informationen). Wählen Sie die entsprechende Registerkarte auf der Registerkarte "Hardware Information" aus, um verschiedene Informationen zu elementaren Produktdaten anzuzeigen. Die Registerkarte **System Information** (Systeminformationen) bietet Informationen wie den Maschinennamen, die Seriennummer und das Modell. In der folgenden Abbildung ist das Fenster "System Information" dargestellt.

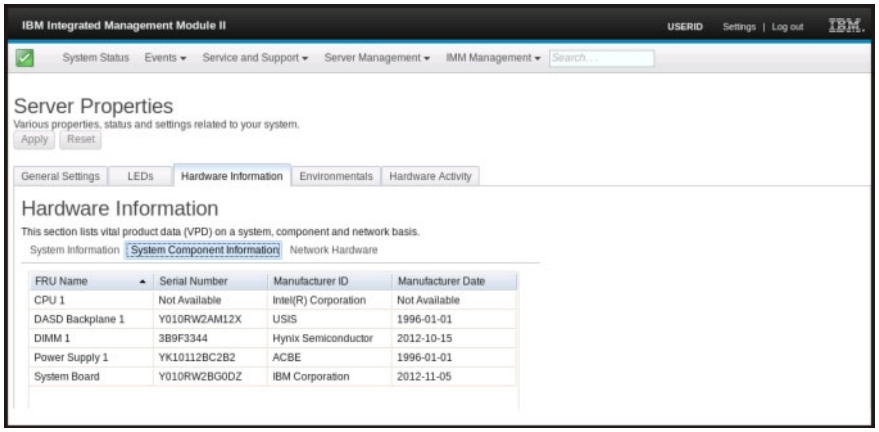


Der Status der Gehäuse-ID-Anzeige (**Enclosure Identify LED**) kann über das Fenster "System Information" angezeigt und geändert werden. Um die Einstellung für **Enclosure Identify LED** zu ändern, klicken Sie auf den Link **Change...** (Ändern). Das folgende Fenster wird geöffnet.

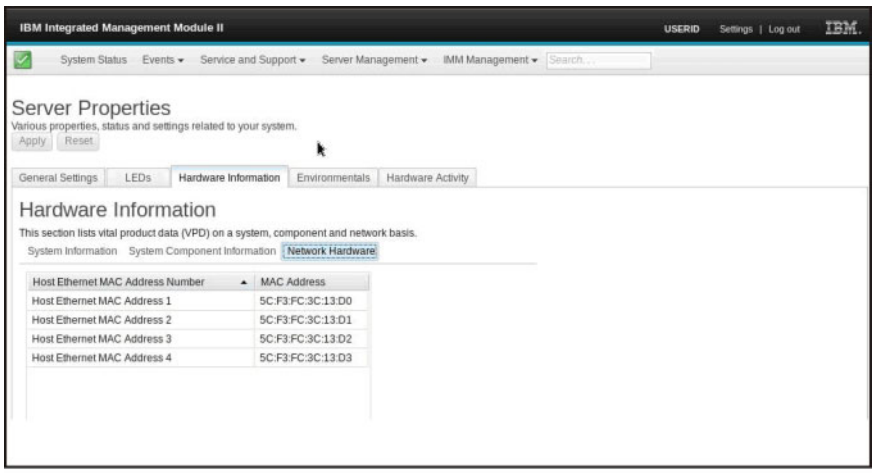
Anmerkung: Die Anzeige "Enclosure Identity" befindet sich an der Vorderseite des Diagnosefelds "Light Path Diagnostics".



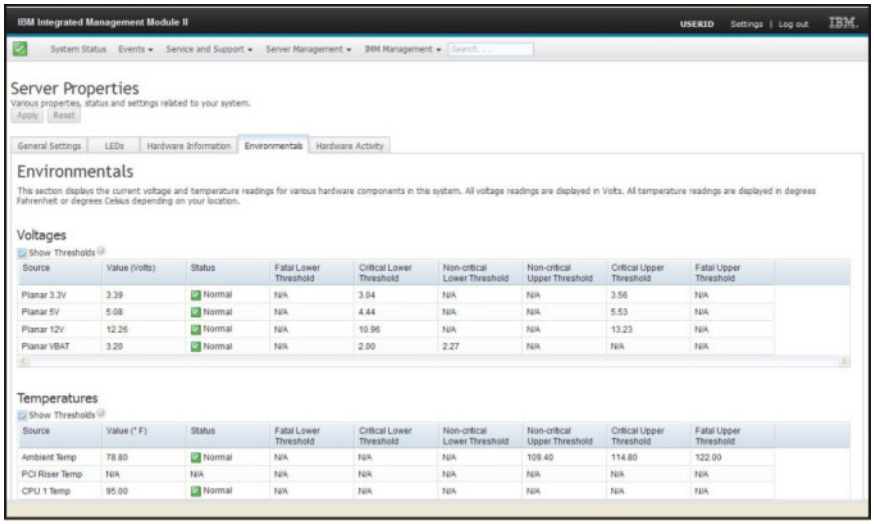
Wählen Sie die Registerkarte **System Component Information** (Informationen zu Systemkomponenten) aus, um Informationen zu Komponenten anzuzeigen. Zu den Informationen zu den Komponenten gehören der Name der FRU, die Seriennummer, die Hersteller-ID und das Herstellungsdatum. In der folgenden Abbildung sehen Sie die Informationen, die angezeigt werden, wenn Sie auf die Registerkarte **System Component Information** klicken.



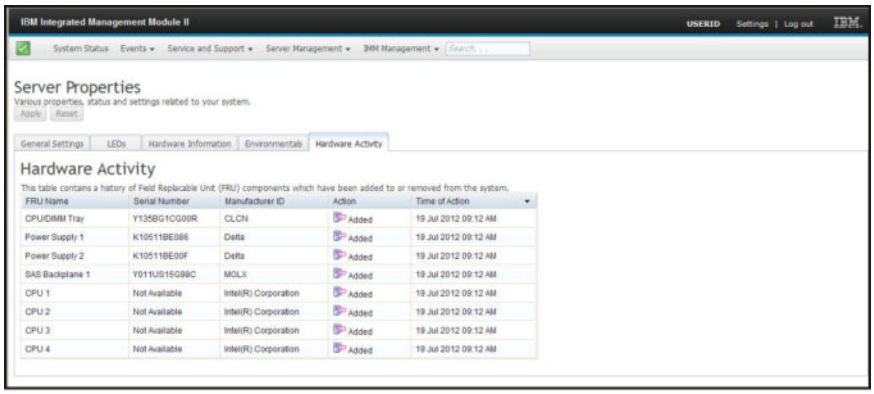
Wählen Sie die Registerkarte **Network Hardware** (Netzhardware) aus, um Informationen zur Netzhardware anzuzeigen. Zu den Informationen zur Netzhardware gehören die Host-Ethernet-MAC-Adressnummer und -MAC-Adresse. In der folgenden Abbildung sehen Sie die Informationen, die angezeigt werden, wenn Sie auf die Registerkarte "Network Hardware" klicken.



Wählen Sie die Registerkarte **Environmentals** (Umgebungsdaten) auf der Seite "Server Properties" (Servereigenschaften) aus, um die Spannungs- und Temperaturwerte der Hardwarekomponenten im System anzuzeigen. Das folgende Fenster wird geöffnet. In der Spalte **Status** der Tabelle werden entweder der normale Betrieb oder Problembereiche im Server angezeigt.



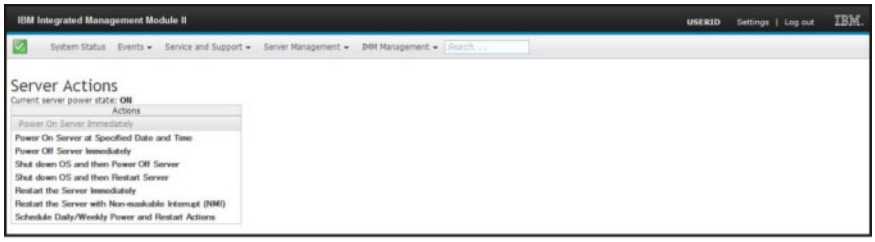
Die Registerkarte **Hardware Activity** (Hardware-Aktivität) auf der Seite "Servereigenschaften" enthält den Verlauf der zum System hinzugefügten oder vom System entfernten Hardware. In der folgenden Abbildung sehen Sie die Informationen, die angezeigt werden, wenn Sie auf die Registerkarte "Hardware Activity" klicken.



Server Power Actions (Serverstromversorgungsaktionen)

Dieser Abschnitt enthält Informationen zur Option "Server Power Actions" (Serverstromversorgungsaktionen) auf der Registerkarte "Server Management" auf der Homepage der IMM2-Webschnittstelle.

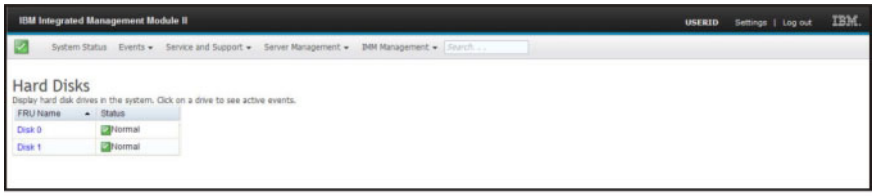
Wählen Sie die Option **Server Power Actions** auf der Registerkarte "Server Management" aus, um eine Liste der Aktionen anzuzeigen, die Sie zum Steuern der Stromversorgung des Servers verwenden können. In der folgenden Abbildung ist ein Beispiel für das Fenster "Server Power Actions" dargestellt.



Sie können auswählen, dass der Server sofort oder zu einem geplanten Zeitpunkt eingeschaltet wird. Sie können auch auswählen, dass das Betriebssystem heruntergefahren und erneut gestartet wird. Weitere Informationen zum Steuern der Stromversorgung des Servers finden Sie unter „Stromversorgungsstatus des Servers steuern” auf Seite 106.

Disks (Platten)

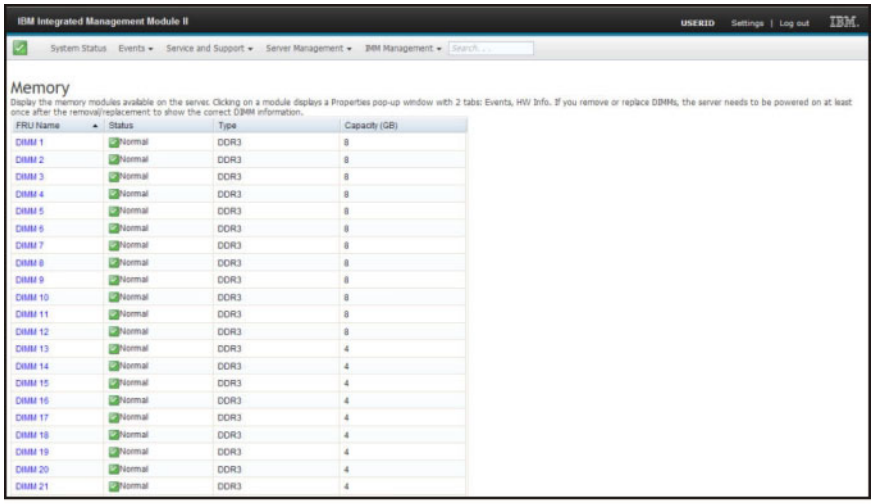
Wählen Sie die Option **Disks** (Platten) auf der Registerkarte "Server Management" (Serververwaltung) aus, um die Festplattenlaufwerke im System anzuzeigen. Die folgende Anzeige wird eingeblendet. Klicken Sie auf ein Festplattenlaufwerk, um die dem Festplattenlaufwerk zugeordneten Ereignisse anzuzeigen.



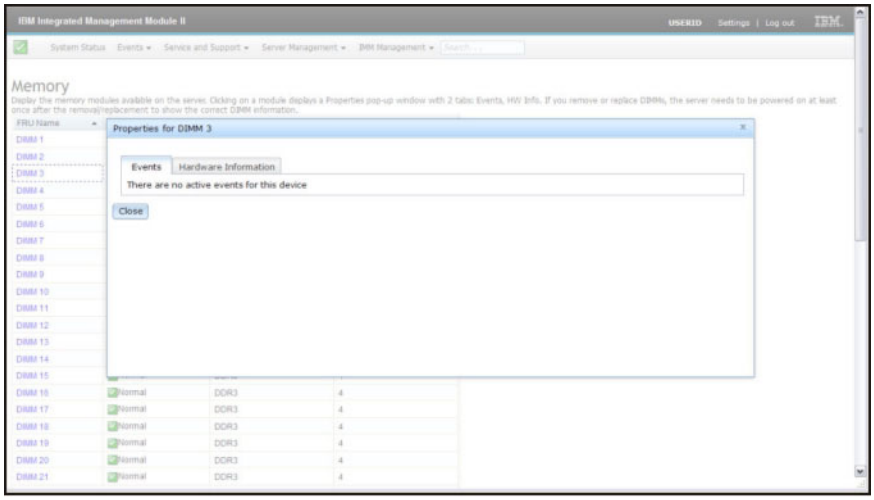
Memory (Speicher)

Wählen Sie auf der Registerkarte "Server Management" die Option **Memory** (Speicher) aus, um Informationen zu den im System installierten Speichermodulen anzuzeigen. Das folgende Fenster wird geöffnet. In der Tabelle wird jedes Speichermodul als Link angezeigt, auf den Sie klicken können, um ausführlichere Informationen zu dem betreffenden Speichermodul abzufragen. In der Tabelle werden außerdem der Status des DIMM, der DIMM-Typ und die DIMM-Kapazität angezeigt.

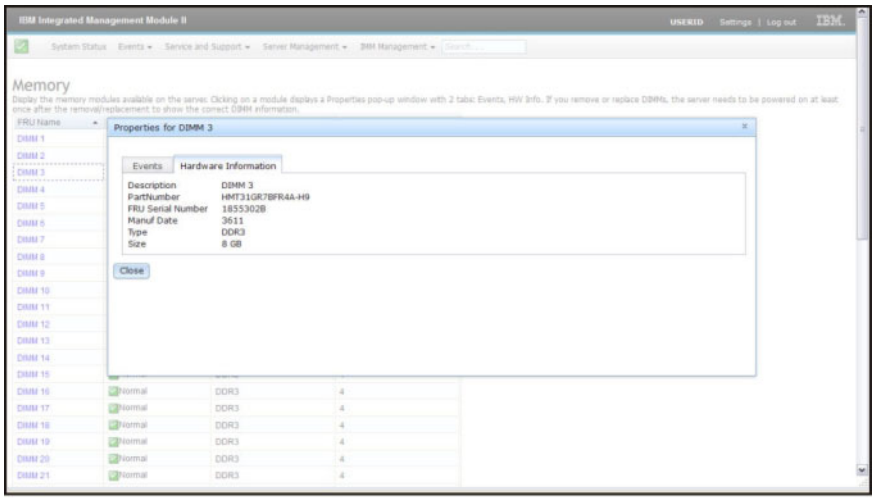
Anmerkung: Wenn Sie ein DIMM entfernen oder ersetzen, müssen Sie das System erneut starten, um die aktualisierten DIMM-Informationen zu den Änderungen anzuzeigen, die Sie an den System-DIMMs vorgenommen haben.



Klicken Sie in der Tabelle auf den Link zu einem **DIMM**, um die aktiven Ereignisse und weitere Informationen zu der Komponente anzuzeigen (wie in der folgenden Abbildung dargestellt).

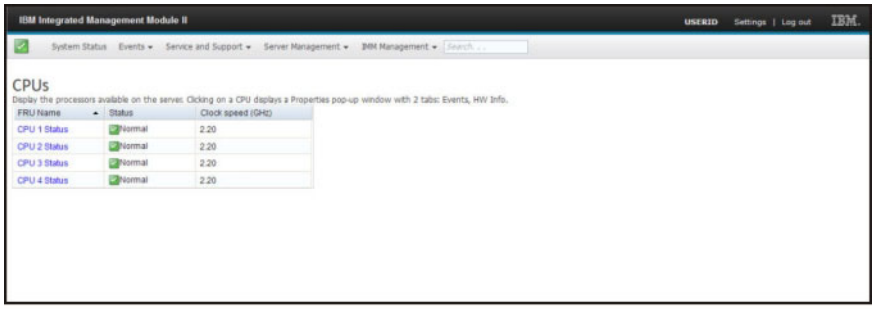


Klicken Sie auf die Registerkarte **Hardware Information**, um Details zu der betreffenden Komponente anzuzeigen, wie z. B. Beschreibung, Teilenummer, FRU-Seriennummer, Produktionsdatum (Woche/Jahr), Typ (z. B. DDR3) und Größe in Gigabyte (wie in der folgenden Abbildung dargestellt).

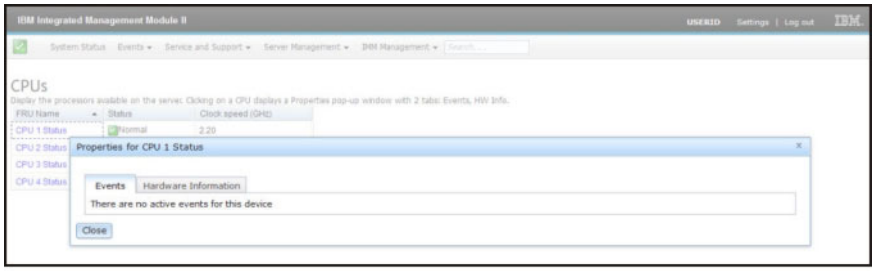


Processors (Prozessoren)

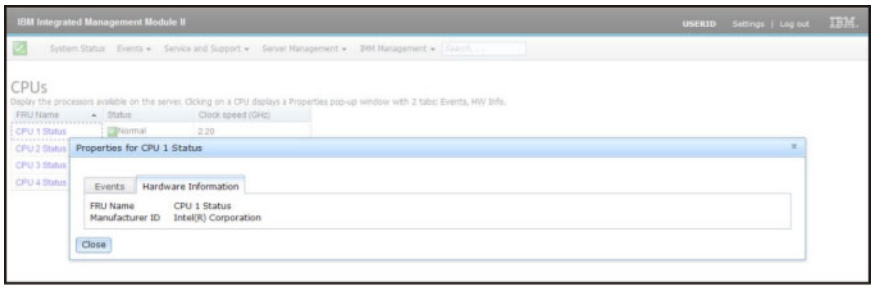
Wählen Sie die Option **Processors** (Prozessoren) auf der Registerkarte "Server Management" (Serververwaltung) aus, um Informationen zu den im System installierten Mikroprozessoren anzuzeigen. Das folgende Fenster wird geöffnet.



Klicken Sie auf einen der **CPU**-Links in der Tabelle, um aktive Ereignisse sowie weitere Informationen zur Komponente anzuzeigen (wie in der folgenden Abbildung dargestellt).



Klicken Sie auf die Registerkarte **Hardware Information** (Hardwareinformationen), um Details zur Komponente, wie z. B. den Namen der FRU (Field-Replaceable Unit, durch den Kundendienst austauschbare Funktionseinheit) und die Hersteller-ID anzuzeigen (wie in der folgenden Abbildung dargestellt).

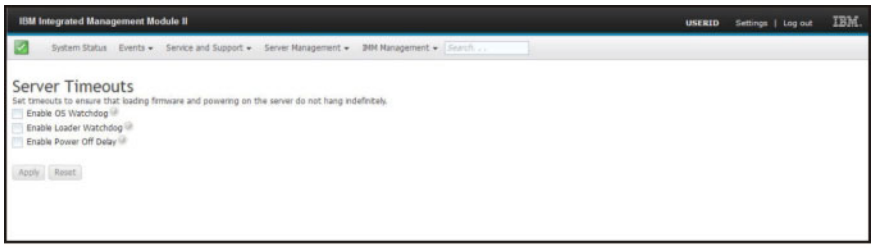


Server Timeouts (Serverzeitlimits)

Wählen Sie die Option **Server Timeouts** (Zeitlimits für den Server) auf der Registerkarte "Server Management" (Serververwaltung) aus, um Zeitlimits festzulegen, die sicherstellen, dass das System bei einer Firmwareaktualisierung oder beim Einschalten nicht auf unabsehbare Zeit hin blockiert wird. Sie können diese Funktion aktivieren, indem Sie die Werte für die Optionen festlegen.

Anmerkung: Bei Serverzeitlimits muss die Inband-USB-Schnittstelle (oder LAN over USB) aktiviert sein, damit Befehle verwendet werden können. Weitere Informationen zum Konfigurieren der USB-Schnittstelle finden Sie unter „USB konfigurieren” auf Seite 84.

In der folgenden Abbildung ist das Fenster "Server Timeouts" dargestellt.



Weitere Informationen zu Zeitlimits für Server finden Sie unter „Serverzeitlimits festlegen” auf Seite 58.

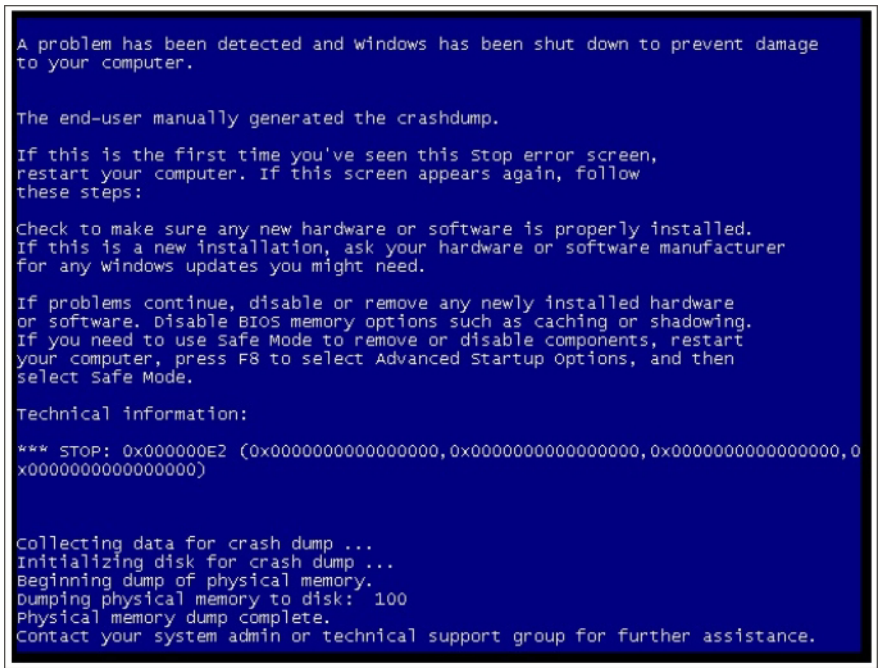
PXE Network Boot (PXE-Netzboot)

Wählen Sie die Option **PXE Network Boot** (PXE-Netzboot) auf der Registerkarte "Server Management" (Serververwaltung) aus, um den Server so zu konfigurieren, dass beim nächsten Neustart des Servers versucht wird, einen PXE-Netzboot durchzuführen. Weitere Informationen zum Konfigurieren eines PXE-Netzboots finden Sie unter „PXE-Netzboot einrichten” auf Seite 121.

Latest OS Failure Screen (Letzte Betriebssystem-Fehleranzeige)

Wählen Sie auf der Registerkarte "Server Management" die Option **Latest OS Failure Screen** (Letzte Betriebssystem-Fehleranzeige) aus, um die Daten zur neuesten Betriebssystem-Fehleranzeige, die vom IMM2 gespeichert wurde, anzuzeigen oder zu löschen. Das IMM2 speichert nur die Informationen zu den aktuellsten Fehlerereignissen und überschreibt die Daten früherer Betriebssystem-Fehleranzeigen, wenn ein neues Fehlerereignis auftritt.

In der folgenden Abbildung ist ein Beispiel für die Betriebssystem-Fehleranzeige dargestellt.



Weitere Informationen zur Option "Latest OS Failure Screen" finden Sie im Abschnitt „Daten der letzten Betriebssystem-Fehleranzeige erfassen” auf Seite 136.

Registerkarte "IMM Management" (IMM-Verwaltung)

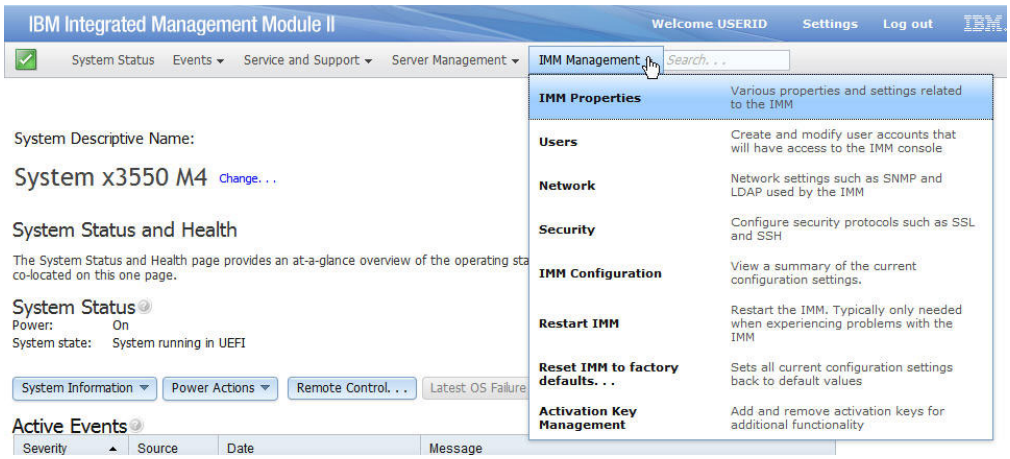
Dieser Abschnitt enthält Informationen zu den Optionen auf der Registerkarte "IMM Management" auf der Homepage der IMM2-Webbenutzerschnittstelle.

Die Optionen auf der Registerkarte "IMM Management" ermöglichen Ihnen das Anzeigen und Ändern der IMM2-Einstellungen. Eine Liste der Optionen und ausführliche Informationen zur Verwendung dieser Optionen zum Konfigurieren des IMM2 finden Sie in Kapitel 4, „IMM2 konfigurieren”, auf Seite 55.

Kapitel 4. IMM2 konfigurieren

Die Registerkarte "IMM Management" enthält Optionen zum Konfigurieren des IMM2. Verwenden Sie die Registerkarte "IMM Management", um Einstellungen des IMM2 anzuzeigen und zu ändern. Die folgenden Optionen sind auf der Registerkarte "IMM Management" aufgeführt (wie in der folgenden Abbildung dargestellt).

- IMM Properties (IMM-Eigenschaften)
- Users (Benutzer)
- Network (Netz)
- Security (Sicherheit)
- IMM Configuration (IMM-Konfiguration)
- Restart IMM (IMM erneut starten)
- Reset IMM to factory defaults (IMM auf werkseitige Voreinstellungen zurücksetzen)
- Activation Key Management (Aktivierungsschlüsselverwaltung)



Über die Seite "Integrated Management Module (IMM) Properties" (Eigenschaften des integrierten Managementmoduls (IMM)) können Sie die folgenden Funktionen ausführen:

- Zugriff auf die Server-Firmwareinformationen
- Datum und Uhrzeit festlegen:
  - Methode zur Einstellung der Uhrzeit des IMM2 auswählen: manuell oder NTP (Network Time Protocol)
  - Für Datum und Uhrzeit des IMM2 die manuelle Einstellungsmethode festlegen
  - Für NTP-Informationen NTP-Einstellungsmethode festlegen
  - Zeitzoneninformationen für das IMM2 festlegen
- Auf Informationen zum seriellen Anschluss des IMM2 zugreifen:
  - Seriellen Anschluss des IMM2 konfigurieren
  - Tastenkombinationen für die Befehlszeilenschnittstelle des IMM2 festlegen

Über die Seite "User Accounts" (Benutzerkonten) können Sie die folgenden Funktionen durchführen:

- IMM2-Benutzerkonten verwalten:
  - Benutzerkonto erstellen
  - Klicken Sie auf einen Benutzernamen, um Eigenschaften für diesen Benutzer zu bearbeiten:
    - Benutzernamen bearbeiten
    - Benutzerkennwort festlegen
    - SNMPv3-Einstellungen für den Benutzer konfigurieren
    - Öffentliche Secure Shell-Authentifizierungsschlüssel (SSH) für den Benutzer verwalten
  - Benutzerkonto löschen
- Allgemeine Anmeldeeinstellungen für Benutzer konfigurieren:
  - Benutzerauthentifizierungsverfahren festlegen
  - Inaktivitätszeitlimit für das Web festlegen
  - Für das IMM2 verfügbare Sicherheitsstufen für Benutzerkonten konfigurieren
- Benutzer anzeigen, die derzeit mit dem IMM2 verbunden sind

Auf der Seite "Network Protocol Properties" (Netzprotokolleigenschaften) können Sie die folgenden Funktionen ausführen:

- Ethernet-Einstellungen konfigurieren:
  - Ethernet-Einstellungen:
    - Hostname
    - Aktivierungs- und Adresseinstellungen von IPv4 und IPv6
  - Erweiterte Ethernet-Einstellungen:
    - Aktivierung von automatischer Vereinbarung
    - MAC-Adressenverwaltung
    - Größte zu übertragende Einheit festlegen
- SNMP-Einstellungen konfigurieren:
  - Aktivierung und Konfiguration von SNMPv1:
    - Kontaktinformationen festlegen
    - Aktivierung und Konfiguration von SNMP-Traps
    - Communityverwaltung
  - Aktivierung und Konfiguration von SNMPv3:
    - Kontaktinformationen festlegen
    - Konfiguration von Benutzerkonten
- DNS-Einstellungen konfigurieren:
  - Adressierungsvorgabe für DNS festlegen (IPv4 oder IPv6)
  - Aktivierung und Konfiguration zusätzlicher DNS-Serveradressierung
- DDNS-Einstellungen konfigurieren:
  - Aktivierung von Dynamic Domain Name System (DDNS)
  - Quelle für Domänennamen aussuchen (benutzerdefiniert oder DHCP-Server)
    - Benutzerdefinierten Domänennamen für benutzerdefinierte, manuell angegebene Quelle festlegen
    - Vom DHCP-Server angegebenen Domänennamen anzeigen
- SMTP-Einstellungen konfigurieren:

  - IP-Adresse oder Hostnamen des SMTP-Servers festlegen
  - SMTP-Server-Portnummer festlegen
  - SMTP-Verbindung testen
- LDAP-Einstellungen konfigurieren:
  - Konfiguration für LDAP-Server festlegen (DNS oder vorkonfiguriert):
    - Bei DNS-definierter LDAP-Serverkonfiguration Suchdomäne festlegen:
      - Suchdomäne von Anmelde-ID extrahieren
      - Manuell definierte Suchdomäne und manuell definierter Servicename
      - Versuchen, Suchdomäne von Anmelde-ID zu extrahieren, dann manuell angegebene Suchdomäne und manuell angegebenen Servicenamen verwenden
    - Bei Verwendung eines vorkonfigurierten LDAP-Servers:
      - Hostnamen oder IP-Adresse für LDAP-Server festlegen
      - LDAP-Server-Portnummer festlegen
  - Definierten Namen für den Stammeintrag des LDAP-Servers festlegen
  - Suchattribut für Benutzer-ID festlegen
  - Bindungsmethode auswählen (anonym, mit konfigurierten Berechtigungsnachweisen, mit Berechtigungsnachweisen für Anmeldung):
    - Bei konfigurierten Berechtigungsnachweisen definierten Namen und Kennwort des Clients festlegen
  - Erweiterte rollenbasierte Sicherheit für Aktivierung von Active Directory-Benutzern:
    - Bei Inaktivierung:
      - Gruppenfilter festlegen
      - Gruppensuchattribut festlegen
      - Anmeldeberechtigungsattribut festlegen
    - Bei Aktivierung Zielnamen des Servers festlegen
- Telnet-Einstellungen konfigurieren:
  - Telnet-Zugriffsaktivierung
  - Maximale Anzahl an Telnet-Sitzungen festlegen
- USB-Einstellungen konfigurieren:
  - Aktivierung von Ethernet over USB
  - Aktivierung und Verwaltung der Weiterleitung von externem Ethernet-Port zu Ethernet-over-USB-Port
- Portzuordnungen konfigurieren:
  - Nummern offener Ports anzeigen
  - Von IMM2-Services verwendete Portnummern festlegen:
    - HTTP
    - HTTPS
    - Telnet-Befehlszeilenschnittstelle
    - SSH-Befehlszeilenschnittstelle
    - SNMP-Agent
    - SNMP Traps (SNMP-Traps)
    - Remote Control (Fernsteuerung)
    - CIM over HTTPS
    - CIM over HTTP

Über die Seite "Security" (Sicherheit) können Sie die folgenden Funktionen ausführen:

- HTTPS-Serveraktivierung und Zertifikatsverwaltung
- Aktivierung von CIM over HTTPS und Zertifikatsverwaltung
- LDAP-Sicherheitsoptionen und Zertifikatsverwaltung
- SSH-Serveraktivierung und Zertifikatsverwaltung

Über die Seite "IMM Configuration" können Sie die folgenden Funktionen ausführen:

- Zusammenfassung der IMM2-Konfiguration anzeigen
- IMM2-Konfiguration sichern oder wiederherstellen
- Sicherungs- oder Wiederherstellungsstatus anzeigen
- IMM2-Konfiguration auf werkseitig vorgenommene Standardeinstellungen zurücksetzen
- Auf den Assistenten für die IMM2-Erstkonfiguration zugreifen

Über die Seite "Restart IMM" können Sie das IMM2 zurücksetzen.

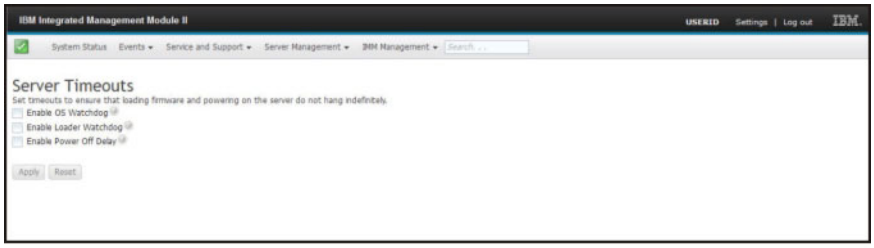
Über die Seite "Reset IMM2 to factory defaults..." (IMM2 auf werkseitige Voreinstellungen zurücksetzen) können Sie die IMM2-Konfiguration auf die werkseitig vorgenommenen Standardeinstellungen zurücksetzen.

Über die Seite "Activation Key Management" (Aktivierungsschlüsselverwaltung) können Sie Aktivierungsschlüssel für optionale FoD-Funktionen (Features On Demand) des IMM2 und des Servers verwalten. Informationen zur FoD-Aktivierungsschlüsselverwaltung finden Sie unter Kapitel 7, „Features on Demand”, auf Seite 143.

Serverzeitlimits festlegen

Verwenden Sie die Option "Server Timeouts" (Serverzeitlimits) zum Festlegen von Zeitlimits, damit der Server während einer Firmwareaktualisierung oder beim Einschalten des Servers nicht unbegrenzt blockiert wird. Sie können diese Funktion aktivieren, indem Sie den Wert für diese Option einstellen, wie in der folgenden Abbildung dargestellt.

Anmerkung: Bei Serverzeitlimits muss die Inband-USB-Schnittstelle (oder LAN over USB) aktiviert sein, um Befehle zu verwenden. Weitere Informationen zur Aktivierung und Inaktivierung der USB-Schnittstelle finden Sie im Abschnitt „USB konfigurieren” auf Seite 84.



Gehen Sie wie folgt vor, um die Werte für das Serverzeitlimit festzulegen:

1. Melden Sie sich an dem IMM2 an, für das Sie die Serverzeitlimits festlegen möchten. (Siehe Abschnitt „Am IMM2 anmelden” auf Seite 10).
2. Klicken Sie auf **Server Management** (Serververwaltung) und wählen Sie anschließend **Server Timeouts** aus.

   Sie können das IMM2 so einstellen, dass es automatisch auf die folgenden Ereignisse reagiert:

   - Das Betriebssystem läuft in einer Endlosschleife
   - Das Betriebssystem wird nicht geladen
3. Aktivieren Sie die Serverzeitlimits, die den Ereignissen entsprechen, auf die das IMM2 automatisch reagieren soll. Eine Beschreibung der Auswahloptionen finden Sie unter "Server timeout selections" (Serverzeitlimitoptionen).
4. Klicken Sie auf **Apply** (Übernehmen).

   Anmerkung: Die Schaltfläche **Reset** (Zurücksetzen) ermöglicht es Ihnen, alle Zeitlimitwerte gleichzeitig zu löschen.

Serverzeitlimitoptionen

Enable OS Watchdog (Betriebssystem-Watchdog aktivieren)
Verwenden Sie das Feld **Enable OS Watchdog**, um die Anzahl an Minuten zwischen Prüfungen des Betriebssystems durch das IMM2 anzugeben. Wenn das Betriebssystem auf eine dieser Prüfungen nicht reagiert, generiert das IMM2 einen Betriebssystem-Zeitlimitalert und startet den Server erneut. Nach dem Neustart des Servers ist der Betriebssystem-Watchdog inaktiviert, bis das Betriebssystem heruntergefahren und der Server aus- und wieder eingeschaltet wird. Wählen Sie zum Festsetzen des Wertes für den Betriebssystem-Watchdog **Enable OS Watchdog** aus und wählen Sie ein Zeitintervall aus dem Menü aus. Wählen Sie zum Ausschalten dieses Watchdogs **Enable OS Watchdog** ab. Zum Aufzeichnen von Betriebssystem-Fehleranzeigen müssen Sie den Watchdog im Feld **Enable OS Watchdog** aktivieren.

Enable Loader Watchdog (Ladeprogramm-Watchdog aktivieren)
Verwenden Sie das Feld **Enable Loader Watchdog**, um anzugeben, wie viele Minuten das IMM2 zwischen der Fertigstellung des POST und dem Starten des Betriebssystems warten soll. Wenn diese Zeitspanne überschritten wird, generiert das IMM2 einen Ladeprogramm-Zeitlimitalert und startet den Server automatisch erneut. Nach dem Neustart des Servers wird das Ladeprogramm-Zeitlimit automatisch inaktiviert, bis das Betriebssystem heruntergefahren und der Server aus- und wieder eingeschaltet wird (oder bis das Betriebssystem startet und die Software erfolgreich geladen wird). Zum Festlegen des Wertes für das Ladeprogramm-Zeitlimit wählen Sie aus, wie lange das IMM2 auf die Fertigstellung des Betriebssystemstarts warten soll. Wählen Sie zum Ausschalten dieses Watchdogs **Enable Loader Watchdog** im Menü ab.

Enable Power Off Delay (Ausschaltverzögerung aktivieren)
Verwenden Sie das Feld **Enable Power Off Delay**, um anzugeben, wie viele Minuten das IMM2-Subsystem darauf warten soll, dass das Betriebssystem herunterfährt, bevor es die Stromversorgung des Systems abschaltet. Zum Festlegen des Wertes für die Ausschaltverzögerung wählen Sie aus, wie lange das IMM2 nach dem Ausschalten des Betriebssystems warten soll. Wählen Sie zum Ausschalten dieses Watchdogs **Enable Loader Watchdog** im Menü ab.

Datum und Uhrzeit für IMM2 einstellen

Anmerkung: Die Einstellungen für Datum und Uhrzeit des IMM2 können auf einem IBM Flex System-Knoten nicht geändert werden.

Wählen Sie die Registerkarte **Date and Time** aus, um das Datum und die Uhrzeit für das IMM2 anzuzeigen oder zu ändern. Das IMM2 verwendet einen eigenen Taktgeber, um alle Ereignisse im Ereignisprotokoll zeitlich zu markieren. Bei Alerts, die per E-Mail und SNMP versendet werden, wird die Taktgebereinstellung zur zeitlichen Markierung verwendet. Zwecks größerer Benutzerfreundlichkeit für Administratoren, die über Fernzugriff Systeme in unterschiedlichen Zeitzonen verwalten, werden Abweichungen von der westeuropäischen Zeit und die Sommerzeit von den Zeiteinstellungen unterstützt. Sie können selbst dann über Fernzugriff auf das Ereignisprotokoll zugreifen, wenn der Server ausgeschaltet oder inaktiviert ist.

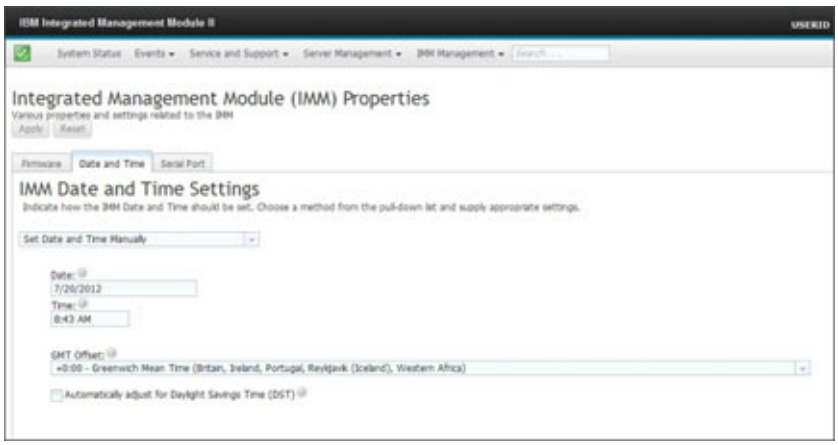
Die Datums- und Uhrzeiteinstellung des IMM2 wirkt sich nur auf den IMM2-Taktgeber und nicht auf den Servertaktgeber aus. Beim IMM2-Taktgeber und beim Servertaktgeber handelt es sich um separate, voneinander unabhängige Taktgeber, die auf unterschiedliche Uhrzeiten eingestellt werden können.

Einstellung für Datum und Uhrzeit ändern (manueller Modus)

Gehen Sie wie folgt vor, um die Uhrzeit und das Datum manuell zu ändern:

1. Klicken Sie in der Liste **Indicate how the IMM date and time should be set** (Angeben, wie das IMM-Datum und die IMM-Uhrzeit festgelegt werden sollen) auf **Set Date and Time Manually** (Datum und Uhrzeit manuell festlegen).
2. Geben Sie im Feld **Date** den laufenden Monat, den Tag und das Jahr ein.
3. Geben Sie im Feld **Time** (Zeit) in den entsprechenden Feldern die Zahlen ein, die der laufenden Stunde und Minute entsprechen.
   - Bei der Stunde muss eine Zahl zwischen 1 und 12 entsprechend einer 12-Stunden-Zeiteinteilung stehen.
   - Bei den Minuten müssen Zahlen zwischen 00 und 59 stehen.
   - Wählen Sie **AM** (vormittags) oder **PM** (nachmittags) aus.
4. Wählen Sie im Feld **GMT offset** (GMT-Abweichung) die Zahl aus, die die Abweichung von der westeuropäischen Zeit in Stunden angibt. Diese Zahl muss der Zeitzone entsprechen, in der sich der Server befindet.
5. Wählen Sie das Kontrollkästchen **Automatically adjust for daylight saving time (DST)** (Automatisch an Sommerzeit anpassen) aus oder wählen Sie es ab, um anzugeben, ob der IMM2-Taktgeber sich automatisch anpasst, wenn die Ortszeit zwischen Standardzeit und Sommerzeit wechselt.

In der folgenden Abbildung ist die Registerkarte "IMM Date and Time" beim manuellen Festlegen von Datum und Uhrzeit dargestellt.

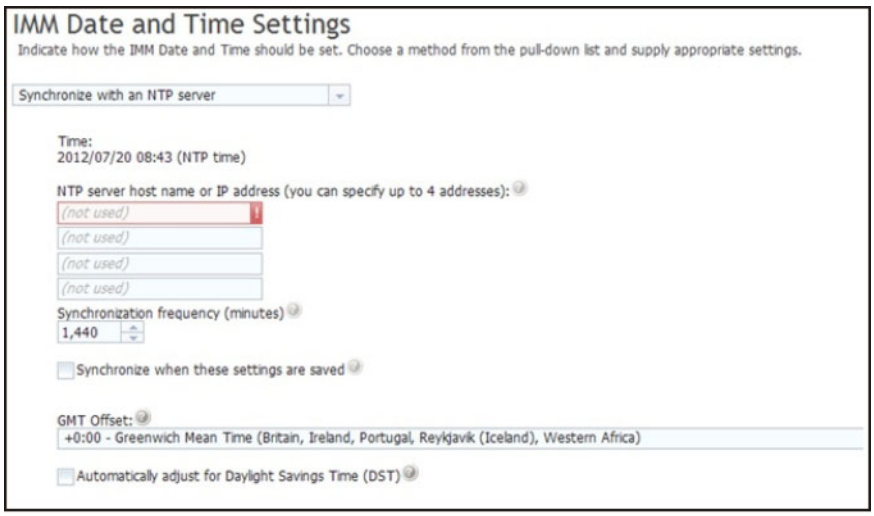


Einstellungen für Datum und Uhrzeit ändern (NTP-Servermodus)

Gehen Sie wie folgt vor, um den IMM2-Taktgeber mit dem Servertaktgeber zu synchronisieren:

1. Klicken Sie in der Liste **Indicate how the IMM date and time should be set** (Angeben, wie das IMM-Datum und die -Uhrzeit festgelegt werden sollen) auf **Synchronize with an NTP server** (Mit einem NTP-Server synchronisieren).
2. Geben Sie im Feld **NTP server host name or IP address** (Hostname oder IP-Adresse des NTP-Servers) den Namen des NTP-Servers an, der für die Taktgebersynchronisation verwendet werden soll.
3. Geben Sie im Feld **Synchronization frequency (in minutes)** (Synchronisationshäufigkeit (in Minuten)) das ungefähre Intervall zwischen den Synchronisationsanforderungen ein. Geben Sie einen Wert zwischen 3 und 1440 Minuten ein.
4. Wählen Sie das Kontrollkästchen **Synchronize when these settings are saved** (Beim Speichern dieser Einstellungen synchronisieren) aus, um eine sofortige Synchronisierung anzufordern, (wenn Sie auf **Apply** klicken) anstatt darauf zu warten, bis das Zeitintervall abgelaufen ist.
5. Wählen Sie im Feld **GMT offset** (GMT-Abweichung) die Zahl aus, die die Abweichung von der westeuropäischen Zeit in Stunden angibt, entsprechend der Zeitzone, in der sich der Server befindet.
6. Wählen Sie das Kontrollkästchen **Automatically adjust for daylight saving time (DST)** (Automatisch an Sommerzeit anpassen) aus oder wählen Sie es ab, um anzugeben, ob der IMM2-Taktgeber sich automatisch anpasst, wenn die Ortszeit zwischen Standardzeit und Sommerzeit wechselt.

In der folgenden Abbildung ist die Registerkarte "IMM Date and Time" beim Synchronisieren mit dem Servertaktgeber dargestellt.



Einstellungen für den seriellen Anschluss konfigurieren

Wählen Sie die Option **Serial Port** (Serieller Anschluss) aus, um die Umleitung des seriellen Anschlusses des Hosts anzugeben. Das IMM2 stellt zwei serielle Anschlüsse bereit, die für serielle Umleitungen verwendet werden:

Serial port 1 (Serieller Anschluss 1) (COM1)
Der serielle Anschluss 1 (COM1) auf System x Servern wird für IPMI Serial over LAN (SOL) verwendet. COM1 kann nur über die IPMI-Schnittstelle konfiguriert werden.

Serial port 2 (Serieller Anschluss 2) (COM2)
Auf Blade-Servern wird der serielle Anschluss 2 (COM2) für SOL verwendet. Auf System x-Gehäuserahmenservern und IBM Flex System-Knoten wird COM2 für serielle Umleitungen über Telnet oder SSH verwendet. COM2 kann nicht über die IPMI-Schnittstelle konfiguriert werden. Auf in einem Gehäuse installierten Servern und auf Turmservern ist COM2 ein interner COM-Anschluss ohne die Möglichkeit eines externen Zugriffs.

Machen Sie in den folgenden Feldern die für die Umleitung des seriellen Anschlusses erforderlichen Angaben:

Baud Rate (Baudrate)
Geben Sie in diesem Feld die Datenübertragungsgeschwindigkeit Ihrer seriellen Anschlussverbindung an. Um die Baudrate festzulegen, wählen Sie eine Datenübertragungsgeschwindigkeit zwischen 9600 und 115200 aus, die der Geschwindigkeit Ihrer seriellen Anschlussverbindung entspricht.

Parity (Parität)
Geben Sie in diesem Feld die Paritätsbits Ihrer seriellen Anschlussverbindung an. Die verfügbaren Optionen lauten "None" (Keine), "Odd" (Ungerade) oder "Even" (Gerade).

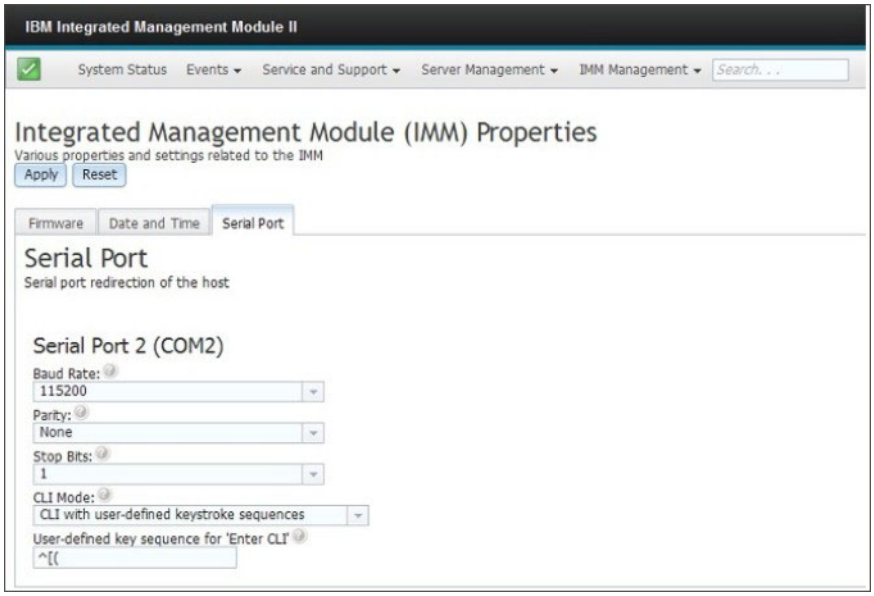
Stop Bits (Stoppbits)
Geben Sie in diesem Feld die Anzahl der Stoppbits Ihrer seriellen Anschlussverbindung an. Die verfügbaren Optionen lauten "1" oder "2".

CLI Mode (CLI-Modus)
Wählen Sie in diesem Feld die Option **CLI with IMM2 compatible keystroke sequences** (CLI mit IMM2-kompatiblen Tastenfolgen) oder, wenn Sie Ihre eigene Tastenkombination verwenden möchten, die Option

CLI with user defined keystroke sequences (CLI mit benutzerdefinierten Tastenfolgen) aus. Wenn Sie **CLI with user defined keystroke sequences** auswählen, müssen Sie die Tastenkombination im Feld **User-defined key sequence for 'Enter CLI'** (Benutzerdefinierte Tastenkombination für 'Enter CLI') definieren.

Nachdem die serielle Umleitung gestartet wurde, wird sie so lange fortgesetzt, bis Sie die Tastenkombination zum Beenden eingeben. Wenn die Tastenkombination zum Beenden eingegeben wird, wird die serielle Umleitung gestoppt und Sie wechseln in den Befehlsmodus in der Telnet- oder SSH-Sitzung zurück. Verwenden Sie das Feld **User-defined key sequence for 'Enter CLI'**, um die Tastenkombination zum Beenden anzugeben.

In der folgenden Abbildung ist die Registerkarte "Serial Port" dargestellt.



Benutzerkonten konfigurieren

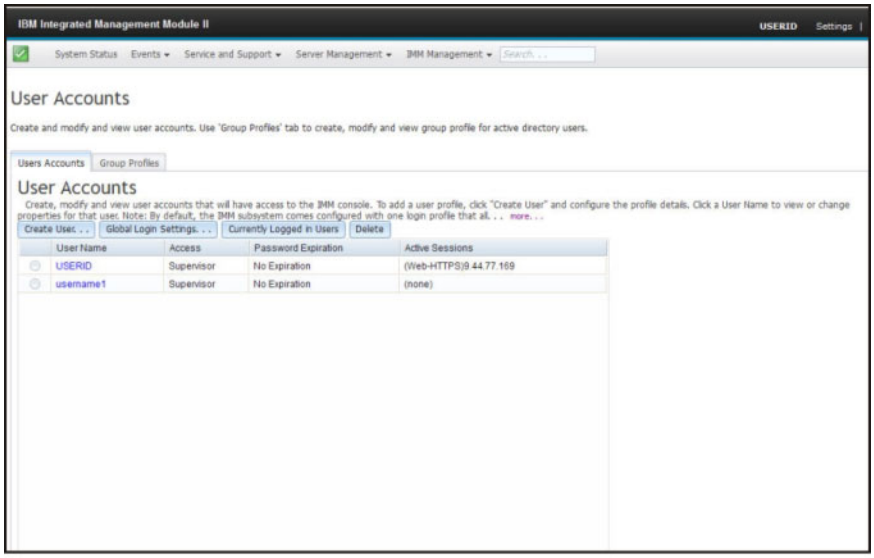
Wählen Sie auf der Registerkarte "IMM Management" (IMM-Verwaltung) die Option **Users** (Benutzer) aus, um Benutzerkonten für das IMM2 zu erstellen und zu ändern und um Gruppenprofile anzuzeigen. Die folgende Informationsnachricht wird angezeigt.

Anmerkung: In einem IBM Flex System-Knoten werden IMM2-Benutzerkonten vom CMM verwaltet.

Benutzerkonten

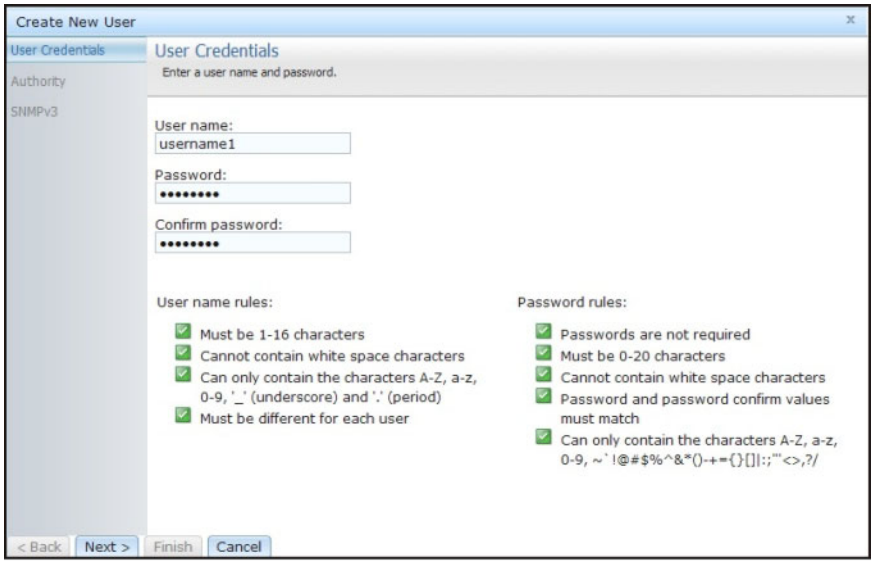
Wählen Sie die Registerkarte **Users Accounts** (Benutzerkonten) aus, um Benutzerkonten zu erstellen, zu ändern und anzuzeigen, wie in der folgenden Abbildung dargestellt.

Anmerkung: Das IMM2-Subsystem wird mit einem Anmeldeprofil geliefert.



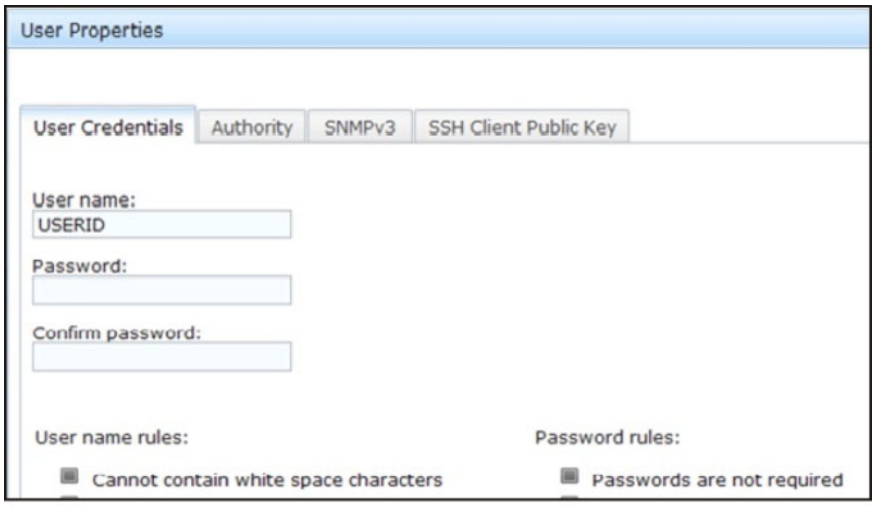
Benutzer erstellen

Klicken Sie auf die Registerkarte **Create User...** (Benutzer erstellen), um ein neues Benutzerkonto zu erstellen. Füllen Sie die folgenden Felder aus: **User name** (Benutzername), **Password** (Kennwort) und **Confirm Password** (Kennwort bestätigen) (wie in der folgenden Abbildung dargestellt).



Benutzereigenschaften

Klicken Sie auf die Registerkarte **User Properties** (Benutzereigenschaften), um ein bestehendes Benutzerkonto zu ändern (wie in der folgenden Abbildung dargestellt).



Benutzerberechtigung

Klicken Sie auf die Registerkarte **Authority** (Berechtigung), um die Benutzerberechtigung festzulegen. Die folgenden Benutzerberechtigungsstufen sind verfügbar:

Supervisor (Administrator)
Für den Benutzer gelten keine Einschränkungen.

Read only (Lesezugriff)
Der Benutzer verfügt nur über Lesezugriff und kann keine Aktionen ausführen, wie z. B. Dateiübertragungen, Einschalt- und Neustartaktionen sowie Remote-Presence-Funktionen.

Custom (Angepasst)
Das Profil für die Benutzerberechtigung kann durch Einstellungen für die Aktionen, die der Benutzer ausführen kann, angepasst werden.

SNMP-Zugriffsberechtigungen

Klicken Sie auf die Registerkarte **SNMPv3**, um SNMP-Zugriff für das Konto festzulegen. Die folgenden Benutzerzugriffsoptionen sind verfügbar:

Authentication protocol (Authentifizierungsprotokoll)
Geben Sie entweder **HMAC-MD5** oder **HMAC-SHA** als Authentifizierungsprotokoll an. Dabei handelt es sich um die Algorithmen, die vom SNMPv3-Sicherheitsmodell für die Authentifizierung verwendet werden. Wenn die Option **Authentication Protocol** nicht aktiviert ist, wird kein Authentifizierungsprotokoll verwendet.

Privacy protocol (Datenschutzprotokoll)
Die Datenübertragung zwischen dem SNMP-Client und dem Agenten kann mithilfe von Verschlüsselung geschützt werden. Folgende Methoden werden unterstützt: **DES** und **AES**. Das Datenschutzprotokoll ist nur dann gültig, wenn für das Authentifizierungsprotokoll entweder **HMAC-MD5** oder **HMAC-SHA** festgelegt wurde.

Privacy password (Datenschutzkennwort)
Geben Sie das Verschlüsselungskennwort in diesem Feld an.

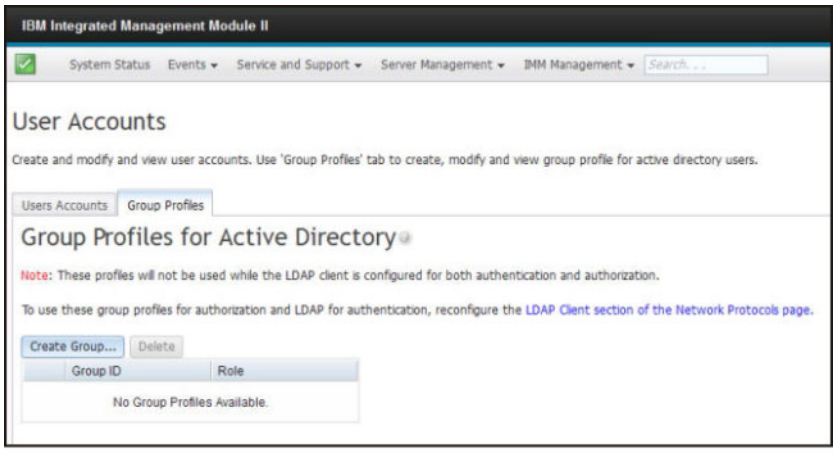
Confirm privacy password (Datenschutzkennwort bestätigen)
Geben Sie das Verschlüsselungskennwort zum Bestätigen nochmals an.

Access type (Zugriffstyp)
Geben Sie als Zugriffstyp entweder **Get** (Abrufen) oder **Set** (Festlegen) an. SNMPv3-Benutzer mit dem Zugriffstyp **Get** können nur Abfrageoperationen ausführen. SNMPv3-Benutzer mit dem Zugriffstyp **Set** können Abfrageoperationen ausführen und Einstellungen ändern (z. B. das Kennwort für einen Benutzer festlegen).

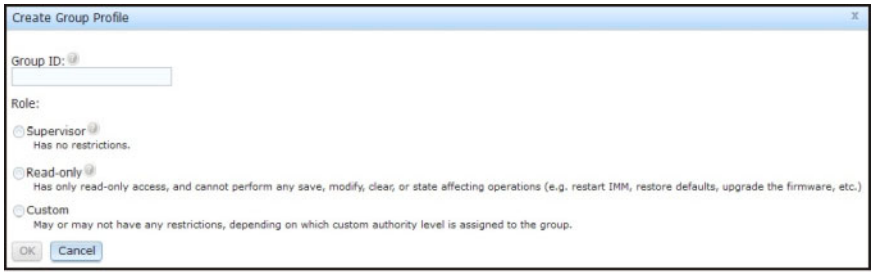
Hostname/IP address for traps (Hostname/IP-Adresse für Traps)
Geben Sie das Trapziel für den Benutzer an. Das kann eine IP-Adresse oder ein Hostname sein. Mithilfe von Traps benachrichtigt der SNMP-Agent die Verwaltungsstation über Ereignisse (z. B. wenn die Temperatur eines Prozessors den Grenzwert überschreitet).

Gruppenprofile

Wählen Sie die Registerkarte **Group Profiles** (Gruppenprofile) aus, um Gruppenprofile zu erstellen, zu ändern oder anzuzeigen (wie in der folgenden Abbildung dargestellt).

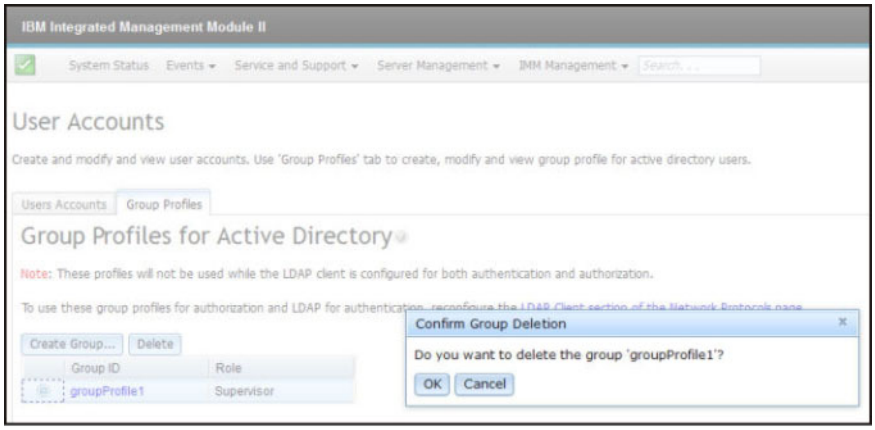


Klicken Sie auf **Create Group** (Gruppe erstellen), um eine neue Benutzergruppe zu erstellen. In der folgenden Abbildung ist das Fenster "Create Group Profile" (Gruppenprofil erstellen) dargestellt.



Geben Sie eine **Group ID** (Gruppen-ID) ein und wählen Sie die **Role** (Rolle) aus (Informationen zu Benutzerberechtigungsstufen finden Sie im Abschnitt „Benutzerberechtigung” auf Seite 65).

Um eine Gruppe zu löschen, klicken Sie auf **Delete** (Löschen). In der folgenden Abbildung ist das Fenster "Confirm Group Deletion" (Löschen von Gruppe bestätigen) dargestellt.



Globale Anmeldeeinstellungen konfigurieren

Auf der Registerkarte "Global login settings" (Globale Anmeldeeinstellungen) können Sie Anmeldeeinstellungen konfigurieren, die für alle Benutzer gelten.

Allgemeine Einstellungen

Geben Sie auf der Registerkarte **General** (Allgemein) an, wie Benutzeranmeldeversuche authentifiziert werden und wie lange (in Minuten) das IMM2 wartet, bevor es die Verbindung einer inaktiven Websitzung trennt. Geben Sie im Feld **User authentication method** (Benutzerauthentifizierungsmethode) an, wie die Benutzer, die versuchen, sich anzumelden, authentifiziert werden sollen. Wählen Sie eine der folgenden Authentifizierungsmethoden aus:

- **Local only** (Nur lokal): Benutzer werden durch eine Suche nach dem lokalen Benutzerkonto authentifiziert, das auf dem IMM2 konfiguriert ist. Wenn keine Übereinstimmung für die Benutzer-ID und das Kennwort vorhanden ist, wird der Zugriff verweigert.
- **LDAP only** (Nur LDAP): Das IMM2 versucht, den Benutzer mithilfe eines LDAP-Servers zu authentifizieren. Bei dieser Authentifizierungsmethode werden die lokalen Benutzerkonten auf dem IMM2 *nicht* durchsucht.
- **Local first, then LDAP** (Zuerst lokal, dann LDAP): Zuerst wird eine lokale Authentifizierung versucht. Falls diese lokale Authentifizierung fehlschlägt, wird eine LDAP-Authentifizierung versucht.
- **LDAP first, then Local** (Zuerst LDAP, dann lokal): Zuerst wird die LDAP-Authentifizierung versucht. Falls die LDAP-Authentifizierung fehlschlägt, wird eine lokale Authentifizierung versucht.

Anmerkungen:

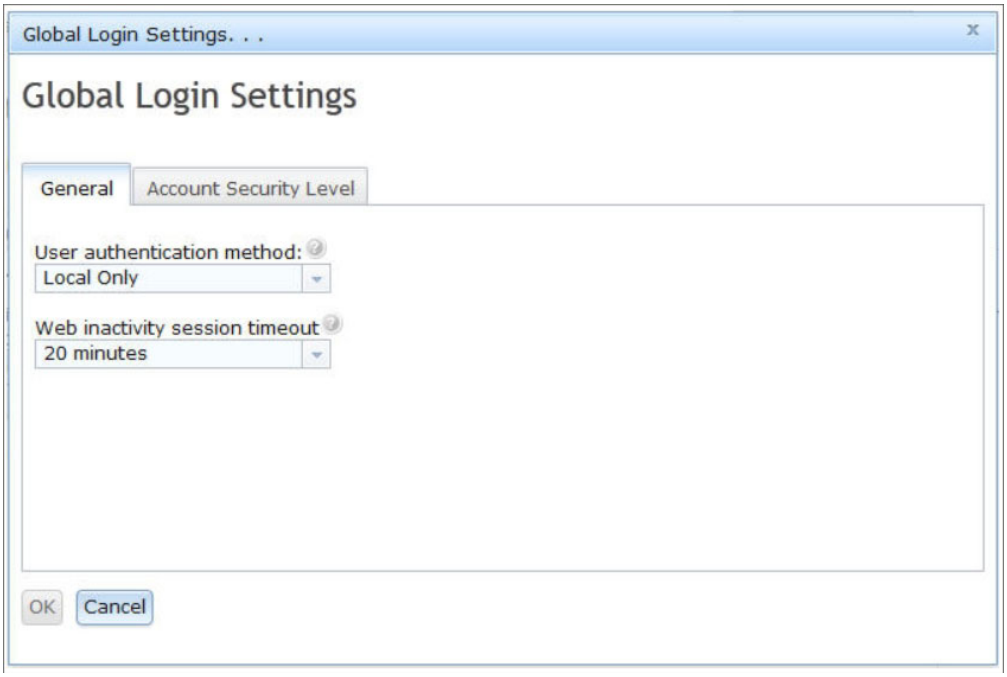
- Nur lokal verwaltete Konten werden für die IPMI- und SNMP-Schnittstellen freigegeben. Diese Schnittstellen unterstützen keine LDAP-Authentifizierung.

- IPMI- und SNMP-Benutzer können sich mithilfe der lokal verwalteten Konten anmelden, wenn für das Feld **User authentication method** die Option **LDAP only** ausgewählt ist.

Geben Sie im Feld **Web inactivity session timeout** (Sitzungszeitlimit bei Webinaktivität) an, wie lange (in Minuten) das IMM2 wartet, bevor es die Verbindung einer inaktiven Websitzung trennt. Wählen Sie **No timeout** (Kein Zeitlimit) aus, um diese Funktion zu inaktivieren. Wählen Sie **User picks timeout** (Benutzer legt Zeitlimit fest) aus, wenn der Benutzer das Zeitlimitintervall während des Anmeldeprozesses festlegen soll.

Das Inaktivitätszeitlimit gilt nur für Webseiten, die *nicht* automatisch aktualisiert werden. Wenn ein Web-Browser fortlaufend Webseitenaktualisierungen anfordert, wenn ein Benutzer zu einer Webseite wechselt, die automatisch aktualisiert wird, wird die Sitzung dieses Benutzers nicht automatisch durch das Inaktivitätszeitlimit beendet. Benutzer können auswählen, ob der Inhalt der Webseiten automatisch alle 60 Sekunden aktualisiert werden soll. Weitere Informationen zur Einstellung für automatisches Aktualisieren finden Sie im Abschnitt „Page Auto Refresh” auf Seite 17.

Die Registerkarte "General" ist in der folgenden Abbildung dargestellt.



Einige IMM2-Webseiten werden automatisch aktualisiert, auch wenn die Einstellung für automatisches Aktualisieren nicht ausgewählt wurde. Folgende IMM2-Webseiten werden automatisch aktualisiert:

- **System Status:** Der System- und der Stromversorgungsstatus werden automatisch alle drei Sekunden aktualisiert.
- **Server Power Actions:** (Serverstromversorgungsaktionen) Der Stromversorgungsstatus wird automatisch alle drei Sekunden aktualisiert.
- **Remote Control:** (Fernsteuerung) Die Schaltflächen zum Starten der Fernsteuerung werden automatisch einmal pro Sekunde aktualisiert. Die Tabelle "Session List" (Sitzungsliste) wird automatisch einmal pro Minute aktualisiert.

Die IMM2-Firmware unterstützt bis zu sechs gleichzeitige Websitzungen. Um Sitzungen für andere Benutzer freizugeben, sollten Sie sich von einer Websitzung abmelden, wenn Sie Ihre Arbeit beendet haben, anstatt sich darauf zu verlassen, dass die Sitzung nach dem Inaktivitätszeitlimit automatisch geschlossen wird.

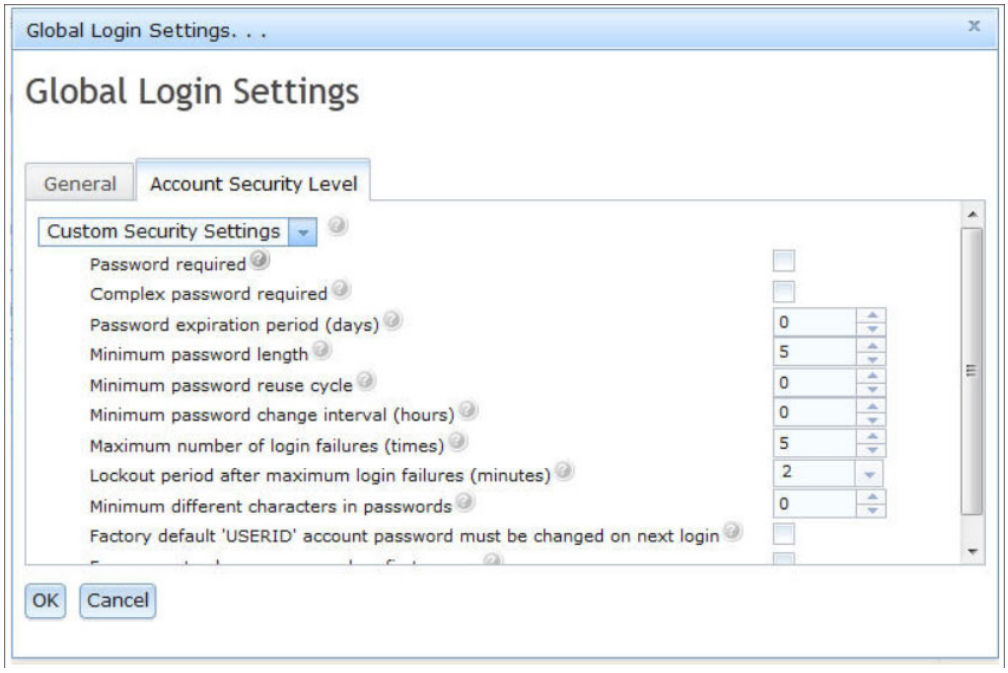
Anmerkung: Wenn Sie das Browserfenster geöffnet lassen, während Sie eine IMM2-Webseite anzeigen, die automatisch aktualisiert wird, wird Ihre Websitzung nicht automatisch aufgrund von Inaktivität geschlossen.

Einstellungen für die Kontensicherheitsrichtlinie

Klicken Sie auf die Registerkarte **Account Security Level** (Kontensicherheitsstufe), um die Einstellung für die Kontensicherheitsrichtlinie auszuwählen. Es gibt drei Stufen von Kontensicherheitsrichtlinieneinstellungen:

- Legacy Security Settings (Traditionelle Sicherheitseinstellungen)
- High Security Settings (Strenge Sicherheitseinstellungen)
- Custom Security Settings (Angepasste Sicherheitseinstellungen)

Die Registerkarte "Account Security Level" ist in der folgenden Abbildung dargestellt.



Wählen Sie die gewünschte Stufe in der Elementliste aus. Bei den Stufen "Legacy Security Settings" und "High Security Settings" sind die Werte für die Richtlinieneinstellungen vordefiniert und können nicht geändert werden. Die Stufe "Custom Security Settings" ermöglicht Benutzern das Anpassen der Sicherheitsrichtlinien nach Bedarf.

In der folgenden Tabelle sind die Werte für alle Stufen der Sicherheitseinstellungen aufgeführt.

Tabelle 3. Werte für Sicherheitseinstellungsrichtlinie

Richtlinien-einstellung/-feld	Legacy Security Settings	High Security Settings	Custom Security Settings
Password required	Nein	Ja	Ja oder Nein

Tabelle 3. Werte für Sicherheitseinstellungsrichtlinie (Forts.)

Richtlinien-einstellung/-feld	Legacy Security Settings	High Security Settings	Custom Security Settings
Complex password required	Nein	Ja	Ja oder Nein
Password expiration period (days)	Keine	90	0 - 365
Minimum password length	Keine	8	5 - 20
Minimum password reuse cycle	Keiner	5	0 - 5
Minimum password change interval (hours)	Keins	24	0 - 240
Maximum number of login failures (times)	5	5	0 - 10
Lockout period after maximum login failures (minutes)	2	60	0 - 240
Minimum different characters in passwords	Keins	2	0 - 19
Factory default 'USERID' account password must be changed on next login	Nein	Ja	Ja oder Nein
Force user to change password on first access	Nein	Ja	Ja oder Nein

Im Folgenden werden die Felder für die Sicherheitseinstellungen beschrieben.

Password required (Kennwort erforderlich)
Dieses Feld gibt an, ob Anmelde-IDs ohne Kennwort erstellt werden können. Wenn das Kontrollkästchen **Password required** ausgewählt wird, muss für alle bereits vorhandenen Anmelde-IDs ohne Kennwort bei der nächsten Anmeldung des betreffenden Benutzers ein Kennwort definiert werden.

Complex password required (Komplexes Kennwort erforderlich)
Wenn komplexe Kennwörter erforderlich sind, gelten für das Kennwort die folgenden Regeln:

- Kennwörter müssen mindestens acht Zeichen lang sein.
- Kennwörter müssen mindestens drei Vorgaben aus den folgenden vier Kategorien erfüllen:
  - Mindestens ein alphabetisches Zeichen in Kleinbuchstaben.
  - Mindestens ein alphabetisches Zeichen in Großbuchstaben.
  - Mindestens ein numerisches Zeichen.
  - Mindestens ein Sonderzeichen.
- Leerzeichen sind nicht zulässig.

- In Kennwörtern dürfen maximal drei gleiche Zeichen aufeinanderfolgen (wie z. B. aaa).
- Kennwörter dürfen keine Wiederholung oder Umkehrung der zugeordneten Benutzer-ID sein.

Wenn keine komplexen Kennwörter erforderlich sind, gelten folgende Regeln für das Kennwort:

- Kennwörter müssen mindestens fünf Zeichen lang sein (oder die Anzahl an Zeichen, die im Feld **Minimum password length** angegeben wurde).
- Kennwörter dürfen keine Leerzeichen enthalten.
- Kennwörter müssen mindestens ein numerisches Zeichen enthalten.
- Das Feld für das Kennwort kann leer sein (nur wenn das Kontrollkästchen **Password Required** nicht ausgewählt ist).

Password expiration period (days) (Kennwortablaufdauer (Tage))
Dieses Feld gibt die maximale zulässige Gültigkeitsdauer des Kennworts an, bevor das Kennwort geändert werden muss. Es werden Werte von 0 bis 365 Tagen unterstützt. Der Standardwert für dieses Feld lautet 0 (inaktiviert).

Minimum password length (Mindestlänge des Kennworts)
Dieses Feld gibt die Mindestlänge des Kennworts an. Für dieses Feld werden 5 bis 20 Zeichen unterstützt. Wenn das Kontrollkästchen **Complex password required** ausgewählt wurde, muss die Mindestlänge des Kennworts mindestens acht Zeichen betragen.

Minimum password reuse cycle (Mindestwiederverwendungszyklus des Kennworts) Dieses Feld gibt die Anzahl an vorherigen Kennwörtern an, die nicht wiederverwendet werden dürfen. Es können bis zu fünf vorherige Kennwörter verglichen werden. Wählen Sie 0 aus, um die Wiederverwendung aller vorherigen Kennwörter zuzulassen. Der Standardwert für dieses Feld lautet 0 (inaktiviert).

Minimum password change interval (hours) (Mindeständerungsintervall für Kennwörter (Stunden))
Dieses Feld gibt an, wie lange ein Benutzer von einer Kennwortänderung bis zur nächsten warten muss. Es werden Werte von 0 bis 240 Stunden unterstützt. Der Standardwert für dieses Feld lautet 0 (inaktiviert).

Maximum number of login failures (times) (Maximale Anzahl an Anmeldefehlern (Anzahl))
Dieses Feld gibt die zulässige Anzahl an fehlgeschlagenen Anmeldeversuchen an, bevor der Benutzer für einen bestimmten Zeitraum gesperrt wird. Es werden Werte von 0 bis 10 unterstützt. Der Standardwert für dieses Feld lautet 0 (inaktiviert).

Lockout period after maximum login failures (minutes) (Aussperrungszeit nach maximaler Anzahl an Anmeldefehlern (Minuten))
Dieses Feld gibt an, wie lange (in Minuten), das IMM2-Subsystem Fernanmeldungsversuche von allen Benutzern sperrt, nachdem mehr als fünf aufeinanderfolgende Anmeldefehler bei einem der Benutzer festgestellt wurden.

Minimum different characters in passwords (Mindestunterschied an Zeichen in Kennwörtern)
Dieses Feld gibt die Mindestanzahl an Zeichen an, in denen sich das neue Kennwort von dem vorherigen Kennwort unterscheiden muss. Es werden Werte von 0 bis 19 unterstützt.

Factory default 'USERID' account password must be changed on next login (Werkseitige Voreinstellung des Kennworts für 'USERID' muss bei der nächsten Anmeldung geändert werden)

Diese Herstelleroption wird bereitgestellt, um das Zurücksetzen des Standardprofils USERID nach der ersten erfolgreichen Anmeldung zu ermöglichen. Wenn dieses Kontrollkästchen ausgewählt wurde, muss das Standardkennwort geändert werden, bevor das Konto verwendet werden kann. Für das neue Kennwort gelten alle aktiven Kennwortdurchsetzungsregeln.

Force user to change password on first access (Benutzer zwingen, das Kennwort beim ersten Zugriff zu ändern)

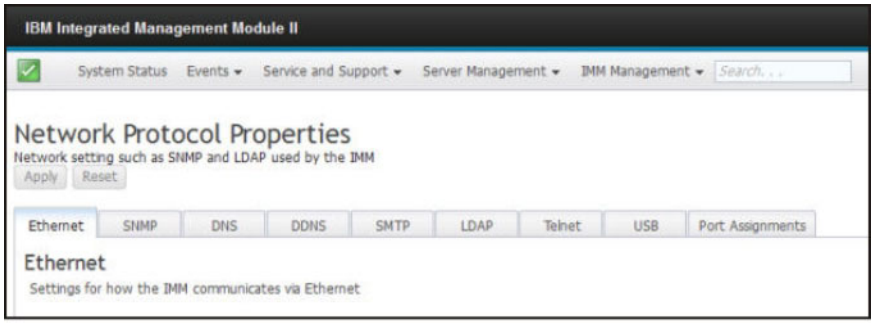
Nachdem ein neuer Benutzer mit einem Standardkennwort konfiguriert wurde, erzwingt die Auswahl dieses Kontrollkästchens, dass der betreffende Benutzer sein Kennwort bei der ersten Anmeldung ändern muss.

Netzprotokolle konfigurieren

Klicken Sie auf der Registerkarte "IMM Management" (IMM-Verwaltung) auf die Option **Network** (Netz), um die Netzeinstellungen anzuzeigen und festzulegen.

Ethernet-Einstellungen konfigurieren

Klicken Sie auf die Registerkarte **Ethernet**, um die IMM2-Ethernet-Einstellungen anzuzeigen oder zu ändern (wie in der folgenden Abbildung dargestellt).



Gehen Sie wie folgt vor, um eine IPv4-Ethernet-Verbindung zu verwenden:

1. Wählen Sie die Option **IPv4** aus. Wählen Sie nun das zugehörige Kontrollkästchen aus.

   Anmerkung: Durch Inaktivieren der Ethernet-Schnittstelle können Sie den Zugriff auf das IMM2 vom externen Netz aus verhindern.
2. Wählen Sie in der Liste **Configure IP address settings** (Einstellungen für IP-Adressen konfigurieren) eine der folgenden Optionen aus:
   - Obtain an IP address from a DHCP server (IP-Adresse von einem DHCP-Server anfordern)
   - Use static IP address (Statische IP-Adresse verwenden)
3. Wenn das IMM2 standardmäßig eine statische IP-Adresse verwenden soll, falls keine Verbindung zu einem DHCP-Server hergestellt werden kann, wählen Sie das entsprechende Kontrollkästchen aus.
4. Geben Sie im Feld **Static address** (Statische Adresse) die IP-Adresse des IMM2 ein.

Anmerkung: Die IP-Adresse muss vier Ganzzahlen von 0 bis 255 enthalten, die durch Punkte voneinander getrennt sind. Sie darf keine Leerzeichen enthalten.

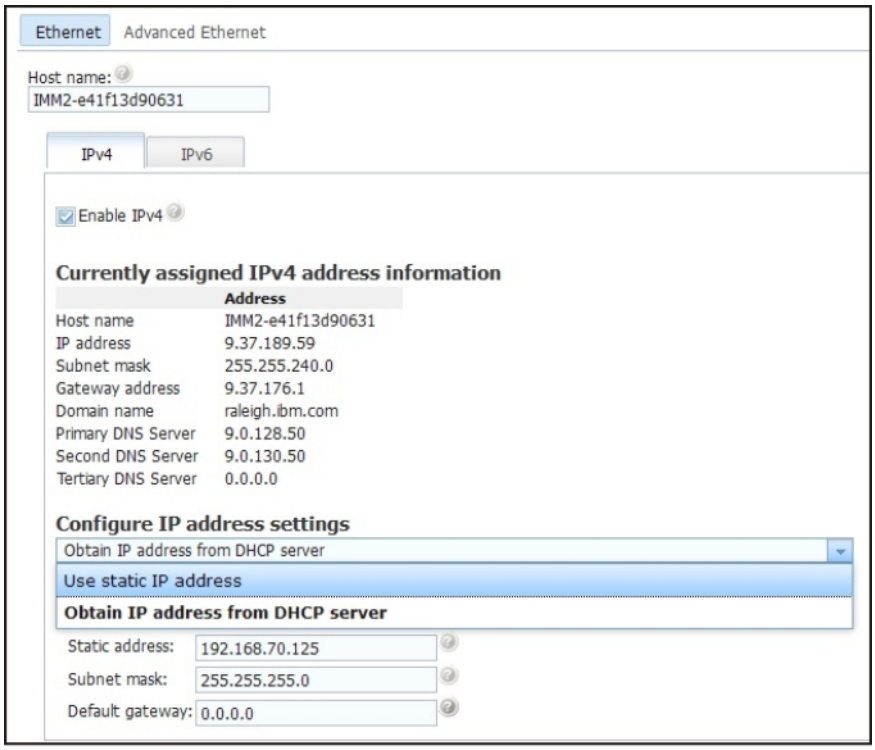
5. Geben Sie im Feld **Subnet mask** (Teilnetzmaske) die Teilnetzmaske ein, die vom IMM2 verwendet wird.

   Anmerkung: Die Teilnetzmaske muss vier Ganzzahlen von 0 bis 255 ohne Leerzeichen oder aufeinanderfolgende Punkte enthalten, wobei die Ganzzahlen durch Punkte voneinander getrennt sind. Die Standardeinstellung ist 255.255.255.0.

6. Geben Sie im Feld **Default Gateway** (Standard-Gateway) Ihren Netz-Gateway-Router ein.

   Anmerkung: Die Gateway-Adresse muss vier Ganzzahlen von 0 bis 255 ohne Leerzeichen oder aufeinanderfolgende Punkte enthalten, wobei die Ganzzahlen durch Punkte voneinander getrennt sind.

In der folgenden Abbildung ist die Registerkarte "Ethernet" dargestellt.



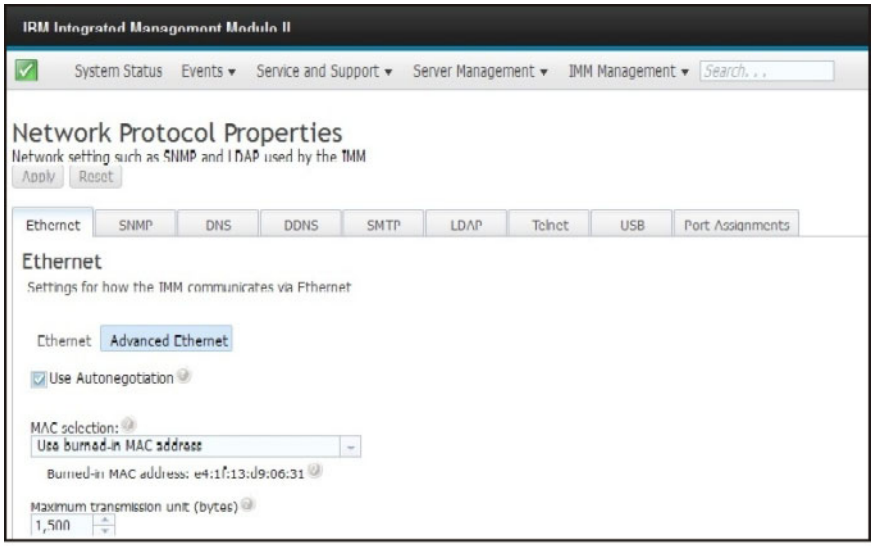
Erweiterte Ethernet-Einstellungen konfigurieren

Klicken Sie auf die Registerkarte **Advanced Ethernet** (Erweitertes Ethernet), um zusätzliche Ethernet-Einstellungen festzulegen. Wählen Sie in der Liste **MAC selection** (MAC-Auswahl) eine der folgenden Optionen aus:

- Used burned in MAC address (Herstellerkennung der MAC-Adresse verwenden)
  - Die Option "Burned-in MAC address" (Herstellerkennung der MAC-Adresse) ist eine eindeutige physische Adresse, die dem IMM2 vom Hersteller zugeordnet wurde. Die Adresse ist ein Anzeigefeld.
- Use locally administered MAC address (Lokal verwaltete MAC-Adresse verwenden)

– Wenn ein Wert angegeben wird, setzt die lokal verwaltete Adresse die Herstellerkennung der MAC-Adresse außer Kraft. Die lokal verwaltete Adresse muss ein Hexadezimalwert von `000000000000` bis `FFFFFFFFFFFF` sein. Dieser Wert muss im Format *xx:xx:xx:xx:xx:xx* angegeben werden, wobei *X* für eine Zahl von 0 bis 9 steht. Das IMM2 unterstützt die Verwendung von Multicastadressen nicht. Das erste Byte einer Multicastadresse ist eine ungerade Zahl (das niedrigstwertige Bit hat den Wert 1). Aus diesem Grund muss das erste Byte eine gerade Zahl sein.

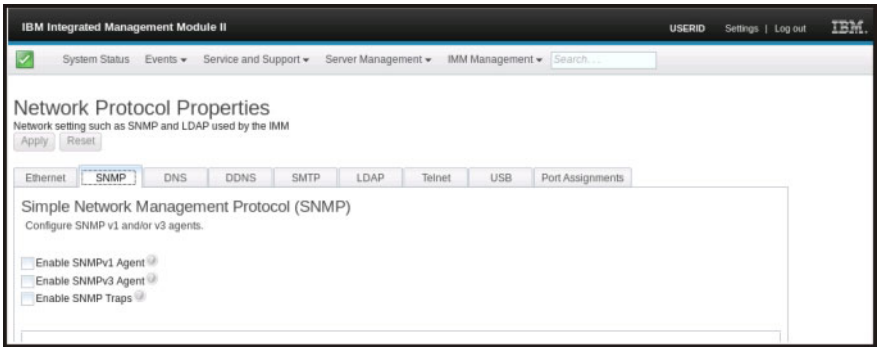
Geben Sie im Feld **Maximum transmission unit** (Größte zu übertragende Einheit) die größte zu übertragende Einheit eines Datenpakets (in Byte) für Ihre Netzschnittstelle an. Der gültige Bereich für die größte zu übertragende Einheit reicht von 60 bis 1500. Der Standardwert für dieses Feld lautet 1500. In der folgenden Abbildung sind die Registerkarte "Advanced Ethernet" und die zugehörigen Felder dargestellt.



Einstellungen für SNMP-Alerts konfigurieren

Gehen Sie wie folgt vor, um die SNMP-Einstellungen für das IMM2 zu konfigurieren.

1. Klicken Sie auf die Registerkarte **SNMP** (wie in der folgenden Abbildung dargestellt).



2. Wählen Sie das entsprechende Kontrollkästchen aus, um den SNMPv1-Agenten, den SNMPv3-Agenten oder SNMP-Traps zu aktivieren.

3. Wenn Sie den SNMPv1-Agenten aktivieren, fahren Sie mit Schritt 4 fort. Wenn Sie den SNMPv3-Agenten aktivieren, fahren Sie mit Schritt 5 fort. Wenn Sie die SNMP-Traps aktivieren, fahren Sie mit Schritt 6 auf Seite 76 fort.
4. Füllen Sie die folgenden Felder aus, wenn Sie den SNMPv1-Agenten aktiviert haben:
   a. Klicken Sie auf die Registerkarte **Contact** (Ansprechpartner). Geben Sie im Feld **Contact person** (Ansprechpartner) den Namen des Ansprechpartners ein. Geben Sie im Feld **Location** (Standort) den Standort (geografische Koordinaten) ein.
   b. Klicken Sie auf die Registerkarte **Communities**, um eine Community zum Definieren der Verwaltungsbeziehungen zwischen SNMP-Agenten und SNMP-Managern zu konfigurieren. Sie müssen mindestens eine Community definieren.

      Anmerkungen:
      - Wenn ein Fenster mit einer Fehlernachricht angezeigt wird, nehmen Sie in den Feldern, die im Fehlerfenster aufgeführt sind, die notwendigen Korrekturen vor. Blättern Sie dann zum Anfang der Seite und klicken Sie auf **Apply** (Übernehmen), um die korrigierten Informationen zu speichern.
      - Sie müssen mindestens eine Community konfigurieren, um diesen SNMP-Agenten zu aktivieren.

      Machen Sie in folgenden Feldern die erforderlichen Angaben:
      1) Geben Sie im Feld **Community Name** (Community-Name) einen Namen oder eine Zeichenfolge zur Authentifizierung ein, um die Community zu benennen.
      2) Wählen Sie im Feld **Access Type** (Zugriffstyp) einen Zugriffstyp aus.
         - Wählen Sie **Trap** aus, um allen Hosts in der Community das Empfangen von Traps zu ermöglichen.
         - Wählen Sie **Get** (Abrufen) aus, um allen Hosts in der Community das Empfangen von Traps und das Abfragen von MIB-Objekten (Management Information Base) zu ermöglichen.
         - Wählen Sie **Set** (Festlegen) aus, um allen Hosts in der Community das Empfangen von Traps sowie das Abfragen und Festlegen von MIB-Objekten (Management Information Base) zu ermöglichen.
   c. Geben Sie im Feld **Host Name** (Hostname) oder im Feld **IP Address** (IP-Adresse) den Hostnamen oder die IP-Adresse der einzelnen Community-Manager ein.
   d. Klicken Sie auf **Apply**, um die vorgenommenen Änderungen zu übernehmen.
5. Füllen Sie die folgenden Felder aus, wenn Sie den SNMPv3-Agenten aktiviert haben:
   a. Klicken Sie auf die Registerkarte **Contact** (Ansprechpartner). Geben Sie im Feld **Contact person** (Ansprechpartner) den Namen des Ansprechpartners ein. Geben Sie im Feld **Location** (Standort) den Standort (geografische Koordinaten) ein.
   b. Klicken Sie auf die Registerkarte **Users** (Benutzer), um die Liste der lokalen Benutzerkonten für die Konsole anzuzeigen.

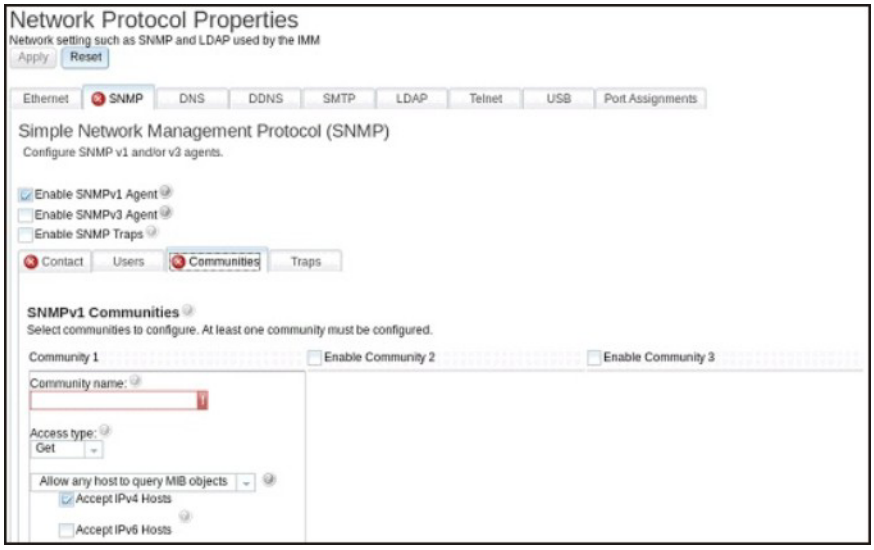
      Anmerkung: Es handelt sich um dieselbe Liste, die über die Option "Users" angezeigt wird. Sie müssen SNMPv3 für alle Benutzerkonten konfigurieren, für die ein SNMPv3-Zugriff erforderlich ist.

c. Klicken Sie auf **Apply**, um die vorgenommenen Änderungen zu übernehmen.

6. Wenn Sie die SNMP-Traps aktivieren, konfigurieren Sie die Ereignisse, die auf der Registerkarte **Traps** gemeldet werden.

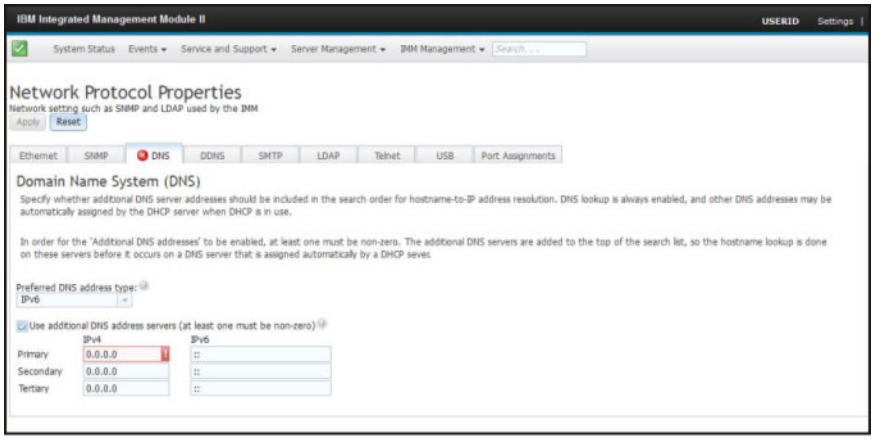
Anmerkung: Bei der Konfiguration von SNMP werden erforderliche Felder, die nicht vollständig sind oder falsche Werte enthalten, mit einem roten X hervorgehoben, das Sie dabei unterstützt, die erforderlichen Felder (richtig) auszufüllen.

In der folgenden Abbildung ist die Registerkarte "SNMP" bei der Konfiguration des SNMPv1-Agenten dargestellt.



DNS konfigurieren

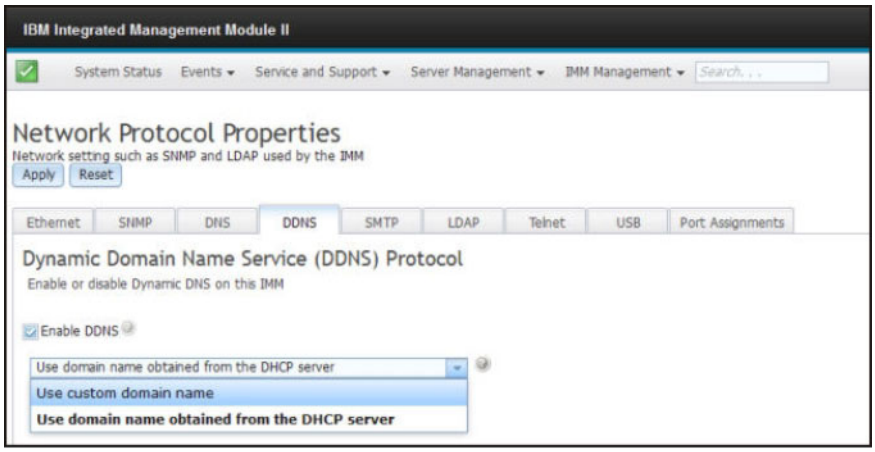
Klicken Sie auf die Registerkarte **DNS**, um die Einstellungen für das IMM2-DNS (Domain Name System) anzuzeigen oder zu ändern. Wenn Sie das Kontrollkästchen **Use additional DNS address servers** (Zusätzliche DNS-Adressserver verwenden) auswählen, können Sie die IP-Adressen von bis zu drei DNS-Servern in Ihrem Netz angeben. Jede IP-Adresse muss aus Ganzzahlen von 0 bis 255 bestehen, die voneinander durch Punkte getrennt sind (wie in der folgenden Abbildung dargestellt).



DDNS konfigurieren

Klicken Sie auf die Registerkarte **DDNS**, um die Einstellungen für das IMM2-DDNS (Dynamic Domain Name System) anzuzeigen oder zu ändern. Wählen Sie das Kontrollkästchen **Enable DDNS** (DDNS aktivieren) aus, um DDNS zu aktivieren. Wenn DDNS aktiviert ist, benachrichtigt das IMM2 einen DNS-Server, wenn die aktive DNS-Konfiguration der konfigurierten Hostnamen, Adressen oder anderer im DNS gespeicherter Informationen in Echtzeit geändert werden sollen.

Wählen Sie eine Option aus der Elementliste aus, um anzugeben, wie der Domänenname des IMM2 ausgewählt werden soll (wie in der folgenden Abbildung dargestellt).



SMTP konfigurieren

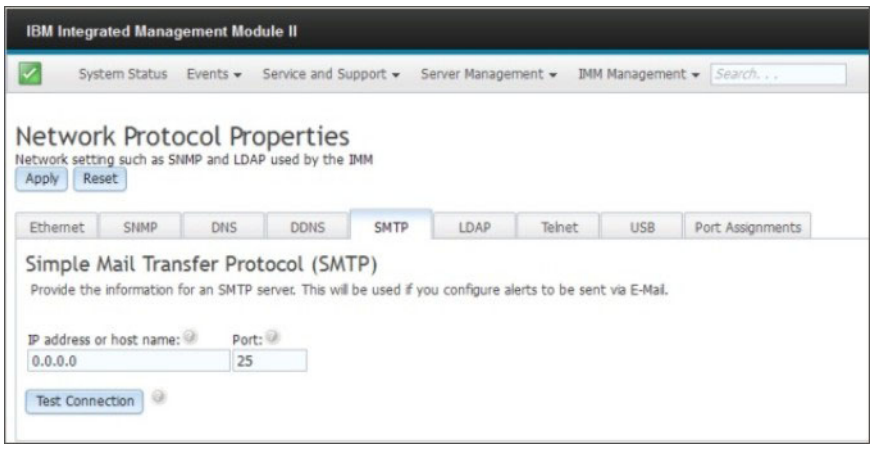
Klicken Sie auf die Registerkarte **SMTP**, um die SMTP-Einstellungen für das IMM2 anzuzeigen oder zu ändern. Füllen Sie die folgenden Felder aus, um SMTP-Einstellungen anzuzeigen oder zu ändern:

IP address or host name (IP-Adresse oder Hostname)
Geben Sie den Hostnamen des SMTP-Servers ein. Geben Sie in diesem Feld die IP-Adresse oder, wenn DNS aktiviert und konfiguriert ist, den Hostnamen des SMTP-Servers ein.

Port Geben Sie die Portnummer für den SMTP-Server ein. Der Standardwert ist 25.

Test connection (Verbindung testen)
Klicken Sie auf **Test Connection**, um eine Test-E-Mail zu senden und zu überprüfen, ob Ihre SMTP-Einstellungen richtig sind.

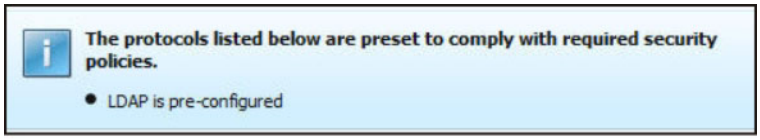
In der folgenden Abbildung ist die Registerkarte "SMTP" dargestellt.



LDAP konfigurieren

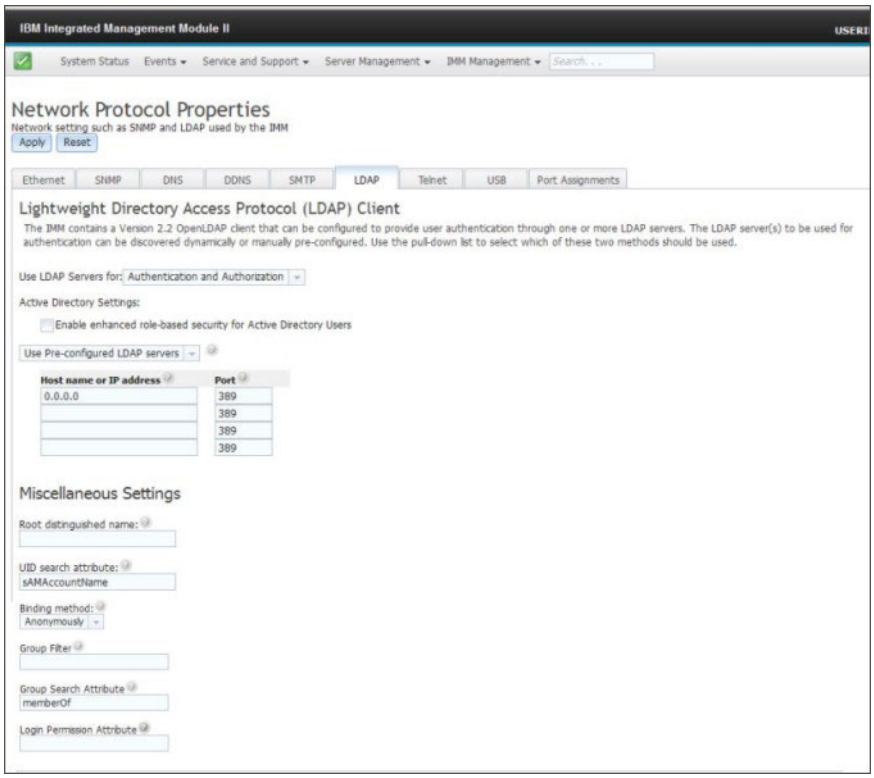
Klicken Sie auf die Registerkarte **LDAP**, um die Einstellungen für den LDAP-Client für das IMM2 anzuzeigen oder zu ändern.

Anmerkung: In einem IBM Flex System-Knoten wird das IMM2 für den LDAP-Server konfiguriert, der auf dem CMM ausgeführt wird. Sie werden in einer Informationsnachricht darauf hingewiesen, dass die LDAP-Einstellungen nicht geändert werden können (wie in der folgenden Abbildung dargestellt).



Mithilfe eines LDAP-Servers kann das IMM2 einen Benutzer durch Abfragen oder Durchsuchen eines LDAP-Verzeichnisses auf einem LDAP-Server ohne Abfragen der lokalen Benutzerdatenbank authentifizieren. Anschließend kann das IMM2 jeden Benutzerzugriff über einen zentralen LDAP-Server authentifizieren. Sie können Berechtigungsstufen auf der Basis der Informationen auf dem LDAP-Server zuordnen. Sie können LDAP auch dazu verwenden, Benutzer und IMM2-Module Gruppen zuzuordnen und eine Gruppenauthentifizierung zusätzlich zu der normalen Benutzerauthentifizierung (Kennwortprüfung) durchzuführen. Ein IMM2 kann z. B. einer oder mehreren Gruppen zugehörig sein. In diesem Fall besteht der Benutzer die Gruppenauthentifizierung nur dann, wenn er zu mindestens einer der Gruppen gehört, die dem IMM2 zugeordnet sind.

In der folgenden Abbildung ist die Registerkarte "LDAP" dargestellt.



Um einen vorkonfigurierten LDAP-Server zu verwenden, füllen Sie die folgenden Felder aus:

Elementliste "LDAP server configuration" (LDAP-Server-Konfiguration)
Wählen Sie **Use Pre-Configured LDAP Server** (Vorkonfigurierten LDAP-Server verwenden) in der Elementliste aus. Die Portnummer für die einzelnen Server ist optional. Wenn in diesem Feld keine Angaben gemacht werden, wird der Standardwert 389 für nicht sichere LDAP-Verbindungen verwendet. Für sichere Verbindungen lautet der Standardwert 636. Sie müssen mindestens einen LDAP-Server konfigurieren.

Root distinguished name (Definierter Name für den Stammeintrag)
Der definierte Name (DN) für den Stammeintrag der Verzeichnisstruktur des LDAP-Servers (z. B. dn=mycompany,dc=com). Dieser definierte Name wird als Basisobjekt für alle Suchvorgänge verwendet.

UID search attribute (UID-Suchattribut)
Wenn als Bindungsmethode **Anonymously** (Anonym) oder **With Configured Credentials** (Mit konfigurierten Berechtigungsnachweisen) festgelegt wurde, folgt der einleitenden Verbindung zum LDAP-Server eine Suchanforderung, die bestimmte Informationen zum Benutzer abruft, einschließlich des definierten Namens (DN), der Anmeldeberechtigungen und der Gruppenmitgliedschaft des Benutzers. Diese Suchanforderung muss den Attributnamen angeben, der für die Benutzer-IDs auf diesem Server steht. Dieser Attributname wird in diesem Feld konfiguriert. Auf Active Directory-Servern lautet der Attributname normalerweise **sAMAccountName**. Auf Novell eDirectory- und OpenLDAP-Servern lautet der Attributname **uid**. Wenn in diesem Feld keine Angaben gemacht werden, lautet der Standardwert **uid**.

Binding method (Bindungsmethode)
Bevor eine Suchanfrage oder eine Abfrage an den LDAP-Server gesendet werden kann, muss eine Bindeanforderung gesendet werden. Mit diesem

Feld wird gesteuert, wie diese einleitende Verbindung zum LDAP-Server ausgeführt wird. Die folgenden Bindungsmethoden sind verfügbar:

- Anonymously (Anonym)
  - Mit dieser Methode wird eine Bindung ohne einen definierten Namen oder ein Kennwort hergestellt. Diese Methode sollte jedoch nicht verwendet werden, da die meisten Server so konfiguriert sind, dass sie Suchanforderungen für bestimmte Benutzersätze nicht zulassen.
- With Configured Credentials (Mit konfiguriertem Berechtigungsnachweis)
  - Mit dieser Methode wird eine Bindung mit einem konfigurierten definierten Namen und einem Kennwort hergestellt.
- With Login Credentials (Mit Berechtigungsnachweis für Anmeldung)
  - Mit dieser Methode wird eine Bindung mit dem Berechtigungsnachweis hergestellt, der beim Anmeldeprozess angegeben wird. Die Benutzer-ID kann als definierter Name, als vollständig qualifizierter Domänenname oder als eine Benutzer-ID angegeben werden, die mit der Angabe unter **UID Search Attribute** (UID-Suchattribut) übereinstimmt, die auf dem IMM2 konfiguriert wurde. Wenn die einleitende Verbindung erfolgreich hergestellt werden kann, wird eine Suche durchgeführt, um einen Eintrag auf dem LDAP-Server zu finden, der zu dem Benutzer gehört, der versucht, sich anzumelden. Falls erforderlich, wird ein zweiter Verbindungsversuch durchgeführt, diesmal mit dem definierten Benutzernamen, der aus dem LDAP-Datensatz des Benutzers abgerufen wurde, und dem Kennwort, das bei der Anmeldung eingegeben wurde. Schlägt dieser Versuch fehl, wird dem Benutzer der Zugriff verweigert. Der zweite Verbindungsversuch wird nur dann durchgeführt, wenn die Bindungsmethoden **Anonymous** oder **With Configured Credentials** verwendet werden.

Group Filter (Gruppenfilter)

Das Feld **Group Filter** (Gruppenfilter) wird für die Gruppenauthentifizierung verwendet. Nachdem der Berechtigungsnachweis des Benutzers erfolgreich überprüft wurde, wird versucht, die Gruppenauthentifizierung durchzuführen. Wenn die Gruppenauthentifizierung fehlschlägt, wird dem Benutzer die Anmeldung verweigert. Wenn der Gruppenfilter konfiguriert ist, gibt er an, zu welchen Gruppen der Serviceprozessor gehört. Das bedeutet, dass der Benutzer zu mindestens einer der konfigurierten Gruppen gehören muss, damit die Gruppenauthentifizierung erfolgreich durchgeführt werden kann. Wenn das Feld **Group Filter** leer ist, ist die Gruppenauthentifizierung automatisch erfolgreich. Wenn der Gruppenfilter konfiguriert wurde, wird versucht, mindestens eine Gruppe in der Liste zu finden, die mit einer Gruppe übereinstimmt, der der Benutzer angehört. Wenn es keine Übereinstimmung gibt, schlägt die Authentifizierung des Benutzers fehl und der Zugriff wird verweigert. Wenn mindestens eine Übereinstimmung vorhanden ist, ist die Gruppenauthentifizierung erfolgreich.

Beim Abgleich muss die Groß-/Kleinschreibung beachtet werden. Der Filter ist auf 511 Zeichen begrenzt und kann aus einem oder aus mehreren Gruppennamen bestehen. Um mehrere Gruppennamen voneinander abzugrenzen, muss das Doppelpunktzeichen (:) verwendet werden. Vorangestellte und nachgestellte Leerzeichen werden nicht beachtet. Alle anderen Leerzeichen werden als Teil des Gruppennamens behandelt. Sie haben die Möglichkeit, auszuwählen, ob Platzhalterzeichen in Gruppennamen verwendet werden sollen oder nicht. Der Filter kann ein bestimmter Gruppenname (z. B. IMMWest), ein Stern (*), der als Platzhalterzeichen für alle an-

deren Zeichen steht, oder ein Platzhalterzeichen mit einem Präfix (z. B. IMM*) sein. Der Standardfilter lautet "IMM*". Wenn die Sicherheitsrichtlinien in Ihrer Installation die Verwendung von Platzhalterzeichen untersagen, können Sie auswählen, dass keine Platzhalterzeichen zulässig sind. Das Platzhalterzeichen (*) wird dann als normales Zeichen und nicht als Platzhalter behandelt. Ein Gruppenname kann als vollständiger definierter Name oder nur mithilfe des *cn*-Teils angegeben werden. Beispiel: Eine Gruppe mit dem definierten Namen "cn=adminGroup,dc=mycompany,dc=com" kann mit dem tatsächlichen definierten Namen oder mit "adminGroup" angegeben werden.

verschachtelte Gruppenmitgliedschaften werden nur in Active Directory-Umgebungen unterstützt. Wenn ein Benutzer z. B. ein Mitglied von GroupA und GroupB ist und GroupA auch ein Mitglied von GroupC ist, ist der Benutzer (implizit) auch ein Mitglied von GroupC. Verschachtelte Suchprozesse werden nach dem Durchsuchen von 128 Gruppen gestoppt. Zuerst werden alle Gruppen einer Ebene durchsucht, bevor Gruppen einer tieferen Ebene durchsucht werden. Schleifen werden nicht erkannt.

Group Search Attribute (Attribut für die Gruppensuche)
In einer Active Directory- oder Novell eDirectory-Umgebung gibt das Feld **Group Search Attribute** den Attributnamen an, der die Gruppen bezeichnet, denen ein Benutzer angehört. In einer Active Directory-Umgebung lautet der Attributname **memberOf**. In einer eDirectory-Umgebung lautet der Attributname **groupMembership**. In einer OpenLDAP-Serverumgebung werden Benutzer normalerweise Gruppen zugeordnet, deren objectClass gleich "PosixGroup" ist. In diesem Kontext gibt dieses Feld den Attributnamen an, der die Mitglieder einer bestimmten PosixGroup bezeichnet. Dieser Attributname lautet **memberUid**. Wenn in diesem Feld keine Angaben gemacht werden, wird für den Attributnamen im Filter standardmäßig **memberOf** verwendet.

Login Permission Attribute (Attribut für die Anmeldeberechtigung)
Wenn ein Benutzer erfolgreich über einen LDAP-Server authentifiziert wird, müssen die Anmeldeberechtigungen für den Benutzer abgerufen werden. Um diese Anmeldeberechtigungen abzurufen, muss der an den Server gesendete Suchfilter den Attributnamen angeben, der den Anmeldeberechtigungen zugeordnet wurde. Das Feld **Login Permission Attribute** gibt den Attributnamen an. Wenn in diesem Feld keine Angaben gemacht werden, werden dem Benutzer standardmäßig Leseberechtigungen zugeordnet, vorausgesetzt, der Benutzer besteht die Benutzer- und die Gruppenauthentifizierung.

Der vom LDAP-Server zurückgegebene Attributwert sucht nach der Suchbegriffszeichenfolge "IBMRBSPermissions=". Auf diese Suchbegriffszeichenfolge muss unmittelbar danach eine Bitfolge (aus bis zu 12 aufeinanderfolgenden Nullen oder Einsen) folgen. Jedes Bit steht für eine Gruppe von Funktionen. Die Bits sind entsprechend ihren Positionen nummeriert. Das erste Bit (links) ist Bitposition 0, das letzte Bit (rechts) ist Bitposition 11. Der Wert 1 in einer Bitposition aktiviert die Funktion, die dieser Bitposition zugeordnet ist. Der Wert 0 in einer Bitposition inaktiviert die Funktion, die dieser Bitposition zugeordnet ist.

Ein gültiges Beispiel ist die Zeichenfolge "IBMRBSPermissions=010000000000". Der Suchbegriff "IBMRBSPermissions=" wird verwendet, damit er in einer beliebigen Position in diesem Feld platziert werden kann. So kann der LDAP-Administrator ein vorhandenes Attribut wiederverwenden und eine Erweiterung des LDAP-Schemas verhindern. Außer-

dem ermöglicht es die Verwendung des Attributs für seine ursprüngliche Bestimmung. Sie können die Suchbegriffszeichenfolge in eine beliebige Position in diesem Feld einfügen. Das verwendete Attribut lässt eine frei formatierte Zeichenfolge zu. Wenn das Attribut erfolgreich abgerufen werden kann, wird der Wert, der vom LDAP-Server zurückgegeben wird, entsprechend den Informationen in der folgenden Tabelle interpretiert.

Tabelle 4. Berechtigungsbits

Bit-position	**Funktion**	**Erläuterung**
0	Deny Always (Nie zulassen)	Die Authentifizierung eines Benutzers schlägt immer fehl. Diese Funktion kann verwendet werden, um einen oder mehrere bestimmte Benutzer, die einer bestimmten Gruppe zugeordnet sind, zu blockieren.
1	Supervisor Access (Administratorzugriff)	Einem Benutzer wird die Administratorberechtigung erteilt. Der Benutzer hat Schreib-/Lesezugriff auf jede Funktion. Wenn Sie dieses Bit einstellen, müssen Sie die anderen Bits nicht einzeln einstellen.
2	Read Only Access (Lesezugriff)	Ein Benutzer hat Lesezugriff und kann keine Wartungsarbeiten (beispielsweise Neustart, fern ausgeführte Aktionen oder Firmwareaktualisierungen) oder Änderungen (wie z. B. Funktionen zum Speichern, Löschen oder Wiederherstellen) durchführen. Bitposition 2 und alle anderen Bits schließen sich gegenseitig aus, wobei Bitposition 2 die niedrigste Vorrangstellung hat. Wenn irgendein anderes Bit gesetzt ist, wird dieses Bit ignoriert.
3	Networking and Security (Netzbetrieb und Sicherheit)	Ein Benutzer kann die Konfiguration für "Security" (Sicherheit), "Network Protocols" (Netzprotokolle), "Network Interface" (Netzschnittstelle), "Port Assignments" (Portzuordnungen) und "Serial Port" (Serieller Anschluss) ändern.
4	User Account Management (Benutzerkontenverwaltung)	Ein Benutzer kann andere Benutzer hinzufügen, ändern oder löschen und die "Global Login Settings" (Globale Anmeldungseinstellungen) im Fenster "Login Profiles" (Anmeldeprofile) ändern.
5	Remote Console Access (Zugriff auf ferne Konsole)	Ein Benutzer kann auf die Remote-Server-Konsole zugreifen.
6	Remote Console and Remote Disk Access (Zugriff auf ferne Konsole und fernen Datenträger)	Ein Benutzer kann auf die Remote-Server-Konsole und die Funktionen für ferne Datenträger für den fernen Server zugreifen.
7	Remote Server Power/Restart Access (Zugriff auf Einschalten/Neustart des fernen Servers)	Der Benutzer kann auf die Einschalt- und Neustartfunktionen für den fernen Server zugreifen.

Tabelle 4. Berechtigungsbits (Forts.)

Bit-position	**Funktion**	**Erläuterung**
8	Basic Adapter Configuration (Basisadapterkonfiguration)	Ein Benutzer kann Konfigurationsparameter auf den Seiten "System Settings" (Systemeinstellungen) und "Alerts" ändern.
9	Ability to Clear Event Logs (Fähigkeit, Ereignisprotokolle zu löschen)	Ein Benutzer kann die Ereignisprotokolle löschen. **Anmerkung:** Alle Benutzer können die Ereignisprotokolle einsehen; um jedoch die Protokolle löschen zu können, muss der Benutzer diese Berechtigungsstufe haben.
10	Advanced Adapter Configuration (Erweiterte Adapterkonfiguration)	Für Benutzer gelten keine Einschränkungen beim Konfigurieren des IMM2. Außerdem verfügt der Benutzer über einen Verwaltungszugriff auf das IMM2. Der Benutzer kann folgende erweiterte Funktionen ausführen: Firmwareaktualisierungen, PXE-Netzboot, werkseitige IMM2-Voreinstellungen wiederherstellen, die Adapterkonfiguration aus einer Konfigurationsdatei ändern und wiederherstellen und das IMM2 erneut starten bzw. zurücksetzen.
11	Reserved (Reserviert)	Diese Bitposition ist für den künftigen Gebrauch reserviert. Wenn keines der Bits gesetzt ist, hat der Benutzer eine Leseberechtigung. Priorität haben die Anmeldeberechtigungen, die direkt aus dem Benutzersatz abgerufen werden. Wenn das Attribut für die Anmeldeberechtigung nicht im Datensatz des Benutzers enthalten ist, wird versucht, die Berechtigungen von den Gruppen abzurufen, zu denen der Benutzer gehört. Dies wird als Teil der Gruppenauthentifizierungsphase ausgeführt. Dem Benutzer wird das inklusive OR aller Bits für alle Gruppen zugewiesen. Das Bit für den Lesezugriff (Position 2) wird nur gesetzt, wenn alle anderen Bits auf null gesetzt werden. Wenn das Bit für "Deny Always" (Position 0) für eine der Gruppen gesetzt ist, wird dem Benutzer der Zugriff verweigert. Das Bit "Deny Always" (Position 0) hat vor allen anderen Bits Vorrang.

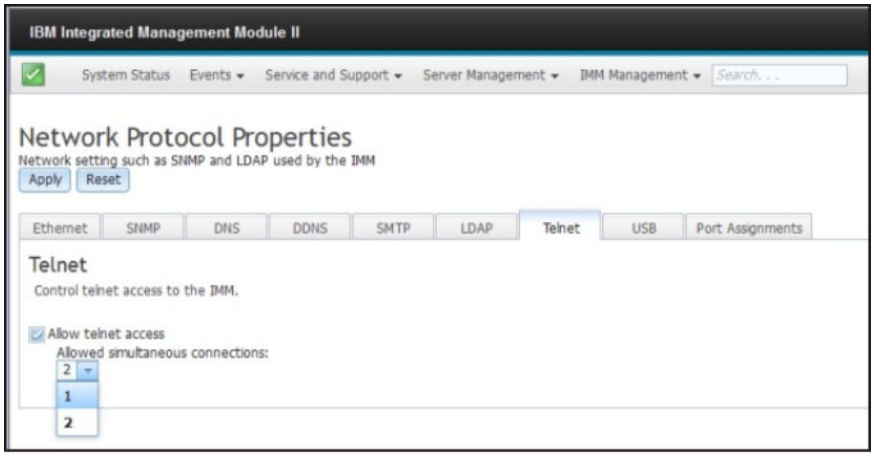
Telnet konfigurieren

Wählen Sie die Registerkarte **Telnet** aus, um die Telnet-Einstellungen für das IMM2 anzuzeigen oder zu ändern. Füllen Sie die folgenden Felder aus, um Telnet-Einstellungen anzuzeigen oder zu ändern:

Allow telnet access (Telnet-Zugriff zulassen)
Wählen Sie das entsprechende Kontrollkästchen aus, wenn das IMM2 einen Telnet-Zugriff zulassen soll.

Allowed simultaneous connections (Zugelassene gleichzeitige Verbindungen)
Wählen Sie mithilfe der Liste **Allowed simultaneous connections** die Anzahl an gleichzeitigen Telnet-Verbindungen aus, die zulässig sind.

In der folgenden Abbildung ist die Registerkarte "Telnet" dargestellt.

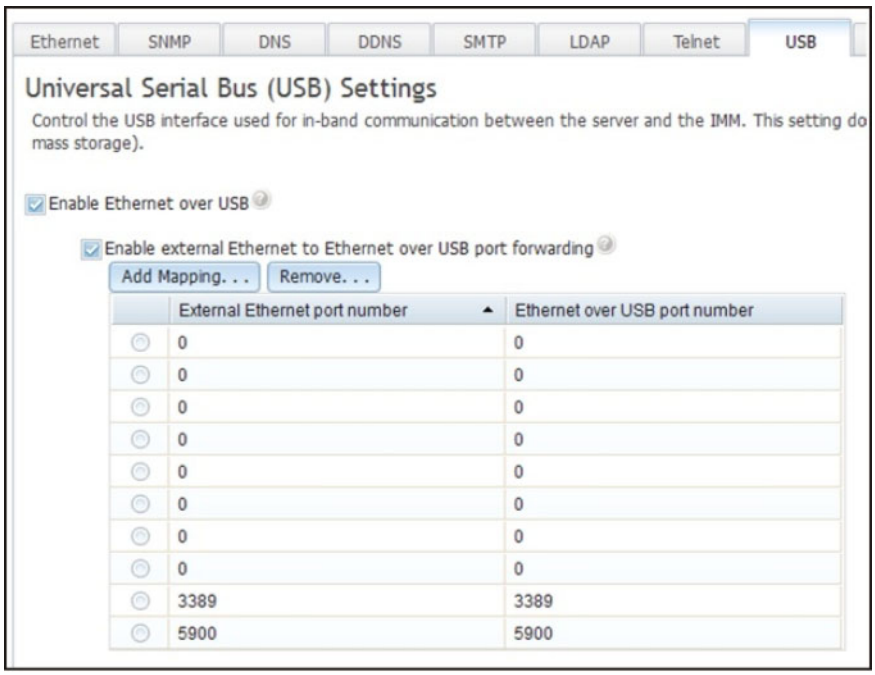


USB konfigurieren

Wählen Sie die Registerkarte **USB** aus, um die IMM2-USB-Einstellungen für das IMM2 anzuzeigen oder zu ändern. Die USB-Inband-Schnittstelle (oder Schnittstelle "LAN over USB") wird für die Inbandkommunikation zum IMM2 verwendet. Klicken Sie auf das Kontrollkästchen **Enable Ethernet over USB** (Ethernet over USB aktivieren), um die IMM2-Schnittstelle "LAN over USB" zu aktivieren oder zu inaktivieren.

Wichtig: Wenn Sie die USB-Inband-Schnittstelle inaktivieren, können Sie keine Inband-Aktualisierung der IMM2-Firmware, der Server-Firmware und der DSA-Firmware mithilfe der Linux- oder Windows-Flashdienstprogramme durchführen. Wenn die USB-Inband-Schnittstelle inaktiviert ist, verwenden Sie die Option "Firmware Server" auf der Registerkarte "Server Management" zum Aktualisieren der Firmware. Wenn Sie die USB-Inband-Schnittstelle inaktivieren, inaktivieren Sie auch die Watchdog-Zeitlimitüberschreitungen, um zu verhindern, dass der Server unerwartet neu startet.

In der folgenden Abbildung ist die Registerkarte "USB" dargestellt.



Die Zuordnung von externen Ethernet-Portnummern zu Ethernet-over-USB-Portnummern können Sie durch Klicken auf das Kontrollkästchen **Enable external Ethernet to Ethernet over USB port forwarding** (Weiterleitung von externem Ethernet-Port zu Ethernet-over-USB-Port) steuern. Füllen Sie anschließend die Zuordnungsinformationen für die Ports aus, für die die Weiterleitung gelten soll.

Portzuordnungen konfigurieren

Wählen Sie die Registerkarte **Port Assignments** (Portzuordnungen) aus, um die Portzuordnungen für das IMM2 anzuzeigen oder zu ändern. Füllen Sie die folgenden Felder aus, um Portzuordnungen anzuzeigen oder zu ändern:

HTTP Geben Sie in diesem Feld die Portnummer für den HTTP-Server des IMM2 an. Der Standardwert ist 80. Gültige Werte für Portnummern liegen im Bereich von 1 bis 65535.

HTTPS
Geben Sie in diesem Feld die Portnummer an, die für Webschnittstellen-HTTPS-SSL-Datenverkehr verwendet wird. Der Standardwert ist 443. Gültige Werte für Portnummern liegen im Bereich von 1 bis 65535.

Telnet CLI (Telnet-Befehlszeilenschnittstelle)
Geben Sie in diesem Feld die Portnummer für die traditionelle Befehlszeilenschnittstelle für die Anmeldung über den Telnet-Service an. Der Standardwert ist 23. Gültige Werte für Portnummern liegen im Bereich von 1 bis 65535.

SSH Legacy CLI (Traditionelle SSH-Befehlszeilenschnittstelle)
Geben Sie in diesem Feld die Portnummer an, die für die traditionelle Befehlszeilenschnittstelle für die Anmeldung über das SSH-Protokoll konfiguriert ist. Der Standardwert ist 22.

SNMP Agent (SNMP-Agent)
Geben Sie in diesem Feld die Portnummer für den SNMP-Agenten an, der auf dem IMM2 ausgeführt wird. Der Standardwert ist 161. Gültige Werte für Portnummern liegen im Bereich von 1 bis 65535.

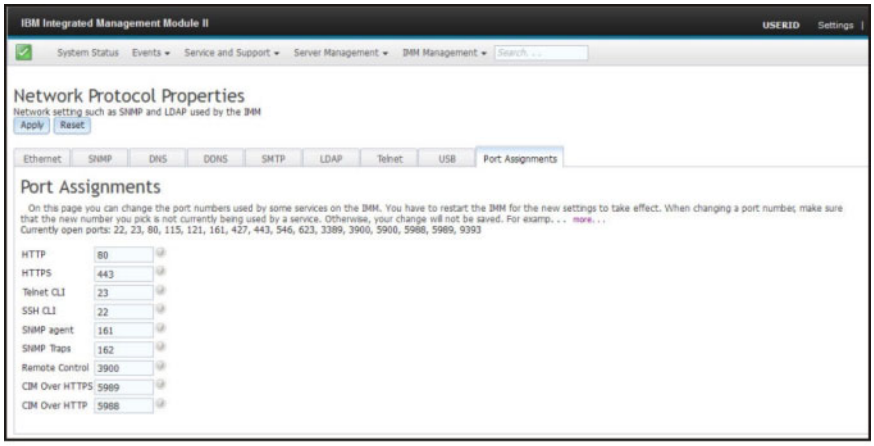
SNMP Traps (SNMP-Traps)
Geben Sie in diesem Feld die Portnummer an, die für SNMP-Traps verwendet wird. Der Standardwert ist 162. Gültige Werte für Portnummern liegen im Bereich von 1 bis 65535.

Remote Control (Fernsteuerung)
Geben Sie in diesem Feld die Portnummer an, die die Fernsteuerungsfunktion für Anzeige und Interaktion mit der Serverkonsole verwendet. Der Standardwert lautet 3900 für in Gehäuse installierte Server und Turmserver.

CIM over HTTP
Geben Sie in diesem Feld die Portnummer für CIM over HTTP an. Der Standardwert ist 5988.

CIM over HTTPS
Geben Sie in diesem Feld die Portnummer für CIM over HTTPS an. Der Standardwert ist 5989.

In der folgenden Abbildung ist die Registerkarte "Port Assignments" dargestellt.



Sicherheitseinstellungen konfigurieren

Klicken Sie auf der Registerkarte "IMM Management" (IMM-Verwaltung) auf die Option **Security** (Sicherheit), um auf die Sicherheitseigenschaften, den Status und die Einstellungen für das IMM2 zuzugreifen und sie zu konfigurieren (wie in der folgenden Abbildung dargestellt).

Um Ihre Änderungen zu übernehmen, klicken Sie oben links im Fenster "IMM Security" auf die Schaltfläche **Apply** (Übernehmen). Um Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Reset Values** (Werte zurücksetzen).

HTTPS-Protokoll konfigurieren

Klicken Sie auf die Registerkarte **HTTPS Server**, um die IMM2-Webschnittstelle so zu konfigurieren, dass sie das sicherere HTTPS-Protokoll und nicht das HTTP-Standardprotokoll verwendet.

Anmerkungen:

- Es kann nur ein Protokoll aktiviert sein.
- Das Aktivieren dieser Option erfordert eine zusätzliche Konfiguration der SSL-Zertifikate.
- Wenn Sie das Protokoll ändern, müssen Sie anschließend den IMM2-Web-Server erneut starten.

Weitere Informationen zu SSL finden Sie im Abschnitt „Übersicht über SSL” auf Seite 92. In der folgenden Abbildung ist die Registerkarte "HTTPS Server" dargestellt.

Anmerkung: Auf manchen Servern werden die IMM2-Sicherheitsstufen möglicherweise von einem anderen Managementsystem gesteuert. In diesen Umgebungen können Sie die oben genannten Aktionen in der IMM2-Webschnittstelle inaktivieren.

Handhabung von HTTPS-Zertifikaten

Verwenden Sie die Optionen im Menü "Actions" für die Handhabung von HTTPS-Zertifikaten. Wenn eine Option inaktiviert ist, müssen Sie möglicherweise zuerst eine andere Aktion ausführen, um diese Option zu aktivieren. Während Sie mit HTTPS-Zertifikaten arbeiten, sollten Sie den HTTPS-Server inaktivieren. Weitere Informationen zur Handhabung von Zertifikaten finden Sie im Abschnitt „Handhabung von SSL-Zertifikaten” auf Seite 92.

Anmerkung: Nachdem Sie die Handhabung von Zertifikaten konfiguriert haben, müssen Sie das IMM2 erneut starten, damit Ihre Änderungen wirksam werden.

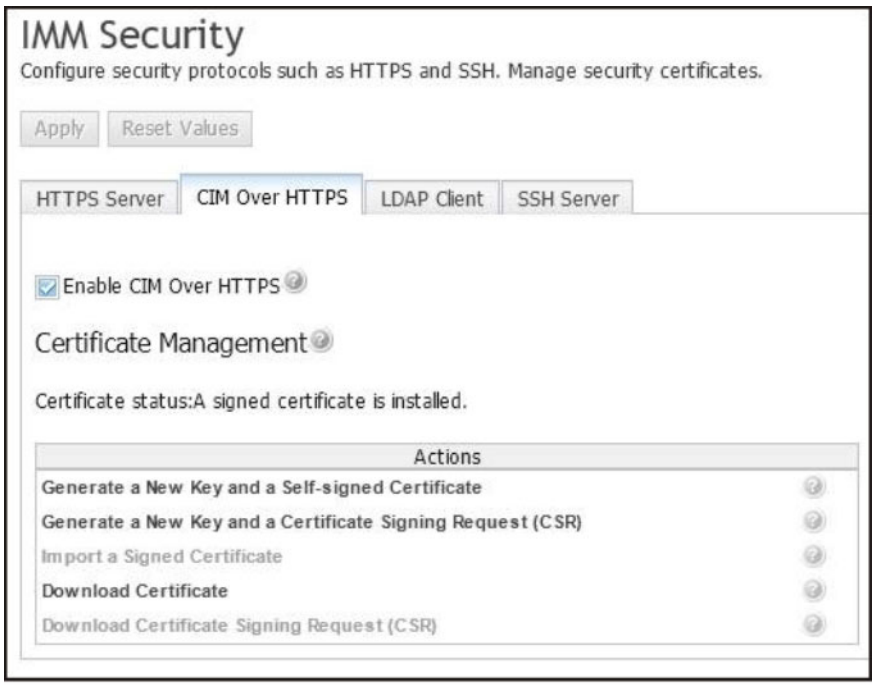
CIM-over-HTTPS-Protokoll konfigurieren

Klicken Sie auf die Registerkarte **CIM over HTTPS**, um die IMM2-Webschnittstelle so zu konfigurieren, dass sie das sicherere CIM-over-HTTPS-Protokoll und nicht das CIM-over-HTTP-Standardprotokoll verwendet.

Anmerkungen:

- Es kann nur ein Protokoll aktiviert sein.
- Das Aktivieren dieser Option erfordert eine zusätzliche Konfiguration der SSL-Zertifikate.
- Wenn Sie das Protokoll ändern, müssen Sie anschließend den IMM2-Web-Server erneut starten.

Weitere Informationen zu SSL finden Sie im Abschnitt „Übersicht über SSL” auf Seite 92. In der folgenden Abbildung ist die Registerkarte "CIM over HTTPS" dargestellt.



Handhabung von CIM-over-HTTPS-Zertifikaten

Verwenden Sie die Optionen im Menü "Actions" für die Handhabung von CIM-over-HTTPS-Zertifikaten. Wenn eine Option inaktiviert ist, müssen Sie möglicherweise zuerst eine andere Aktion ausführen, um diese Option zu aktivieren. Weitere Informationen zur Handhabung von Zertifikaten finden Sie im Abschnitt „Handhabung von SSL-Zertifikaten” auf Seite 92.

Anmerkung: Nachdem Sie die Handhabung von Zertifikaten konfiguriert haben, müssen Sie das IMM2 erneut starten, damit Ihre Änderungen wirksam werden.

Protokoll für LDAP-Client konfigurieren

Klicken Sie auf die Option **LDAP Client**, um das sicherere LDAP-over-SSL-Protokoll anstatt des LDAP-Standardprotokolls zu verwenden.

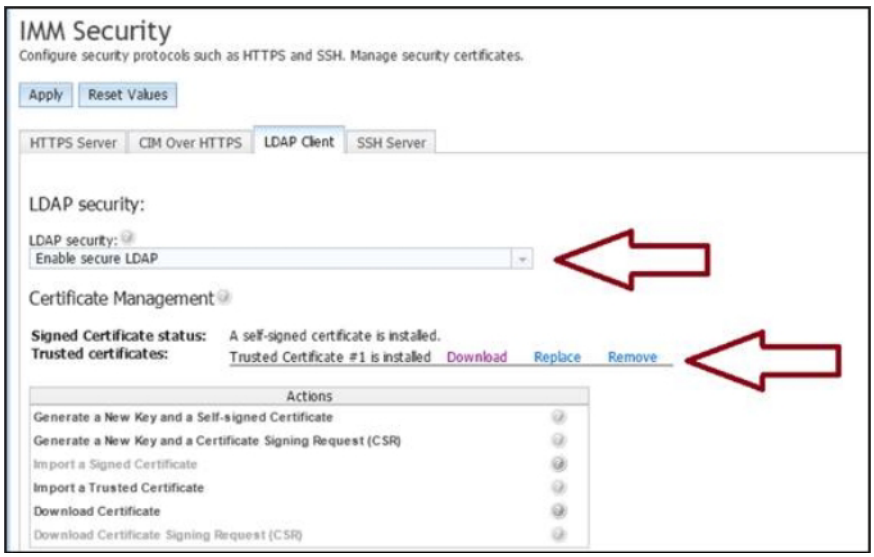
Anmerkung: Das Aktivieren dieser Option erfordert eine zusätzliche Konfiguration der SSL-Zertifikate.
Weitere Informationen zu SSL finden Sie im Abschnitt „Übersicht über SSL” auf Seite 92. In der folgenden Abbildung ist die Registerkarte "LDAP Client" dargestellt.

Handhabung von Zertifikaten für sicheren LDAP-Client

Verwenden Sie die Optionen im Menü "Actions" für die Handhabung von LDAP-over-SSL-Zertifikaten. Wenn eine Option inaktiviert ist, müssen Sie möglicherweise zuerst eine andere Aktion ausführen, um diese Option zu aktivieren. Während Sie mit HTTPS-Zertifikaten arbeiten, sollten Sie den HTTPS-Server inaktivieren. Weitere Informationen zur Handhabung von Zertifikaten finden Sie im Abschnitt „Handhabung von SSL-Zertifikaten" auf Seite 92. Nachdem Sie das vertrauenswürdige Zertifikat (Trusted Certificate) installiert haben, können Sie LDAP over SSL aktivieren, wie in der folgenden Abbildung dargestellt.

Anmerkungen:

- Änderungen am IMM2 werden sofort wirksam.
- Ihr LDAP-Server muss SSL3 (Secure Socket Layer 3) oder TLS (Transport Layer Security) unterstützen, damit er kompatibel mit dem sicheren LDAP-Client des IMM2 ist.



Secure Shell-Server konfigurieren

Klicken Sie auf die Registerkarte **SSH Server**, um die IMM2-Webschnittstelle so zu konfigurieren, dass sie das sicherere SSH-Protokoll und nicht das Telnet-Standardprotokoll verwendet.

Anmerkung:

- Für diese Option ist keine Zertifikatsverwaltung erforderlich.
- Das IMM2 erstellt anfangs einen SSH-Server-Schlüssel. Wenn Sie einen neuen SSH-Server-Schlüssel generieren möchten, klicken Sie im Menü "Actions" auf **Generate SSH Server Private Host Key** (Privaten SSH-Server-Host-Schlüssel generieren).
- Nachdem Sie diese Aktion abgeschlossen haben, müssen Sie das IMM2 erneut starten, damit Ihre Änderungen wirksam werden.

Die Registerkarte "SSH Server" ist in der folgenden Abbildung dargestellt.

Übersicht über SSL

SSL ist ein Sicherheitsprotokoll, das eine geschützte Datenübertragung bereitstellt. SSL ermöglicht Client-/Serveranwendungen eine Datenübertragung, die gegen das Ausspionieren, das Manipulieren von Daten während der Übertragung und das Fälschen von Nachrichten geschützt ist. Sie können das IMM2 so konfigurieren, dass die SSL-Unterstützung für verschiedene Verbindungsmöglichkeiten, wie z. B. den sicheren Web-Server (HTTPS), die sichere LDAP-Verbindung (LDAPS), CIM over HTTPS oder den SSH-Server, verwendet wird. Sie können die SSL-Einstellungen mit der Option "Security" (Sicherheit) auf der Registerkarte "IMM Management" (IMM-Verwaltung) anzeigen oder ändern. Außerdem haben Sie auf dieser Seite die Möglichkeit, SSL zu aktivieren oder zu inaktivieren und die für SSL erforderlichen Zertifikate zu verwalten.

Handhabung von SSL-Zertifikaten

Sie können SSL mit einem selbst signierten Zertifikat oder mit einem von einer unabhängigen Zertifizierungsstelle signierten Zertifikat verwenden. Ein selbst signiertes Zertifikat ist die einfachste Methode für die Verwendung von SSL, allerdings stellt es ein geringes Sicherheitsrisiko dar. Das Risiko besteht darin, dass der SSL-Client keine Möglichkeit hat, beim ersten Verbindungsversuch zwischen Client und Server die Identität des SSL-Servers zu prüfen. Beispielsweise besteht die Möglichkeit, dass ein anderer Anbieter die Identität des IMM2-Web-Servers vortäuschen und Daten zwischen dem tatsächlichen IMM2-Web-Server und dem Web-Browser des Benutzers abfangen könnte. Wenn das selbst signierte Zertifikat beim ersten Verbindungsaufbau zwischen dem Browser und dem IMM2 in den Zertifikatsspeicher des Browsers importiert wird, sind alle künftigen Datenübertragungen für diesen Browser sicher (vorausgesetzt, dass bei der ersten Verbindung kein Angriff erfolgt ist).

Mehr Sicherheit erhalten Sie, wenn Sie ein Zertifikat verwenden, das von einer Zertifizierungsstelle (CA) signiert ist. Klicken Sie auf **Generate a New Key and a Certificate Signing Request (CSR)** (Einen neuen Schlüssel und eine Zertifikatssignieranforderung (CSR) generieren) im Menü "Actions" (Aktionen), um ein signiertes Zertifikat zu erhalten. Senden Sie dann die Zertifikatssignieranforderung (CSR) an eine Zertifizierungsstelle (CA) und fordern Sie dort ein Endzertifikat an. Sobald Sie das Endzertifikat erhalten haben, klicken Sie auf **Import a Signed Certificate** (Ein signiertes Zertifikat importieren) im Menü "Actions", um es ins IMM2 zu importieren.

Die Aufgabe der Zertifizierungsstelle (CA) ist es, die Identität des IMM2 zu überprüfen. Ein Zertifikat enthält digitale Signaturen für die Zertifizierungsstelle (CA) und das IMM2. Wenn eine anerkannte Zertifizierungsstelle (CA) das Zertifikat ausstellt oder wenn das Zertifikat der Zertifizierungsstelle (CA) bereits in den Web-Browser importiert wurde, kann der Browser das Zertifikat validieren und den IMM2-Web-Server eindeutig identifizieren.

Das IMM2 erfordert ein Zertifikat für die Verwendung mit HTTPS-Servern, CIM over HTTPS und sicheren LDAP-Clients. Außerdem müssen für den sicheren LDAP-Client ebenfalls ein oder mehrere vertrauenswürdige Zertifikate importiert werden. Das vertrauenswürdige Zertifikat wird vom sicheren LDAP-Client verwendet, um den LDAP-Server sicher zu identifizieren. Das vertrauenswürdige Zertifikat ist das Zertifikat der Zertifizierungsstelle (CA), die das Zertifikat des LDAP-Servers signiert hat. Wenn der LDAP-Server selbst signierte Zertifikate verwendet, kann das vertrauenswürdige Zertifikat das Zertifikat des LDAP-Servers selbst sein. Sie müssen zusätzliche vertrauenswürdige Zertifikate importieren, wenn Sie in Ihrer Konfiguration mehrere LDAP-Server verwenden.

Verwaltung von SSL-Zertifikaten

Wenn Sie IMM2-Zertifikate verwalten, erhalten Sie eine Liste mit Aktionen oder eine Teilliste (wie in der folgenden Abbildung dargestellt).

Wenn derzeit ein Zertifikat installiert ist, können Sie die Aktion **Download Certificate** (Zertifikat herunterladen) im Menü "Actions" verwenden, um das derzeit installierte Zertifikat oder eine Zertifikatssignieranforderung herunterzuladen. Zertifikate, die abgeblendet sind, sind derzeit *nicht* installiert. Der sichere LDAP-Client erfordert, dass der Benutzer ein vertrauenswürdiges Zertifikat importiert. Klicken Sie auf **Import a Trusted Certificate** (Ein vertrauenswürdiges Zertifikat importieren) im Menü "Actions" (Aktionen). Klicken Sie nach Generierung einer Zertifikatssignieranforderung auf **Import a Signed Certificate** im Menü "Actions".

Wenn Sie eine der "Generate"-Aktionen ausführen, wird das Fenster "Generate New Key and Self-signed Certificate" (Neuen Schlüssel und selbst signiertes Zertifikat generieren) geöffnet (wie in der folgenden Abbildung dargestellt).

Das Fenster "Generate New Key and Self-signed Certificate" fordert Sie auf, die Pflicht- und Wahlfelder auszufüllen. Sie *müssen* die Pflichtfelder ausfüllen. Klicken Sie nach Angabe Ihrer Informationen auf **Ok**, um den Vorgang abzuschließen. Das Fenster "Certificate Generated" (Zertifikat generiert) wird geöffnet (wie in der folgenden Abbildung dargestellt).

IMM-Konfiguration wiederherstellen und ändern

Wählen Sie auf der Registerkarte "IMM Management" (IMM-Verwaltung) die Option **IMM Configuration** (IMM-Konfiguration) aus, um folgende Aktionen ausführen zu können:

- Zusammenfassung der IMM2-Konfiguration anzeigen
- IMM2-Konfiguration sichern oder wiederherstellen
- Sicherungs- oder Wiederherstellungsstatus anzeigen
- IMM2-Konfiguration auf die werkseitig vorgenommenen Standardeinstellungen zurücksetzen
- Auf den Assistenten für die IMM2-Erstkonfiguration zugreifen

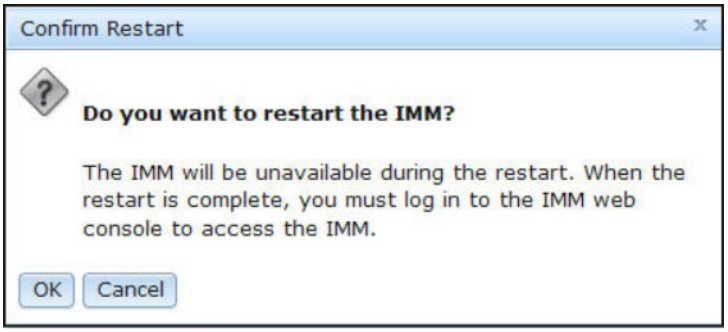
IMM2 erneut starten

Wählen Sie die Option **Restart IMM** (IMM erneut starten) auf der Registerkarte "IMM Management" (IMM-Verwaltung) aus, um das IMM2 erneut zu starten. Nur Benutzer mit Administratorberechtigung können diese Funktion ausführen. Wenn Ethernet-Verbindungen vorübergehend unterbrochen wurden, müssen Sie sich am IMM2 anmelden, um auf die IMM2-Webschnittstelle zuzugreifen.

Gehen Sie wie folgt vor, um das IMM2 erneut zu starten:

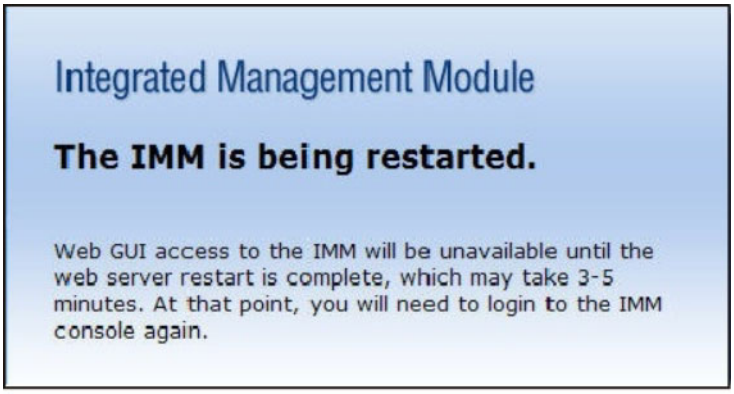
1. Melden Sie sich am IMM2 an. Weitere Informationen hierzu finden Sie im Abschnitt „Am IMM2 anmelden" auf Seite 10.
2. Klicken Sie auf die Registerkarte **IMM Management** und anschließend auf **Restart IMM**.
3. Klicken Sie auf die Schaltfläche **OK** im Fenster "Confirm Restart" (Neustart bestätigen). Das IMM2 wird erneut gestartet.

   In der folgenden Abbildung ist das Fenster "Confirm Restart" dargestellt.



Wenn Sie das IMM2 erneut starten, werden Ihre TCP/IP- oder Modemverbindungen unterbrochen.

In der folgenden Abbildung ist das Benachrichtigungsfenster dargestellt, das angezeigt wird, während das IMM2 erneut gestartet wird.



4. Melden Sie sich erneut an, um die IMM2-Schnittstelle zu verwenden (Anweisungen hierzu finden Sie im Abschnitt „Am IMM2 anmelden” auf Seite 10).

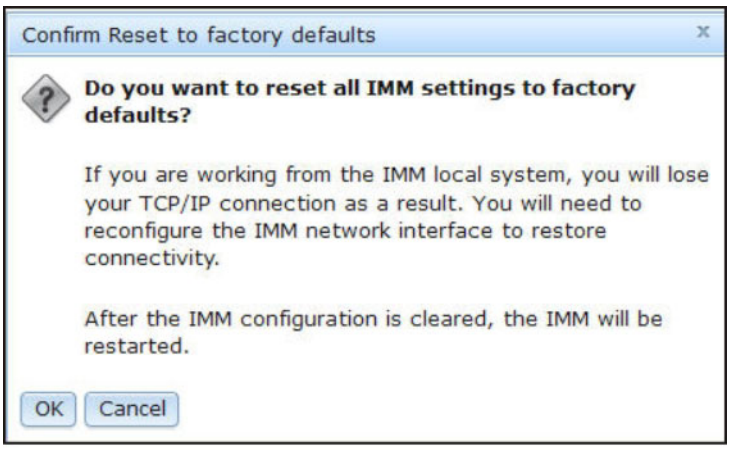
IMM2 auf die werkseitigen Voreinstellungen zurücksetzen

Wählen Sie die Option **Reset IMM to factory defaults...** (IMM auf werkseitige Voreinstellungen zurücksetzen) aus der Registerkarte "IMM Management" (IMM-Verwaltung) aus, um das IMM2 auf die werkseitigen Voreinstellungen zurückzusetzen. Nur Benutzer mit Administratorberechtigung können diese Funktion ausführen. Wenn Ethernet-Verbindungen vorübergehend unterbrochen wurden, müssen Sie sich am IMM2 anmelden, um auf die IMM2-Webschnittstelle zuzugreifen.

Achtung: Wenn Sie die Option "Reset IMM to factory defaults" verwenden, gehen alle Änderungen, die Sie am IMM2 vorgenommen haben, verloren.

Gehen Sie wie folgt vor, um die werkseitigen Voreinstellungen des IMM2 wiederherzustellen:

1. Melden Sie sich am IMM2 an. Weitere Informationen hierzu finden Sie im Abschnitt „Am IMM2 anmelden” auf Seite 10.
2. Klicken Sie auf die Registerkarte **IMM Management** und anschließend auf **IMM Reset to factory defaults...**.
3. Klicken Sie auf die Schaltfläche **OK** im Fenster "Confirm Reset to factory defaults" (Zurücksetzen auf werkseitige Voreinstellungen bestätigen) (wie in der folgenden Abbildung dargestellt).



Anmerkung: Nach Abschluss der Konfiguration des IMM2 wird dieses erneut gestartet. Wenn es sich um einen lokalen Server handelt, wird Ihre TCP/IP-Verbindung unterbrochen und Sie müssen die Netzschnittstelle rekonfigurieren, um wieder eine funktionsfähige Verbindung herzustellen.

4. Melden Sie sich erneut am IMM2 an, um die IMM2-Webschnittstelle zu verwenden (Anweisungen hierzu finden Sie im Abschnitt „Am IMM2 anmelden" auf Seite 10).
5. Rekonfigurieren Sie die Netzschnittstelle, um wieder eine funktionsfähige Verbindung herzustellen.

Aktivierungsschlüsselverwaltung

Klicken Sie auf der Registerkarte "IMM Management" (IMM-Verwaltung) auf die Option **Activation Key Management** (Aktivierungsschlüsselverwaltung), um die einzelnen Funktionen der Aktivierungsschlüssel für optionale FoD (Features on Demand) für das IMM2 und den Server zu verwalten. Weitere Informationen zur FoD-Aktivierungsschlüsselverwaltung finden Sie in Kapitel 7, „Features on Demand", auf Seite 143.

Kapitel 5. Serverstatus überwachen

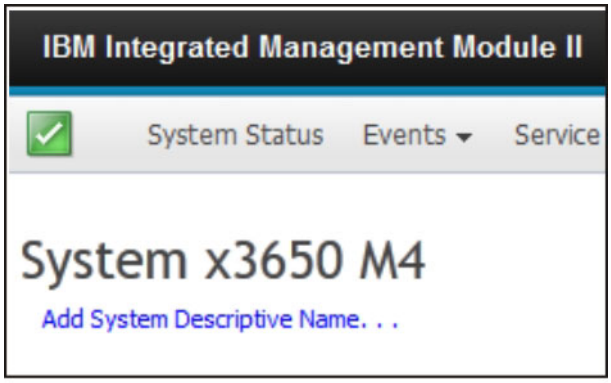
Dieses Kapitel enthält Informationen zum Anzeigen und Überwachen der Informationen zu dem Server, auf den Sie zugreifen.

Systemstatus anzeigen

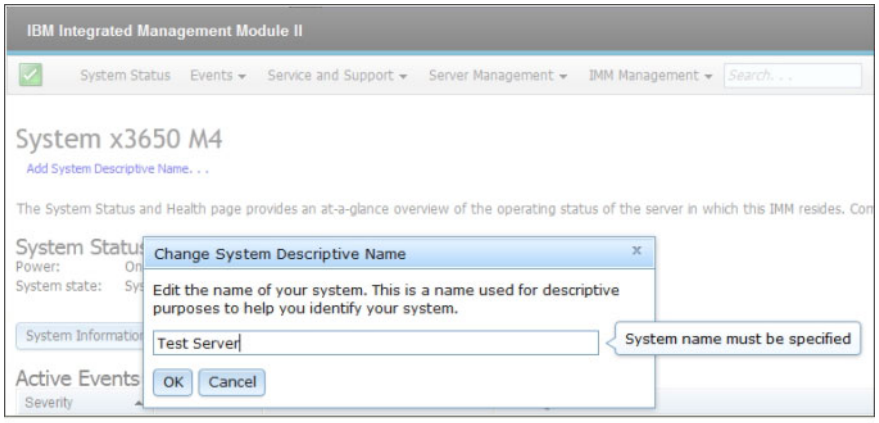
Die Seite "System Status" (Systemstatus) bietet eine Übersicht über den Betriebsstatus des IMM2-Servers. Auf dieser Seite werden Informationen zum Hardwarezustand des Servers und zu aktiven Ereignissen auf dem Server angezeigt.

Anmerkung: Wenn Sie über die Seite "System Status" auf eine andere Seite zugreifen, können Sie zur Seite "System Status" zurückkehren, indem Sie in den Menüoptionen oben auf der Seite auf **System Status** klicken.

Sie können zum IMM2 einen beschreibenden Namen hinzufügen, damit Sie die einzelnen IMM2-Module voneinander unterscheiden können. Klicken Sie unten auf den Link **Add System Descriptive Name...** (Beschreibenden Systemnamen hinzufügen) unter dem Serverproduktnamen, um einen Namen festzulegen, der dem IMM2 zugeordnet werden soll (wie in der folgenden Abbildung dargestellt).

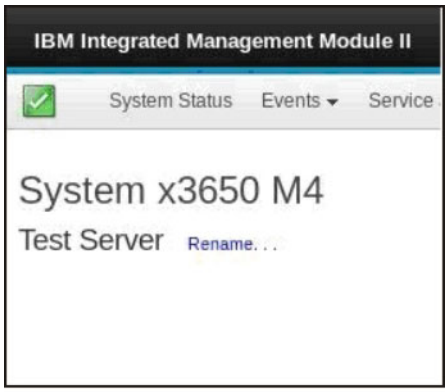


Geben Sie im Fenster "Change System Descriptive Name" (Beschreibenden Systemnamen ändern) einen Namen an, der dem IMM2 zugeordnet werden soll (wie in der folgenden Abbildung dargestellt).



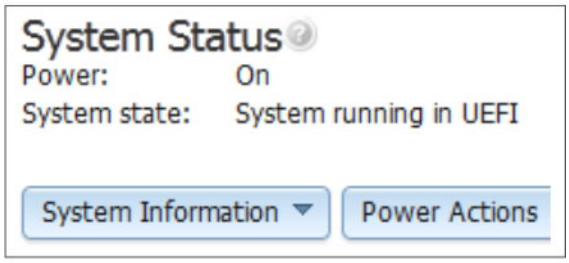
Sie können den beschreibenden Systemnamen ändern, indem Sie neben dem beschreibenden Systemnamen auf den Link **Rename...** (Umbenennen) klicken.

In der folgenden Abbildung ist der Link "Rename" dargestellt.



Auf der Seite "System Status" werden der Stromversorgungsstatus und der Betriebsstatus des Servers angezeigt. Angezeigt wird der Serverstatus zum Zeitpunkt des Öffnens der Seite "System Status".

In der folgenden Abbildung sind die Felder **Power** (Stromversorgung) und **System state** (Systemstatus) dargestellt.



Der Server kann sich in einem der Systemstatus befinden, die in der folgenden Tabelle aufgeführt sind.

Tabelle 5. Systemstatusbeschreibungen

Status	Beschreibung
System power off/State unknown (Stromversorgung des Systems ausgeschaltet/Status unbekannt)	Der Server ist ausgeschaltet.
System on/starting UEFI (System eingeschaltet/UEFI wird gestartet)	Der Server ist eingeschaltet, aber die UEFI wird noch nicht ausgeführt.
System running in UEFI (System wird in UEFI ausgeführt)	Der Server ist eingeschaltet und die UEFI wird ausgeführt.
System stopped in UEFI (System wurde in UEFI gestoppt)	Der Server ist eingeschaltet; die UEFI hat einen Fehler erkannt und ihre Ausführung wurde beendet.

Tabelle 5. Systemstatusbeschreibungen (Forts.)

Status	Beschreibung
Booting OS or in unsupported OS (Betriebssystem wird gebootet oder es wird ein nicht unterstütztes Betriebssystem gebootet)	Der Server kann sich aus einem der folgenden Gründe in diesem Status befinden: • Das Ladeprogramm des Betriebssystems wurde gestartet, aber das Betriebssystem wird nicht ausgeführt. • Die Ethernet-over-USB-Schnittstelle des IMM2 ist inaktiviert. • Das Betriebssystem hat die Treiber, die die Ethernet-over-USB-Schnittstelle unterstützen, nicht geladen.
OS booted (Betriebssystem gebootet)	Das Betriebssystem des Servers wird ausgeführt.
Suspend to RAM (Aussetzen in RAM)	Der Server wurde in den Bereitschafts- oder Ruhemodus versetzt.

Die folgenden Menüoptionen auf der Seite "System Status" bieten zusätzliche Serverinformationen und -aktionen, die auf dem Server ausgeführt werden können.

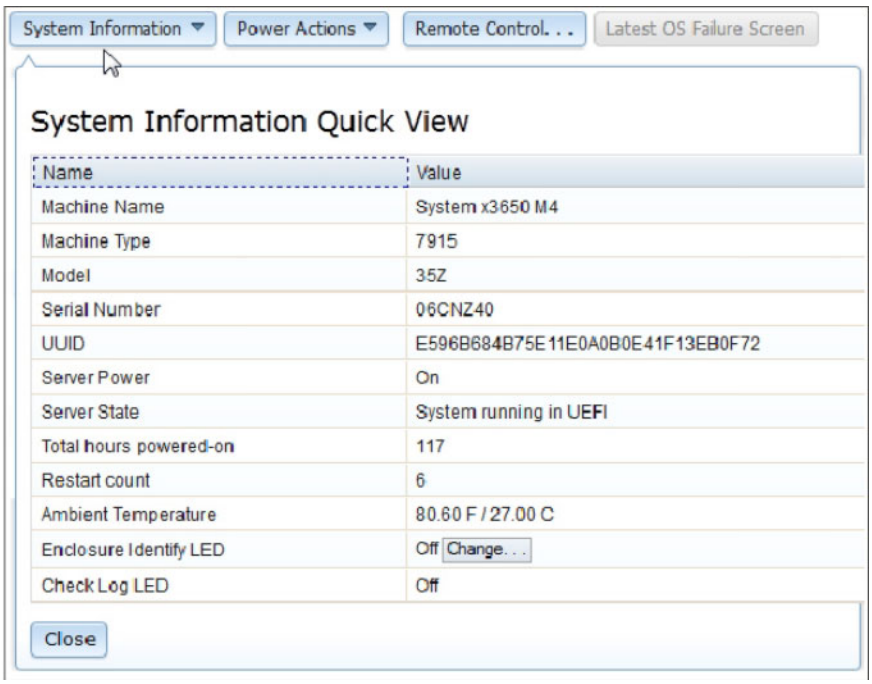
- System Information (Systeminformationen)
- Power Actions (Stromversorgungsaktionen)
- Remote Control (Fernsteuerung, weitere Informationen hierzu finden Sie unter „Remote-Presence- und Fernsteuerungsfunktionen" auf Seite 107)
- Latest OS Failure Screen (Letzte Betriebssystem-Fehleranzeige, weitere Informationen hierzu finden Sie unter „Daten der letzten Betriebssystem-Fehleranzeige erfassen" auf Seite 136)

Systeminformationen anzeigen

Das Menü "System Information" (Systeminformationen) stellt eine Zusammenfassung allgemeiner Serverinformationen bereit. Klicken Sie auf die Registerkarte **System Information** auf der Seite "System Status", um die folgenden Informationen anzuzeigen:

- Machine name (Name der Maschine)
- Machine type (Maschinentyp)
- Model (Modell)
- Serial number (Seriennummer)
- Universally Unique Identifier (UUID)
- Server power (Serverstromversorgung)
- Server state (Serverstatus)
- Total hours powered on (Gesamtbetriebsdauer in Stunden)
- Restart count (Zähler für Neustart)
- Ambient temperature (Umgebungstemperatur)
- Enclosure identity LED (Gehäuse-ID-Anzeige)
- Check log LED (Protokollprüfanzeige)

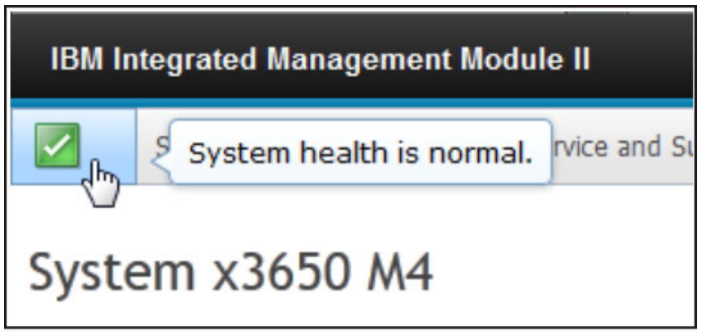
In der folgenden Abbildung ist das Fenster "System Information" dargestellt.



Serverzustand anzeigen

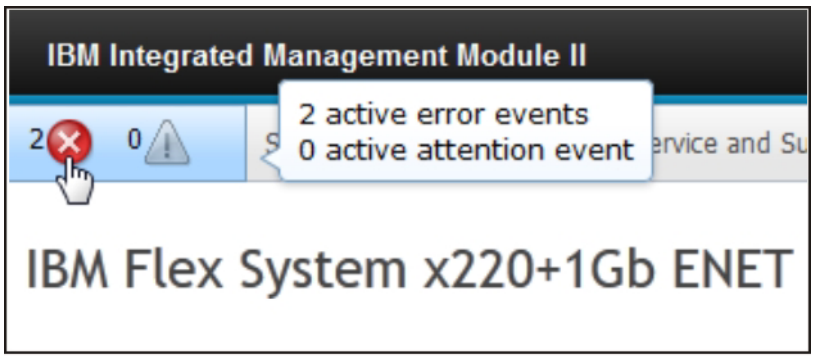
Der Serverzustand wird unter der Titelleiste in der linken oberen Ecke der Seite "System Status" (Systemstatus) angezeigt und ist durch ein Symbol designiert. Ein grünes Häkchen gibt an, dass die Server-Hardware normal funktioniert. Bewegen Sie Ihren Cursor über das grüne Häkchen, um eine Kurzmeldung zum Serverzustand zu erhalten.

In der folgenden Abbildung ist ein Beispiel für einen Server, der normal funktioniert, dargestellt.



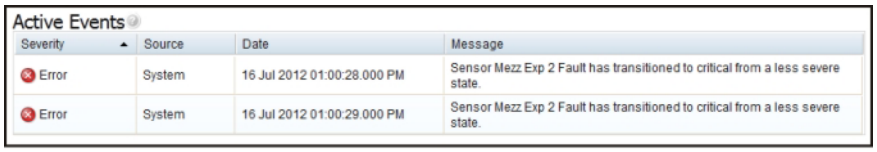
Ein gelbes Dreieck gibt an, dass eine Warnbedingung vorliegt. Ein roter Kreis gibt an, dass eine Fehlerbedingung vorliegt.

In der folgenden Abbildung ist ein Beispiel für einen Server mit aktiven Fehlerereignissen dargestellt.



Wenn ein Warnsymbol (gelbes Dreieck) oder ein Fehlersymbol (roter Kreis) angezeigt wird, klicken Sie auf das Symbol, um die entsprechenden Ereignisse im Abschnitt "Active Events" (Aktive Ereignisse) der Seite "System Status" anzuzeigen.

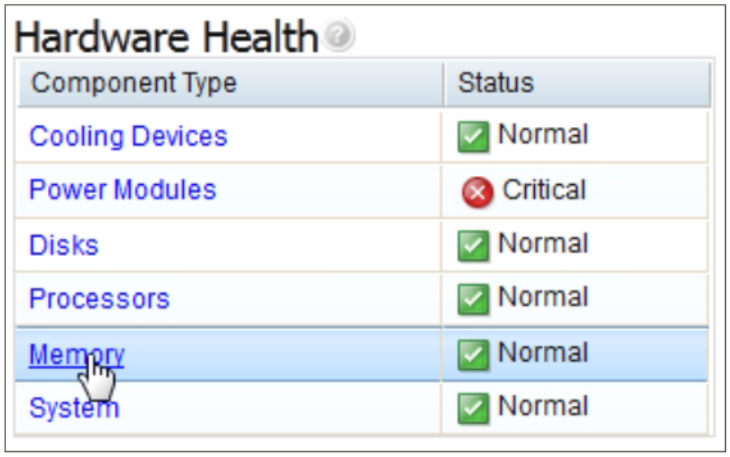
In der folgenden Abbildung ist ein Beispiel für den Abschnitt "Active Events" mit Fehlerbedingungen dargestellt.



Hardwarezustand anzeigen

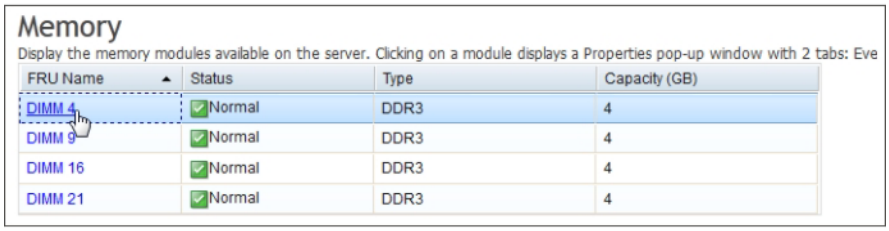
Im Abschnitt "Hardware Health" (Hardwarezustand) der Seite "System Status" (Systemstatus) sind die Server-Hardware-Komponenten aufgelistet. Hier wird der Allgemeinzustand jeder Komponente, die durch das IMM2 überwacht wird, angezeigt. Der angezeigte Allgemeinzustand einer Komponente entspricht möglicherweise dem kritischsten Status aller einzelnen Komponenten eines Komponententyps. Beispiel: Auf einem Server können mehrere Stromversorgungsmodule installiert sein und bis auf ein Stromversorgungsmodul funktionieren alle normal. Aufgrund des Stromversorgungsmoduls, das nicht fehlerfrei funktioniert, wird der Status der Komponente "Power Modules" (Stromversorgungsmodule) als kritisch angezeigt.

In der folgenden Abbildung ist der Abschnitt "Hardware Health" der Seite "System Status" dargestellt.



Jede Komponente wird als Link angezeigt, auf den Sie klicken können, um genauere Informationen zu erhalten. Wenn Sie einen Komponententyp (Component Type) auswählen, wird eine Tabelle angezeigt, in der alle Komponenten dieses Komponententyps aufgelistet sind.

In der folgenden Abbildung sind Komponenten für den Komponententyp "Memory" (Speicher) dargestellt.

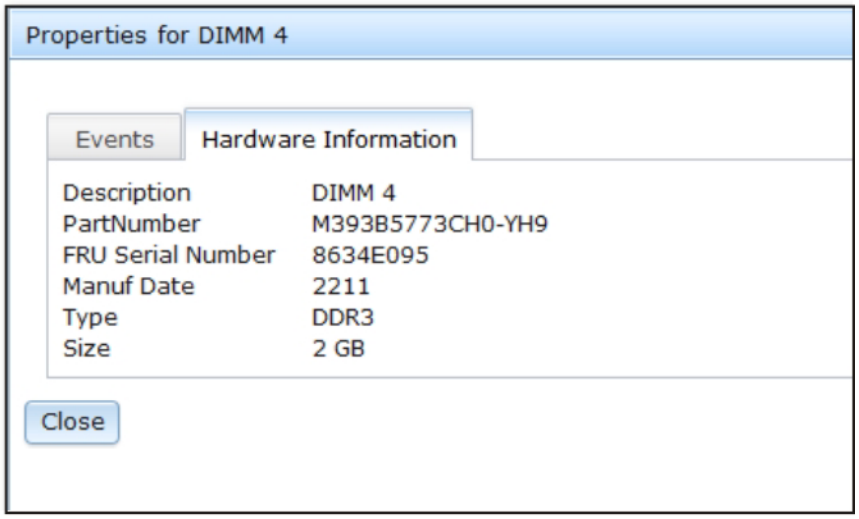


Sie können auf einen einzelnen FRU-Link (Field Replaceable Unit) in der Tabelle klicken, um weitere Informationen zu dieser Komponente zu erhalten. Alle aktiven Ereignisse für die Komponente werden auf der Registerkarte "Events" (Ereignisse) angezeigt.

In der folgenden Abbildung ist die Registerkarte "Events" für DIMM 4 dargestellt.

Falls vorhanden, sind für die Komponente auf der Registerkarte "Hardware Information" (Hardwareinformationen) möglicherweise weitere Informationen angegeben.

In der folgenden Abbildung ist die Registerkarte "Hardware Information" für DIMM 4 dargestellt.



Kapitel 6. IMM2-Tasks ausführen

Verwenden Sie die Informationen in diesem Abschnitt und in Kapitel 3, „Übersicht über die IMM2-Webbenutzerschnittstelle”, auf Seite 17, um die folgenden Tasks zur Steuerung des IMM2 auszuführen.

Auf der Registerkarte "System Status" (Systemstatus) können Sie folgende Tasks ausführen:

- Serverzustand anzeigen
- Serverinformationen anzeigen, z. B. Servername, Servertyp und Seriennummer
- Serverstromversorgung und Neustartaktivitäten anzeigen
- Stromversorgungsstatus des Servers über Fernzugriff steuern
- Serverkonsole über Fernzugriff verwenden
- Eine Platte oder ein Plattenimage über Fernzugriff an den Server anhängen
- Aktive Ereignisse anzeigen
- Hardwarezustand der Serverkomponenten anzeigen

Anmerkung: Die Seite "System Status" wird nach dem Anmelden am IMM2 angezeigt. Auf dieser Seite sind allgemeine Informationen und Aktionen zusammengestellt.

Auf der Registerkarte "Events" (Ereignisse) können Sie folgende Tasks ausführen:

- Ereignisprotokollverlauf verwalten
- Ereignisempfänger für E-Mail-Benachrichtigungen verwalten
- Ereignisempfänger für syslog-Benachrichtigungen verwalten

Auf der Registerkarte "Services and Support" (Services und Support) können Sie folgende Tasks ausführen:

- Servicedaten für Ihren Server manuell abrufen

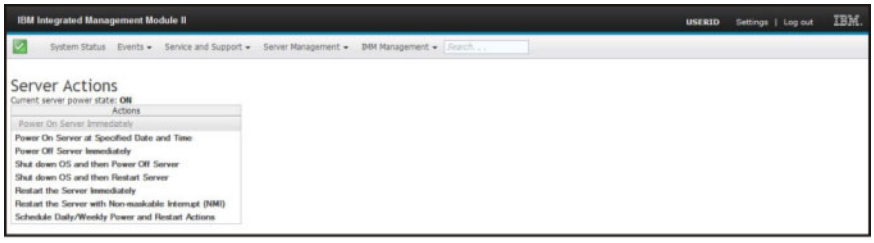
Auf der Registerkarte "Server Management" (Serververwaltung) können Sie Optionen zum Ausführen folgender Tasks auswählen:

- Mit der Option "Server Firmware" (Server-Firmware) können Sie Firmwareversionen der Serverkomponenten anzeigen und aktualisieren.
- Mit der Option "Remote Control" (Fernsteuerung) können Sie Ihre Serverkonsole über Fernzugriff anzeigen und mit ihr interagieren:
  - Stromversorgungsstatus des Servers über Fernzugriff steuern
  - Serverkonsole über Fernzugriff verwenden
  - CD-Laufwerk, DVD-Laufwerk, Diskettenlaufwerk, USB-Flashlaufwerk oder Plattenimage über Fernzugriff Ihrem Server zuordnen
- Mit der Option "Server Properties" (Servereigenschaften) können Sie Parameter festlegen, um das Ermitteln des Servers zu unterstützen.
- Mit der Option "Server Power Actions" (Serverstromversorgungsaktionen) können Sie den Server einschalten, ausschalten und erneut starten.
- Mit der Option "Disks" (Festplatten) können Sie die im Server installierten Festplattenlaufwerke und ihnen zugeordnete Ereignisse anzeigen.
- Mit der Option "Memory" (Speicher) können Sie Informationen zu im Server installierten Speichermodulen anzeigen.

- Mit der Option "Processor" (Prozessor) können Sie Informationen zu im Server installierten Mikroprozessoren anzeigen.
- Mit der Option "Server Timeouts" (Serverzeitlimits) können Sie Zeitlimits festlegen, damit der Server während einer Firmwareaktualisierung oder beim Einschalten des Servers nicht unbegrenzt blockiert wird.
- Mit der Option "PXE Network Boot" (PXE-Netzboot) können Sie Bootversuche der Server-Ausführungsumgebung vor dem Start einrichten.
- Mit der Option "Latest OS Failure Screen" (Letzte Betriebssystem-Fehleranzeige) können Sie die Daten aus der Fehleranzeige des Betriebssystems erfassen und speichern.
- Mit der Option "Power Management" können Sie den Systemstromverbrauch und die Netzteilkapazität anzeigen sowie Parameter für den Systemstromverbrauch festlegen.

Stromversorgungsstatus des Servers steuern

Die Option "Power Actions" (Stromversorgungsaktionen) enthält eine Liste von Aktionen, mit der Sie die Serverstromversorgung steuern können (wie in der folgenden Abbildung dargestellt). Sie können den Server sofort oder zu einem geplanten Zeitpunkt einschalten. Sie können auch das Betriebssystem herunterfahren und anschließend erneut starten.



Gehen Sie wie folgt vor, um Aktionen zur Stromversorgung und zum Neustart des Servers auszuführen:

1. Führen Sie einen der folgenden Schritte aus, um auf das Menü "Power Actions" zuzugreifen:
   - Klicken Sie auf der Seite "System Status" auf die Registerkarte **Power Actions**.
   - Klicken Sie auf der Registerkarte "Server Management" auf **Server Power Actions**.
2. Wählen Sie die Serveraktion aus der Menüliste "Actions" aus.

Die folgende Tabelle enthält eine Beschreibung der Stromversorgungs- und Neustartaktionen, die auf dem Server ausgeführt werden können.

Tabelle 6. Stromversorgungsaktionen und Beschreibungen

Stromversorgungsaktion	Beschreibung
Power on server immediately (Server sofort einschalten)	Wählen Sie dieses Aktionselement aus, um den Server einzuschalten und das Betriebssystem zu booten.

Tabelle 6. Stromversorgungsaktionen und Beschreibungen (Forts.)

Stromversorgungsaktion	Beschreibung
Power on server at specified date and time (Server an einem bestimmten Datum und zu einer bestimmten Uhrzeit einschalten)	Wählen Sie dieses Aktionselement aus, um einen Zeitplan für den Server zu erstellen, sodass er automatisch an einem bestimmten Datum, zu einer bestimmten Uhrzeit eingeschaltet wird.
Power off server immediately (Server sofort ausschalten)	Wählen Sie dieses Aktionselement aus, um den Server auszuschalten, ohne das Betriebssystem herunterzufahren.
Shut down operating system and then power off server (Betriebssystem herunterfahren und dann Server ausschalten) [1]	Wählen Sie dieses Aktionselement aus, um das Betriebssystem herunterzufahren und den Server anschließend auszuschalten.
Shut down OS and then restart server (Betriebssystem herunterfahren und Server anschließend erneut starten) [1]	Wählen Sie dieses Aktionselement aus, um einen Warmstart des Betriebssystems durchzuführen.
Restart the server immediately (Server sofort erneut starten)	Wählen Sie dieses Aktionselement aus, um den Server sofort aus- und anschließend wieder einzuschalten, ohne das Betriebssystem herunterzufahren.
Restart the server with non-maskable interrupt (NMI) (Server mit NMI erneut starten)	Wählen Sie dieses Aktionselement aus, um ein NMI für ein blockiertes System zu erzwingen. Die Auswahl dieses Aktionselements ermöglicht es dem Plattformbetriebssystem, einen Hauptspeicherauszug zu erstellen, der für die Fehlerbehebung des blockierten Systems verwendet werden kann. Die IMM2-Firmware verwendet den automatischen Warmstart der NMI-Einstellung von "UEFI F1" im Menü "Setup", um zu bestimmen, ob ein Warmstart nach dem NMI erforderlich ist.
Schedule daily/weekly power and restart actions (Tägliche/Wöchentliche Aktionen zum Einschalten und erneuten Starten planen)	Wählen Sie dieses Aktionselement aus, um tägliche oder wöchentliche Aktionen zum Einschalten und zum erneuten Starten für den Server zu planen.

1. Falls sich das Betriebssystem im Bildschirmschonermodus oder im gesperrten Modus befindet, wenn die Anforderung zum Herunterfahren gesendet wird, kann das IMM2 möglicherweise keinen ordnungsgemäßen Systemabschluss einleiten. Das IMM2 führt dann einen Kaltstart oder einen Systemabschluss nach Ablaufen des Ausschaltverzögerungsintervalls durch, während das Betriebssystem möglicherweise noch ausgeführt wird.

Remote-Presence- und Fernsteuerungsfunktionen

Sie können die IMM2-Fernsteuerungsfunktion oder die Remote-Presence-Funktion in der IMM2-Webschnittstelle verwenden, um die Serverkonsole anzuzeigen und mit ihr zu interagieren. Sie können dem Server ein CD- oder DVD-Laufwerk, ein Diskettenlaufwerk, ein USB-Flashlaufwerk oder ein Plattenimage zuordnen, das sich auf Ihrem Computer befindet. Die Remote-Presence-Funktion ist mit den IMM2 Premium-Funktionen verfügbar und kann nur über die IMM2-Webschnittstelle verwendet werden. Sie müssen sich am IMM2 mit einer Benutzer-ID anmelden, die über Administratorzugriff verfügt, um die Fernsteuerungsfunktionen verwenden zu können. Weitere Informationen zum Durchführen eines Upgrades von IMM2 Basic oder IMM2 Standard auf IMM2 Premium finden Sie im Abschnitt

„Upgrade für IMM2 durchführen" auf Seite 4. Informationen dazu, welche IMM2-Version auf Ihrem Server installiert ist, finden Sie in der mit dem Server gelieferten Dokumentation.

Verwenden Sie die Fernsteuerungsfunktionen, um folgende Aktionen auszuführen:

- Zeigen Sie, unabhängig vom Serverzustand, über Fernzugriff Videos mit einer Grafikauflösung von bis zu 1600 x 1200 bei 75 Hz an.
- Greifen Sie mithilfe der Tastatur und der Maus eines fernen Clients über Fernzugriff auf den Server zu.
- Ordnen Sie das CD- oder DVD-Laufwerk, das Diskettenlaufwerk und das USB-Flashlaufwerk einem fernen Client zu. Ordnen Sie ISO- und Diskettenimagedateien als virtuelle Laufwerke zu, die zur Verwendung durch den Server verfügbar sind.
- Laden Sie ein Diskettenimage in den IMM2-Speicher hoch und ordnen Sie es dem Server als virtuelles Laufwerk zu.

IMM2-Firmware und Java- oder ActiveX-Applet aktualisieren

Dieser Abschnitt enthält Informationen zum Aktualisieren der Firmware sowie des Java- und des ActiveX-Applets.

Wichtig: Das IMM2 verwendet ein Java-Applet oder ein ActiveX-Applet, um die Remote-Presence-Funktion auszuführen. Wenn das IMM2 auf die neueste Firmwareversion aktualisiert wird, werden auch das Java-Applet und das ActiveX-Applet auf die neueste Version aktualisiert. Java stellt zuvor verwendete Applets standardmäßig in den örtlichen Zwischenspeicher. Nach einer Flashaktualisierung der IMM2-Firmware ist das vom Server verwendete Java-Applet möglicherweise nicht auf dem neuesten Stand.

Um diesen Fehler zu beheben, inaktivieren Sie das Zwischenspeichern. Welche Methode verwendet wird, hängt von der Plattform und von der Java-Version ab. Die folgenden Schritte gelten für Oracle Java 1.5 unter Windows:

1. Klicken Sie auf **Start → Settings (Einstellungen) → Control Panel (Steuerkonsole)**.
2. Klicken Sie zweimal auf **Java Plug-in 1.5**. Das Fenster "Control Panel" des Java-Plug-in wird geöffnet.
3. Klicken Sie auf die Registerkarte **Cache** (Zwischenspeicher).
4. Wählen Sie eine der folgenden Optionen:
   - Wählen Sie das Kontrollkästchen **Enable Caching** (Zwischenspeichern aktivieren) ab, damit die Java-Zwischenspeicherung immer inaktiviert ist.
   - Klicken Sie auf **Clear Caching** (Zwischenspeichern abwählen). Wenn Sie diese Option auswählen, müssen Sie nach jeder IMM2-Firmwareaktualisierung auf **Clear Caching** klicken.

Weitere Informationen zur Aktualisierung von IMM2-Firmware finden Sie im Abschnitt „Server-Firmware aktualisieren" auf Seite 122.

Remote-Presence-Funktion aktivieren

Die Remote-Presence-Funktion des IMM2 ist nur in IMM2 Premium verfügbar. Weitere Informationen zum Durchführen eines Upgrades von IMM Standard auf IMM Premium finden Sie im Abschnitt „Upgrade für IMM2 durchführen” auf Seite 4.

Nachdem Sie den Aktivierungsschlüssel für das IMM2 Premium-Upgrade gekauft und erhalten haben, installieren Sie ihn. Lesen Sie dazu „Aktivierungsschlüssel installieren” auf Seite 143.

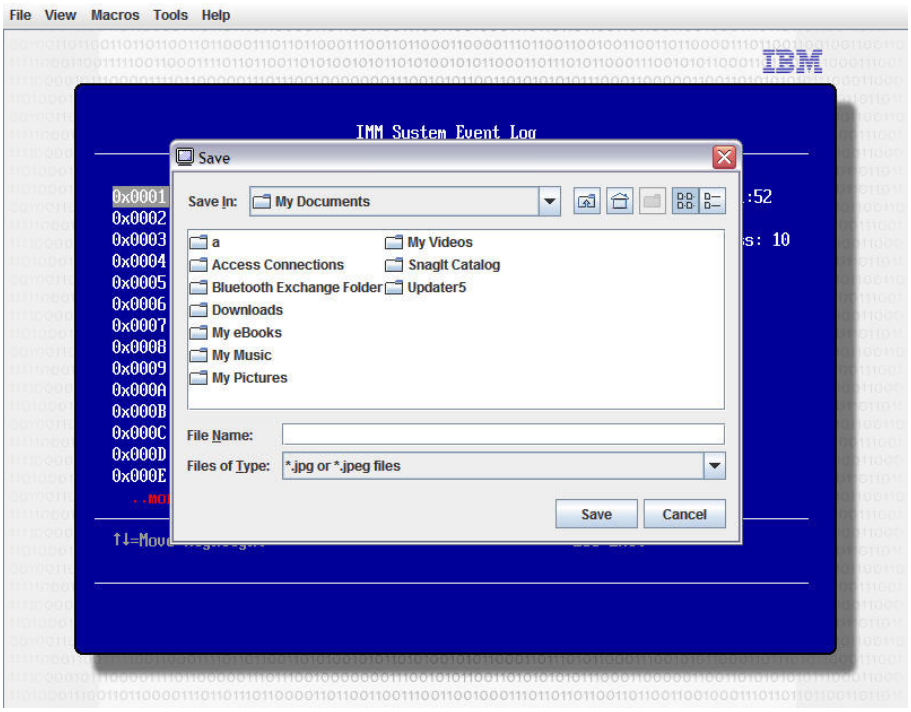
Anzeigenerfassung per Fernsteuerung

Die Anzeigenerfassungsfunktion im Fenster Video Viewer erfasst die Inhalte des Serverbildschirms. Gehen Sie wie folgt vor, um eine Bildschirmanzeige zu erfassen und zu speichern:

1. Klicken Sie im Fenster Video Viewer auf **File** (Datei).
2. Wählen Sie aus dem Menü **Capture to File** (in Datei speichern) aus.
3. Wenn Sie dazu aufgefordert werden, geben Sie einen Namen für die Bilddatei ein und speichern Sie sie an dem Ort, den Sie auf dem lokalen Client auswählen.

   Anmerkung: Der Java-Client speichert das Anzeigenerfassungsbild als eine Datei vom Typ JPG. Der ActiveX-Client speichert das Anzeigenerfassungsbild als eine Datei vom Typ BMP.

   In der folgenden Abbildung ist das Fenster dargestellt, in dem Sie den Standort für die Bilddatei angeben und den Namen der Bilddatei eingeben können.



Modi der Fernsteuerung im Video Viewer

Um die Ansicht im Fenster "Video Viewer" zu ändern, klicken Sie auf **View** (Ansicht). Die folgenden Menüoptionen sind verfügbar:

Hide Status Bar (Statusleiste ausblenden)
Blendet die Statusleiste aus, die den Zustand der Tasten für den Großschreibmodus, die numerische Verriegelung und das Blättern anzeigt. Diese Option ist nur bei eingeblendeter Statusleiste verfügbar.

Show Status Bar (Statusleiste einblenden)
Blendet die Statusleiste ein, die den Zustand der Tasten für den Großschreibmodus, die numerische Verriegelung und das Blättern anzeigt. Diese Option ist nur bei ausgeblendeter Statusleiste verfügbar.

Refresh (Aktualisieren)
Der Video Viewer aktualisiert die Bildschirmanzeige mit den Videodaten vom Server.

Full Screen (Gesamtanzeige)
Der Video Viewer verwendet den gesamten Client-Desktop für die Videoanzeige. Diese Option ist nur dann verfügbar, wenn der Video Viewer nicht im Gesamtanzeigemodus ausgeführt wird.

Windowed (Fenstermodus)
Der Video Viewer wechselt vom Gesamtanzeigemodus in den Fenstermodus. Diese Option ist nur dann verfügbar, während der Video Viewer im Gesamtanzeigemodus ausgeführt wird.

Fit (Eingepasst)
Die Größe des Video Viewers wird so verändert, dass die Zielarbeitsoberfläche vollständig und ohne einen zusätzlichen Rand oder Schiebeleisten angezeigt wird. Der Client-Desktop muss groß genug sein, um das größenangepasste Fenster anzuzeigen.

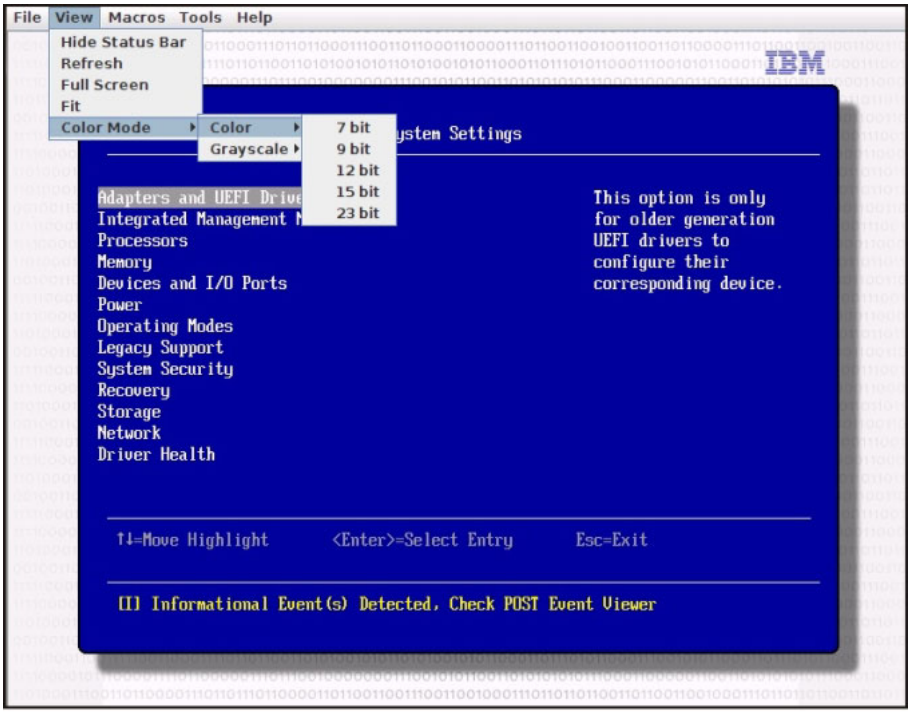
Fernsteuerung des Videofarbmodus

Wenn Ihre Verbindung zum fernen Server eine begrenzte Bandbreite hat, können Sie den Bandbreitenbedarf des Video Viewer verringern, indem Sie die Farbeinstellungen im Video Viewer-Fenster anpassen.

Anmerkung: Das IMM2 bietet eine Menüoption, die es ermöglicht, die Farbtiefe anzupassen, um bei geringer Bandbreite die übertragene Datenmenge zu verringern. Diese Menüoption ersetzt den Bandbreiten-Schieberegler der Schnittstelle beim Remote Supervisor Adapter II.

Gehen Sie wie folgt vor, um den Videofarbmodus zu ändern:

1. Klicken Sie im Fenster Video Viewer auf **View** (Ansicht).
2. Klicken Sie auf **Color Mode** (Farbmodus). Es sind zwei Farbmodusoptionen verfügbar (wie in der folgenden Abbildung dargestellt):
   - Farbe: 7-, 9-, 12-, 15- und 23-Bit
   - Grauskala: 16, 32, 64 und 128 Grautöne



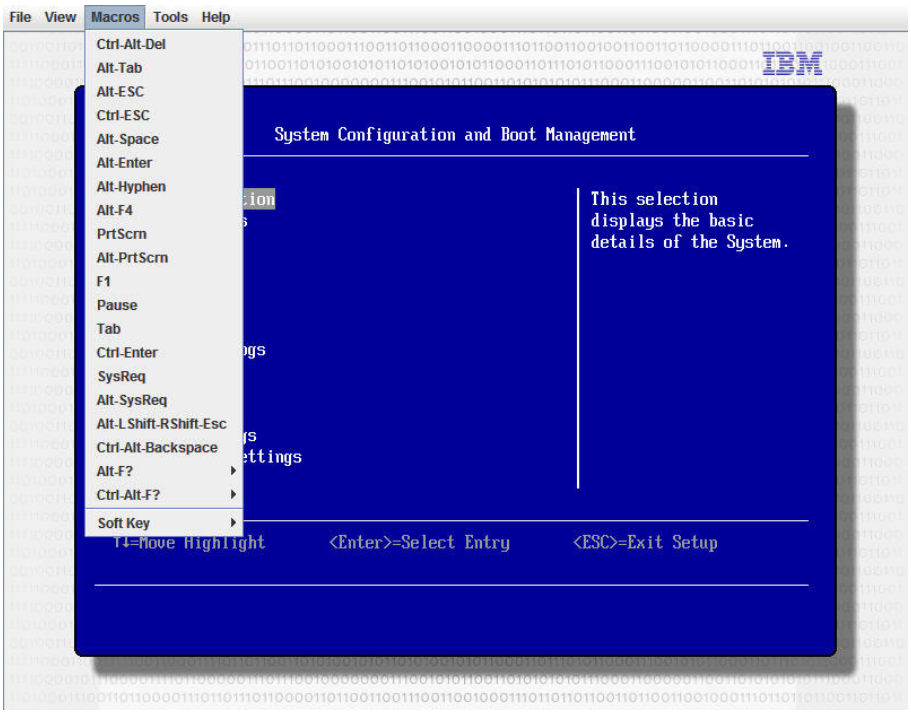
3. Wählen Sie die Einstellung für die Farbe oder die Graustufe aus.

Tastaturunterstützung per Fernsteuerung

Das Betriebssystem auf dem Clientserver, den Sie verwenden, fängt bestimmte Tastenkombinationen ab, etwa "Strg + Alt + Entf" in Microsoft Windows, anstatt sie an den Blade-Server zu übertragen. Andere Tasten wie etwa F1 verursachen möglicherweise gleichzeitig eine Aktion auf dem Server und auf Ihrem Computer.

Gehen Sie wie folgt vor, um Tastenkombinationen zu verwenden, die den fernen Server und nicht den lokalen Client beeinflussen:

1. Klicken Sie im Fenster Video Viewer auf **Macros**.
2. Wählen Sie eine der vordefinierten Tastenkombinationen aus dem Menü oder wählen Sie **Soft Key** (Programmfunktionssymbol) aus, um eine benutzerdefinierte Tastenkombination auszuwählen oder hinzuzufügen (wie in der folgenden Abbildung dargestellt).



Verwenden Sie die Menüoption **Macros** von Video Viewer, um spezielle Schaltflächen zu erstellen oder zu bearbeiten, mit deren Hilfe Tastatureingaben an den Server gesendet werden können.

Gehen Sie wie folgt vor, um spezielle Schaltflächen zu erstellen und zu bearbeiten:

1. Klicken Sie im Fenster "Video Viewer" auf **Macros**.
2. Wählen Sie **Soft Key** und dann **Add** (Hinzufügen) aus. Ein neues Fenster wird geöffnet.
3. Klicken Sie auf **New**, um eine neue Tastenkombination hinzuzufügen, oder wählen Sie eine Tastenkombination und klicken Sie auf **Delete** (Löschen), um eine bestehende Tastenkombination zu entfernen.
4. Wenn Sie eine neue Kombination hinzufügen, geben Sie die Tastenkombination ein, die Sie in dem Fenster definieren möchten, das sich öffnet, nachdem **New** ausgewählt wurde, und klicken Sie dann auf **OK**.
5. Wenn Sie damit fertig sind, Tastenkombinationen zu definieren oder zu entfernen, klicken Sie auf **OK**.

Unterstützung für internationale Tastatur

Der Video Viewer verwendet plattformspezifischen nativen Code, um Tastaturereignisse abzufangen und direkt auf die Daten zur physischen Taste zuzugreifen. Der Client erkennt die Ereignisse der physischen Tasten und übergibt sie an den Server. Der Server erkennt dieselbe physische Tastatureingabe, die der Client festgestellt hat, und unterstützt alle Standardtastaturbelegungen. Die einzige Einschränkung dabei ist, dass das Ziel und der Client dieselbe Tastaturbelegung verwenden. Wenn ein ferner Benutzer eine andere Tastaturbelegung als der Server verwendet, kann der Benutzer die Serverbelegung umschalten, während der ferne Zugriff erfolgt, und anschließend wieder zurückschalten.

Tastaturdurchgriffsmodus

Der Tastaturdurchgriffsmodus inaktiviert die Behandlung der meisten Sondertastenkombinationen auf dem Client, sodass sie direkt an den Server übergeben werden können. Dies bietet eine Alternative zur Verwendung der Makros.

Einige Betriebssysteme definieren bestimmte Tastatureingaben als außerhalb der Steuerung einer Anwendung, sodass das Verhalten des Durchgriffsmechanismus unabhängig vom Server ausgeführt wird. Beispiel: In einer Linux-Sitzung bewirkt die Tastenkombination Strg+Alt+F2 einen Wechsel zur virtuellen Konsole 2. Es gibt keinen Mechanismus zum Abfangen dieser Tastenfolge und daher auch keine Möglichkeit für den Client, diese Tastatureingaben direkt an das Ziel zu übergeben. Die einzige Option in diesem Fall ist die Verwendung der Tastaturmakros, die für diese Zweck definiert wurden.

Gehen Sie wie folgt vor, um den Tastaturdurchgriffsmodus zu aktivieren oder zu inaktivieren:

1. Klicken Sie im Fenster "Video Viewer" auf **Tools**.
2. Wählen Sie aus dem Menü **Session Options** (Sitzungsoptionen) aus.
3. Wenn sich das Fenster "Session Options" öffnet, klicken Sie auf die Registerkarte **General** (Allgemein).
4. Wählen Sie das Kontrollkästchen **Pass all keystrokes to target** (Alle Tastatureingaben an Ziel übergeben) aus, um den Tastaturdurchgriffsmodus zu aktivieren oder zu inaktivieren.
5. Klicken Sie auf **OK**, um die Auswahl zu speichern.

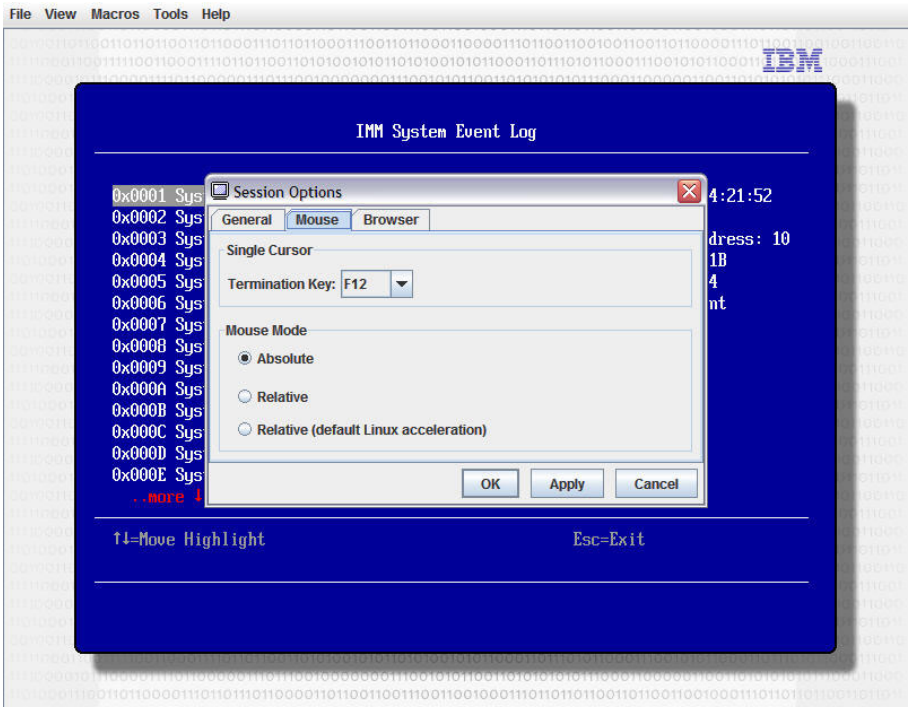
Mausunterstützung per Fernsteuerung

Im Fenster "Video Viewer" haben Sie verschiedene Möglichkeiten der Maussteuerung, einschließlich absolute Maussteuerung, relative Maussteuerung und Einzelcursormodus.

Absolute und relative Maussteuerung

Gehen Sie wie folgt vor, um auf die absoluten und relativen Optionen zum Steuern der Maus zuzugreifen:

1. Klicken Sie im Fenster "Remote Control" (Fernsteuerung) auf **Tools**.
2. Wählen Sie aus dem Menü **Session Options** (Sitzungsoptionen) aus.
3. Wenn sich das Fenster "Session Options" öffnet, klicken Sie auf die Registerkarte **Mouse** (Maus) (wie in der folgenden Abbildung dargestellt).



4. Wählen Sie einen der folgenden Mausmodi aus:
   - **Absolute:** (Absolut)

     Der Client sendet Mauspositionsnachrichten an den Server, die immer relativ zum Ursprung (oberer linker Bereich) des Anzeigebereichs sind.
   - **Relative:** (Relativ)

     Der Client sendet die Mausposition als relative Position im Hinblick auf die vorherige Position.
   - **Relative (default Linux acceleration):** (Relativ (Linux-Standardbeschleunigung))

     Der Client wendet einen Beschleunigungsfaktor an, um die Maus besser auf Linux-Ziele abzustimmen. Die Beschleunigungseinstellungen wurden ausgewählt, um die Kompatibilität mit Linux-Distributionen zu maximieren.

Einzelcursormodus

Manche Betriebssysteme richten die lokalen und fernen Cursor nicht aneinander aus, was zu Abweichungen zwischen den lokalen und fernen Mauszeigern führt. Beim Einzelcursormodus wird der lokale Client ausgeblendet, während die Maus sich innerhalb des Video Viewer-Fensters befindet. Bei aktiviertem Einzelcursormodus sehen Sie nur den fernen Cursor. Um den Einzelcursormodus zu aktivieren, klicken Sie im Video Viewer-Fenster auf **Tools > Single Cursor** (Tools, Einzelcursor).

Anmerkung: Wenn der Video Viewer im Einzelcursormodus läuft, können Sie die Maus nicht verwenden, um in ein anderes Fenster zu wechseln oder außerhalb des KVM-Clientfensters auf etwas zu klicken, da es keinen lokalen Cursor gibt.

Drücken Sie zum Inaktivieren des Einzelcursormodus die dafür festgelegte Beendigungstaste. Klicken Sie zum Anzeigen der festgelegten Beendigungstaste (Termination Key) oder um eine andere Beendigungstaste festzulegen auf **Tools > Session Options > Mouse** (Tools, Sitzungsoptionen, Maus).

Fernsteuerung der Stromversorgung

Vom Fenster "Video Viewer" können Sie Serverbefehle für Stromversorgung und Neustart versenden, ohne zum Web-Browser zurückzukehren. Gehen Sie wie folgt vor, um die Stromversorgung des Servers über den Video Viewer zu steuern:

1. Klicken Sie im Fenster "Video Viewer" auf **Tools**.
2. Klicken Sie auf **Power**. Wählen Sie einen der folgenden Befehle aus:

   On Schaltet die Stromversorgung des Servers ein.

   Off Schaltet die Stromversorgung des Servers aus.

   Reboot (Warmstart)
   Startet den Server erneut.

   Cycle (Aus- und wieder einschalten)
   Schaltet die Stromversorgung des Servers erst aus, dann wieder ein.

Leistungsstatistiken anzeigen

Um die Leistungsstatistik des Video Viewers im Fenster "Video Viewer" anzuzeigen, klicken Sie auf **Tools** und dann auf **Stats**. Die folgenden Informationen werden angezeigt:

Frame Rate (Vollbildrate)
Ein gleitender Durchschnittswert der Anzahl an Bildern, die pro Sekunde durch den Client entschlüsselt wird.

Bandwidth (Bandbreite)
Ein gleitender Durchschnittswert der Gesamtzahl an Kilobytes pro Sekunde, die der Client empfängt.

Compression (Komprimierung)
Ein gleitender Durchschnittswert der Bandbreitenverkleinerung aufgrund von Videokomprimierung. Dieser Wert wird häufig mit "100.0%" angegeben. Er wird auf ein Zehntel Prozent gerundet.

Packet Rate (Paketübertragungsrate)
Ein gleitender Durchschnittswert der Anzahl an Videopaketen, die pro Sekunde empfangen wird.

Remote Desktop Protocol starten

Wenn der Windows-basierte RDP-Client (Remote Desktop Protocol) installiert ist, können Sie einen RDP-Client anstelle des KVM-Clients verwenden. Der ferne Server muss so konfiguriert sein, dass er RDP-Verbindungen empfangen kann.

Beschreibung der Funktion "Anklopfen"

Wenn alle verfügbaren Fernsteuerungssitzungen besetzt sind (eine Option im Einzelbenutzermodus oder vier Optionen im Mehrbenutzermodus), hat ein anderer Webbenutzer die Möglichkeit, eine Anforderung zum Trennen der Verbindung an einen Fernsteuerungsbenutzer zu senden, der die Funktion "Anklopfen" aktiviert hat, falls dieser Benutzer nicht bereits eine Anforderung zum Trennen der Verbindung von einem anderen Webbenutzer erhalten hat.

Wenn der Fernsteuerungsbenutzer, der die Funktion "Anklopfen" aktiviert hat, die Anforderung akzeptiert oder nicht innerhalb des Zeitlimits auf die Anforderung antwortet, wird die Fernsteuerungssitzung beendet und für den Webbenutzer reserviert, der diese Anforderung gesendet hat.

Wenn der Webbenutzer, der die Anforderung zum Trennen der Verbindung gesendet hat, nicht innerhalb von fünf Minuten eine Java- oder ActiveX-Fernsteuerungssitzung mit der reservierten Fernsteuerungssitzung startet, erlischt die Reservierung der Fernsteuerungssitzung für diesen Webbenutzer.

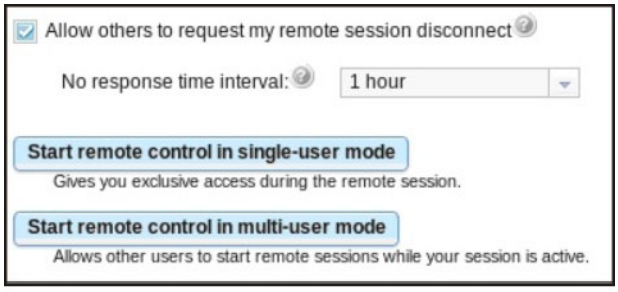
Gehen Sie wie folgt vor, um die Funktion "Anklopfen" zu aktivieren:

1. Öffnen Sie die Seite "Remote Control" (Fernsteuerung) über eine der folgenden Menüoptionen:
   - Klicken Sie auf der Registerkarte "Server Management" auf **Remote Control**.
   - Klicken Sie auf der Seite "System Status" auf **Remote Control...**.
2. Wählen Sie das Kontrollkästchen **Allow others to request my remote session disconnect** (Anforderungen zum Trennen der Verbindung meiner fernen Sitzung durch andere Benutzer zulassen) aus.

   Anmerkung: Für die Verwendung der Fernsteuerungsfunktion muss mindestens ein weiterer Benutzer vorhanden sein, der das Kontrollkästchen **Allow others to request my remote session disconnect** ausgewählt hat.
3. Wählen Sie im Feld **No response time interval** (Zeitintervall, in dem keine Antwort erfolgt) ein Zeitintervall aus.
4. Starten Sie die Fernsteuerungssitzung, indem Sie den Benutzermodus auswählen. Wählen Sie einen der folgenden Modi aus:
   - Start remote control in single-user mode (Fernsteuerung im Einzelbenutzermodus starten)
   - Start remote control in multi-user mode (Fernsteuerung im Mehrbenutzermodus starten)

   Anmerkung: Die Funktion "Anklopfen" wird automatisch aktiviert.

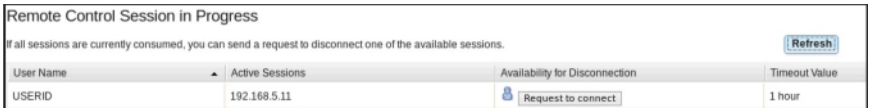
In der folgenden Abbildung sind die Felder dargestellt, die in Schritt 2 bis 4 beschrieben wurden.



Gehen Sie wie folgt vor, um eine ferne Sitzung anzufordern:

1. Klicken Sie auf **Refresh** (Aktualisieren), um die Fernsteuerungssitzung anzuzeigen, die derzeit aktiv ist.

   In der folgenden Abbildung ist das Fenster "Remote Control Session in Progress" (Aktive Fernsteuerungssitzung) dargestellt.

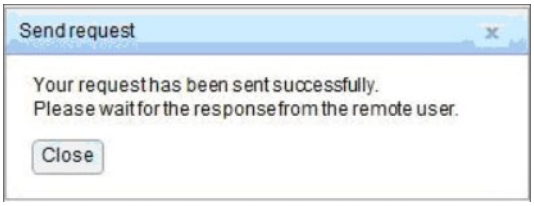


Im Feld **Availability for Disconnection** (Verfügbarkeit für das Trennen der Verbindung) wird eine der folgenden Antworten angezeigt:

- **Request to connect** (Verbindung ist angefordert): Dieser Text wird angezeigt, wenn der Fernsteuerungsbenutzer die Funktion "Anklopfen" aktiviert hat und derzeit keine Anforderung zum Trennen der Verbindung von einem anderen Webbenutzer erhalten hat. Der aktuelle Webbenutzer hat keine Anforderung zum Trennen der Verbindung an den Fernsteuerungsbenutzer gesendet.
- **Waiting for response** (Warten auf Antwort): Dieser Text wird angezeigt, wenn der Fernsteuerungsbenutzer die Anforderung zum Trennen der Verbindung des aktuellen Webbenutzers verarbeitet. Der aktuelle Webbenutzer kann eine Anforderung zum Abbrechen an den Fernsteuerungsbenutzer senden, indem er auf die Schaltfläche **Cancel** (Abbrechen) klickt.
- **Other request is pending** (Andere Anforderung ist anstehend): Dieser Text wird in einer der folgenden Situationen angezeigt:
  - Der Fernsteuerungsbenutzer verarbeitet die Anforderung zum Trennen der Verbindung eines anderen Webbenutzers.
  - Der Fernsteuerungsbenutzer hat die Funktion "Anklopfen" aktiviert und der aktuelle Webbenutzer wartet auf die Antwort auf die Anforderung zum Trennen der Verbindung, die von einem anderen Fernsteuerungsbenutzer gesendet wurde.
- **Not available** (Nicht verfügbar): Dieser Text wird in einer der folgenden Situationen angezeigt:
  - Es sind nicht alle Fernsteuerungssitzungen besetzt. Ob der Fernsteuerungsbenutzer die Funktion "Anklopfen" aktiviert hat oder nicht, hat keine Auswirkungen auf diese Situation.
  - Alle Fernsteuerungssitzungen sind besetzt und der Fernsteuerungsbenutzer hat die Funktion "Anklopfen" nicht aktiviert.
  - Diese Fernsteuerungsverbindung ist fünf Minuten lang für einen anderen Benutzer reserviert.

2. Klicken Sie auf **Request to connect**, um eine Anforderung zum Trennen der Verbindung an den Fernsteuerungsbenutzer zu senden.

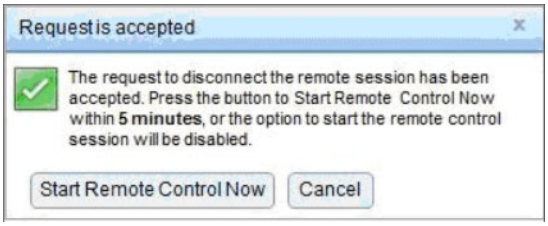
   In der folgenden Abbildung ist das Fenster dargestellt, das angezeigt wird, wenn die Anforderung erfolgreich gesendet wurde.



   Wenn der Fernsteuerungsbenutzer die Anforderung zum Trennen der Verbindung akzeptiert, muss der Webbenutzer die Fernsteuerungssitzung innerhalb von fünf Minuten starten. Wenn der Webbenutzer die Sitzung nicht innerhalb von fünf Minuten startet, ist die Sitzung nicht mehr reserviert.

   In den folgenden Abbildungen sind die Informationen dargestellt, die angezeigt werden, wenn die Anforderung zum Trennen der Verbindung akzeptiert wird.

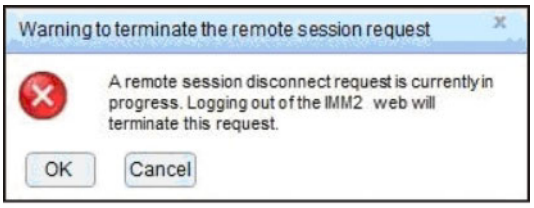
   In der folgenden Abbildung wird die Anforderung zum Trennen der Verbindung im reservierten Zustand dargestellt.



In der folgenden Abbildung wird die Anforderung zum Trennen der Verbindung im nicht reservierten Zustand dargestellt.

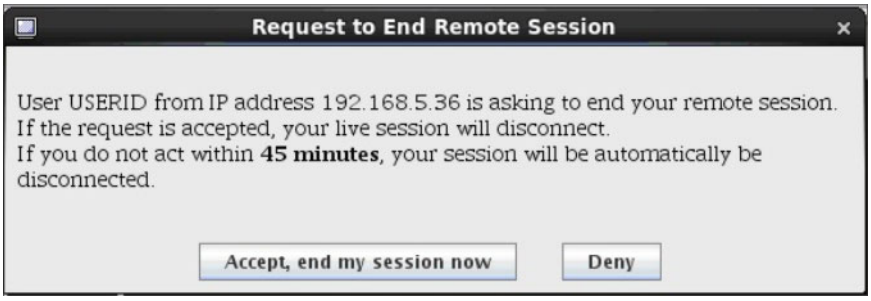
Wenn der Fernsteuerungsbenutzer die Anforderung zum Trennen der Verbindung zurückweist, erhält der Benutzer, der die Anforderung zum Trennen der Verbindung gesendet hat, eine Benachrichtigung, dass die Anforderung zurückgewiesen wurde (wie in der folgenden Abbildung dargestellt).

Wenn der Webbenutzer versucht, sich vom IMM2 abzumelden, bevor er eine Nachricht zu seiner Anforderung erhalten hat, erhält der Webbenutzer eine Nachricht (wie in der folgenden Abbildung dargestellt).

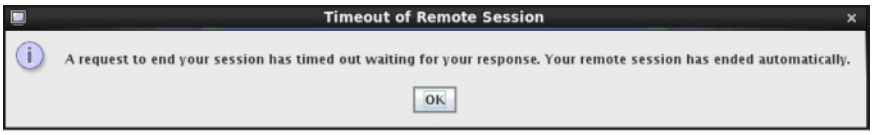


Nachdem der Fernsteuerungsbenutzer die Anforderung erhalten hat, muss er in dem ausgewählten Zeitintervall entscheiden, ob er die ferne Sitzung freigibt, bevor er die Fernsteuerungssitzung startet. Das Fenster "Request to End Remote Session" (Anforderung zur Beendigung der fernen Sitzung) wird angezeigt, um den Fernsteuerungsbenutzer an die verbleibende Zeit zu erinnern.

Das Fenster "Request to End Remote Session" ist in der folgenden Abbildung dargestellt.



Wenn der Fernsteuerungsbenutzer **Accept, end my session now** (Akzeptieren, meine Sitzung jetzt beenden) auswählt, wird die Anzeigefunktion für die ferne Sitzung automatisch geschlossen. Wenn der Fernsteuerungsbenutzer **Deny** (Zurückweisen) auswählt, behält der Fernsteuerungsbenutzer die ferne Sitzung. Nachdem die Anforderung zur Beendigung der fernen Sitzung (Request to End Remote Session) beendet wird, wird die ferne Sitzung automatisch freigegeben und das folgende Fenster wird geöffnet.



Ferner Datenträger

Über das Fenster "Virtual Media Session" können Sie dem Server ein CD- oder DVD-Laufwerk, ein Diskettenlaufwerk oder ein USB-Flashlaufwerk zuordnen oder Sie können ein Plattenimage auf Ihrem Computer angeben, das der Server verwenden kann. Sie können das Laufwerk für verschiedene Funktionen verwenden, z. B. zum erneuten Starten (Booten) des Servers, zum Installieren neuer Software auf dem Server und zum Installieren oder Aktualisieren des Betriebssystems auf dem Server. Sie haben Zugriff auf den fernen Datenträger. Die Laufwerk und Plattenimages werden auf dem Server als USB-Laufwerke angezeigt.

Anmerkungen:

- Die folgenden Serverbetriebssysteme verfügen über USB-Unterstützung. Bei der Funktionalität für ferne Datenträger ist USB-Unterstützung erforderlich.
  - Microsoft Windows-Server 2003: Web, Std, Ent, DC (SP2, R2, SBS)
  - Microsoft Windows-Server 2008 SP2: Std, SBS, EBS
  - Microsoft Windows-Server 2008 R2
  - SUSE Linux Enterprise-Server von Version 10 SP3: x86_64
  - SUSE Linux Enterprise Server von Version 11: x86,_64
  - Red Hat Enterprise Linux Enterprise-Server von Version 3.7: x86, x86_64
  - Red Hat Enterprise Linux Enterprise-Server von Version 4.8: x86, x86_64
  - Red Hat Enterprise Linux Enterprise-Server von Version 5.5: x86, x86_64
  - Red Hat Enterprise Linux Enterprise-Server von Version 6.0: x86, x86_64
  - ESX 4.5: 4.0 U1
- Für den Client-Server ist das Plug-in Java 1.5 oder eine aktuellere Version erforderlich.
- Der Client-Server muss über einen Mikroprozessor vom Typ Intel Pentium III (oder neuer) mit 700 MHz oder mehr (oder über einen funktional entsprechenden Mikroprozessor) verfügen.

Zugriff auf die Fernsteuerung

Gehen Sie wie folgt vor, um eine Fernsteuerungssitzung zu starten und auf einen fernen Datenträger zuzugreifen:

1. Klicken Sie im Fenster "Video Viewer" auf **Tools**.
2. Klicken Sie auf **Launch Virtual Media** (virtuellen Datenträger starten). Das Fenster "Video Viewer" wird geöffnet.

Anmerkung: Wenn vor dem Öffnen des Fensters "Video Viewer" das Kontrollkästchen **Encrypt disk and KVM data during transmission** (Disketten- und KVM-Daten während der Übertragung verschlüsseln) ausgewählt wurde, werden die Daten auf dem Datenträger mit ADES verschlüsselt.

Das Fenster "Virtual Media Session" ist von dem Fenster "Video Viewer" getrennt. Im Fenster "Virtual Media Session" sind alle Laufwerke auf dem Client aufgelistet, die als ferne Laufwerke zugeordnet werden können. Im Fenster "Virtual Media Session" können Sie außerdem ISO-Image- und Diskettenimage-Dateien als virtuelle Laufwerke zuordnen. Jedes zugeordnete Laufwerk kann als schreibgeschützt gekennzeichnet werden. Die CD- und DVD-Laufwerke sowie die ISO-Images sind immer schreibgeschützt.

Laufwerkzuordnung festlegen und aufheben

Wählen Sie zum Zuordnen eines Laufwerks das Kontrollkästchen **Select** (Auswählen) neben dem Laufwerk aus, das Sie zuordnen möchten.

Anmerkung: Ein CD- oder DVD-Laufwerk muss Datenträger enthalten, bevor es zugeordnet wird. Wenn das Laufwerk leer ist, werden Sie aufgefordert, eine CD oder eine DVD in das Laufwerk einzulegen.

Klicken Sie auf die Schaltfläche **Mount Selected** (Auswahl anhängen), um das ausgewählte Laufwerk bzw. die ausgewählten Laufwerke anzuhängen oder und zuzuordnen.Wenn Sie auf **Add Image** (Bild hinzufügen) klicken, können Disketten- und ISO-Imagedateien zur Liste verfügbarer Laufwerke hinzugefügt werden. Wenn die Disketten- oder ISO-Imagedatei im Fenster "Virtual Media Session" angeführt wird, kann sie genau wie die anderen Laufwerke zugeordnet werden.Klicken Sie zum Aufheben der Laufwerkzuordnung auf die Schaltfläche **Unmount All** (Alle abhängen). Bevor die Laufwerkzuordnungen aufgehoben werden, müssen Sie Ihren Wunsch bestätigen, dass die Laufwerkzuordnungen aufgehoben werden sollen.

Anmerkung: Nachdem Sie bestätigt haben, dass die Laufwerkzuordnungen aufgehoben werden sollen, werden sämtliche Laufwerke abgehängt. Sie können Laufwerke nicht einzeln abhängen.

Sobald ein Bild zur Liste hinzugefügt und das Kontrollkästchen **Map** (Zuordnung) ausgewählt wurde (vorausgesetzt, das Bild eignet sich zum Hochladen auf den IMM2-Speicher für die RDOC-Funktion), öffnet sich ein Fenster mit der Option, das Bild auf den Server zu übertragen. Wenn Sie **Yes** auswählen, geben Sie einen Namen für das Bild ein.

Anmerkung: Geben Sie keine Sonderzeichen wie etwa ein Et-Zeichen (&) oder Leerzeichen im Namen ein.

Durch das Hochladen eines Bildes kann die Festplatte an den Server angehängt bleiben, sodass Sie später Zugriff auf die Festplatte haben, auch nachdem die IMM2-Webschnittstellensitzung beendet wurde. Auf dem IMM2 können mehrere Bilder gespeichert werden; der insgesamt beanspruchte Speicherplatz darf jedoch

50 Mb nicht überschreiten. Um die Imagedatei aus dem Speicher herunterzuladen, wählen Sie deren Namen im Fenster "RDOC Setup" (RDOC-Konfiguration) aus und klicken Sie auf **Delete** (Löschen).

Fernsteuerung beenden

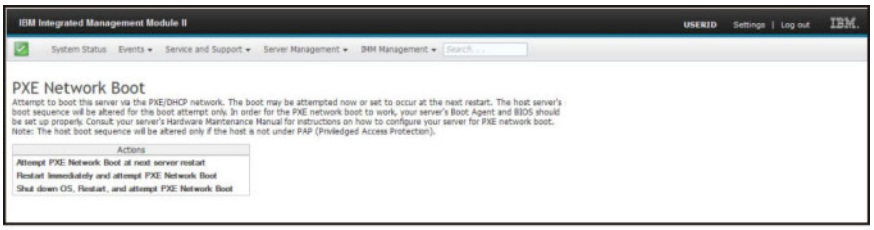
Schließen Sie die Fenster "Video Viewer" und "Virtual Media Session", wenn Sie die Verwendung der Fernsteuerungsfunktion beendet haben.

PXE-Netzboot einrichten

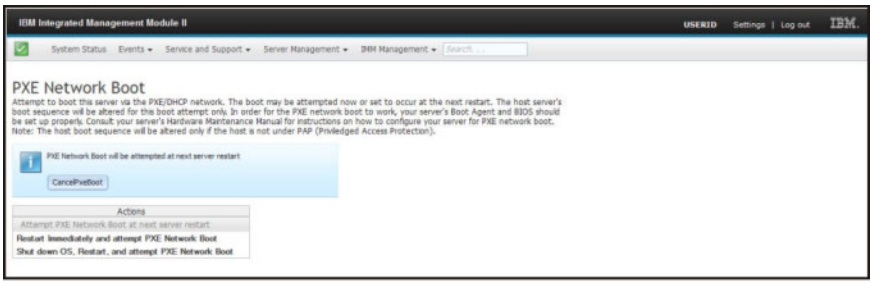
Verwenden Sie die Option "PXE Network Boot" (PXE-Netzboot), um Bootversuche der Server-Ausführungsumgebung vor dem Start einzurichten. Führen Sie die folgenden Schritte aus, um Ihren Server für den Versuch eines PXE-Netzboots (Preboot Execution Environment) beim nächsten Serverneustart einzurichten.

1. Melden Sie sich am IMM2 an. Weitere Informationen finden Sie im Abschnitt „Am IMM2 anmelden" auf Seite 10.
2. Klicken Sie auf **Server Management** (Serververwaltung) und wählen Sie anschließend **PXE Network Boot** aus.

   Das folgende Fenster wird geöffnet.



3. Wählen Sie aus den Optionen von "Actions" (Aktionen) die Option **Attempt PXE Network Boot at next server restart** (Bei nächstem Serverneustart PXE-Netzboot versuchen) aus. Das folgende Fenster wird geöffnet.

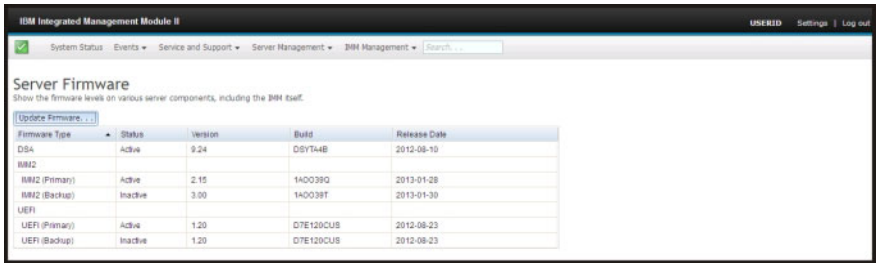


   Wenn Sie die Auswahl zurücknehmen möchten, klicken Sie auf **CancelPxeBoot** (PXE-Boot abbrechen). Das folgende Fenster zum Bestätigen des Abbruchs (Confirm Cancel) wird geöffnet.

Server-Firmware aktualisieren

In der Option "Server Firmware" werden die Firmwareversionen angezeigt und Sie können hier die DSA-, IMM2- und UEFI-Firmware aktualisieren. Die aktuellen Versionen der IMM2-, UEFI- und DSA-Firmware werden angezeigt. Dies umfasst die Versionstypen "Active" (Aktiv), "Primary" (Primär) und "Backup" (Sicherungskopie).

In der folgenden Abbildung ist die Seite "Server Firmware" dargestellt.



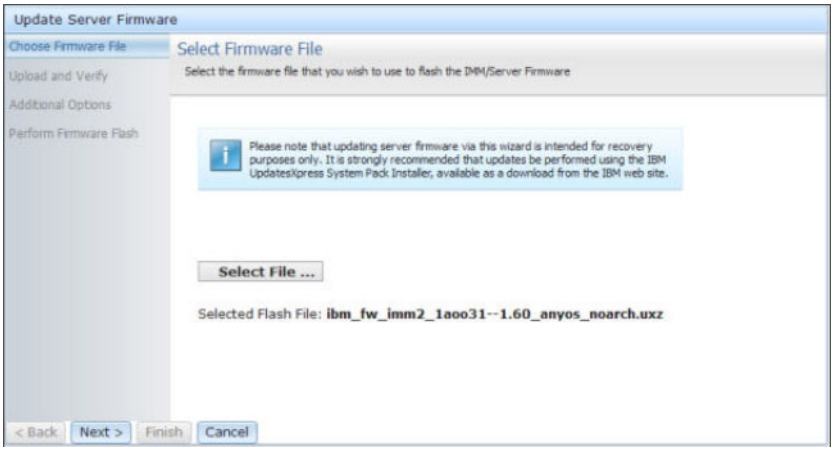
Der aktuelle Status und die aktuellen Versionen der IMM2-, UEFI- und DSA-Firmware werden angezeigt, einschließlich der primären Versionen und der Sicherungsversionen. Der Status der Firmware wird in drei Kategorien angegeben:

- **Active** (aktiv): Die Firmware ist aktiv.
- **Inactive** (inaktiv): Die Firmware ist inaktiv.
- **Pending** (anstehend): Die Firmware befindet sich im Wartestatus vor der Aktivierung.

Achtung: Die Installation der falschen Firmware könnte eine Serverstörung verursachen. Bevor Sie eine Firmware- oder Einheitentreiberaktualisierung installieren, lesen Sie alle Readme- und Änderungsprotokolldateien, die mit der heruntergeladenen Aktualisierung bereitgestellt werden. Diese Dateien enthalten wichtige Informationen zur Aktualisierung und zur Installationsprozedur der Aktualisierung, einschließlich Informationen zu besonderen Prozeduren bei der Aktualisierung von einer frühen Firmware- oder Einheitentreiberversion auf die neueste Version.

Gehen Sie wie folgt vor, um die Server-Firmware zu aktualisieren:

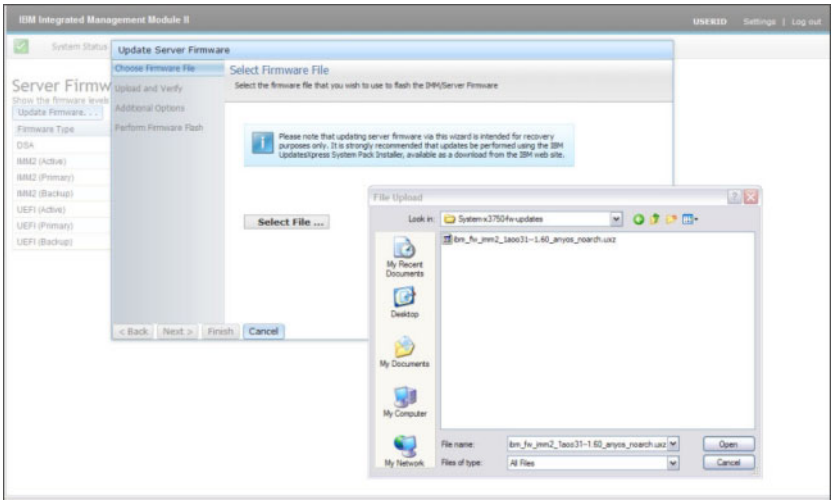
1. Klicken Sie in der Menüliste "Server Management" auf **Server Firmware**.
2. Klicken Sie auf **Update Firmware** (Firmware aktualisieren). Das Fenster "Update Server Firmware" (Server-Firmware aktualisieren) wird geöffnet (wie in der folgenden Abbildung dargestellt).



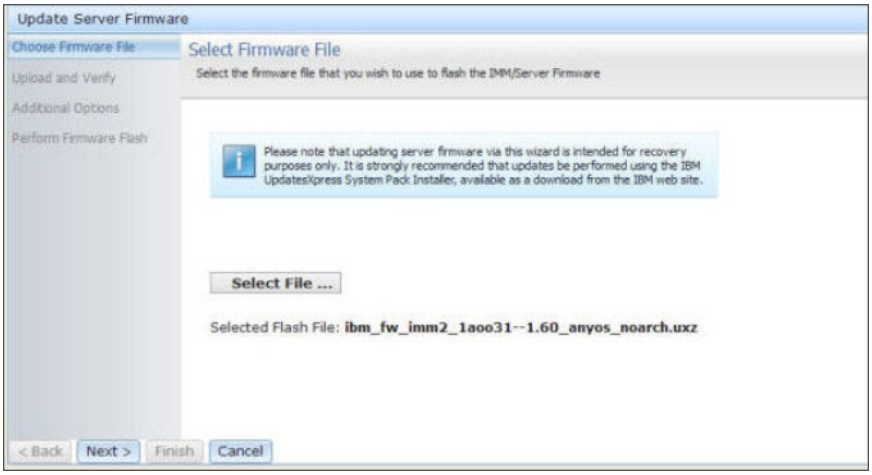
3. Lesen Sie den Warnhinweis, bevor Sie mit dem nächsten Schritt fortfahren.
4. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf **Cancel** (Abbrechen) und kehren Sie zum vorherigen Fenster "Server Firmware" zurück.
   - Klicken Sie auf **Select File...** (Datei auswählen), um die gewünschte Firmwaredatei zum Durchführen eines Flash-Updates der Server-Firmware auszuwählen.

     Anmerkung: Alle anderen Optionen sind beim ersten Öffnen des Fensters "Update Server Firmware" abgeblendet.

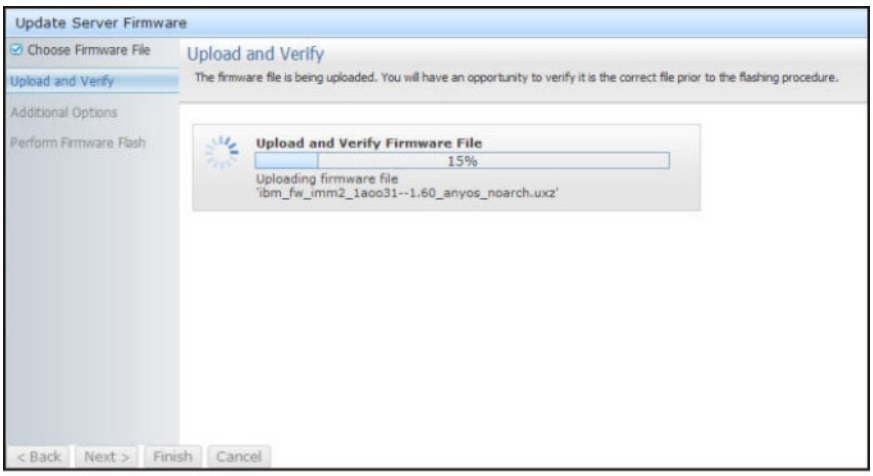
     Wenn Sie auf **Select File...** klicken, wird das Fenster "File Upload" (Hochladen von Datei) geöffnet (wie in der folgenden Abbildung dargestellt). In diesem Fenster können Sie nach der gewünschten Datei suchen.



5. Navigieren Sie zu der Datei, die Sie auswählen möchten, und klicken Sie auf **Open** (Öffnen). Sie kehren zum Fenster "Update Server Firmware" zurück. Die ausgewählte Datei wird angezeigt (wie in der folgenden Abbildung dargestellt).

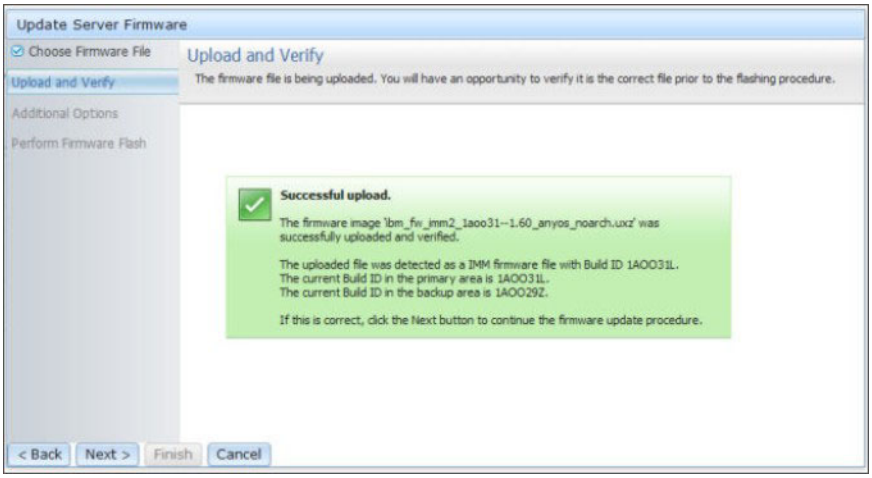


6. Klicken Sie auf **Next >** (Weiter), um die ausgewählte Datei hochzuladen und zu prüfen. Eine Fortschrittsanzeige wird angezeigt, während die Datei hochgeladen und geprüft wird (wie in der folgenden Abbildung dargestellt).



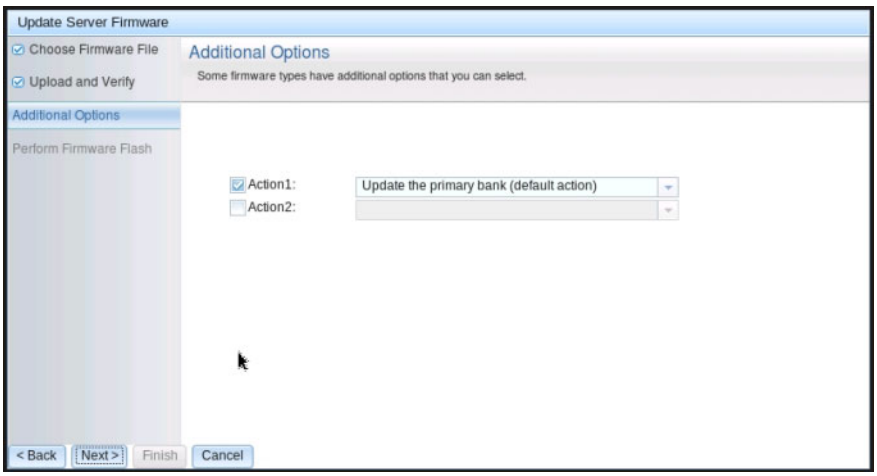
Sie können dieses Statusfenster anzeigen, um zu prüfen, ob Sie die richtige Datei zur Aktualisierung ausgewählt haben. Das Statusfenster enthält Informationen zum Dateityp der Firmware, die aktualisiert wird, wie DSA, IMM oder UEFI.

Nachdem die Firmwaredatei erfolgreich hochgeladen und geprüft wurde, erscheint ein Fenster mit der Meldung, dass das Hochladen erfolgreich war (Successful upload) (wie in der folgenden Abbildung dargestellt).

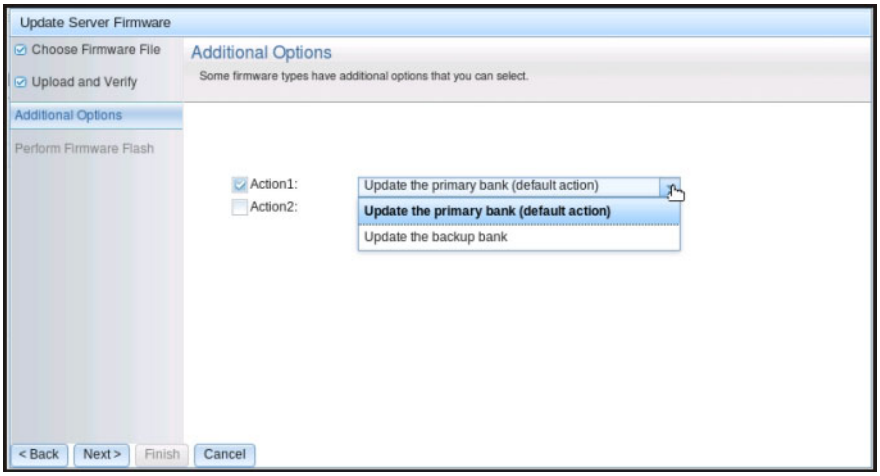


7. Klicken Sie auf **Next >**, wenn die Informationen richtig sind. Klicken Sie auf **< Back** (Zurück), wenn Sie Ihre Auswahl ändern möchten.

   Wenn Sie auf **Next >** klicken, wird eine Gruppe zusätzlicher Optionen angezeigt (wie in der folgenden Abbildung dargestellt).



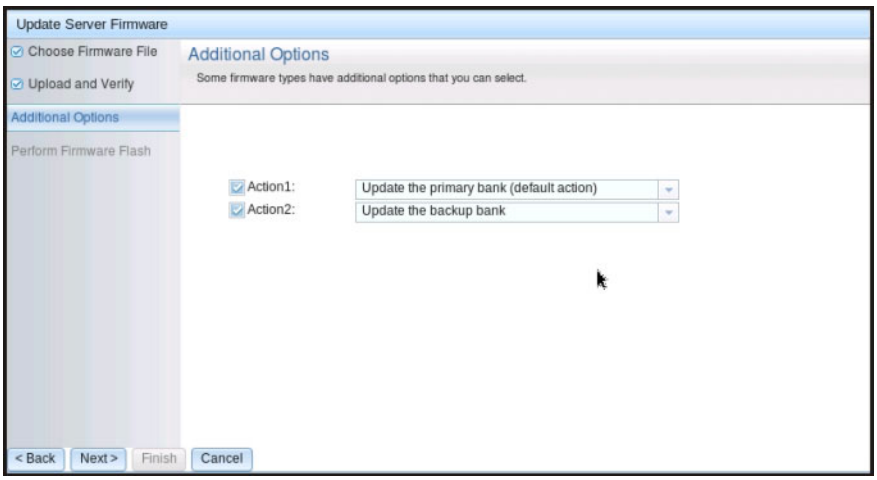
8. Im Dropdown-Menü neben dem Feld **Action 1** (Aktion 1) können Sie die Aktion **Update the primary bank (default action)** (primäre Speichergruppe aktualisieren (Standardaktion)) oder die Aktion **Update the backup bank** (Sicherungsspeichergruppe aktualisieren) auswählen (wie in der folgenden Abbildung dargestellt).



Nachdem Sie eine Aktion ausgewählt haben, kehren Sie zur vorherigen Anzeige zurück. Die angeforderte Zusatzaktion wird angezeigt.

Nachdem die ausgewählte Aktion geladen wurde, werden diese Aktion und ein neues Dropdown-Menü **Action 2** (Aktion 2) angezeigt (wie in der folgenden Abbildung dargestellt).

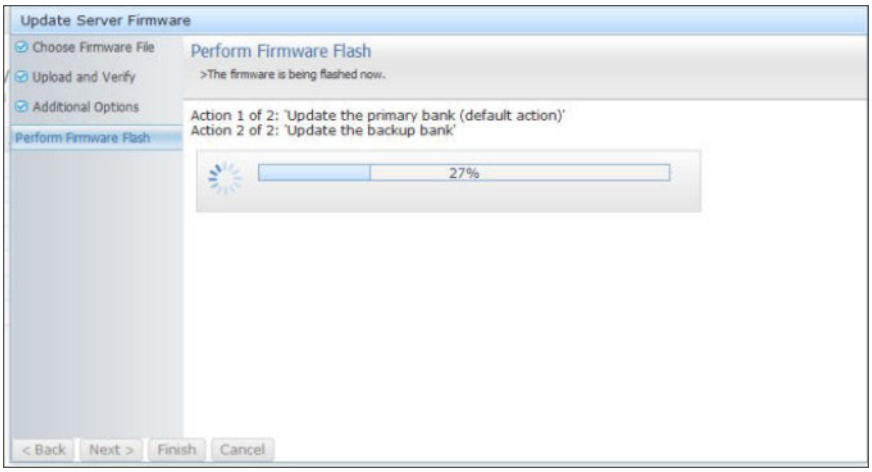
Anmerkung: Um eine Aktion zu inaktivieren und die Auswahl zusätzlicher Optionen erneut zu starten, klicken Sie auf das Kontrollkästchen neben der zugehörigen Aktion.



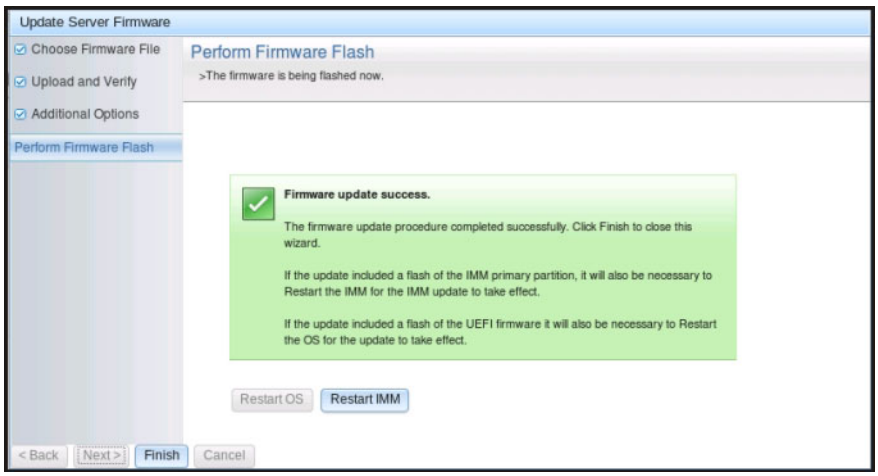
In der vorherigen Anzeige sehen Sie, dass für "Action 1" die primäre Speichergruppe zum Aktualisieren ausgewählt ist. Sie können auch auswählen, dass die Sicherungsspeichergruppe unter "Action 2" aktualisiert werden soll (wie in der vorherigen Abbildung dargestellt). Die primäre Speichergruppe und die Sicherungsspeichergruppe werden gleichzeitig aktualisiert, wenn Sie auf **Next >** klicken.

Anmerkung: "Action 1" muss sich von "Action 2" unterscheiden.

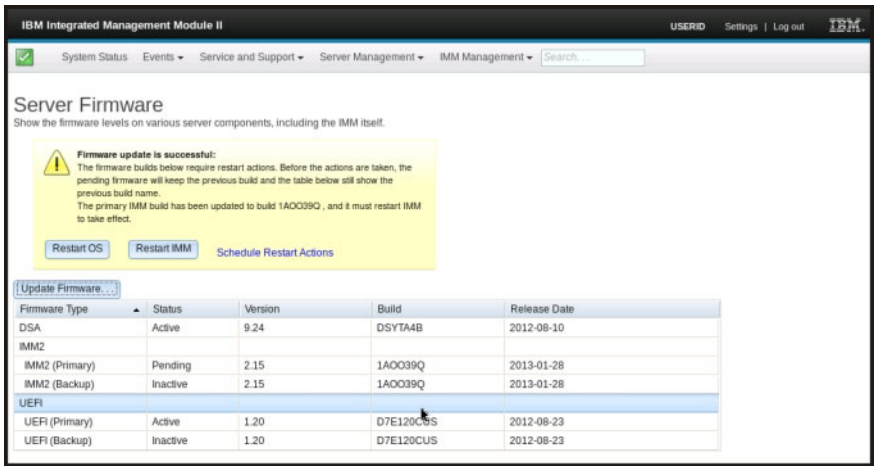
Eine Fortschrittsanzeige zeigt den Fortschritt der Aktualisierung der primären Speichergruppe und der Sicherungsspeicherguppe an (wie in der folgenden Abbildung dargestellt).



Wenn die Firmwareaktualisierung erfolgreich abgeschlossen wurde, wird das folgende Fenster geöffnet. Wählen Sie die zugehörige Operation entsprechend den angezeigten Inhalten aus, um den Aktualisierungsprozess abzuschließen.



Wenn die primäre Firmwareaktualisierung nicht abgeschlossen wurde, wird das folgende Fenster geöffnet, wenn die Anzeige "Server Firmware" aufgerufen wird.



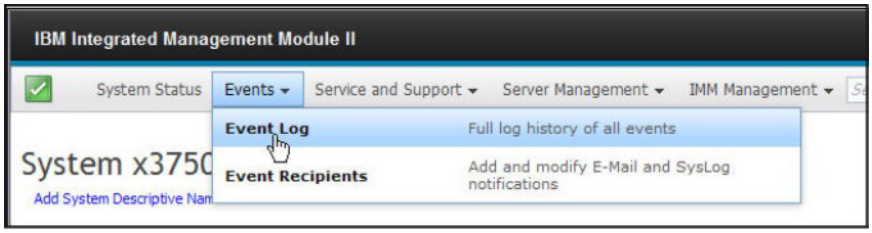
Systemereignisse verwalten

Das Menü "Events" (Ereignisse) ermöglicht es Ihnen, den Verlauf des Ereignisprotokolls (Event Log) und die Ereignisempfänger (Event Recipients) für E-Mail- und syslog-Benachrichtigungen zu verwalten.

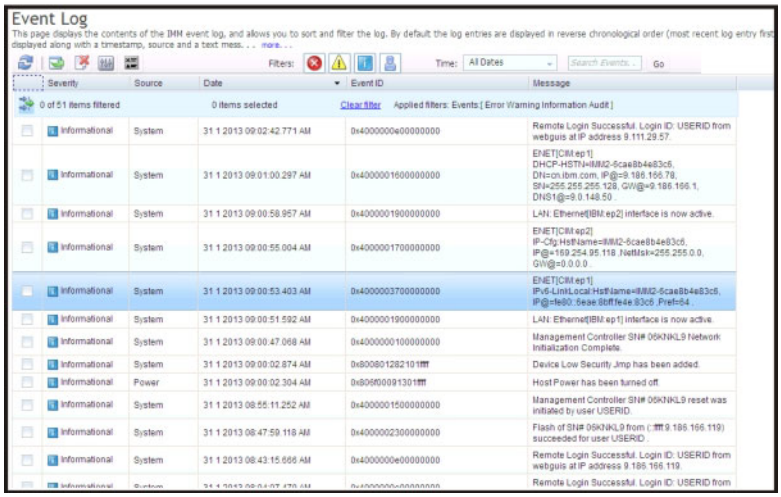
Ereignisprotokoll verwalten

Klicken Sie auf die Option **Event Log** (Ereignisprotokoll), um das Fenster "Event Log" anzuzeigen. Das Fenster "Event Log" beinhaltet eine Beschreibung der Ereignisse, die durch das IMM2 gemeldet werden, und Informationen zu allen Fernzugriffsversuchen und Konfigurationsänderungen. Alle Ereignisse im Protokoll besitzen eine Zeitmarke, die die Datums- und Uhrzeiteinstellungen des IMM2 verwendet. Einige Ereignisse generieren Alerts, falls sie im Fenster "Event Recipients" (Ereignisempfänger) entsprechend konfiguriert wurden. Im Ereignisprotokoll können Sie Ereignisse auch sortieren und filtern.

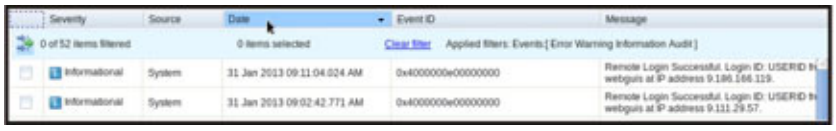
Klicken Sie auf die Option **Event Log**. Das folgende Fenster wird geöffnet.



Nach Auswahl der Option "Event Log" wird das folgende Fenster geöffnet.



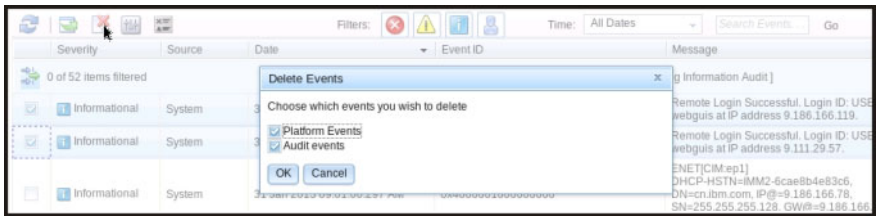
Um Ereignisse im Ereignisprotokoll zu sortieren und zu filtern, wählen Sie die entsprechende Spaltenüberschrift aus (wie in der folgenden Abbildung dargestellt).



Sie können mithilfe der Schaltfläche **Export** alle oder ausgewählte Ereignisse aus dem Ereignisprotokoll speichern. Um bestimmte Ereignisse auszuwählen, wählen Sie auf der Hauptseite von "Event Log" ein oder mehr Ereignisse aus und klicken Sie mit der linken Maustaste auf die Schaltfläche **Export** (Exportieren) (wie in der folgenden Abbildung dargestellt).

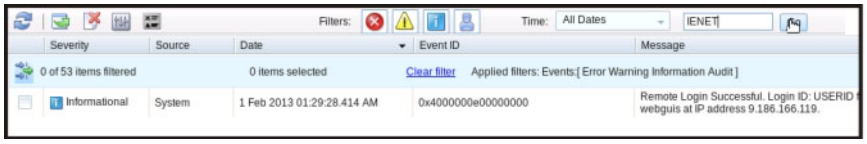
Klicken Sie auf **Delete Events** (Ereignisse löschen), um auszuwählen, welche Ereignistypen Sie löschen möchten. Sie müssen die Kategorie der Ereignisse, die Sie löschen möchten, auswählen.

In der folgenden Abbildung ist das Fenster "Delete Events" dargestellt.



Um den Typ der Ereignisprotokolleinträge auszuwählen, die Sie anzeigen möchten, klicken Sie auf die entsprechende Schaltfläche (wie in der folgenden Abbildung dargestellt).

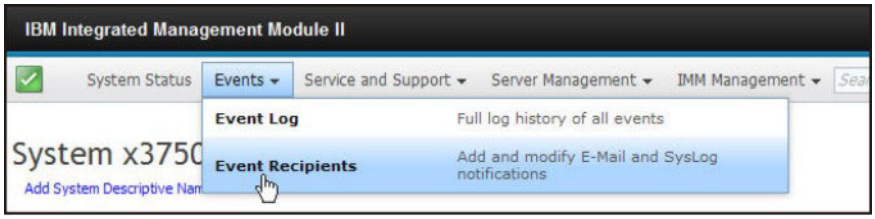
Um nach bestimmten Ereignistypen oder Suchbegriffen zu suchen, geben Sie den betreffenden Ereignistyp oder den Suchbegriff im Feld **Search Events** (Ereignisse suchen) ein. Klicken Sie dann auf **Go** (Start) (wie in der folgenden Abbildung dargestellt).



Benachrichtigung zu Systemereignissen

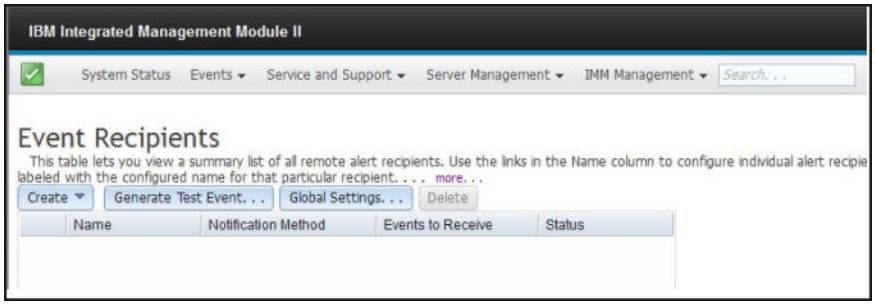
Wählen Sie die Option **Event Recipients** (Ereignisempfänger) aus, um E-Mail- und syslog-Benachrichtigungen hinzuzufügen und zu ändern.

In der folgenden Abbildung ist die Auswahl der Option "Event Recipients" dargestellt.

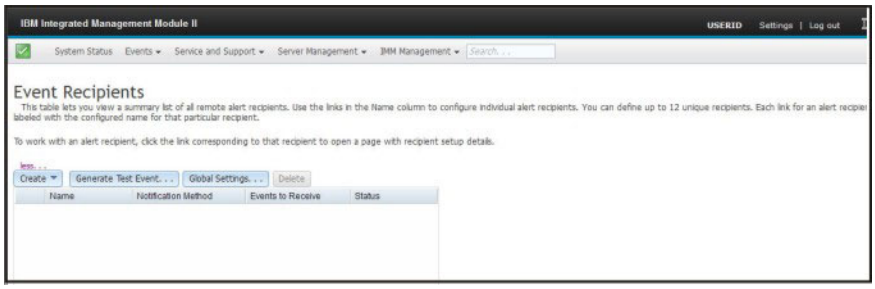


Mithilfe der Option "Event Recipients" können Sie die Empfänger von Benachrichtigungen über Systemereignisse verwalten. Sie können die einzelnen Empfänger konfigurieren und die Einstellungen verwalten, die auf alle Ereignisempfänger angewendet werden. Sie können außerdem ein Testereignis erstellen, um zu überprüfen, ob die Benachrichtigungsfunktion funktioniert.

In der folgenden Abbildung ist die Seite "Event Recipients" dargestellt.



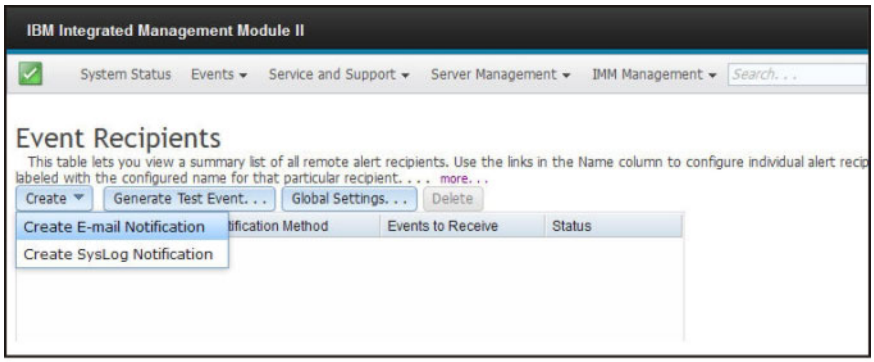
In der folgenden Abbildung sind weitere Informationen dargestellt, die angezeigt werden, wenn Sie auf den Link **more** (mehr) auf der Seite "Event Recipients" klicken.



E-Mail- und syslog-Benachrichtigungen erstellen

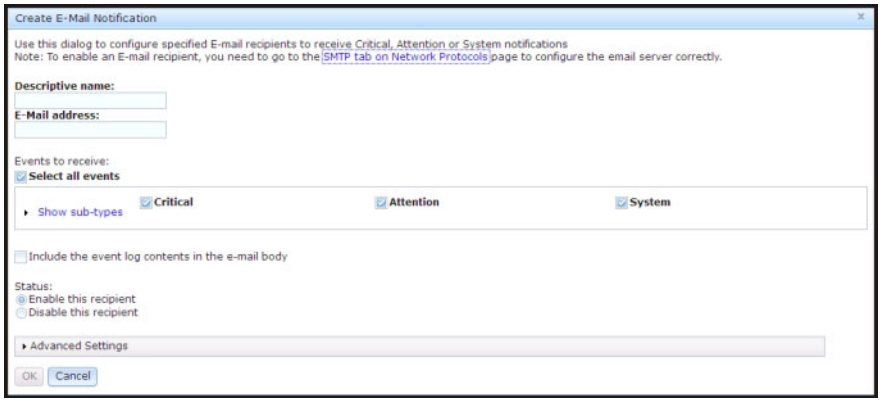
Wählen Sie die Registerkarte **Create** (Erstellen) aus, um E-Mail- und syslog-Benachrichtigungen zu erstellen.

In der folgenden Abbildung sind die verfügbaren Optionen im Menü "Create" dargestellt.

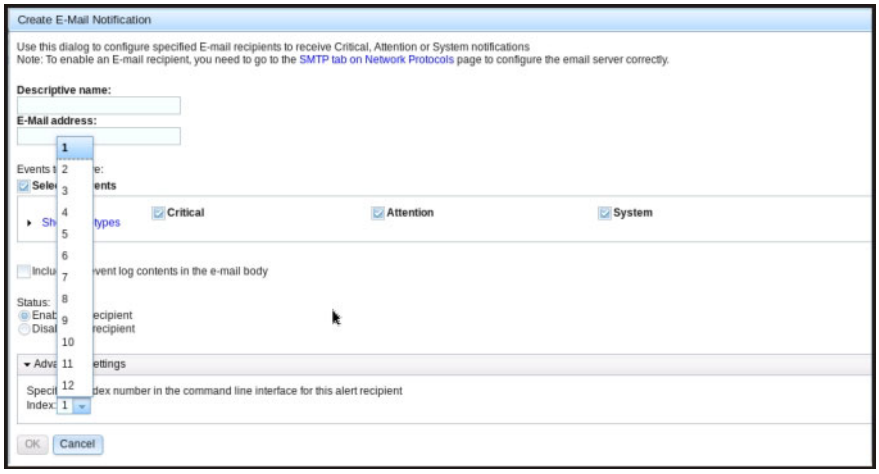


Mit der Option **Create E-mail Notification** (E-Mail-Benachrichtigung erstellen) können Sie eine Empfangs-E-Mail-Adresse einrichten und die Ereignistypen auswählen, über die Sie benachrichtigt werden möchten. Außerdem können Sie auf **Advanced Settings** (Erweiterte Einstellungen) klicken, um die Startindexzahl auszuwählen. Um das Ereignisprotokoll in die E-Mail einzufügen, wählen Sie das Kontrollkästchen **Include the event log contents in the e-mail body** (Ereignisprotokollinhalte in den E-Mail-Text einfügen) aus.

In der folgenden Abbildung ist die Anzeige "Create E-mail Notification" dargestellt.

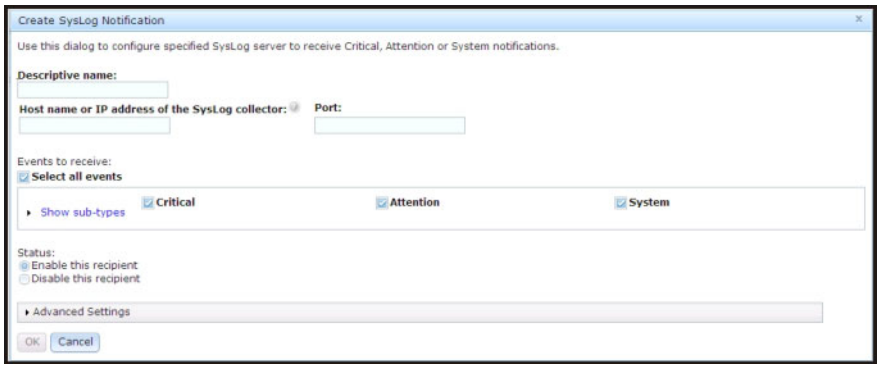


In der folgenden Abbildung sind die Optionen des Teilfensters "Advanced Settings" dargestellt.

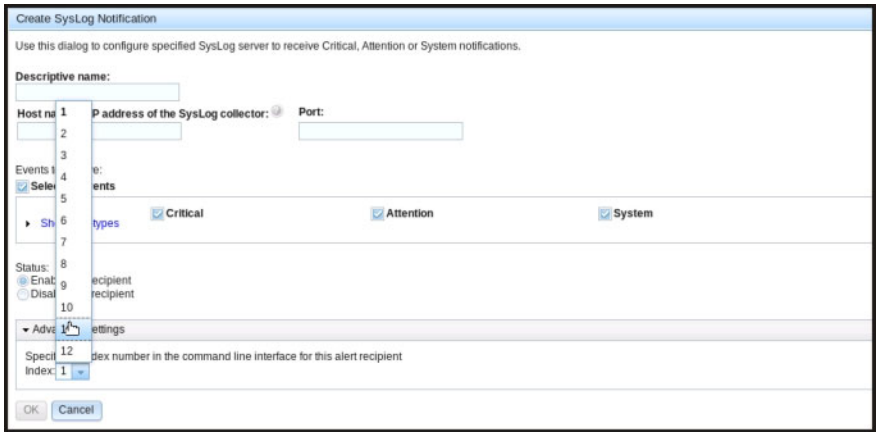


Mit der Option **Create Syslog Notification** (syslog-Benachrichtigung erstellen) können Sie den Hostnamen und die IP-Adresse des syslog-Collectors einrichten und die Ereignistypen auswählen, über die Sie benachrichtigt werden möchten. Sie können auf **Advanced Settings** klicken, um die Startindexzahl auszuwählen. Sie können außerdem den Port auswählen, den Sie für diesen Benachrichtigungstyp verwenden möchten.

In der folgenden Abbildung ist die Anzeige "Create Syslog Notification" dargestellt.



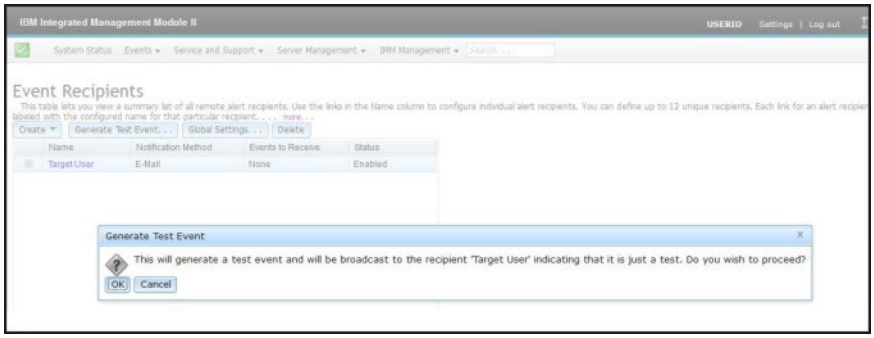
In der folgenden Abbildung sind die Optionen des Teilfensters "Advanced Settings" dargestellt.



Testereignisse generieren

Verwenden Sie die Registerkarte **Generate Test Event...** (Testereignis generieren), um eine Test-E-Mail an eine bestimmte E-Mail-Adresse zu senden. Klicken Sie nach Auswahl der Ereignisbenachrichtigung auf **OK**, um ein Testereignis zu generieren. Das Testereignis mit dem Hinweis, dass es sich um einen Test handelt, wird an den Empfänger gesendet.

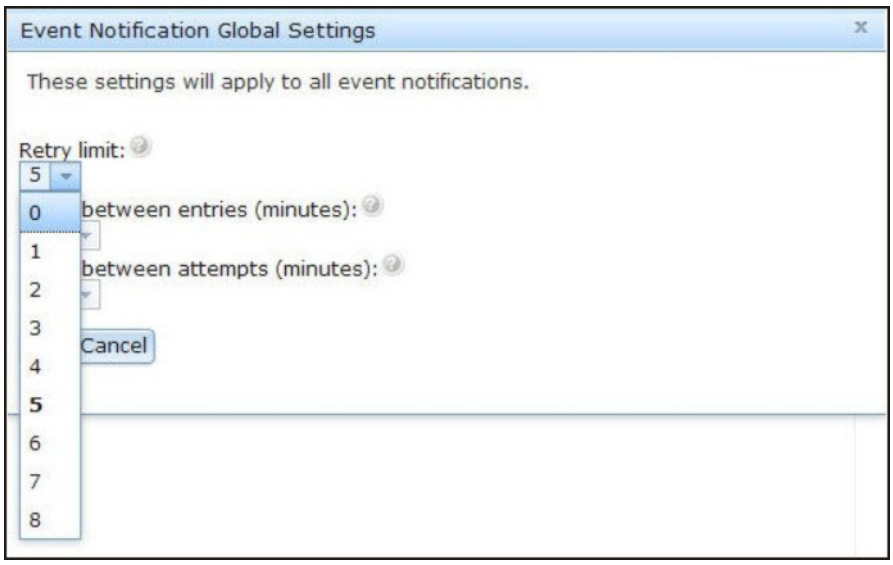
In der folgenden Abbildung ist das Fenster "Generate Test Event" dargestellt.



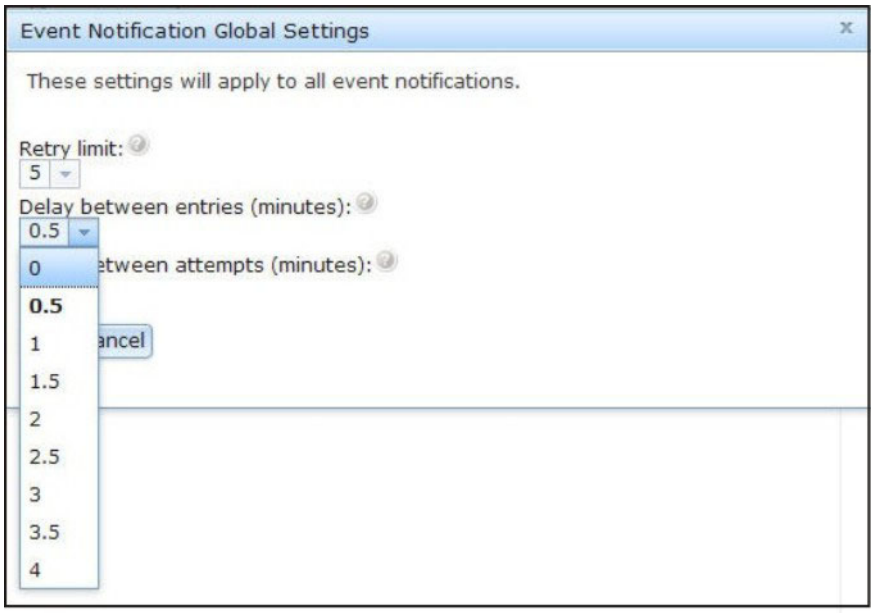
Wiederholungslimit für Benachrichtigungen festlegen

Verwenden Sie die Registerkarte **Global Settings...** (Globale Einstellungen), um ein Wiederholungslimit für die Ereignisbenachrichtigungen festzulegen. Bestimmen Sie das Verzögerungsintervall zwischen den Ereignisbenachrichtigungen (in Minuten) und zwischen den Versuchen (in Minuten).

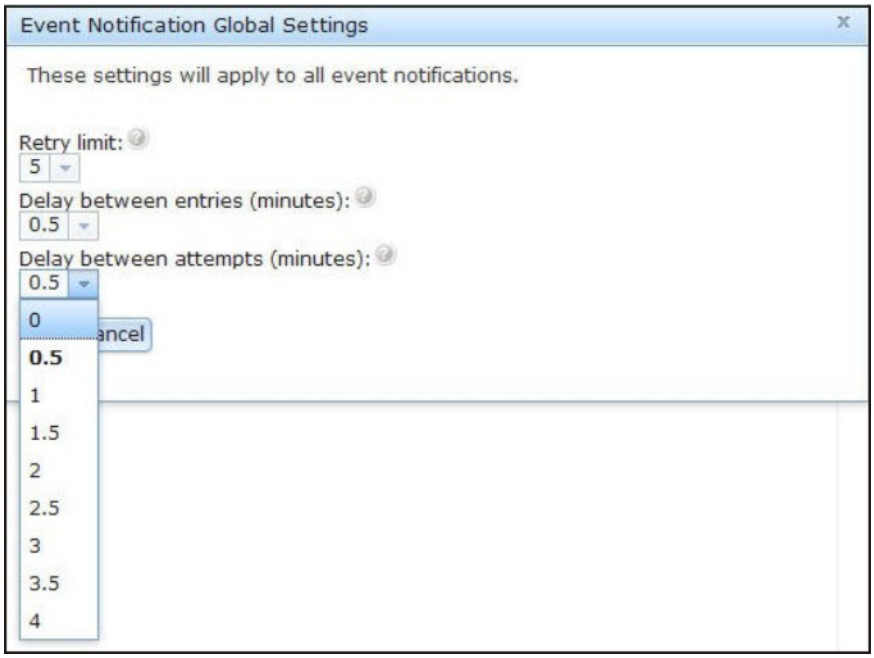
In der folgenden Abbildung sind die Einstellungen für die Option "Retry limit" (Wiederholungslimit) dargestellt.



In der folgenden Abbildung sind die Einstellungen für die Option "Delay between entries (minutes)" (Verzögerung zwischen Einträgen (Minuten)) dargestellt.



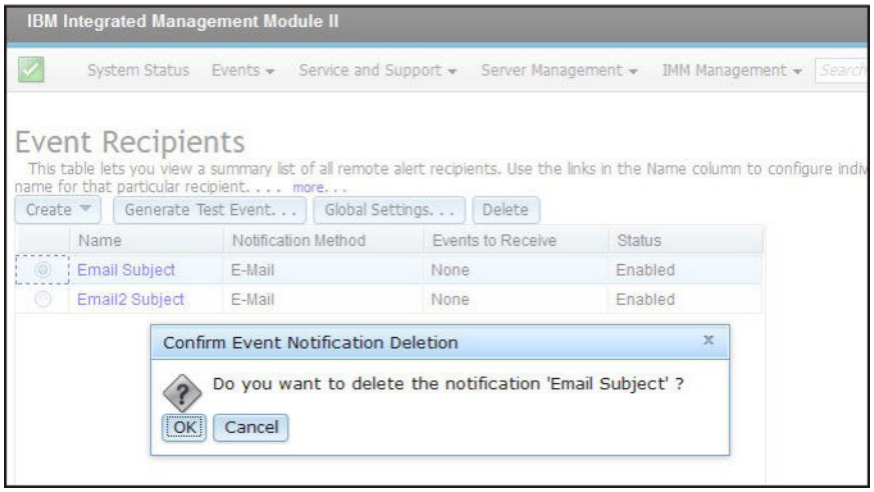
In der folgenden Abbildung sind die Einstellungen für die Option "Delay between attempts (minutes)" (Verzögerung zwischen Versuchen (Minuten)) dargestellt.



E-Mail- oder syslog-Benachrichtigungen löschen

Verwenden Sie die Registerkarte **Delete** (Löschen), um ein E-Mail- oder syslog-Benachrichtigungsziel zu löschen.

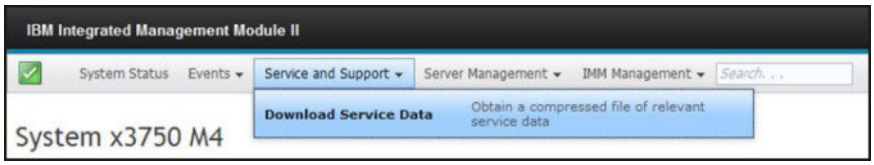
In der folgenden Abbildung ist das Fenster "Confirm Event Notification Deletion" (Löschen der Ereignisbenachrichtigung bestätigen) dargestellt.



Informationen für Service und Support erfassen

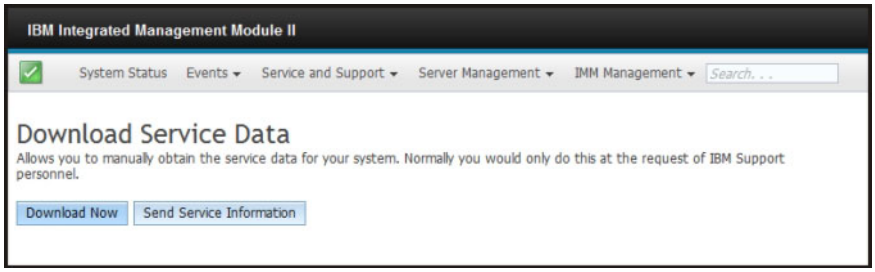
Klicken Sie auf die Option **Download Service Data** (Servicedaten herunterladen) im Menü "Service and Support" (Service und Support), um Informationen zum Server zu erfassen. Diese kann der IBM Support verwenden, um Sie bei der Lösung Ihres Problems zu unterstützen.

In der folgenden Abbildung ist das Menü "Service and Support" dargestellt.



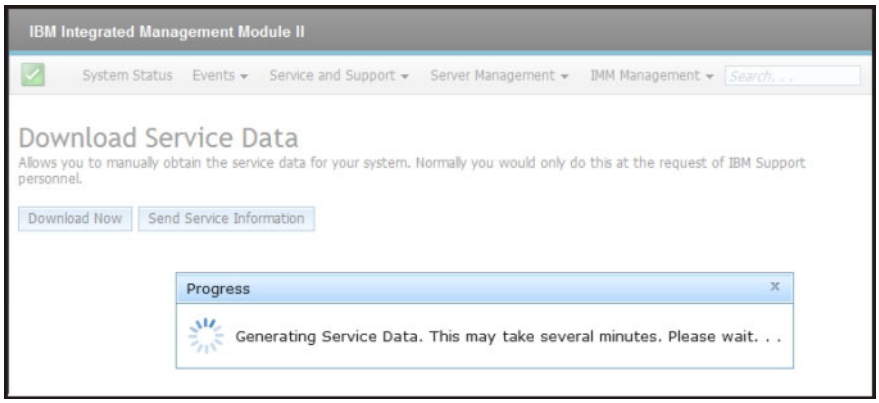
Klicken Sie auf die Schaltfläche **Download Now** (Jetzt herunterladen), wenn Sie die Daten für Service und Support herunterladen möchten.

In der folgenden Abbildung ist das Fenster "Download Service Data" (Servicedaten herunterladen) dargestellt.

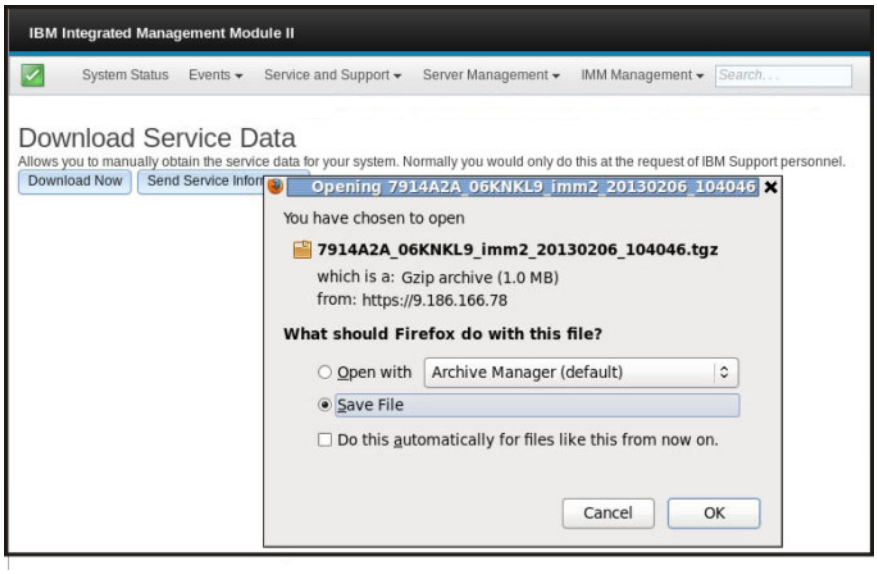


Der Erfassungsprozess der Daten für Service und Support wird gestartet. Dieser Prozess dauert ein paar Minuten; es werden die Servicedaten zum Speichern in einer Datei generiert.

Das folgende Fortschrittsfenster wird angezeigt, während die Servicedaten generiert werden.



Nachdem der Prozess beendet wurde, werden Sie dazu aufgefordert, den Speicherort für die Datei anzugeben. Ein Beispiel dafür finden Sie in der folgenden Abbildung.



Daten der letzten Betriebssystem-Fehleranzeige erfassen

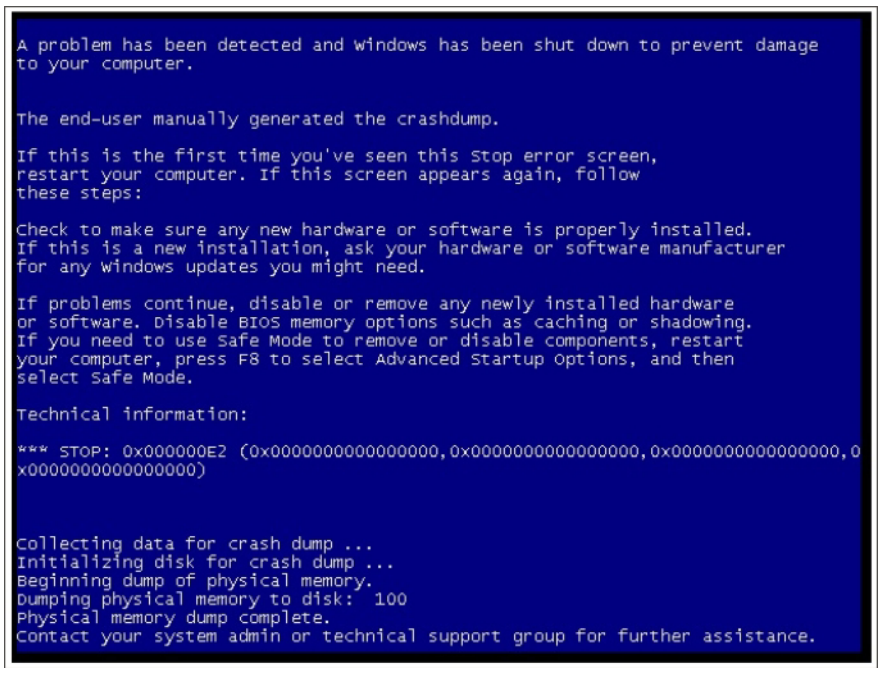
Verwenden Sie die Option "Latest OS Failure Screen" (Letzte Betriebssystem-Fehleranzeige), um die Daten der Betriebssystem-Fehleranzeige zu erfassen und zu speichern. Das IMM2 speichert nur die Informationen zu den aktuellsten Fehlerereignissen und überschreibt die Daten früherer Betriebssystem-Fehleranzeigen, wenn ein neues Fehlerereignis auftritt. Die Funktion "OS Watchdog" (Betriebssystem-Watchdog) muss aktiviert sein, damit Sie die Betriebssystem-Fehleranzeige erfassen können. Wenn ein Ereignis eintritt, durch das die Ausführung des Betriebssystems gestoppt wird, wird die Funktion "OS Watchdog" ausgelöst. Die Erfassung der Betriebssystem-Fehleranzeige ist nur mit der IMM2-Funktion "Advanced Level" verfügbar. Informationen zur Funktionalitätsstufe des IMM2, das in Ihrem Server installiert ist, finden Sie in der Dokumentation zum Server.

Um ein Bild einer Betriebssystem-Fehleranzeige über Fernzugriff anzuzeigen, wählen Sie eine der folgenden Menüoptionen aus:

- **Latest OS Failure Screen** auf der Registerkarte "Server Management"
- Registerkarte **Latest OS Failure Screen** auf der Seite "System Status"

Anmerkung: Wenn eine Betriebssystem-Fehleranzeige nicht erfasst wurde, wird die Registerkarte "Latest OS Failure Screen" auf der Seite "System Status" abgeblendet angezeigt und kann nicht ausgewählt werden.

In der folgenden Abbildung ist die Betriebssystem-Fehleranzeige dargestellt.

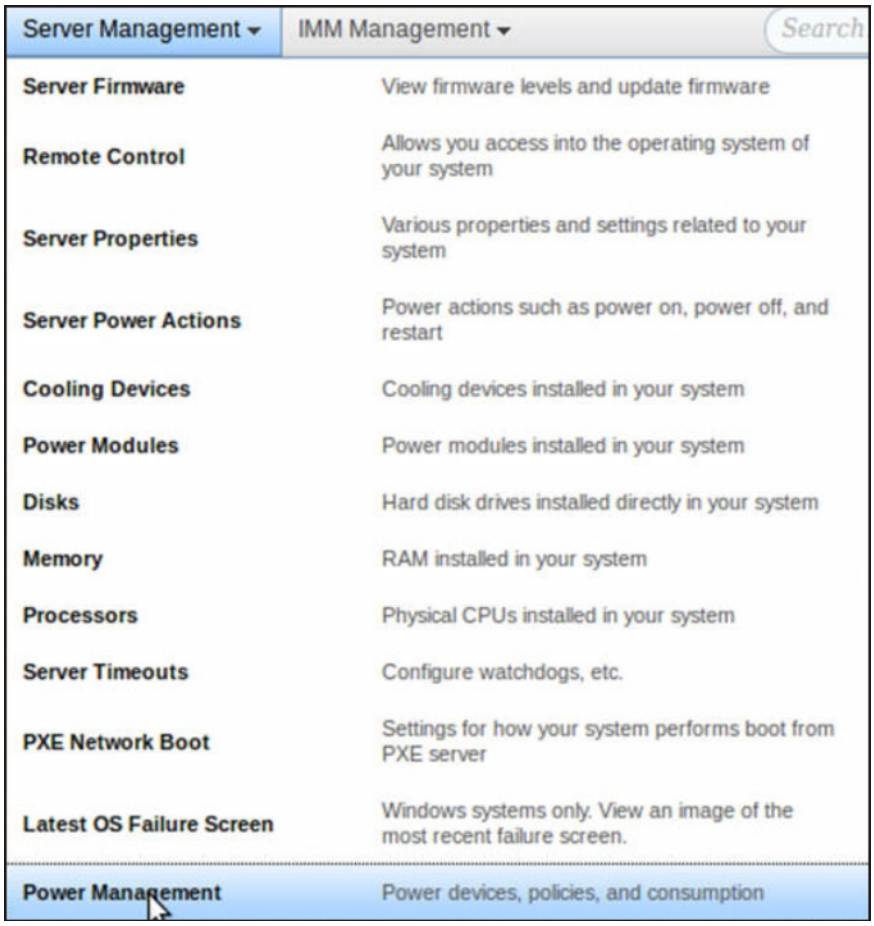


Serverstromversorgung verwalten

Verwenden Sie die Registerkarte "Power Management", um die folgenden Tasks auszuführen:

- Zeigen Sie Informationen zu installierten Netzteilen an.
- Steuern Sie, wie die "Leistung" der Stromversorgung verwaltet wird.
- Steuern Sie die gesamte Stromversorgung des Systems.
- Zeigen Sie Informationen zu installierten Netzteilen und der aktuellen Stromversorgungskapazität an.
- Zeigen Sie das Verlaufsprotokoll zur Stromverbrauchsmenge an.

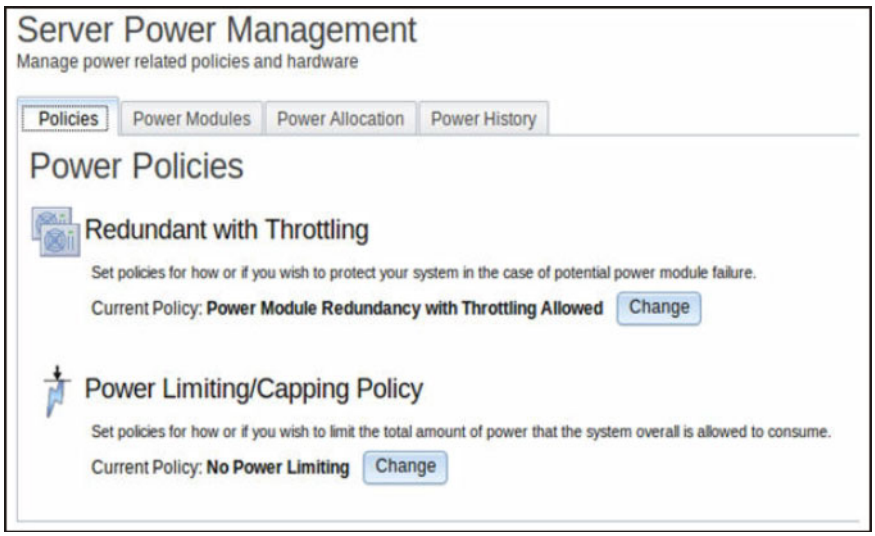
Wählen Sie die Option **Power Management** (Stromverbrauchssteuerung) unter der Registerkarte "Server Management" (Serververwaltung) aus, um Informationen zur Stromverbrauchssteuerung anzuzeigen und Funktionen zur Stromverbrauchssteuerung auszuführen (wie in der folgenden Abbildung dargestellt).



Stromversorgung und gesamte Stromversorgung des Systems steuern

Klicken Sie auf die Registerkarte **Policies** (Richtlinien), um zu steuern, wie die Stromversorgung verwaltet wird. Außerdem können Sie optional die gesamte Stromversorgung des Systems über "Active Energy Manager" steuern, indem Sie eine Begrenzungsrichtlinie festlegen (wie in der folgenden Abbildung dargestellt).

Anmerkung: Die Registerkarte **Policies** ist in einem IBM Flex System-Knoten nicht verfügbar.



Um die Richtlinie auszuwählen, die Sie zum Schützen Ihres Servers bei Ausfall eines Stromversorgungsmoduls verwenden möchten, klicken Sie im Fenster "Power Policies" (Stromversorgungsrichtlinien) auf die Schaltfläche **Change** (Ändern) von "Current Policy" (Aktuelle Richtlinie) für die Option "Redundant with Throttling" (Redundant mit Leistungsdrosselung).

Anmerkung: Durch Auswahl einer Stromversorgungsrichtlinie können Sie einen Kompromiss zwischen Redundanz und verfügbarer Leistung finden.

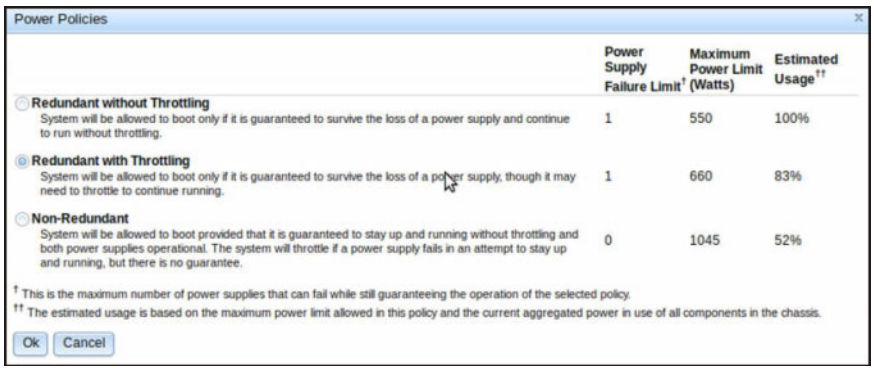
Die Auswahlmöglichkeiten für die Stromversorgungsrichtlinie sind:

Redundant without Throttling (Redundant ohne Leistungsdrosselung)
Das Booten des Servers ist zulässig, wenn garantiert ist, dass der Server den Ausfall eines Netzteils übersteht und ohne Leistungsdrosselung in Betrieb bleiben kann.

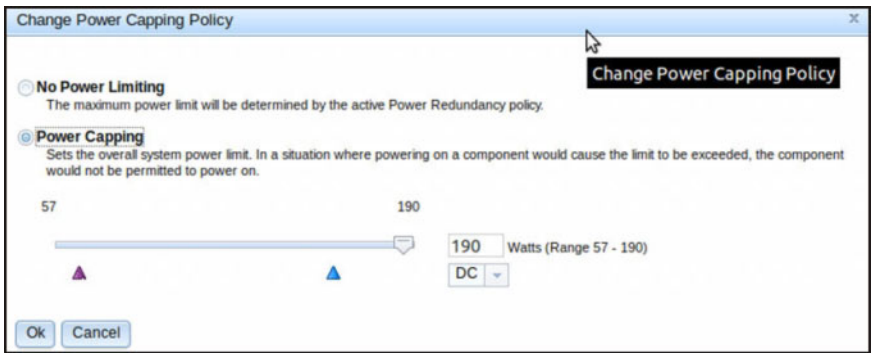
Redundant with Throttling (Redundant mit Leistungsdrosselung)
Das Booten des Servers ist zulässig, wenn garantiert ist, dass der Server den Ausfall eines Netzteils übersteht, aber möglicherweise ist eine Leistungsdrosselung des Servers notwendig, damit er in Betrieb bleibt.

Non-Redundant (Nicht redundant)
Das Booten des Servers ist zulässig, wenn garantiert ist, dass der Server ohne Leistungsdrosselung in Betrieb bleibt und beide Stromversorgungsmodule betriebsbereit sind. Die Leistung des Servers wird gedrosselt, wenn der Versuch, den Betrieb eines Netzteils aufrechtzuerhalten, fehlschlägt; es gibt jedoch keine Garantie dafür.

Das folgende Fenster wird geöffnet, wenn Sie die Schaltfläche **Change** für die Option "Redundant with Throttling" auswählen.



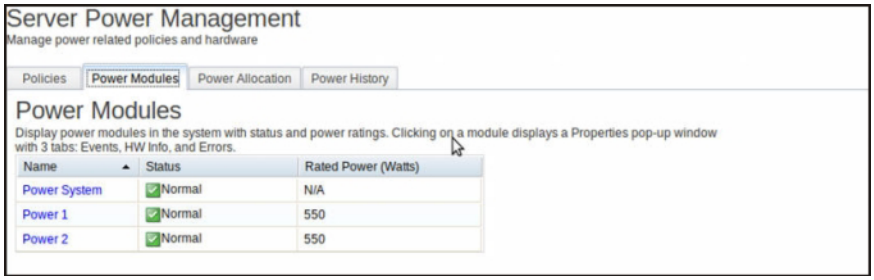
Über "Active Energy Manager" können Sie einen Grenzwert für den zulässigen Gesamtnetzstromverbrauch des Servers festlegen. Um einen Grenzwert für den Stromverbrauch des Servers festzulegen, klicken Sie im Fenster "Power Policies" auf die Schaltfläche **Change** von "Current Policy" für die Option "Power Limiting/ Capping Policy" (Netzstrombegrenzung/Begrenzungsrichtlinie). Das Fenster "Change Power Capping Policy" (Netzstrombegrenzungsrichtlinie ändern) wird geöffnet (wie in der folgenden Abbildung dargestellt).



Wählen Sie die Schaltfläche **Power Capping** (Netzstrombegrenzung) aus und verschieben Sie die Schiebereglermarke auf die gewünschte Wattleistung. Der Pfeil rechts unter der Schiebereglermarke zeigt die minimale Einstellung an, die durch "Active Energy Manager" garantiert werden kann. Der Pfeil links unter der Schiebereglermarke zeigt den maximalen Stromverbrauch des Systems in den letzten 24 Stunden an. Diese beiden Pfeile stellen einen Richtwert für das Festlegen eines Grenzwerts für die Netzstrombegrenzung dar.

Aktuell installierte Netzteile anzeigen

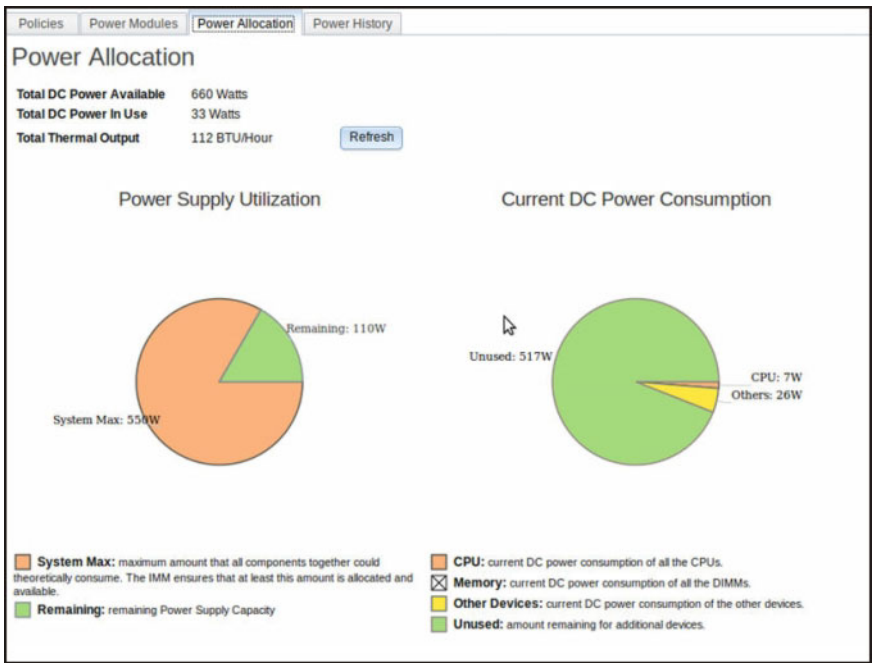
Klicken Sie auf die Registerkarte **Power Modules** (Stromversorgungsmodule), um Informationen zu aktuell installierten Netzteilen anzuzeigen (wie in der folgenden Abbildung dargestellt).



Der Name jedes Stromversorgungsmoduls im Server wird zusammen mit dem Status und der Belastbarkeit der einzelnen Netzteile angezeigt. Um weitere Informationen zu einem Stromversorgungsmodul anzuzeigen, klicken Sie auf den Namen eines Stromversorgungsmoduls. Das Fenster "Properties" (Eigenschaften) wird geöffnet. Es enthält drei Registerkarten für das ausgewählte Modul: Events (Ereignisse), HW Info (Hardware-Info) und Errors (Fehler).

Stromversorgungskapazität anzeigen

Klicken Sie auf die Registerkarte **Power Allocation** (Netzstromzuordnung), um anzuzeigen, wie viel der Stromversorgungskapazität verwendet wird, und um den aktuellen Gleichstromverbrauch des Servers anzuzeigen (wie in der folgenden Abbildung dargestellt).



Verlaufsprotokoll zum Stromverbrauch

Klicken Sie auf die Registerkarte **Power History** (Verlaufsprotokoll zum Stromverbrauch), um für einen ausgewählten Zeitraum anzuzeigen, wie viel Strom vom System verbraucht wird. Über die Registerkarte **Chart** (Diagramm) können Sie den Zeitraum auswählen. Außerdem haben Sie auch die Möglichkeit, den Wechsel- oder Gleichstrom anzuzeigen. Der durchschnittliche, maximale und minimale Stromverbrauch wird angezeigt (wie in der folgenden Abbildung dargestellt).

Kapitel 7. Features on Demand

Mit der Funktion "Features on Demand" (FoD) von IMM2 können Sie optionale Server- und Systemmanagementfunktionen installieren und verwalten.

Für Ihren Server gibt es mehrere Stufen von IMM2-Firmwarefunktionalitäten und -Funktionen. Die Stufen der auf Ihrem Server installierten IMM2-Firmwarefunktionen variieren je nach Hardwaretyp. Informationen dazu, welche Arten von IMM2-Hardware und -Funktionen in Ihrem Server installiert sind, finden Sie in der Dokumentation im Lieferumfang Ihres Servers.

Sie können die IMM2-Funktionen aktualisieren, indem Sie einen FoD-Aktivierungsschlüssel erwerben und installieren. Zusätzliche ausführliche Informationen zu FoD finden Sie im *Features on Demand User's Guide* unter http://www.ibm.com/systems/x/fod/.

Anmerkung: Auf Servern mit IMM2-Grundstufenfunktionalität ist das IBM Integrated Management Module Standard Upgrade vor dem Installieren der Funktionalität des IBM Integrated Management Module Advanced Upgrade erforderlich.

Um einen FoD-Aktivierungsschlüssel anzufordern, kontaktieren Sie Ihren IBM Ansprechpartner oder Ihren IBM Geschäftspartner oder rufen Sie die folgende Seite auf: http://www.ibm.com/systems/x/fod/.

Verwenden Sie die IMM2-Webschnittstelle oder die IMM2-Befehlszeilenschnittstelle, um manuell einen FoD-Aktivierungsschlüssel zu installieren, mit dem Sie eine optionale Funktion verwenden können, die Sie erworben haben. Beachten Sie Folgendes, bevor Sie einen Schlüssel aktivieren:

- Der FoD-Aktivierungsschlüssel muss sich auf dem System befinden, das Sie verwenden, um sich am IMM2 anzumelden.
- Sie müssen die FoD-Option angefordert und deren Berechtigungscode per Post oder E-Mail erhalten haben.

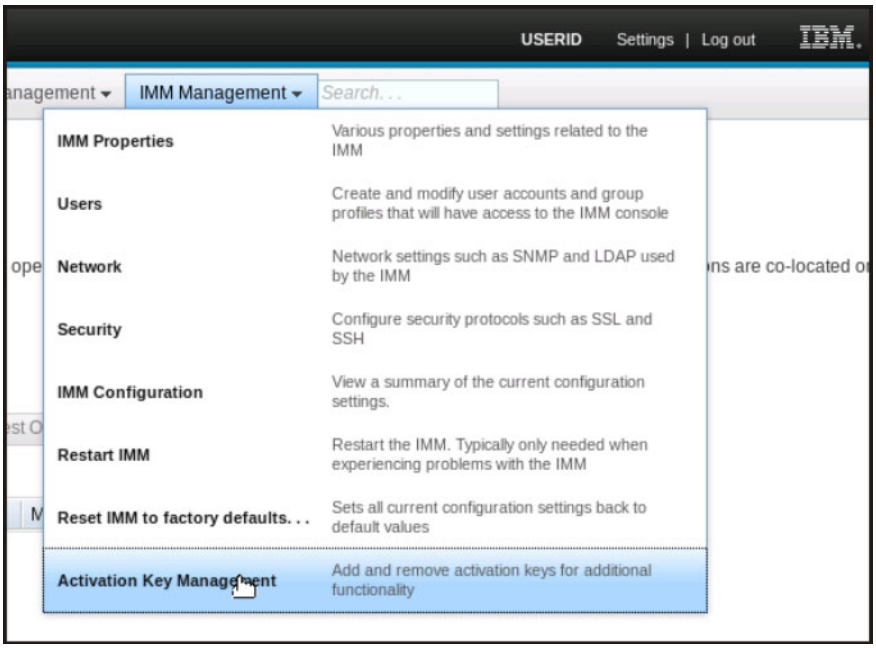
Informationen zur Verwaltung eines FoD-Aktivierungsschlüssels mithilfe der IMM2-Webschnittstelle finden Sie unter „Aktivierungsschlüssel installieren", „Aktivierungsschlüssel entfernen" auf Seite 146 oder „Aktivierungsschlüssel exportieren" auf Seite 147. Informationen zur Verwaltung eines FoD-Aktivierungsschlüssels mithilfe der IMM2-Befehlszeilenschnittstelle finden Sie unter „Befehl "keycfg"" auf Seite 176.

Aktivierungsschlüssel installieren

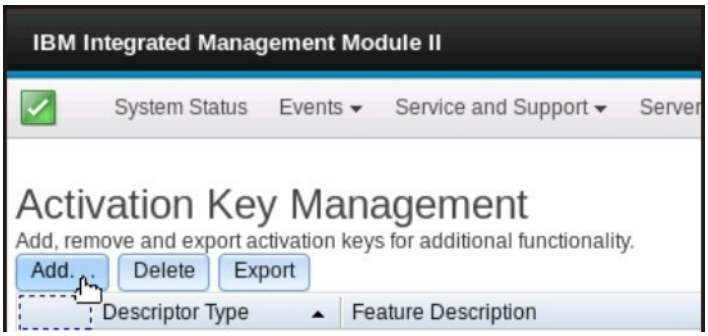
Sie können einen FoD-Aktivierungsschlüssel installieren, um eine Zusatzfunktion zu Ihrem Server hinzuzufügen.

Gehen Sie wie folgt vor, um einen FoD-Aktivierungsschlüssel zu installieren:

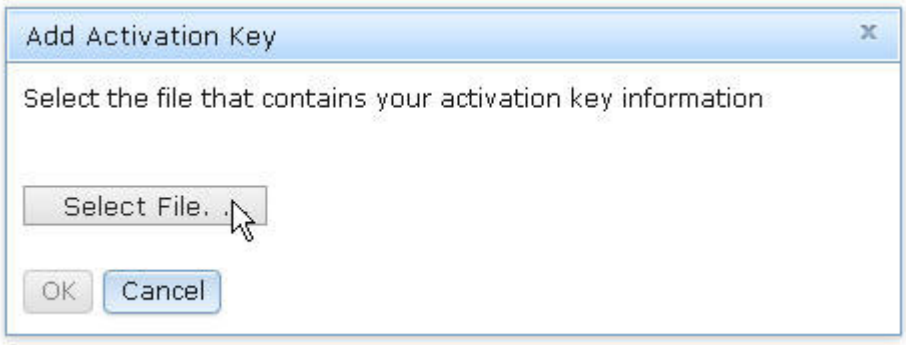
1. Melden Sie sich am IMM2 an. Weitere Informationen hierzu finden Sie im Abschnitt „Am IMM2 anmelden" auf Seite 10.
2. Klicken Sie in der IMM2-Webschnittstelle auf die Registerkarte **IMM Management** (IMM-Verwaltung). Klicken Sie anschließend auf **Activation Key Management** (Aktivierungsschlüsselverwaltung).



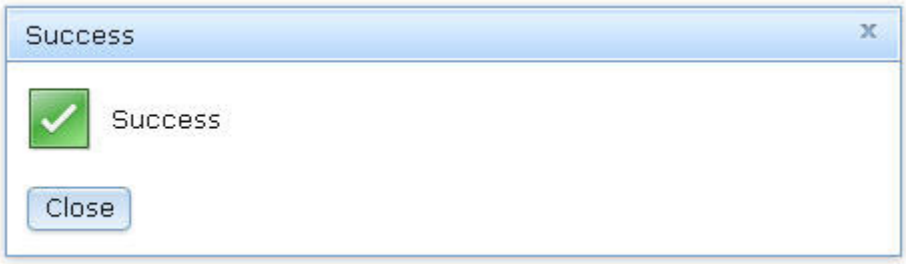
3. Klicken Sie auf der Seite "Activation Key Management" auf **Add...** (Hinzufügen).



4. Klicken Sie im Fenster "Add Activation Key" (Aktivierungsschlüssel hinzufügen) auf **Select File...** (Datei auswählen). Wählen Sie nun die Aktivierungsschlüsseldatei aus, die Sie im Fenster "File Upload" (Hochladen von Datei) hinzufügen möchten, und klicken Sie auf **Open**, um die Datei hinzuzufügen, oder klicken Sie auf **Cancel**, um die Installation zu stoppen. Um das Hinzufügen des Schlüssels fertigzustellen, klicken Sie im Fenster "Add Activation Key" auf **OK** oder klicken Sie auf **Cancel**, um die Installation zu stoppen.

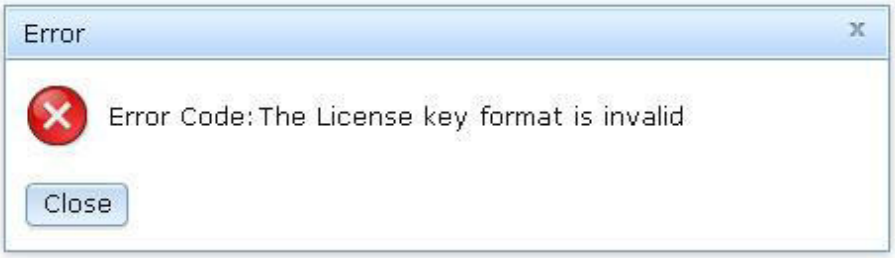


Das Fenster "Success" (Erfolg) gibt an, dass der Aktivierungsschlüssel installiert wurde.

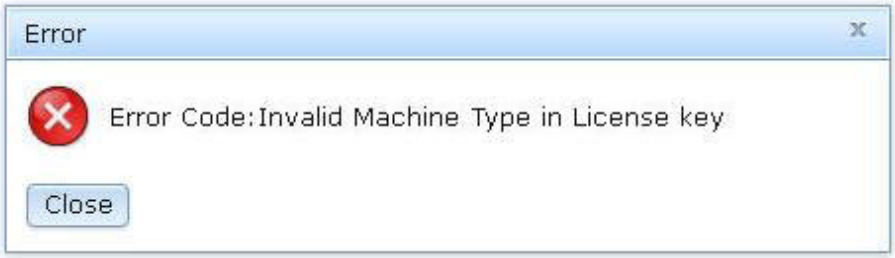


Anmerkung:

- Wenn der Aktivierungsschlüssel nicht gültig ist, wird das folgende Fehlernachrichtenfenster angezeigt.

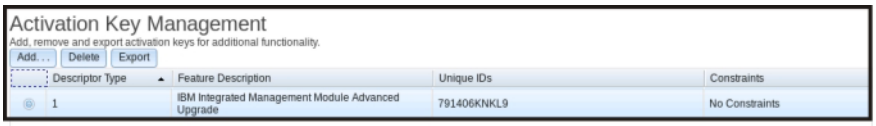


- Wenn Sie versuchen, den Aktivierungsschlüssel auf einem Maschinentyp zu installieren, der die FoD-Funktion nicht unterstützt, wird das folgende Fehlernachrichtenfenster angezeigt.



5. Klicken Sie auf **OK**, um das Fenster "Success" zu schließen.

   Der ausgewählte Aktivierungsschlüssel wird zum Server hinzugefügt und erscheint auf der Seite "Activation Key Management".

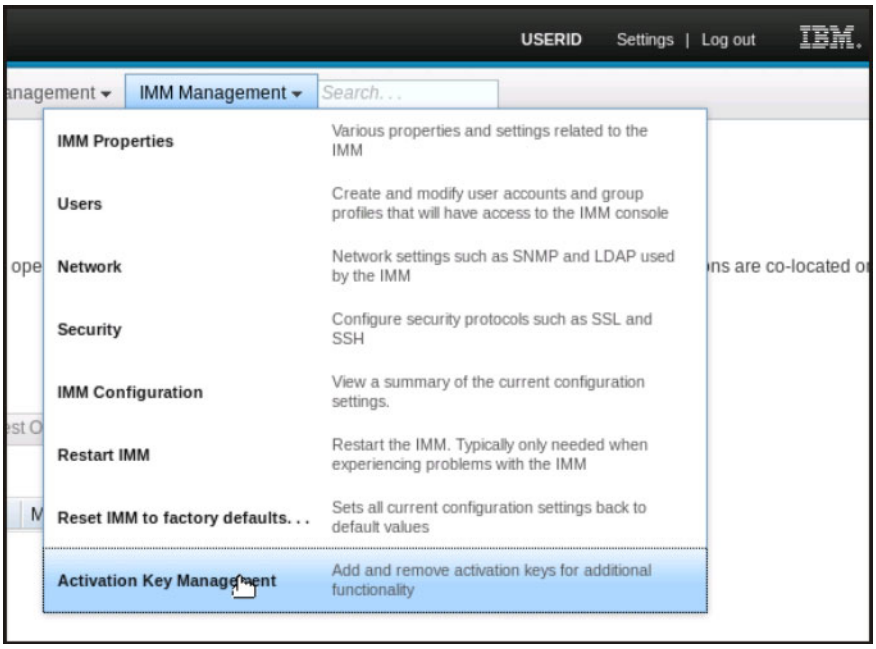


Aktivierungsschlüssel entfernen

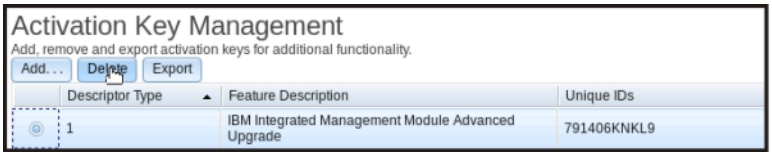
Sie können einen FoD-Aktivierungsschlüssel entfernen, um eine Zusatzfunktion auf Ihrem Server zu löschen.

Gehen Sie wie folgt vor, um einen FoD-Aktivierungsschlüssel zu entfernen:

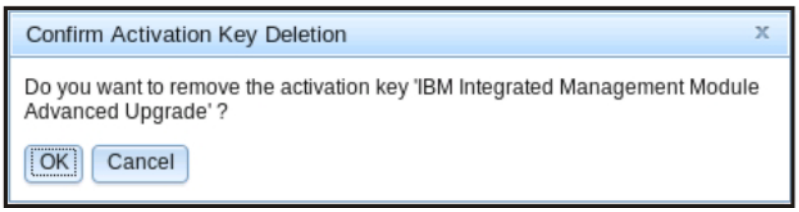
1. Melden Sie sich am IMM2 an. Weitere Informationen hierzu finden Sie im Abschnitt „Am IMM2 anmelden" auf Seite 10.
2. Klicken Sie in der IMM2-Webschnittstelle auf die Registerkarte **IMM Management** (IMM-Verwaltung). Klicken Sie anschließend auf **Activation Key Management** (Aktivierungsschlüsselverwaltung).



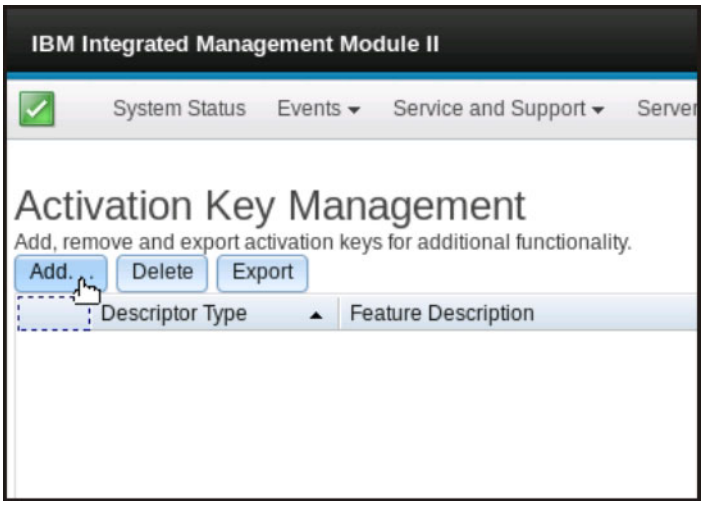
3. Wählen Sie auf der Seite "Activation Key Management" den Aktivierungsschlüssel aus, den Sie entfernen möchten. Klicken Sie anschließend auf **Delete** (Löschen).



4. Klicken Sie im Fenster "Confirm Activation Key Deletion" (Löschen des Aktivierungsschlüssels bestätigen) auf **OK**, um das Löschen des Aktivierungsschlüssels zu bestätigen, oder klicken Sie auf **Cancel**, um die Schlüsseldatei zu behalten.



Der ausgewählte Aktivierungsschlüssel wird vom Server entfernt und nicht mehr auf der Seite "Activation Key Management" angezeigt.

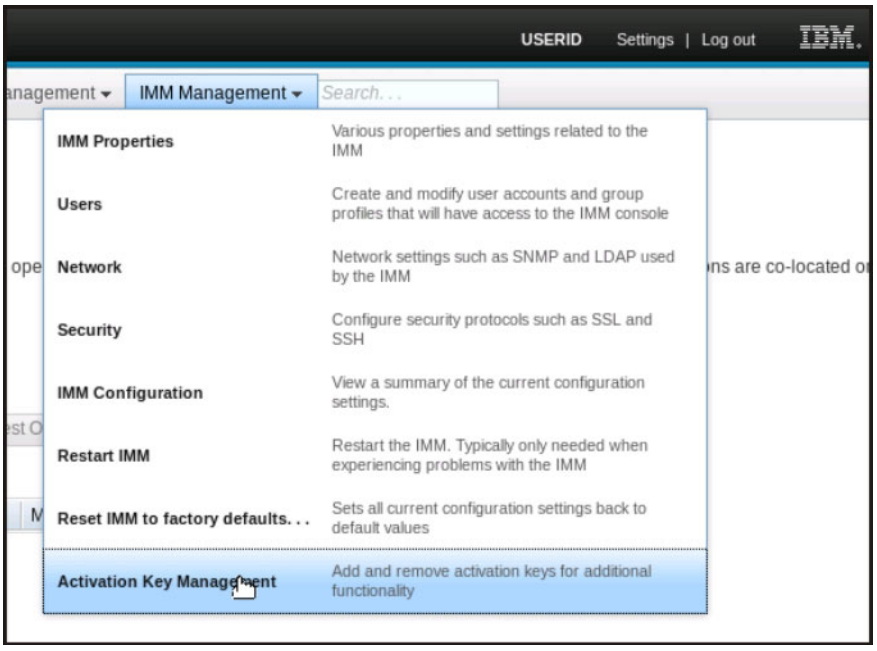


Aktivierungsschlüssel exportieren

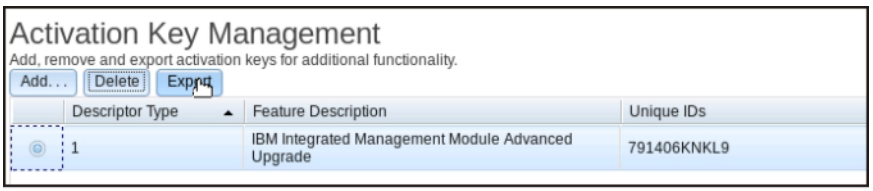
Sie können einen FoD-Aktivierungsschlüssel exportieren, um eine Zusatzfunktion vom Server zu exportieren.

Gehen Sie wie folgt vor, um einen FoD-Aktivierungsschlüssel zu exportieren:

1. Melden Sie sich am IMM2 an. Weitere Informationen hierzu finden Sie im Abschnitt „Am IMM2 anmelden" auf Seite 10.
2. Klicken Sie in der IMM2-Webschnittstelle auf die Registerkarte **IMM Management** (IMM-Verwaltung). Klicken Sie anschließend auf **Activation Key Management** (Aktivierungsschlüsselverwaltung).



3. Wählen Sie auf der Seite "Activation Key Management" den Aktivierungsschlüssel aus, den Sie exportieren möchten. Klicken Sie anschließend auf **Export** (Exportieren).



4. Klicken Sie im Fenster "Confirm Activation Key Export" (Export des Aktivierungsschlüssels bestätigen) auf **OK**, um das Exportieren des Aktivierungsschlüssels zu bestätigen, oder klicken Sie auf **Cancel** (Abbrechen), um das Exportieren des Schlüssels abzubrechen.

5. Wählen Sie das Speicherverzeichnis für die Datei aus. Der ausgewählte Aktivierungsschlüssel wird vom Server exportiert.

Kapitel 8. Befehlszeilenschnittstelle

Verwenden Sie die IMM2-Befehlszeilenschnittstelle (CLI) für den Zugriff auf das IMM2, ohne die Webschnittstelle verwenden zu müssen. Diese Schnittstelle stellt einen Teil der Managementfunktionen bereit, die von der Webschnittstelle bereitgestellt werden.

Sie können über eine Telnet- oder eine SSH-Sitzung auf die Befehlszeilenschnittstelle zugreifen. Bevor Sie CLI-Befehle absetzen können, müssen Sie durch das IMM2 authentifiziert werden.

IMM2 mit IPMI verwalten

Anfangs ist beim IMM2 die Benutzer-ID 1 auf den Benutzernamen "USERID" und das Kennwort "PASSW0RD" (mit einer Null anstelle des Buchstabens "O") eingestellt. Dieser Benutzer hat Administratorzugriff.

Wichtig: Ändern Sie für größere Sicherheit diesen Benutzernamen und das zugehörige Kennwort bei der Erstkonfiguration.

Das IMM2 bietet außerdem die folgenden IPMI-Funktionen (Intelligent Peripheral Management Interface) zur Verwaltung ferner Server:

Befehlszeilenschnittstellen
Die Befehlszeilenschnittstelle gewährt durch das IPMI 2.0-Protokoll direkten Zugriff auf Serververwaltungsfunktionen. Sie können IPMItool verwenden, um Befehle zum Steuern der Stromversorgung am Server, zum Anzeigen von Serverinformationen und zum Identifizieren des Servers auszugeben. Weitere Informationen zu IPMItool finden Sie im Abschnitt „IPMItool verwenden".

Serial over LAN
Verwenden Sie zum Verwalten von Servern von einem fernen Standort aus IPMItool, um eine SOL-Verbindung (Serial over LAN) herzustellen. Weitere Informationen zu IPMItool finden Sie im Abschnitt „IPMItool verwenden".

IPMItool verwenden

IPMItool bietet diverse Tools, die Sie zum Verwalten und Konfigurieren eines IPMI-Systems verwenden können. Sie können IPMItool intern oder extern verwenden, um das IMM2 zu verwalten und zu konfigurieren.

Gehen Sie für weitere Informationen zu IPMItool oder zum Herunterladen von IPMItool auf http://sourceforge.net/.

Zugriff auf die Befehlszeilenschnittstelle

Um auf die Befehlszeilenschnittstelle zuzugreifen, starten Sie eine Telnet- oder SSH-Sitzung mit der IP-Adresse des IMM2 (weitere Informationen hierzu finden Sie im Abschnitt „Seriell-zu-Telnet- oder -SSH-Umleitung konfigurieren" auf Seite 150).

Anmeldung an der Befehlszeilensitzung

Gehen Sie wie folgt vor, um sich an der Befehlszeile anzumelden:

1. Stellen Sie eine Verbindung mit dem IMM2 her.
2. Wenn Sie nach dem Benutzernamen gefragt werden, geben Sie die Benutzer-ID ein.
3. Wenn Sie nach dem Kennwort gefragt werden, geben Sie das Kennwort ein, das Sie zur Anmeldung am IMM2 verwenden.

   Sie werden an der Befehlszeile angemeldet. Die Befehlszeilenaufforderung lautet `system>`. Die Befehlszeilensitzung wird aufrechterhalten, bis Sie in der Befehlszeile `exit` (Verlassen) eingeben. Dann werden Sie abgemeldet und die Sitzung wird beendet.

Seriell-zu-Telnet- oder -SSH-Umleitung konfigurieren

Die Seriell-zu-Telnet- oder -SSH-Umleitung ermöglicht es einem Systemadministrator, das IMM2 als seriellen Terminal-Server zu verwenden. Auf einen seriellen Serveranschluss kann ein Zugriff von eine Telnet- oder SSH-Verbindung aus erfolgen, wenn die serielle Umleitung aktiviert ist.

Anmerkungen:

1. Das IMM2 ermöglicht maximal zwei geöffnete Telnet-Sitzungen gleichzeitig. Über die beiden Telnet-Sitzungen kann unabhängig voneinander ein Zugriff auf die seriellen Anschlüsse erfolgen, sodass mehrere Benutzer einen umgeleiteten seriellen Anschluss gleichzeitig anzeigen können.
2. Mit dem Befehl **console 1** für die Befehlszeilenschnittstelle wird eine Sitzung für serielle Umleitung mit dem COM-Anschluss gestartet.

Beispielsitzung

```
telnet 192.168.70.125 (Press Enter.)
Connecting to 192.168.70.125... username: USERID (Press Enter.)
password: ******** (Press Enter.)
system> console 1 (Press Enter.)
```

Der gesamte Datenverkehr von COM2 wird nur zur Telnet-Sitzung umgeleitet. Der gesamte Datenverkehr von der Telnet- oder SSH-Sitzung wird zu COM2 umgeleitet.

```
ESC (
```

Geben Sie die Tastenkombination zum Beenden ein, um zur Befehlszeilenschnittstelle zurückzukehren. In diesem Beispiel drücken Sie die Taste "Esc" und geben dann eine linke Klammer ein. Die Eingabeaufforderung der Befehlszeilenschnittstelle erscheint und gibt an, dass Sie zur Befehlszeilenschnittstelle des IMM2 zurückgekehrt sind.

```
system>
```

Befehlssyntax

Lesen Sie die folgenden Richtlinien, bevor Sie die Befehle verwenden:

- Jeder Befehl weist das folgende Format auf:

  `Befehl [`*`Argumente`*`] [-`*`Optionen`*`]`
- In der Befehlssyntax muss die Groß-/Kleinschreibung beachtet werden.
- Der Befehlsname wird in Kleinbuchstaben angegeben.

- Alle Argumente müssen direkt auf den Befehl folgen. Die Optionen wiederum folgen direkt auf die Argumente.
- Vor jeder Option steht ein Bindestrich (-). Eine Option kann als Kurzoption (ein einzelner Buchstabe) oder als Langoption (mehrere Buchstaben) angegeben werden.
- Wenn eine Option ein Argument aufweist, ist dieses Argument obligatorisch. Beispiel:

  ```
  ifconfig eth0 -i 192.168.70.34 -g 192.168.70.29 -s 255.255.255.0
  ```

  Dabei ist **ifconfig** der Befehl, "eth0" ist ein Argument und "-i", "-g" und "-s" sind Optionen. In diesem Beispiel weisen alle drei Optionen Argumente auf.
- Eckige Klammern geben an, dass ein Argument oder eine Option optional ist. Dabei sind die eckigen Klammern nicht Teil des Befehls, den Sie eingeben.

Merkmale und Einschränkungen

Die Befehlszeilenschnittstelle weist folgende Merkmale und Einschränkungen auf:

- Mehrere gleichzeitige Befehlszeilenschnittstellensitzungen sind mit verschiedenen Zugriffsmethoden (Telnet oder SSH) zulässig. Es können höchstens zwei Telnet-Befehlszeilensitzungen gleichzeitig aktiv sein.

  Anmerkung: Die Anzahl der Telnet-Sitzung ist konfigurierbar. Gültige Werte sind 0, 1 und 2. Der Wert 0 bedeutet, dass die Telnet-Schnittstelle inaktiviert ist.
- Es ist ein Befehl pro Zeile zulässig (maximal 160 Zeichen, einschließlich Leerzeichen).
- Für lange Befehle gibt es kein Fortsetzungszeichen. Die einzige Editierfunktion ist die Rückschritttaste, mit der Sie das zuvor eingegebene Zeichen löschen können.
- Sie können die Aufwärts- und die Abwärtspfeiltaste verwenden, um durch die letzten acht Befehle zu blättern. Mit dem Befehl **history** können Sie eine Liste der letzten acht Befehle anzeigen, die sie anschließend als Direktaufruf zum Ausführen eines Befehls verwenden können, wie im folgenden Beispiel dargestellt:

  ```
  system> history
   0 ifconfig eth0
   1 readlog
   2 readlog
   3 readlog
   4 history
  system> !0
  -state enabled
  -c dthens
  -i 192.168.70.125
  -g 0.0.0.0
  -s 255.255.255.0
  -n IMM2A00096B9E003A
  -r auto
  -d auto
  -m 1500
  -b 00:09:6B:9E:00:3A
  -l 00:00:00:00:00:00
  system>
  ```
- In der Befehlszeilenschnittstelle liegt der Ausgabepuffergrenzwert bei 2 KB. Es gibt keine Pufferung. Die Ausgabe eines einzelnen Befehls darf 2048 Zeichen nicht überschreiten. Dieser Grenzwert gilt nicht im Modus für serielle Umleitung (die Daten werden bei der seriellen Umleitung gepuffert).
- Die Ausgabe eines Befehls erscheint in der Anzeige, nachdem die Ausführung des Befehls beendet ist. Dadurch ist es für Befehle unmöglich, den Echtzeitaus-

führungsstatus zu melden. Beispiel: Im ausführlichen Modus des Befehls **flashing** wird der Vorgang des Blinkens nicht in Echtzeit angezeigt. Er wird erst angezeigt, nachdem die Befehlsausführung beendet ist.

- Der Befehlsausführungsstatus wird durch einfache Textnachrichten angegeben, wie im folgenden Beispiel dargestellt:

```
system> power on
ok
system> power state
Power: On
State: System power off/State unknown
system>
```

- In der Befehlssyntax muss die Groß-/Kleinschreibung beachtet werden.
- Zwischen einer Option und dem zugehörigen Argument muss mindestens ein Leerzeichen stehen. Im Beispiel `ifconfig eth0 -i192.168.70.133` ist die Befehlssyntax falsch. Die richtige Syntax lautet `ifconfig eth0 -i 192.168.70.133`.
- Alle Befehle verfügen über die Optionen `-h, -help` und `?`, mit denen Hilfe zur Syntax angezeigt werden kann. Alle der folgenden Beispiele haben dasselbe Ergebnis:

```
system> power -h
system> power -help
system> power ?
```

- Einige der Befehle, die in den folgenden Abschnitten beschrieben werden, sind möglicherweise für Ihre Systemkonfiguration nicht verfügbar. Um eine Liste der von Ihrer Konfiguration unterstützten Befehle anzuzeigen, verwenden Sie die Hilfsoption oder die Option "?", wie in den folgenden Beispielen dargestellt:

```
system> help
system> ?
```

Alphabetische Befehlsliste

Die vollständige Liste aller Befehle der IMM2-Befehlszeilenschnittstelle in alphabetischer Reihenfolge lautet wie folgt:

Dienstprogrammbefehle

Folgende Dienstprogrammbefehle sind verfügbar:

Befehl "exit"

Mit dem Befehl **exit** können Sie sich abmelden und die Sitzung der Befehlszeilenschnittstelle beenden.

Befehl "help"

Mit dem Befehl **help** können Sie eine Liste aller Befehle und eine Kurzbeschreibung zu den einzelnen Befehlen anzeigen. Sie können auch **?** an der Eingabeaufforderung eingeben.

Befehl "history"

Mit dem Befehl **history** können Sie eine indexierte Protokollliste der letzten acht Befehle anzeigen, die ausgegeben wurden. Die Indizes können dann als Direktaufrufe (mit davor stehendem !) verwendet werden, um die Befehle aus dieser Protokollliste erneut auszugeben.

Beispiel:

```
system> history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMM2A00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system>
```

Überwachungsbefehle

Folgende Überwachungsbefehle sind verfügbar:

- „Befehl "clearlog"“
- „Befehl "fans"“ auf Seite 155
- „Befehl "ffdc"“ auf Seite 155
- „Befehl "led"“ auf Seite 156
- „Befehl "readlog"“ auf Seite 158
- „Befehl "show"“ auf Seite 159
- „Befehl "syshealth"“ auf Seite 159
- „Befehl "temps"“ auf Seite 159
- „Befehl "volts"“ auf Seite 160
- „Befehl "vpd"“ auf Seite 160

Befehl "clearlog"

Mit dem Befehl **clearlog** können Sie das Ereignisprotokoll des IMM2 löschen. Um diesen Befehl verwenden zu können, müssen Sie über die Berechtigung zu Löschen von Ereignisprotokollen verfügen.

Befehl "fans"

Mit dem Befehl **fans** können Sie die Geschwindigkeit der einzelnen Serverlüfter anzeigen.

Beispiel:

```
system> fans
fan1 75%
fan2 80%
fan3 90%
system>
```

Befehl "ffdc"

Verwenden Sie den Befehl **ffdc** (first failure data capture, Erfassung von Fehlerdaten beim ersten Auftreten), um Servicedaten zu generieren und an den IBM Support zu übertragen.

Die folgende Liste enthält Befehle, die zusammen mit dem Befehl **ffdc** verwendet werden können:

- **generate** erstellt eine neue Servicedatendatei
- **status** überprüft den Status der Servicedatendatei
- **copy** kopiert die vorhandenen Servicedaten
- **delete** löscht die vorhandenen Servicedaten

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-t	Typennummer	1 (Prozessorspeicherauszug) und 4 (Servicedaten). Der Standardwert ist 1.
-f [1]	Name der fernen Datei oder des SFTP-Zielverzeichnisses.	Verwenden Sie für SFTP den vollständigen Pfad oder einen abschließenden Schrägstrich (/) für den Verzeichnisnamen (~/ oder /tmp/). Der Standardwert ist der vom System generierte Name.
--ip [1]	Adresse des TFTP/SFTP-Servers.	
-pn [1]	Portnummer des TFTP/SFTP-Servers.	Der Standardwert ist 69/22.
-u [1]	Benutzername für den SFTP-Server.	
-pw [1]	Kennwort für den SFTP-Server.	
1. Zusätzliches Argument für die Befehle **generate** und **copy**		

Syntax:

```
ffdc [Optionen]
Option:
  -t 1 oder 4
  -f  -ip IP-Adresse
  -pn Portnummer
  -u Benutzername
  -pw Kennwort
```

Beispiel:

```
system> ffdc generate
Generating ffdc...
system> ffdc status
Type 1 ffdc: in progress
system> ffdc copy -t 1 -ip 192.168.70.230 -u User2 -pw Passw0rd -f /tmp/
Waiting for ffdc.....
Copying ffdc...
ok
system> ffdc status
Type 1 ffdc: completed
8737AC1_DSY0123_imm2_120317-153327.tgz
```

```
system> ffdc generate
Generating ffdc...
system> ffdc status
Type 1 ffdc: in progress
system> ffdc status
Type 1 ffdc: in progress
system> ffdc copy -ip 192.168.70.230
Copying ffdc...
ok
system> ffdc status
Type 1 ffdc: completed
8737AC1_DSY0123_imm2_120926-105320.tgz
system>
```

Befehl "led"

Verwenden Sie den Befehl **led**, um den Zustand von Anzeigen anzuzeigen und festzulegen.

- Wird der Befehl **led** ohne Optionen ausgeführt, so wird der Status von Anzeigen im Bedienfeld angezeigt.
- Die Befehlsoption **led -d** muss gemeinsam mit der Befehlsoption **led -identify on** angewendet werden.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-l	Den Status aller Anzeigen auf dem System und dessen Unterkomponenten abrufen	
-chklog	Anzeige für Prüfprotokoll ausschalten	off
-identify	Zustand der Gehäusebestimmungsanzeige ändern	off, on, blink
-d	Identifikationsanzeige für einen angegebenen Zeitraum einschalten	Zeitraum (Sekunden)

Syntax:

```
led [Optionen]
Option:
  -l  -chklog off
  -identify Zustand
  -d Zeit
```

Beispiel:

```
system> led
Fault                Off
Identify             On            Blue
Chklog               Off
Power                Off

system> led -l
Label                Location                 State         Color
Battery              Planar                   Off
BMC Heartbeat        Planar                   Blink         Green
BRD                  Lightpath Card           Off
Channel A            Planar                   Off
Channel B            Planar                   Off
Channel C            Planar                   Off
Channel D            Planar                   Off
Channel E            Planar                   Off
Chklog               Front Panel              Off
CNFG                 Lightpath Card           Off
CPU                  Lightpath Card           Off
CPU 1                Planar                   Off
CPU 2                Planar                   Off
DASD                 Lightpath Card           Off
DIMM                 Lightpath Card           Off
DIMM 1               Planar                   Off
DIMM 10              Planar                   Off
DIMM 11              Planar                   Off
DIMM 12              Planar                   Off
DIMM 13              Planar                   Off
DIMM 14              Planar                   Off
DIMM 15              Planar                   Off
DIMM 16              Planar                   Off
DIMM 2               Planar                   Off
DIMM 3               Planar                   Off
DIMM 4               Planar                   Off
DIMM 5               Planar                   Off
DIMM 6               Planar                   Off
DIMM 7               Planar                   Off
DIMM 8               Planar                   Off
DIMM 9               Planar                   Off
FAN                  Lightpath Card           Off
FAN 1                Planar                   Off
FAN 2                Planar                   Off
FAN 3                Planar                   Off
Fault                Front Panel (+)          Off
Identify             Front Panel (+)          On            Blue
LINK                 Lightpath Card           Off
LOG                  Lightpath Card           Off
NMI                  Lightpath Card           Off
OVER SPEC            Lightpath Card           Off
PCI 1                FRU                      Off
PCI 2                FRU                      Off
PCI 3                FRU                      Off
PCI 4                FRU                      Off
Planar               Planar                   Off
Power                Front Panel (+)          Off
PS                   Lightpath Card           Off
RAID                 Lightpath Card           Off
Riser 1              Planar                   Off
Riser 2              Planar                   Off
SAS ERR              FRU                      Off
SAS MISSING          Planar                   Off
SP                   Lightpath Card           Off
TEMP                 Lightpath Card           Off
VRM                  Lightpath Card           Off
system>
```

Befehl "readlog"

Mit dem Befehl **readlog** können Sie jeweils fünf IMM2-Ereignisprotokolleinträge anzeigen. Die Einträge werden in der Reihenfolge vom aktuellsten bis zum ältesten Eintrag angezeigt.

readlog zeigt die ersten fünf Einträge im Ereignisprotokoll an, angefangen mit dem aktuellsten Eintrag (bei seiner ersten Ausführung), und dann die nächsten fünf für jeden nachfolgenden Aufruf.

readlog -a zeigt alle Einträge im Ereignisprotokoll an, angefangen mit dem aktuellsten Eintrag.

readlog -f setzt den Zähler zurück und zeigt die ersten fünf Einträge im Ereignisprotokoll an, angefangen mit dem aktuellsten Eintrag.

readlog -date ***date*** zeigt Ereignisprotokolleinträge für das angegebene Datum im Format mm/tt/jj an. Es kann sich um eine Liste handeln, in der die einzelnen Datumsangaben durch ein Pipe-Zeichen (|) voneinander getrennt sind.

readlog -sev ***severity*** zeigt Ereignisprotokolleinträge des angegebenen Schweregrades an (E, W, I). Es kann sich um eine Liste handeln, in der die einzelnen Schweregrade durch ein Pipe-Zeichen (|) voneinander getrennt sind.

readlog -i ***ip_address*** legt die IPv4- oder die IPv6-IP-Adresse des TFTP- oder SFTP-Servers fest, auf dem das Ereignisprotokoll gespeichert wird. Die Befehlsoptionen **-i** und **-l** werden gemeinsam verwendet, um den Standort anzugeben.

readlog -l ***filename*** legt den Dateinamen der Ereignisprotokolldatei fest. Die Befehlsoptionen **-i** und **-l** werden gemeinsam verwendet, um den Standort anzugeben.

readlog -pn ***port_number*** zeigt die Portnummer des TFTP- oder SFTP-Servers an oder legt sie fest (Standard: 69/22).

readlog -u ***username*** gibt den Benutzernamen für den SFTP-Server an.

readlog -pw ***password*** gibt das Kennwort für den SFTP-Server an.

Syntax:

```
readlog [Optionen]
Option:
  -a  -f  -date Datum
  -sev Schweregrad
  -i IP-Adresse
  -l Dateiname
  -pn Portnummer
  -u Benutzername
  -pw Kennwort
```

Beispiel:

```
system> readlog -f
1 I SERVPROC 12/18/03 10:18:58 Remote Login Successful.
Login ID:''USERID' CLI authenticated from 192.168.70.231 (Telnet).'
2 I SERVPROC 12/18/03 10:12:22 Remote Login successful.
Login ID: ''USERID' from web browser at IP@=192.168.70.231'
3 E SERVPROC 12/18/03 10:10:37 Failure reading I2C device.
4 E SERVPROC 12/18/03 10:10:37 Environmental monitor not responding.
5 E SERVPROC 12/18/03 10:10:37 Failure reading I2C device.
system> readlog
6 E SERVPROC 12/18/03 10:09:31 Fan 2 Fault. Multiple fan failures
7 E SERVPROC 12/18/03 10:09:31 Fan 1 Fault. Single fan failure
8 I SERVPROC 12/18/03 10:09:25 Ethernet[0] Link Established at 100Mb, Full Duplex.
```

```
9 I SERVPROC 12/18/03 10:09:24 Ethernet[0] configured to do Auto Speed/Auto Duplex.
10 I SERVPROC 12/18/03 10:09:24 Ethernet[0] MAC Address currently
being used: 0x00-09-6B-CA-0C-80
system>
```

Befehl "show"

Mit dem Befehl **show** können Sie einfache Einstellungen des IMM2 anzeigen.

- Mit dem Befehl **show** werden über den Befehl **set** festgelegte Werte angezeigt.
- Einstellungen sind wie in einer Verzeichnisbaumstruktur angeordnet. Verwenden Sie die Befehlsoption **show -r**, um die vollständige Verzeichnisstruktur anzuzeigen.
- Manche dieser Einstellungen, etwa Umgebungsvariablen, werden vom CLI verwendet.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
value	Anzuzeigender Pfadwert oder Einstellungswert	
-r	Einstellungen rekursiv anzeigen	

Syntax:

```
show [Optionen]
Option:
  value
  -r
```

Befehl "syshealth"

Mit dem Befehl **syshealth** können Sie eine Zusammenfassung des Serverzustands anzeigen. Es werden der Stromversorgungsstatus, der Systemstatus, der Zähler für den Neustart und der Status der IMM2-Software angezeigt.

Beispiel:

```
system> syshealth
Power On
State System on/starting UEFI
Restarts 71
system>
```

Befehl "temps"

Mit dem Befehl **temps** können Sie alle Temperaturwerte und Temperaturschwellenwerte anzeigen. Dieselben Temperaturwerte werden auch in der Webschnittstelle angezeigt.

Beispiel:

```
system> temps
Temperatures are displayed in degrees Fahrenheit/Celsius
        WR      W       T      SS      HS
---------------------------------------
CPU1   65/18  72/22  80/27  85/29  90/32
```

```
CPU2   58/14  72/22  80/27  85/29  90/32
DASD1  66/19  73/23  82/28  88/31  92/33
Amb    59/15  70/21  83/28  90/32  95/35
system>
```

Anmerkungen:

1. Die Ausgabe weist die folgenden Spaltenüberschriften auf:
   WR: Warnungzurücksetzung
   W: Warnung
   T: Temperatur (aktueller Wert)
   SS: Normaler Systemabschluss
   HS: Erzwungener Systemabschluss
2. Alle Temperaturwerte sind in Grad Fahrenheit/Grad Celsius angegeben.

Befehl "volts"

Mit dem Befehl **volts** können Sie alle Spannungswerte und Spannungsschwellenwerte anzeigen. Dieselben Spannungswerte werden auch in der Webschnittstelle angezeigt.

Beispiel:

```
system> volts
      HSL   SSL   WL    WRL   V     WRH   WH   SSH    HSH
-------------------------------------------------------------
5v    5.02  4.00  4.15  4.50  4.60  5.25  5.50  5.75  6.00
3.3v  3.35  2.80  2.95  3.05  3.10  3.50  3.65  3.70  3.85
12v   12.25 11.10 11.30 11.50 11.85 12.15 12.25 12.40 12.65
-5v   -5.10 -5.85 -5.65 -5.40 -5.20 -4.85 -4.65 -4.40 -4.20
-3.3v -3.35 -4.10 -3.95 -3.65 -3.50 -3.10 -2.95 -2.80 -2.70
VRM1                        3.45
VRM2                        5.45
system>
```

Anmerkung: Die Ausgabe weist die folgenden Spaltenüberschriften auf:

HSL: Erzwungener Systemabschluss (Unterspannung)
SSL: Normaler Systemabschluss (Unterspannung)
WL: Warnung (Unterspannung)
WRL: Warnungszurücksetzung (Unterspannung)
V: Spannung (aktueller Wert)
WRH: Warnungszurücksetzung (Überspannung)
WH: Warnung (Überspannung)
SSH: Normaler Systemabschluss (Überspannung)
HSH: Erzwungener Systemabschluss (Überspannung)

Befehl "vpd"

Mit dem Befehl **vpd** können Sie elementare Produktdaten für das System (sys), das IMM2 (imm), das Server-BIOS (uefi), Dynamic System Analysis Preboot des Servers (dsa), die Server-Firmware (fw) und die Serverkomponenten (comp) anzeigen. Dieselben Informationen werden auch in der Webschnittstelle angezeigt.

Syntax:

```
vpd [Optionen]
Option:
  -sys
```

```
-imm
-uefi
-dsa
-fw
-comp
```

Verwenden Sie den Befehl "vpd", um elementare Produktdaten für verschiedene Komponenten des Servers anzuzeigen.

Option	Beschreibung
-sys	zeigt elementare Produktdaten für das System an
-imm	zeigt elementare Produktdaten für den IMM2-Controller an
-uefi	zeigt elementare Produktdaten für das BIOS an
-dsa	zeigt elementare Produktdaten für die Diagnose an
-fw	zeigt elementare Produktdaten für die Systemfirmware an
-comp	zeigt elementare Produktdaten für die Systemkomponenten an

Beispiel:

```
system> vpd -dsa
Type     Version      Build     ReleaseDate
----     -------      -----     ------
DSA      9,25         DSYTA5A   2012/07/31
system>
```

Steuerbefehle für Serverstromversorgung und -neustart

Folgende Befehle für Serverstromversorgung und -neustart sind verfügbar:

- „Befehl "power"“
- „Befehl "pxeboot"“ auf Seite 162
- „Befehl "reset"“ auf Seite 162

Befehl "power"

Mit dem Befehl **power** können Sie die Stromversorgung des Servers steuern. Um die Befehle vom Typ **power** ausgeben zu können, müssen Sie über eine Zugriffsberechtigung für Stromversorgung und Neustarts verfügen.

power on - Die Serverstromversorgung wird eingeschaltet.

power off - Die Serverstromversorgung wird ausgeschaltet. Mit der Option **-s** wird das Betriebssystem heruntergefahren, bevor der Server ausgeschaltet wird.

power state - Zeigt den Serverstromversorgungszustand (on oder off) und den aktuellen Zustand des Servers an.

power cycle - Schaltet die Serverstromversorgung zunächst aus und dann wieder ein. Mit der Option **-s** wird das Betriebssystem heruntergefahren, bevor der Server ausgeschaltet wird.

Syntax:

```
power on
power off [-s]
power state
power cycle [-s]
```

Befehl "pxeboot"

Mit dem Befehl **pxeboot** können Sie die Bedingung für die Ausführungsumgebung vor dem Starten (Preboot eXecution Environment - PXE) anzeigen und einstellen.

Wird **pxeboot** ohne Optionen ausgeführt, so wird auf die aktuelle PXE-Einstellung zurückgegriffen. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-en	Legt die PXE-Bedingung für den nächsten Systemwiederanlauf fest	enabled, disabled

Syntax:

```
pxeboot [Optionen]
Option:
  -en Zustand
```

Beispiel:

```
system> pxeboot
-en disabled
system>
```

Befehl "reset"

Mit dem Befehl **reset** können Sie den Server erneut starten. Um diesen Befehl ausgeben zu können, müssen Sie über eine Zugriffsberechtigung für Stromversorgung und Neustarts verfügen. Mit der Option **-s** wird das Betriebssystem heruntergefahren, bevor der Server erneut gestartet wird.

Syntax:

```
reset [Option]
Option:
-s
```

Befehl zur seriellen Umleitung

Es gibt einen Befehl zur seriellen Umleitung: den „Befehl "console"“.

Befehl "console"

Mit dem Befehl **console** können Sie eine Konsolensitzung mit serieller Umleitung zum designierten seriellen Anschluss des IMM2 starten.

Syntax:

```
console 1
```

Konfigurationsbefehle

Folgende Konfigurationsbefehle sind verfügbar:

- „Befehl "accseccfg"“ auf Seite 163
- „Befehl "alertcfg"“ auf Seite 165
- „Befehl "asu"“ auf Seite 166
- „Befehl "backup"“ auf Seite 169

Befehl "accseccfg"

Mit dem Befehl **accseccfg** können Sie Kontosicherheitseinstellungen anzeigen und konfigurieren.

Wird der Befehl **accseccfg** ohne Optionen ausgeführt, so werden alle Informationen zur Kontensicherheit angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-legacy	Legt für die Accountsicherheit eine vordefinierte Gruppe von traditionellen Standardwerten fest.	
-high	Legt für die Accountsicherheit eine vordefinierte Gruppe von hohen Standardwerten fest.	
-custom	Stellt Kontosicherheit auf benutzerdefinierte Werte ein	

Option	Beschreibung	Werte
-am	Legt Benutzerauthentifizierungsverfahren fest	local, ldap, localldap, ldaplocal
-lp	Aussperrungszeit nach erreichter Höchstzahl an Anmeldefehlern (Minuten)	0, 1, 2, 5, 10, 15, 20, 30, 60, 120, 180 oder 240 Minuten. Der Standardwert beträgt 60, wenn "High Security" (hohes Sicherheitsniveau) aktiviert ist, und 2, wenn "Legacy Security" (traditionelle Sicherheit) aktiviert ist. Bei einem Wert von 0 wird diese Funktion inaktiviert.
-pe	Zeitraum bis Verfallsdatum des Kennworts (Tage)	0 bis 365 Tage
-pr	Kennwort erforderlich	on, off
-pc	Regeln zur Kennwortkomplexität	on, off
-pd	Mindestanzahl unterschiedlicher Zeichen für ein Kennwort	0 bis 19 Zeichen
-pl	Kennwortlänge	1 bis 20 Zeichen
-ci	Mindestintervall für Kennwortänderung (Stunden)	0 bis 240 Stunden
-lf	Maximale Anzahl an Anmeldefehlern	0 bis 10
-chgdft	Standardkennwort nach erster Anmeldung ändern	on, off
-chgnew	Neues Benutzerkennwort nach erster Anmeldung ändern	on, off
-rc	Wiederverwendungszyklus für Kennwort	0 bis 5
-wt	Sitzungszeitlimit bei Webinaktivität (Minuten)	1, 5, 10, 15, 20, keine Angabe oder 'user'

Syntax:

```
accseccfg [Optionen]
Option:
  -legacy
  -high
  -custom
  -am Authentifizierungsmethode
  -lp Lockout-Zeitraum
  -pe Zeitraum
  -pr Zustand
  -pc Zustand
  -pd Anzahl an Zeichen
  -pl Anzahl an Zeichen
  -ci Mindestintervall
  -lf Anzahl an Fehlern
```

```
  -chgdft Zustand
  -chgnew Zustand
  -rc Wiederverwendungszyklus
  -wt Zeitlimit
```

Beispiel:

```
system> accseccfg
-legacy
-am local
-lp 2
-pe 0
-pr off
-pd 1
-pl 4
-ci 0
-lf 0
-chgdft off
-chgnew off
-rc 0
-wt user
system>
```

Befehl "alertcfg"

Mit dem Befehl **alertcfg** können Sie die Parameter für allgemeine ferne Alerts des IMM2 anzeigen und konfigurieren.

Wird der Befehl **alertcfg** ohne Optionen ausgeführt, so werden alle Parameter für allgemeine ferne Alerts angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-dr	Legt fest, wie viel Zeit zwischen Wiederholungsversuchen liegen soll, bevor das IMM2 erneut einen Alert sendet	Minutenangaben von "0" bis "4.0" (für 4,0 Minuten), in Inkrementen von einer halben Minute
-da	Legt fest, wie viel Zeit vergehen soll, bevor das IMM2 einen Alert an den nächsten Empfänger auf der Liste sendet	Minutenangaben von "0" bis "4.0" (für 4,0 Minuten), in Inkrementen von einer halben Minute
-rl	Legt fest, wie oft das IMM2 zusätzlich versucht, einen Alert zu senden, wenn vorherige Versuche nicht erfolgreich waren	0 bis 8

Syntax:

```
alertcfg [Optionen]
  Optionen:
   -rl Begrenzung_für_Neuversuche
   -dr Verzögerung_vor_Neuversuch
   -da Agentenverzögerung
```

Beispiel:

```
system>alertcfg
-dr 1.0
-da 2.5
-rl 5
system>
```

Befehl "asu"

Befehle des Dienstprogramms für erweiterte Einstellungen werden verwendet, um UEFI-Einstellungen festzulegen. Das Hostsystem muss erneut gestartet werden, damit Änderungen an UEFI-Einstellungen wirksam werden.

Die folgende Tabelle enthält eine Untermenge von Befehlen, die zusammen mit dem Befehl **asu** verwendet werden können.

Tabelle 7. ASU-Befehle

Befehl	Beschreibung	Wert
delete	Verwenden Sie diesen Befehl, um eine Instanz oder einen Datensatz einer Einstellung zu löschen. Bei der Einstellung muss es sich um eine Instanz handeln, für die das Löschen zulässig ist, z. B. "iSCSI.AttemptName.1".	*Einstellung_Instanz*
help	Verwenden Sie diesen Befehl, um Hilfetext zu einer oder mehreren Einstellungen anzuzeigen.	*Einstellung*
set	Verwenden Sie diesen Befehl, um den Wert einer Einstellung zu ändern. Legen Sie als UEFI-Einstellung den Eingabewert fest. **Anmerkungen:** • Legen Sie ein oder mehrere Paare aus Einstellung und Wert fest. • Die Einstellung kann Platzhalterzeichen enthalten, wenn sie für eine einzelne Einstellung gilt. • Der Wert muss in Anführungszeichen gesetzt werden, wenn er Leerzeichen enthält. • Sortierlistenwerte werden durch das Gleichheitszeichen (=) getrennt. Beispiel: set B*.Bootorder "CD/DVD Rom=Hard Disk 0=PXE Network."	*Einstellung Wert*

Tabelle 7. ASU-Befehle (Forts.)

Befehl	Beschreibung	Wert
showgroups	Verwenden Sie diesen Befehl, um die verfügbaren Einstellungsgruppen anzuzeigen. Dieser Befehl zeigt die Namen der bekannten Gruppen an. Gruppennamen können je nach den installierten Einheiten variieren.	*Einstellung*
show	Verwenden Sie diesen Befehl, um den aktuellen Wert einer oder mehrerer Einstellungen anzuzeigen.	*Einstellung*
showvalues	Verwenden Sie diesen Befehl, um alle möglichen Werte für eine oder mehrere Einstellungen anzuzeigen. **Anmerkungen:** • Dieser Befehl zeigt Informationen zu den zulässigen Werten für die Einstellung an. • Die minimale und maximale Anzahl der für diese Einstellung zulässigen Instanzen werden angezeigt. • Der Standardwert wird angezeigt, falls er verfügbar ist. • Der Standardwert steht zwischen einer öffnenden und einer schließenden spitzen Klammer (< und >). • Die Textwerte zeigen die minimale und die maximale Länge sowie den regulären Ausdruck.	*Einstellung*
Anmerkungen: • In der Befehlssyntax ist *Einstellung* der Name einer Einstellung, die Sie anzeigen oder ändern möchten, und *Wert* ist der Wert, den Sie für die Einstellung festlegen. • Für *Einstellung* können mehrere Werte angegeben werden, außer bei Verwendung des Befehls **set**. • Der Wert für *Einstellung* kann Platzhalterzeichen enthalten, z. B. einen Stern (*) oder ein Fragezeichen (?). • Bei *Einstellung* kann es sich um eine Gruppe, einen Einstellungsnamen oder den Wert **all** (alles) handeln.		

In der folgenden Liste sind einige Beispiele für die Befehlssyntax für den Befehl **asu** dargestellt:

- Um alle Befehlsoptionen für den Befehl "asu" anzuzeigen, geben Sie `asu --help` ein.

- Um die ausführliche Hilfe für alle Befehle anzuzeigen, geben Sie `asu -v --help` ein.
- Um die ausführliche Hilfe zu einem Befehl anzuzeigen, geben Sie `asu -v set --help` ein.
- Um einen Wert zu ändern, geben Sie `asu set` *`Wert der Einstellung`* ein.
- Um den aktuellen Wert anzuzeigen, geben Sie `asu show` *`Einstellung`* ein.
- Um Einstellungen im Langformat anzuzeigen, geben Sie `asu show -l -b all` ein.
- Um alle möglichen Werte für eine Einstellung anzuzeigen, geben Sie `asu showvalues` *`Einstellung`* an.

  Beispiel für den Befehl **show values**:

```
system> asu showvalues S*.POST*
SystemRecovery.POSTWatchdogTimer==<Disable>=Enable
SystemRecovery.POSTWatchdogTimerValue=numeric min=5 max=20 step=1 default=5
system>
```

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-b[1]	Im Batchformat anzeigen.	
--help[3]	Befehlssyntax und -optionen anzeigen. Die Option "--help" wird vor den Befehl gesetzt, wie z. B. **asu --help show**.	
--help[3]	Hilfe zum Befehl anzeigen. Die Option "--help" wird hinter den Befehl gesetzt, z. B. **asu show --help**.	
-l[1]	Name der Einstellung im Langformat (Konfigurationsgruppe einschließen).	
-m[1]	Name der Einstellung im Mischformat (Konfigurations-ID verwenden).	
-v[2]	Ausführliche Ausgabe.	

1. Die Optionen "-b", "-l" und "-m" werden nur zusammen mit dem Befehl **show** verwendet.
2. Die Option "-v" wird nur zwischen **asu** und dem Befehl verwendet.
3. Die Option "--help" kann zusammen mit jedem Befehl verwendet werden.

Syntax:

```
asu [Optionen] command
[cmd-Optionen]
Optionen:
   -v ausführliche Ausgabe
   --help Haupthilfetext anzeigen
cmd-Optionen:
   --help Hilfe zum Befehl
```

Anmerkung: Weitere Befehlsoptionen finden Sie bei den einzelnen Befehlen.

Verwenden Sie die asu-Transaktionsbefehle, um mehrere UEFI-Einstellungen festzulegen und um Batchmodusbefehle zu erstellen und auszuführen. Verwenden Sie die Befehle **tropen** und **trset**, um eine Transaktionsdatei, die mehrere Einstellungen enthält, anzuwenden. Eine Transaktion mit einer angegebenen ID wird mit dem Befehl **tropen** geöffnet. Einstellungen werden mithilfe des Befehls **trset** zur Gruppe hinzugefügt. Die abgeschlossene Transaktion wird mithilfe des Befehls **trcommit** festgeschrieben. Wenn Sie mit der Transaktion fertig sind, kann diese mithilfe des Befehls **trrm** gelöscht werden.

Anmerkung: Die Operation zum Wiederherstellen der UEFI-Einstellungen erstellt eine Transaktion mit einer ID unter Verwendung einer willkürlichen dreistelligen Zahl.

Die folgende Tabelle enthält Transaktionsbefehle, die zusammen mit dem Befehl **asu** verwendet werden können.

Tabelle 8. Transaktionsbefehle

Befehl	Beschreibung	Wert
tropen *ID*	Dieser Befehl erstellt eine neue Transaktionsdatei mit mehreren festzulegenden Einstellungen.	*ID* ist die ID-Zeichenfolge aus 1-3 alphanumerischen Zeichen.
trset *ID*	Dieser Befehl fügt eine oder mehrere Einstellungen oder Wertepaare zu einer Transaktion hinzu.	*ID* ist die ID-Zeichenfolge aus 1-3 alphanumerischen Zeichen.
trlist *ID*	Dieser Befehl zeigt zuerst die Inhalte der Transaktionsdatei an. Dies kann hilfreich sein, wenn die Transaktionsdatei in der CLI-Shell erstellt wird.	*ID* ist die ID-Zeichenfolge aus 1-3 alphanumerischen Zeichen.
trcommit *ID*	Dieser Befehl schreibt die Inhalte der Transaktionsdatei fest und führt sie aus. Die Ergebnisse der Ausführung sowie eventuelle Fehler werden angezeigt.	*ID* ist die ID-Zeichenfolge aus 1-3 alphanumerischen Zeichen.
trrm *ID*	Dieser Befehl entfernt die Transaktionsdatei, nachdem sie festgeschrieben wurde.	*ID* ist die ID-Zeichenfolge aus 1-3 alphanumerischen Zeichen.

Beispiel für das Erstellen mehrerer UEFI-Einstellungen:

```
asu tropen TR1
asu trset TR1 UEFI.BootModes.SystemBootMode "UEFI and Legacy"
asu trset TR1 BootOrder.BootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 BootOrder.WolBootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 UEFI.DevicesandIOPorts.Com1BaudRate 115200
asu trset TR1 UEFI.DevicesandIOPorts.Com1DataBits 8
asu trset TR1 UEFI.DevicesandIOPorts.Com1FlowControl Disable
asu trset TR1 UEFI.DevicesandIOPorts.Com1Parity None
asu trset TR1 UEFI.DevicesandIOPorts.Com1StopBits 1
asu trset TR1 UEFI.DevicesandIOPorts.COMPort1 Enable
asu trcommit TR1
```

Befehl "backup"

Mit dem Befehl **backup** können Sie eine Sicherungsdatei mit den aktuellen Systemsicherheitseinstellungen erstellen.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-f	Name der Sicherungsdatei	Gültiger Dateiname
-pp	Kennwort oder Verschlüsselungstext, mithilfe dessen Kennwörter innerhalb der Sicherungsdatei verschlüsselt sind	Gültiges Passwort oder durch Anführungszeichen begrenzter Verschlüsselungstext
-ip	IP-Adresse des TFTP-/SFTP-Servers	Gültige IP-Adresse
-pn	Portnummer des TFTP-/SFTP-Servers	Gültige Portnummer (Standard 69/22)
-u	Benutzername für SFTP-Server	Gültiger Benutzername
-pw	Kennwort für SFTP-Server	Gültiges Kennwort
-fd	Dateiname für die XML-Beschreibung von CLI-Sicherungsbefehlen	Gültiger Dateiname

Syntax:

```
backup [Optionen]
Option:
  -f Dateiname
  -pp Kennwort
  -ip IP-Adresse
  -pn Portnummer
  -u Benutzername
  -pw Kennwort
  -fd Dateiname
```

Beispiel:

```
system> backup –f imm-back.cli –pp xxxxxx –ip 192.168.70.200
ok
system>
```

Befehl "dhcpinfo"

Mit dem Befehl **dhcpinfo** können Sie die durch den DHCP-Server zugeordnete IP-Konfiguration für eth0 anzeigen, wenn die Schnittstelle automatisch durch einen DHCP-Server konfiguriert wird. Mit dem Befehl **ifconfig** können Sie DHCP aktivieren oder inaktivieren.

Syntax:

```
dhcpinfo eth0
```

Beispiel:

```
system> dhcpinfo eth0

-server : 192.168.70.29
-n     : IMM2A-00096B9E003A
-i     : 192.168.70.202
```

```
-g     : 192.168.70.29
-s     : 255.255.255.0
-d     : linux-sp.raleigh.ibm.com
-dns1   : 192.168.70.29
-dns2   : 0.0.0.0
-dns3   : 0.0.0.0
-i6    : 0::0
-d6    : *
-dns61  : 0::0
-dns62  : 0::0
-dns63  : 0::0
system>
```

In der folgenden Tabelle wird die Ausgabe dieses Beispiels beschrieben.

Option	Beschreibung
-server	DHCP-Server, der die Konfiguration zugeordnet hat
-n	Zugeordneter Hostname
-i	Zugeordnete IPv4-Adresse
-g	Zugeordnete Gateway-Adresse
-s	Zugeordnete Teilnetzmaske
-d	Zugeordneter Domänenname
-dns1	Primäre IP-Adresse des IPv4-DNS-Servers
-dns2	Sekundäre IPv4-DNS-IP-Adresse
-dns3	Tertiäre IP-Adresse des IPv4-DNS-Servers
-i6	IPv6-Adresse
-d6	IPv6-Domänenname
-dns61	Primäre IP-Adresse des IPv6-DNS-Servers
-dns62	Sekundäre IPv6-DNS-IP-Adresse
-dns63	Tertiäre IP-Adresse des IPv6-DNS-Servers

Befehl "dns"

Mit dem Befehl **dns** können Sie die DNS-Konfiguration des IMM2 anzeigen und einstellen.

Wird der Befehl **dns** ohne Optionen ausgeführt, so werden alle Informationen zur DNS-Konfiguration angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-state	DNS-Zustand	on, off
-ddns	DDNS-Zustand	enabled, disabled
-i1	Primäre IP-Adresse des IPv4-DNS-Servers	IP-Adresse im IP-Adressformat mit Trennzeichen.
-i2	Sekundäre IPv4-DNS-IP-Adresse	IP-Adresse im IP-Adressformat mit Trennzeichen.
-i3	Tertiäre IP-Adresse des IPv4-DNS-Servers	IP-Adresse im IP-Adressformat mit Trennzeichen.
-i61	Primäre IP-Adresse des IPv6-DNS-Servers	IP-Adresse im IPv6-Format.

Option	Beschreibung	Werte
-i62	Sekundäre IPv6-DNS-IP-Adresse	IP-Adresse im IPv6-Format.
-i63	Tertiäre IP-Adresse des IPv6-DNS-Servers	IP-Adresse im IPv6-Format.
-p	IPv4-/IPv6-Priorität	ipv4, ipv6

Syntax:

```
dns [Optionen]
Option:
  -state Zustand
  -ddns Zustand
  -i1 Erste_IPv4-IP-Adresse
  -i2 Zweite_IPv4-IP-Adresse
  -i3 Dritte_IPv4-IP-Adresse
  -i61 Erste_IPv6-IP-Adresse
  -i62 Zweite_IPv6-IP-Adresse
  -i63 Dritte_IPv6-IP-Adresse
  -p Priorität
```

Anmerkung: Im folgenden Beispiel ist eine IMM2-Konfiguration mit aktiviertem DNS dargestellt.

Beispiel:

```
system> dns
-state  : enabled
-i1     : 192.168.70.202
-i2     : 192.168.70.208
-i3     : 192.168.70.212
-i61    : fe80::21a:64ff:fee6:4d5
-i62    : fe80::21a:64ff:fee6:4d6
-i63    : fe80::21a:64ff:fee6:4d7
-ddns   : enabled
-ddn    : ibm.com
-ddncur  : ibm.com
-dnsrc  : dhcp
-p     : ipv6

system>
```

In der folgenden Tabelle wird die Ausgabe dieses Beispiels beschrieben.

Option	Beschreibung
-state	Zustand des DNS (on oder off)
-i1	Primäre IP-Adresse des IPv4-DNS-Servers
-i2	Sekundäre IPv4-DNS-IP-Adresse
-i3	Tertiäre IP-Adresse des IPv4-DNS-Servers
-i61	Primäre IP-Adresse des IPv6-DNS-Servers
-i62	Sekundäre IPv6-DNS-IP-Adresse
-i63	Tertiäre IP-Adresse des IPv6-DNS-Servers
-ddns	Zustand des DDNS (enabled oder disabled)
-dnsrc	Bevorzugter DDNS-Domänenname (dhcp oder manual)
-ddn	Manuell angegebenes DDN
-ddncur	Aktuelles DDN (Lesezugriff)

Option	Beschreibung
-p	Bevorzugte DNS-Server (`ipv4` oder `ipv6`)

Befehl "ethtousb"

Mit dem Befehl **ethtousb** können Sie die Portzuordnung für Ethernet zu Ethernet over USB anzeigen und konfigurieren.

Mit diesem Befehl können Sie für Ethernet over USB eine externe Ethernet-Portnummer einer anderen Portnummer zuordnen.

Wird der Befehl **ethtousb** ohne Optionen ausgeführt, so werden Informationen zu Ethernet über USB angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-en	Zustand von Ethernet über USB	enabled, disabled
-m*x*	Portzuordnung für Index *x* konfigurieren	Durch einen Doppelpunkt (:) getrenntes Portpaar in der Form *port1:port2* Dabei gilt: • die Portindexnummer *x* wird in der Befehlsoption als Ganzzahl zwischen 1 und 10 angegeben. • Bei *port1* des Portpaares handelt es sich um die externe Ethernet-Portnummer. • Bei *port2* des Portpaares handelt es sich um die Ethernet-over-USB-Portnummer.
-rm	Portzuordnung für angegebenen Index entfernen	1 bis 10 Über den Befehl **ethtousb** ohne Optionen werden Portzuordnungsindizes angezeigt.

Syntax:

```
ethtousb [Optionen]
Option:
  -en Zustand
  -mx Portpaar
  -rm Zuordnungsindex
```

Beispiel:

```
system> ethtousb  -en enabled -m1 100:200 -m2 101:201
system> ethtousb
 -en enabled
 -m1 100:200
 -m2 101:201
system> ethtousb -rm 1
system>
```

Befehl "gprofile"

Mit dem Befehl **gprofile** können Sie Gruppenprofile für das IMM2 anzeigen und konfigurieren.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-clear	Löscht eine Gruppe	enabled, disabled
-n	Der Name der Gruppe	Zeichenfolge mit bis zu 63 Zeichen für *Gruppenname*. Der *Gruppenname* muss eindeutig sein.
-a	Rollenbasierte Berechtigungsstufe	supervisor, operator, rbs <Rollenliste>: nsc|am|rca|rcvma|pr|bc|cel|ac Die Rollenlistenwerte werden in einer Liste, in der die einzelnen Werte durch Pipe-Zeichen voneinander getrennt sind, angegeben.
-h	Zeigt die Befehlssyntax und die Optionen an	

Syntax:

```
gprofile [1 - 16
Bereichsnummer_des_Gruppenprofils] [options]
Optionen:
-clear Status
-n  Gruppenname
-a  Berechtigungsebene:
    -nsc Netzbetrieb und Sicherheit
    -am Benutzerkontenverwaltung
    -rca Zugriff auf ferne Konsole
    -rcvma Zugriff auf ferne Konsole und fernen Datenträger
    -pr Zugriff auf Einschalten/Neustart eines fernen Servers
    -bc Allgemeine Adapterkonfiguration
    -cel Fähigkeit zum Löschen von Ereignisprotokollen
    -ac Erweiterte Adapterkonfiguration
-h Hilfe
```

Befehl "ifconfig"

Mit dem Befehl **ifconfig** können Sie die Ethernet-Schnittstelle konfigurieren. Geben Sie `ifconfig eth0` ein, um die aktuelle Ethernet-Schnittstellenkonfiguration anzuzeigen. Um die Konfiguration der Ethernet-Schnittstelle zu ändern, geben Sie die entsprechenden Optionen gefolgt von den Werten ein. Um die Schnittstellenkonfiguration ändern zu können, müssen Sie mindestens über die Berechtigung "Adapter Networking and Security Configuration" (Konfiguration von Adapternetzbetrieb und -sicherheit) verfügen.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-state	Schnittstellenstatus	disabled, enabled
-c	Konfigurationsmethode	dhcp, static, dthens ("dthens" entspricht der Option **Try dhcp server, if it fails use static config** (Nach DHCP-Server suchen. Falls das fehlschlägt, statische Konfiguration verwenden) in der Webschnittstelle)
-i	Statische IP-Adresse	Adresse im gültigen Format
-g	Gateway-Adresse	Adresse im gültigen Format
-s	Teilnetzmaske	Adresse im gültigen Format

Option	Beschreibung	Werte
-n	Hostname	Zeichenfolge von bis zu 63 Zeichen. Die Zeichenfolge kann Buchstaben, Ziffern, Punkte, Unterstriche und Bindestriche enthalten.
-r	Übertragungs-geschwindigkeit	10, 100, auto
-d	Duplexmodus	full, half, auto
-m	MTU	Numerisch zwischen 60 und 1500
-l	LAA	MAC-Adressenformat. Multicastadressen sind nicht zulässig (das erste Byte muss gerade sein).
-dn	Domänenname	Domänenname im gültigen Format
-auto	Einstellung für automatische Vereinbarung, die bestimmt, ob die Netzeinstellungen für die Übertragungs-geschwindigkeit und den Duplexmodus konfigurierbar sind.	true, false
-nic	NIC-Zugriff	shared, dedicated
-address_table	Tabelle der automatisch generierten IPv6-Adressen und ihre Präfixlängen **Anmerkung:** Diese Option wird nur dann angezeigt, wenn IPv6 und die statusunabhängige automatische Konfiguration aktiviert sind.	Dieser Wert ist schreibgeschützt und nicht konfigurierbar.
-ipv6	IPv6-Status	disabled, enabled
-lla	Lokale Verbindungsadresse **Anmerkung:** Die lokale Verbindungsadresse wird nur angezeigt, wenn IPv6 aktiviert ist.	Die lokale Linkadresse wird vom IMM2 bestimmt. Dieser Wert ist schreibgeschützt und nicht konfigurierbar.
-ipv6static	Statischer IPv6-Status	disabled, enabled
-i6	Statische IP-Adresse	Statische IP-Adresse für Ethernet-Kanal 0 im IPv6-Format
-p6	Länge des Adresspräfix	Numerisch zwischen 1 und 128
-g6	Gateway oder Standardroute	IP-Adresse für das Gateway oder die Standardroute für Ethernet-Kanal 0 im IPv6-Format.
-dhcp6	DHCPv6-Status	disabled, enabled
-sa6	Statusunabhängiger IPv6-Status mit automatischer Konfiguration	disabled, enabled

Syntax:

```
ifconfig eth0 [Optionen]
Optionen:
  -state Schnittstellenstatus
```

```
-c Konfigurationsmethode
-i Statische_IPv4-IP-Adresse
-g IPv4-Gateway-Adresse
-s Teilnetzmaske
-n Hostname
-r Übertragungsgeschwindigkeit
-d Duplexmodus
-m MTU
-l Lokal_verwalteter_MAC
-dn Domänenname
-auto Zustand
-nic Zustand
-address_table
-ipv6 Zustand
-ipv6static Zustand
-sa6 Zustand
-i6 Statische_IPv6-IP-Adresse
-g6 IPv6-Gateway-Adresse
-p6 Länge
```

Beispiel:

```
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMM2A00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system> ifconfig eth0 -c static -i 192.168.70.133
Diese Konfigurationsänderungen werden nach der nächsten Zurücksetzung des IMM2 aktiv.
system>
```

Anmerkung: Die Option **-b** in der Anzeige von "ifconfig" steht für die Herstellerkennung der MAC-Adresse. Die Herstellerkennung der MAC-Adresse ist schreibgeschützt und nicht konfigurierbar.

Befehl "keycfg"

Verwenden Sie den Befehl **keycfg**, um Aktivierungsschlüssel anzuzeigen, hinzuzufügen oder zu löschen. Über diese Schlüssel wird der Zugriff auf optionale FoD-Funktionen (Features on Demand) des IMM2 gesteuert.

- Wird **keycfg** ohne Optionen ausgeführt, so wird die Liste installierter Aktivierungsschlüssel angezeigt. Die angezeigten Schlüsselinformationen umfassen eine Indexzahl für jeden Aktivierungsschlüssel, den Aktivierungsschlüsseltyp, das Datum, bis zu dem der Schlüssel gültig ist, die Anzahl verbleibender Verwendungen, den Schlüsselstatus und eine Beschreibung des Schlüssels.
- Durch Dateiübertragung neue Aktivierungsschlüssel hinzufügen.
- Löschen Sie alte Schlüssel, indem Sie die Zahl des Schlüssels oder den Schlüsseltyp angeben. Beim Löschen von Schlüsseln nach Typ wird nur der erste Schlüssel eines bestimmten Typs gelöscht.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-add	Aktivierungsschlüssel hinzufügen	Werte für die Befehlsoptionen -ip, -pn, -u, -pw und -f.

Option	Beschreibung	Werte
-ip	IP-Adresse des TFTP-Servers mit hinzuzufügendem Aktivierungsschlüssel	Gültige IP-Adresse für TFTP-Server.
-pn	Portnummer für TFTP-/SFTP-Server mit hinzuzufügendem Aktivierungsschlüssel	Gültige Portnummer für TFTP-/SFTP-Server (Standard 69/22).
-u	Benutzername für SFTP-Server mit hinzuzufügendem Aktivierungsschlüssel	Gültiger Benutzername für SFTP-Server
-pw	Kennwort für SFTP-Server mit hinzuzufügendem Aktivierungsschlüssel	Gültiges Kennwort für SFTP-Server
-f	Dateiname für hinzuzufügenden Aktivierungsschlüssel	Gültiger Dateiname für Aktivierungsschlüsseldatei.
-del	Aktivierungsschlüssel nach Indexzahl löschen	Gültige Indexzahl für Aktivierungsschlüssel aus **keycfg**-Liste.
-deltype	Aktivierungsschlüssel nach Schlüsseltyp löschen	Gültiger Wert für Schlüsseltyp.

Syntax:

```
keycfg [Optionen]
Option:
  -add     -ip IP-Adresse
     -pn Portnummer
     -u Benutzername
     -pw Kennwort
     -f Dateiname
  -del Schlüsselindex
  -deltype Schlüsseltyp
```

Beispiel:

```
system> keycfg
ID  Type  Valid         Uses  Status   Description
1   4     10/10/2010    5     "valid"  "IMM remote presence"
2   3     10/20/2010    2     "valid"  "IMM feature"
system>
```

Befehl "ldap"

Mit dem Befehl **ldap** können Sie die Konfigurationsparameter des LDAP-Protokolls anzeigen und konfigurieren.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-a	Benutzerauthentifizierungsverfahren	"local only", "LDAP only", "local first then LDAP", "LDAP first then local"

Option	Beschreibung	Werte
-aom	Modus nur für Authentifizierung	enabled, disabled
-b	Bindungsmethode	"anonymous", "bind with ClientDN and password", "bind with Login Credential"
-c	Definierter Name des Clients	Zeichenfolge mit bis zu 127 Zeichen für *Definierter_Name_des_Clients*
-d	Suchdomäne	Zeichenfolge mit bis zu 63 Zeichen für *Suchdomäne*
-f	Gruppenfilter	Zeichenfolge mit bis zu 127 Zeichen für *Gruppenfilter*
-fn	Gesamtstrukturname	Für aktive Verzeichnisumgebungen. Zeichenfolge mit bis zu 127 Zeichen.
-g	Gruppensuchattribut	Zeichenfolge mit bis zu 63 Zeichen für *Gruppensuchattribut*
-l	Anmeldeberechtigungsattribut	Zeichenfolge mit bis zu 63 Zeichen für *Zeichenfolge*
-p	Clientkennwort	Zeichenfolge mit bis zu 15 Zeichen für *Clientkennwort*
-pc	Clientkennwort bestätigen	Zeichenfolge mit bis zu 15 Zeichen für *Bestätigungskennwort* Befehlssyntax: ldap -p *Clientkennwort* -pc *Bestätigungskennwort* Diese Option ist erforderlich, wenn Sie das Clientkennwort ändern. Sie vergleicht das Argument *Bestätigungskennwort* mit dem Argument *Clientkennwort*. Der Befehl schlägt fehl, wenn die beiden Argumente nicht miteinander übereinstimmen.
-r	Definierter Name des Stammeintrags (DN)	Zeichenfolge mit bis zu 127 Zeichen für *definierter_Rootname*
-rbs	Erweiterte rollenbasierte Sicherheit für Active Directory-Benutzer	enabled, disabled
-s1ip	Hostname/IP-Adresse von Server 1	Zeichenfolge mit bis zu 127 Zeichen oder eine IP-Adresse für *Hostname/IP-Adresse*
-s2ip	Hostname/IP-Adresse von Server 2	Zeichenfolge mit bis zu 127 Zeichen oder eine IP-Adresse für *Hostname/IP-Adresse*
-s3ip	Hostname/IP-Adresse von Server 3	Zeichenfolge mit bis zu 127 Zeichen oder eine IP-Adresse für *Hostname/IP-Adresse*
-s4ip	Hostname/IP-Adresse von Server 4	Zeichenfolge mit bis zu 127 Zeichen oder eine IP-Adresse für *Hostname/IP-Adresse*
-s1pn	Portnummer von Server 1	Eine numerische Portnummer mit bis zu 5 Ziffern für *Portnummer*
-s2pn	Portnummer von Server 2	Eine numerische Portnummer mit bis zu 5 Ziffern für *Portnummer*
-s3pn	Portnummer von Server 3	Eine numerische Portnummer mit bis zu 5 Ziffern für *Portnummer*
-s4pn	Portnummer von Server 4	Eine numerische Portnummer mit bis zu 5 Ziffern für *Portnummer*

Option	Beschreibung	Werte
-t	Zielname des Servers	Wenn die Option "-rbs" aktiviert ist, gibt dieses Feld einen Zielnamen an, der mithilfe des Snap-in-Tools für die rollenbasierte Sicherheit auf dem Active Directory-Server einer oder mehreren Rollen zugeordnet werden kann.
-u	UID-Suchattribut	Zeichenfolge mit bis zu 63 Zeichen für *Suchattribut*
-v	LDAP-Serveradresse über DNS abrufen	off, on
-h	Zeigt die Befehlssyntax und die Optionen an	

Syntax:

```
ldap [Optionen]
Optionen:
   -a loc|ldap|locld|ldloc
   -aom enable/disabled
   -b anon|client|login
   -c Definierter_Name_des_Clients
   -d Suchdomäne
   -f Gruppenfilter
   -fn Gesamtstrukturname
   -g Gruppensuchattribut
   -l Zeichenfolge
   -p Clientkennwort
   -pc Bestätigungskennwort
   -r definierter_Rootname
   -rbs enable/disabled
   -s1ip Hostname/IP-Adresse
   -s2ip Hostname/IP-Adresse
   -s3ip Hostname/IP-Adresse
   -s4ip Hostname/IP-Adresse
   -s1pn Portnummer
   -s2pn Portnummer
   -s3pn Portnummer
   -s4pn Portnummer
   -t Name
   -u Suchattribut
   -v off|on
   -h
```

Befehl "ntp"

Mit dem Befehl **ntp** können Sie das Network Time Protocol (NTP) anzeigen und konfigurieren.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-en	Aktiviert oder inaktiviert das Network Time Protocol.	enabled, disabled
-i[1]	Name oder IP-Adresse des Network Time Protocol-Servers. Hierbei handelt es sich um die Indexnummer des Network Time Protocol-Servers.	Der Name des NTP-Servers, der für die Taktgebersynchronisation verwendet werden soll.Die Reichweite der Indexnummer des NTP-Servers reicht von -i1 bis -i4.

Option	Beschreibung	Werte
-f	Die Häufigkeit (in Minuten), mit der der IMM2-Taktgeber mit dem Network Time Protocol-Server synchronisiert wird	3 - 1440 Minuten
-synch	Fordert eine sofortige Synchronisation mit dem Network Time Protocol-Server an	Mit diesem Parameter werden keine Werte verwendet.
1. -i entspricht i1.		

Syntax:

```
ntp [Optionen]
Optionen:
-en Zustand
-i  Hostname/IP-Adresse
-f  Häufigkeit
-synch
```

Beispiel:

```
system> ntp
-en: disabled
-f: 3 minutes
-i: not set
```

Befehl "passwordcfg"

Mit dem Befehl **passwordcfg** können Sie die Kennwortparameter anzeigen und konfigurieren.

Option	Beschreibung
-legacy	Legt für die Accountsicherheit eine vordefinierte Gruppe von traditionellen Standardwerten fest.
-high	Legt für die Accountsicherheit eine vordefinierte Gruppe von hohen Standardwerten fest.
-exp	Maximale Gültigkeitsdauer des Kennworts (0 - 365 Tage). Der Wert "0" bedeutet, dass das Kennwort nie abläuft.
-cnt	Anzahl der vorherigen Kennwörter, die nicht erneut verwendet werden dürfen.
-nul	Lässt Konten ohne Kennwort zu (yes | no)
-h	Zeigt die Befehlssyntax und die Optionen an

Syntax:

```
passwordcfg [Optionen]
Optionen: {-high}|{-legacy}|{-exp|-cnt|-nul}
-legacy
-high
-exp:
-cnt:
-nul:
-h
```

Beispiel:

```
system> passwordcfg
Security Level: Legacy
system> passwordcfg -exp 365
ok
system> passwordcfg -nul yes
ok
system> passwordcfg -cnt 5
ok
system> passwordcfg
Security Level: Customize
-exp: 365
-cnt: 5
-nul: allowed
```

Befehl "ports"

Mit dem Befehl **ports** können Sie IMM2-Ports anzeigen und konfigurieren.

Wird der Befehl **ports** ohne Optionen ausgeführt, so werden Informationen für alle IMM2-Ports angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-open	Offene Ports anzeigen	
-reset	Ports auf Standardeinstellungen zurücksetzen	
-httpp	HTTP-Portnummer	Standardportnummer: 80
-httpsp	HTTPS-Portnummer	Standardportnummer: 443
-telnetp	Traditionelle Telnet-CLI-Portnummer	Standardportnummer: 23
-sshp	Traditionelle SSH-CLI-Portnummer	Standardportnummer: 22
-snmpap	SNMP-Agenten-Portnummer	Standardportnummer: 161
-snmptp	SNMP-Traps-Portnummer	Standardportnummer: 162
-rpp	Remote-Presence-Portnummer	Standardportnummer: 3900
-cimhp	CIM-over-HTTP-Portnummer	Standardportnummer: 5988
-cimhsp	CIM-over-HTTPS-Portnummer	Standardportnummer: 5989

Syntax:

```
ports [Optionen]
Option:
  -open
  -reset
  -httpp Portnummer
  -httpsp Portnummer
  -telnetp Portnummer
  -sshp Portnummer
  -snmpap Portnummer
```

```
-snmptp Portnummer
-rpp Portnummer
-cimhp Portnummer
-cimhsp Portnummer
```

Beispiel:

```
System> Ports
-httpp 80
-httpsp 443
-rpp 3900
-snmpap 161
-snmptp 162
-sshp 22
-telnetp 23
-cimhp 5988
-cimhsp 5989
system>
```

Befehl "portcfg"

Mit dem Befehl **portcfg** können Sie das IMM2 für die Funktion zur seriellen Umleitung konfigurieren.

Das IMM2 muss so konfiguriert sein, dass es mit den Servereinstellungen für interne serielle Anschlüsse übereinstimmt. Um die Konfiguration des seriellen Anschlusses zu ändern, geben Sie die entsprechenden Optionen gefolgt von den Werten ein. Um die Konfiguration des seriellen Anschlusses ändern zu können, müssen Sie mindestens über die Berechtigung "Adapter Networking and Security Configuration" (Konfiguration von Adapternetzbetrieb und -sicherheit) verfügen.

Anmerkung: Der externe serielle Anschluss des Servers kann vom IMM2 nur für die IPMI-Funktion verwendet werden. Die Befehlszeilenschnittstelle wird durch den seriellen Anschluss nicht unterstützt. Die Optionen **serred** und **cliauth**, die in der Befehlszeilenschnittstelle von Remote Supervisor Adapter II vorhanden waren, werden nicht unterstützt.

Wird der Befehl **portcfg** ohne Optionen ausgeführt, so wird die Konfiguration des seriellen Anschlusses angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Anmerkung: Die Anzahl an Datenbits (8) ist in der Hardware festgelegt und kann nicht geändert werden.

Option	Beschreibung	Werte
-b	Baudrate	9600, 19200, 38400, 57600, 115200
-p	Parität	none, odd, even
-s	Bits stoppen	1, 2
-climode	CLI-Modus	0, 1, 2 Dabei gilt: • 0 = none: Die Befehlszeilenschnittstelle wird inaktiviert • 1 = cliems: Die Befehlszeilenschnittstelle wird mit EMS-kompatiblen Tastenfolgen aktiviert • 2 = cliuser: Die Befehlszeilenschnittstelle wird mit benutzerdefinierten Tastenfolgen aktiviert

Syntax:

```
portcfg [Optionen]
 Optionen:
   -b Baudrate
   -p Parität
   -s Bits_stoppen
   -climode Modus
```

Beispiel:

```
system> portcfg
-b       :    57600
-climode :    2 (CLI mit benutzerdefinierter Tastenfolge)
-p  :    even
-s       :    1
system> portcfg -b 38400
ok
system>
```

Befehl "restore"

Mit dem Befehl **restore** können Sie Systemeinstellungen aus einer Sicherungsdatei wiederherstellen.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-f	Name der Sicherungsdatei	Gültiger Dateiname
-pp	Kennwort oder Verschlüsselungstext, mithilfe dessen Kennwörter innerhalb der Sicherungsdatei verschlüsselt sind	Gültiges Passwort oder durch Anführungszeichen begrenzter Verschlüsselungstext
-ip	IP-Adresse des TFTP-/SFTP-Servers	Gültige IP-Adresse
-pn	Portnummer des TFTP-/SFTP-Servers	Gültige Portnummer (Standard 69/22)
-u	Benutzername für SFTP-Server	Gültiger Benutzername
-pw	Kennwort für SFTP-Server	Gültiges Kennwort

Syntax:

```
restore [Optionen]
Option:
  -f Dateiname
  -pp Kennwort
  -ip IP-Adresse
  -pn Portnummer
  -u Benutzername
  -pw Kennwort
```

Beispiel:

```
system> restore –f imm-back.cli –pp xxxxxx –ip 192.168.70.200
ok
system>
```

Befehl "restoredefaults"

Mit dem Befehl **restoredefaults** können Sie alle IMM2-Einstellungen auf die werkseitige Voreinstellung zurücksetzen.

- Für den Befehl **restoredefaults** gibt es keine Optionen.
- Sie werden aufgefordert, den Befehl zu bestätigen, bevor dieser verarbeitet wird.

Syntax:

```
restoredefaults
```

Beispiel:

```
system> restoredefaults

This action will cause all IMM settings to be set to factory defaults.

If this is the local system, you will lose your TCP/IP connection as a result.
You will need to reconfigure the IMM network interface to restore connectivity.
After the IMM configuration is cleared, the IMM will be restarted.

Proceed? (y/n)
Y
Restoring defaults...
```

Befehl "set"

Mit dem Befehl **set** können Sie Einstellungen des IMM2 ändern.

- Manche Einstellungen des IMM2 können einfach durch den Befehl **set** geändert werden.
- Manche dieser Einstellungen, etwa Umgebungsvariablen, werden vom CLI verwendet.
- Mit dem Befehl **show** können Sie über den Befehl **set** festgelegte Werte anzeigen.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
value	Wert für angegebenen Pfad oder angegebene Einstellung festlegen	Entsprechender Wert für angegebenen Pfad oder angegebene Einstellung.

Syntax:

```
set [Optionen]
Option:
  value
```

Befehl "smtp"

Mit dem Befehl **smtp** können Sie Einstellungen für die SMTP-Schnittstelle anzeigen und konfigurieren.

Wird der Befehl **smtp** ohne Optionen ausgeführt, so werden alle Informationen zur SMTP-Schnittstelle angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-auth	Authentifizierungs-support für SMTP	enabled, disabled

Option	Beschreibung	Werte
-authepw	verschlüsseltes Kennwort für die SMTP-Authentifizierung	Gültige Kennwort-Zeichenkette
-authmd	SMTP-Authentifizierungsverfahren	CRAM-MD5, LOGIN
-authn	Benutzername zur SMTP-Authentifizierung	Zeichenkette (auf 256 Zeichen begrenzt).
-authpw	SMTP-Authentifizierungskennwort	Zeichenkette (auf 256 Zeichen begrenzt).
-pn	SMTP-Portnummer	Gültige Portnummer.
-s	IP-Adresse oder Hostname des SMTP-Servers	Gültige IP-Adresse oder gültiger Hostname (auf 63 Zeichen begrenzt).

Syntax:

```
smtp [Optionen]
Option:
  -auth enabled|disabled
  -authepw Kennwort
  -authmd CRAM-MD5|LOGIN
  -authn Benutzername
  -authpw Kennwort
  -s IP-Adresse_oder_Hostname
  -pn Portnummer
```

Beispiel:

```
system> smtp
-s test.com
-pn 25
system>
```

Befehl "snmp"

Mit dem Befehl **snmp** können Sie die SNMP-Schnittstelleninformationen anzeigen und konfigurieren.

Wird der Befehl **snmp** ohne Optionen ausgeführt, so werden alle Informationen zur SNMP-Schnittstelle angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-a	SNMPv1-Agent	on, off **Anmerkung:** Folgende Kriterien müssen zur Aktivierung des SNMPv1-Agenten erfüllt sein: • Über die Befehlsoption "-cn" angegebener Ansprechpartner für das IMM2. • Über die Befehlsoption "-l" angegebener Standort des IMM2. • Mindestens ein über eine der "-c*x*"-Befehlsoptionen angegebener SNMP-Community-Name. • Mindestens eine gültige IP-Adresse wird über eine der "-c*x*i*y*"-Befehlsoptionen für jede SNMP-Community angegeben.

Option	Beschreibung	Werte
-a3	SNMPv3-Agent	on, off **Anmerkung:** Folgende Kriterien müssen zum Aktivieren des SNMPv3-Agenten erfüllt sein: • Über die Befehlsoption "-cn" angegebener Ansprechpartner für das IMM2. • Über die Befehlsoption "-l" angegebener Standort des IMM2.
-t	SNMP-Traps	on, off
-l	IMM2-Standort	Zeichenkette (auf 47 Zeichen begrenzt). **Anmerkung:** • Argumente mit Leerzeichen müssen in Anführungszeichen gesetzt werden. Führende oder nachgestellte Leerzeichen sind in Argumenten nicht zulässig. • Löschen Sie beim IMM2-Standort den Inhalt, indem Sie kein Argument angeben oder indem Sie eine leere Zeichenkette als Argument angeben, etwa "".
-cn	Ansprechpartner für IMM2	Zeichenkette (auf 47 Zeichen begrenzt). **Anmerkung:** • Argumente mit Leerzeichen müssen in Anführungszeichen gesetzt werden. Führende oder nachgestellte Leerzeichen sind in Argumenten nicht zulässig. • Löschen Sie beim IMM2-Ansprechpartner den Inhalt, indem Sie kein Argument angeben oder indem Sie eine leere Zeichenkette als Argument angeben, etwa "".
-c*x*	Name von SNMP-Community *x*	Zeichenkette (auf 15 Zeichen begrenzt). **Anmerkung:** • *x* wird in der Befehlsoption mit 1, 2 oder 3 angegeben, um die Communitynummer anzuzeigen. • Argumente mit Leerzeichen müssen in Anführungszeichen gesetzt werden. Führende oder nachgestellte Leerzeichen sind in Argumenten nicht zulässig. • Löschen Sie bei einem SNMP-Community-Namen den Inhalt, indem Sie kein Argument angeben oder indem Sie eine leere Zeichenkette als Argument angeben, etwa "".
-c*x*i*y*	IP-Adresse oder Hostname *y* von SNMP-Community *x*	Gültige IP-Adresse oder gültiger Hostname (auf 63 Zeichen begrenzt). **Anmerkung:** • *x* wird in der Befehlsoption mit 1, 2 oder 3 angegeben, um die Communitynummer anzuzeigen. • *y* wird in der Befehlsoption mit 1, 2 oder 3 angegeben, um die Nummer der IP-Adresse oder des Hostnamens anzuzeigen. • Eine IP-Adresse oder ein Hostname darf nur Punkte, Unterstriche, Minuszeichen, Buchstaben und Ziffern enthalten. Eingebettete Leerzeichen oder aufeinanderfolgende Punkte sind nicht zulässig. • Löschen Sie den Inhalt bei der IP-Adresse oder beim Hostnamen einer SNMP-Community, indem Sie kein Argument angeben.

Option	Beschreibung	Werte
-ca*x*	Zugriffstyp bei SNMPv3-Community *x*	get, set, trap **Anmerkung:** *x* wird in der Befehlsoption mit 1, 2 oder 3 angegeben, um die Communitynummer anzuzeigen.

Syntax:

```
snmp [Optionen]
Option:
  -a Zustand
  -a3 Zustand
  -t Zustand
  -l Standort
  -cn Name_des_Ansprechpartners
  -c1 Name_von_SNMP-Community_1
  -c2 Name_von_SNMP-Community_2
  -c3 Name_von_SNMP-Community_3
  -c1i1 IP-Adresse_oder_Hostname_1_von_Community_1
  -c1i2 IP-Adresse_oder_Hostname_2_von_Community_1
  -c1i3 IP-Adresse_oder_Hostname_3_von_Community_1
  -c2i1 IP-Adresse_oder_Hostname_1_von_Community_2
  -c2i2 IP-Adresse_oder_Hostname_2_von_Community_2
  -c2i3 IP-Adresse_oder_Hostname_3_von_Community_2
  -c3i1 IP-Adresse_oder_Hostname_1_von_Community_3
  -c3i2 IP-Adresse_oder_Hostname_2_von_Community_3
  -c3i3 IP-Adresse_oder_Hostname_3_von_Community_3
  -ca1 Zugriffstyp_von_Community_1
  -ca2 Zugriffstyp_von_Community_2
  -ca3 Zugriffstyp_von_Community_3
```

Beispiel:

```
system> snmp
-a Enabled
-a3 Enabled
-t Enabled
-l RTC,NC
-cn Snmp Test
-c1 public
-c1i1 192.44.146.244
-c1i2 192.44.146.181
-c1i3 192.44.143.16
-ca1 set
-ch1 specific
-c2 private
-c2i1 192.42.236.4
-c2i2
-c2i3
-ca2 get
-ch2 specific
-c3
-c3i1
-c3i2
-c3i3
-ca3 get
-ch3 ipv4only
system>
```

Befehl "snmpalerts"

Mit dem Befehl **snmpalerts** können Sie über SNMP Alerts verwalten.

Wird **snmpalerts** ohne Optionen ausgeführt, so werden alle SNMP-Alerteinstellungen angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-status	SNMP-Alertstatus	on, off
-crt	Legt kritische Ereignisse fest, die Alerts senden	all, none, custom:te | vo | po | di | fa | cp | me | in | re | ot Benutzerdefinierte Einstellungen für kritische Alerts werden mithilfe einer Liste, in der die einzelnen Werte durch Pipe-Zeichen voneinander getrennt sind, mit Werten in der Form **snmpalerts -crt custom:te | vo** angegeben; benutzerdefinierte Werte sind: • te: kritischer Temperaturschwellenwert überschritten • vo: kritischer Spannungsschwellenwert überschritten • po: kritischer Netzausfall • di: Fehler beim Festplattenlaufwerk • fa: Lüfterfehler • cp: Mikroprozessorfehler • me: Speicherfehler • in: Hardwareinkompatibilität • re: Stromversorgungsredundanzfehler • ot: alle anderen kritischen Ereignisse
-crten	Alerts bei kritischen Ereignissen senden	enabled, disabled
-wrn	Legt Warnungsereignisse fest, die Alerts senden	all, none, custom:rp | te | vo | po | fa | cp | me | ot Benutzerdefinierte Einstellungen für Warnungsalerts werden mithilfe einer Liste, in der die einzelnen Werte durch Pipe-Zeichen voneinander getrennt sind, mit Werten in der Form **snmpalerts -wrn custom:rp | te** angegeben; benutzerdefinierte Werte sind: • rp: Warnung bei Stromversorgungsredundanz • te: Warnungstemperaturschwellenwert überschritten • vo: Warnungsspannungsschwellenwert überschritten • po: Warnungsnetzschwellenwert überschritten • fa: unkritischer Lüfterfehler • cp: Mikroprozessor in beeinträchtigtem Zustand • me: Speicherwarnung • ot: alle anderen Warnungsereignisse
-wrnen	Alerts bei Warnungsereignissen senden	enabled, disabled

Option	Beschreibung	Werte
-sys	Legt Routineereignisse fest, die Alerts senden	all, none, custom:lo | tio | ot | po | bf | til | pf | el | ne Benutzerdefinierte Einstellungen für Routinealerts werden mithilfe einer Liste, in der die einzelnen Werte durch Pipe-Zeichen voneinander getrennt sind, mit Werten in der Form **snmpalerts -sys custom:lo | tio** angegeben; benutzerdefinierte Werte sind: • lo: erfolgreiche Fernanmeldung • tio: Zeitlimit des Betriebssystems • ot: alle anderen Informations- und Systemereignisse • po: Stromversorgung des Systems ein/aus • bf: Bootfehler des Betriebssystems • til: Watchdog-Zeitlimitüberschreitung des Betriebssystemladeprogramms • pf: vorhergesagter Fehler (PFA - Predictive Failure Analysis) • el: Ereignisprotokoll zu 75% voll • ne: Netzänderung
-sysen	Alerts bei Routineereignissen senden	enabled, disabled

Syntax:

```
snmpalerts [Optionen]
   Optionen:
     -status Status
     -crt Ereignistyp
     -crten Zustand
     -wrn Ereignistyp
     -wrnen Zustand
     -sys Ereignistyp
     -sysen Zustand
```

Befehl "srcfg"

Verwenden Sie den Befehl **srcfg**, um die Tastenkombination für den Zugang zur Befehlszeilenschnittstelle vom Modus für serielle Umleitung anzugeben. Um die Konfiguration der seriellen Umleitung zu ändern, geben Sie die entsprechenden Optionen gefolgt von den Werten ein. Um die Konfiguration der seriellen Umleitung ändern zu können, müssen Sie mindestens über die Berechtigung "Adapter Networking and Security Configuration" (Konfiguration von Adapternetzbetrieb und -sicherheit) verfügen.

Anmerkung: Die IMM2-Hardware sieht keine Pass-Through-Fähigkeit zwischen seriellen Anschlüssen vor. Daher werden die Optionen `-passthru` und `entercliseq`, die in der Befehlszeilenschnittstelle des Remote Supervisor Adapter II vorhanden sind, nicht unterstützt.

Wird der Befehl **srcfg** ohne Optionen ausgeführt, so wird die aktuelle Tastenfolge für die serielle Umleitung angezeigt. In der folgenden Tabelle sind die Argumente für die Befehlsoption `srcfg -entercliseq` aufgelistet.

Option	Beschreibung	Werte
-entercliseq	Tastenfolge für Befehlszeilen-schnittstelle ein-geben	Benutzerdefinierte Tastenfolge für den Zugang zur Befehlszeilenschnittstelle. **Anmerkung:** Diese Sequenz muss mindestens ein Zeichen und darf höchstens 15 Zeichen enthalten. Das Winkelzeichen (^) hat in dieser Sequenz eine spezielle Bedeutung. Es steht bei Tastatureingaben, die 'Strg'-Sequenzen zugeordnet sind (beispielsweise ^[für die Abbruchtaste und ^M für einen Zeilenumbruch), für 'Strg'. Jedes Auftreten von '^' wird als Teil einer 'Strg'-Sequenz interpretiert. Eine vollständige Liste mit 'Strg'-Sequenzen finden Sie in der ASCII-Konvertierungstabelle. Der Standardwert für dieses Feld ist ^[(, d. h. die Abbruchtaste gefolgt von einer (.

Syntax:

```
srcfg [Optionen]
Optionen:
-entercliseq entercli_keyseq
```

Beispiel:

```
system> srcfg
-entercliseq ^[Q
system>
```

Befehl "sshcfg"

Mit dem Befehl **sshcfg** können Sie die SSH-Parameter anzeigen und konfigurieren.

Wird der Befehl **sshcfg** ohne Optionen ausgeführt, so werden alle SSH-Parameter angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-cstatus	Zustand von SSH-CLI	enabled, disabled
-hk gen	Privaten Schlüssel für SSH-Server generieren	
-hk rsa	Öffentlichen Schlüssel von Server-RSA anzei-gen	

Syntax:

```
sshcfg [Optionen]
Option:
  -cstatus Zustand
  -hk gen
  -hk rsa
```

Beispiel:

```
system> sshcfg
-cstatus enabled
CLI SSH port 22
ssh-rsa 2048 bit fingerprint: b4:a3:5d:df:0f:87:0a:95:f4:d4:7d:c1:8c:27:51:61
1 SSH public keys installed
system>
```

Befehl "ssl"

Mit dem Befehl **ssl** können Sie die SSL-Parameter anzeigen und konfigurieren.

Anmerkung: Bevor Sie einen SSL-Client aktivieren können, muss ein Clientzertifikat installiert werden.

Wird der Befehl **ssl** ohne Optionen ausgeführt, so werden SSL-Parameter angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-ce	Aktiviert oder inaktiviert einen SSL-Client	on, off
-se	Aktiviert oder inaktiviert einen SSL-Server	on, off
-cime	Aktiviert oder inaktiviert CIM over HTTPS auf dem SSL-Server	on, off

Syntax:

```
portcfg [Optionen]
 Optionen:
  -ce Zustand
  -se Zustand
  -cime Zustand
```

Parameter: Die folgenden Parameter erscheinen in der Optionsstatusanzeige für den Befehl **ssl** und werden nur über die Befehlszeilenschnittstelle ausgegeben:

Server secure transport enable (Sichere Serverübertragung aktivieren)
Diese Statusanzeige ist schreibgeschützt und kann nicht direkt festgelegt werden.

Server Web/CMD key status (Server-Web/CMD-Schlüsselstatus)
Diese Statusanzeige ist schreibgeschützt und kann nicht direkt festgelegt werden. Folgende Befehlszeilenausgabewerte sind möglich:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

SSL server CSR key status (CSR-Schlüssel für SSL-Server)
Diese Statusanzeige ist schreibgeschützt und kann nicht direkt festgelegt werden. Folgende Befehlszeilenausgabewerte sind möglich:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

SSL Client LDAP key status (LDAP-Schlüssel für SSL-Client)
Diese Statusanzeige ist schreibgeschützt und kann nicht direkt festgelegt werden. Folgende Befehlszeilenausgabewerte sind möglich:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

SSL Client CSR key status (CSR-Schlüssel für SSL-Client)

Diese Statusanzeige ist schreibgeschützt und kann nicht direkt festgelegt werden. Folgende Befehlszeilenausgabewerte sind möglich:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

Befehl "sslcfg"

Verwenden Sie den Befehl **sslcfg**, um SSL für das IMM2 anzuzeigen und zu konfigurieren und um Zertifikate zu verwalten.

Wird der Befehl **sslcfg** ohne Optionen ausgeführt, so werden alle Informationen zur SSL-Konfiguration angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-server	SSL-Serverstatus	enabled, disabled **Anmerkung:** Der SSL-Server kann nur bei Vorliegen eines gültigen Zertifikats aktiviert werden.
-client	SSL-Clientstatus	enabled, disabled **Anmerkung:** Der SSL-Client kann nur bei Vorliegen eines gültigen Server- oder Clientzertifikats aktiviert werden.
-cim	CIM-over-HTTPS-Status	enabled, disabled **Anmerkung:** CIM over HTTPS kann nur bei Vorliegen eines gültigen Server- oder Clientzertifikats aktiviert werden.
-cert	Selbst signiertes Zertifikat generieren	server, client, sysdir **Anmerkung:** • Werte für die Befehlsoptionen **-c**, **-sp**, **-cl**, **-on** und **-hn** sind bei der Erstellung eines selbst signierten Zertifikats erforderlich. • Werte für die Befehlsoptionen **-cp**, **-ea**, **-ou**, **-s**, **-gn**, **-in** und **-dq** sind bei der Erstellung eines selbst signierten Zertifikats optional.
-csr	Zertifikatssignieranforderung generieren	server, client, sysdir **Anmerkung:** • Werte für die Befehlsoptionen **-c**, **-sp**, **-cl**, **-on** und **-hn** sind bei der Erstellung einer Zertifikatssignieranforderung erforderlich. • Werte für die Befehlsoptionen **-cp**, **-ea**, **-ou**, **-s**, **-gn**, **-in**, **-dq**, **-cpwd** und **-un** sind bei der Erstellung einer Zertifikatssignieranforderung optional.

Option	Beschreibung	Werte
-i	IP-Adresse für TFTP-/ SFTP-Server	Gültige IP-Adresse **Anmerkung:** Beim Hochladen eines Zertifikats und beim Herunterladen eines Zertifikats oder einer Zertifikatssignieranforderung muss eine IP-Adresse für den TFTP- oder SFTP-Server angegeben werden.
-pn	Portnummer des TFTP-/SFTP-Servers	Gültige Portnummer (Standard 69/22)
-u	Benutzername für SFTP-Server	Gültiger Benutzername
-pw	Kennwort für SFTP-Server	Gültiges Kennwort
-l	Dateiname des Zertifikats	Gültiger Dateiname **Anmerkung:** Beim Herunterladen oder Hochladen eines Zertifikats oder einer Zertifikatssignieranforderung ist ein Dateiname erforderlich. Wenn beim Herunterladen kein Dateiname angegeben wird, wird der Standardname für die Datei verwendet und angezeigt.
-dnld	Zertifikatsdatei herunterladen	Bei dieser Option sind keine Argumente erforderlich; es müssen jedoch Werte für die Befehlsoptionen **-cert** oder **-csr** angegeben werden (abhängig davon, welcher Zertifikatstyp heruntergeladen wird). Bei dieser Option sind keine Argumente erforderlich; es müssen jedoch Werte für die Befehlsoption **-i** und die (optionale) Befehlsoption **-l** angegeben werden.
-upld	Importiert Zertifikatsdatei	Bei dieser Option sind keine Argumente erforderlich, es müssen jedoch Werte für die Befehlsoptionen **-cert**, **-i** und **-l** angegeben werden.
-tc*x*	Vertrauenswürdiges Zertifikat *x* für SSL-Client	import, download, remove **Anmerkung:** Die vertrauenswürdige Zertifikatsnummer *x* wird in der Befehlsoption als Ganzzahl zwischen 1 und 3 angegeben.
-c	Land	Landescode (2 Buchstaben) **Anmerkung:** Erforderlich bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-sp	Land oder Bundesland	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) **Anmerkung:** Erforderlich bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-cl	Ort oder Standort	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 50 Zeichen) **Anmerkung:** Erforderlich bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-on	Name des Unternehmens	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) **Anmerkung:** Erforderlich bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.

Option	Beschreibung	Werte
-hn	IMM2-Hostname	Zeichenkette (höchstens 60 Zeichen) **Anmerkung:** Erforderlich bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-cp	Ansprechpartner	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) **Anmerkung:** Optional bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-ea	E-Mail-Adresse des Ansprechpartners	Gültige E-Mail-Adresse (höchstens 60 Zeichen) **Anmerkung:** Optional bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-ou	Organisationseinheit	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) **Anmerkung:** Optional bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-s	Nachname	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) **Anmerkung:** Optional bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-gn	Vorname	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) **Anmerkung:** Optional bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-in	Initialen	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 20 Zeichen) **Anmerkung:** Optional bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-dq	Qualifikationsmerkmal des Domänennamens	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) **Anmerkung:** Optional bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-cpwd	Kennwort abfragen	Zeichenkette (mindestens 6 Zeichen, höchstens 30 Zeichen) **Anmerkung:** Optional bei der Erstellung einer Zertifikatssignieranforderung.
-un	Unstrukturierter Name	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) **Anmerkung:** Optional bei der Erstellung einer Zertifikatssignieranforderung.

Syntax:

```
sslcfg [Optionen]
Option:
  -server Zustand
  -client Zustand
  -cim Zustand
  -cert Zertifikatstyp
```

```
  -csr Zertifikatstyp
  -i IP-Adresse
  -pn Portnummer
  -u Benutzername
  -pw Kennwort
  -l Dateiname
  -dnld
  -upld
  -tcx Maßnahme
  -c Landescode
  -sp Land_oder_Bundesland
  -cl Ort_oder_Standort
  -on Name_des_Unternehmens
  -hn IMM-Hostname
  -cp Ansprechpartner
  -ea E-Mail-Adresse
  -ou Organisationseinheit
  -s Nachname
  -gn Vorname
  -in Initialen
  -dq Qualifikationsmerkmal_des_Domänennamens
  -cpwd Kennwort_abfragen
  -un Unstrukturierter_Name
```

Beispiel:

```
system> sslcfg
-server enabled
-client disabled
-sysdir enabled
SSL Server Certificate status:
 A self-signed certificate is installed
SSL Client Certificate status:
 A self-signed certificate is installed
SSL CIM Certificate status:
 A self-signed certificate is installed
SSL Client Trusted Certificate status:
 Trusted Certificate 1: Not available
 Trusted Certificate 2: Not available
 Trusted Certificate 3: Not available
 Trusted Certificate 4: Not available
system>
```

Befehl "telnetcfg"

Mit dem Befehl **telnetcfg** können Sie Telnet-Einstellungen anzeigen und konfigurieren.

Wird der Befehl **telnetcfg** ohne Optionen ausgeführt, so wird der Telnet-Zustand angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-en	Telnet-Zustand	disabled (inaktiviert), 1, 2 **Anmerkung:** Wenn Telnet nicht inaktiviert wird, ist es für entweder einen oder zwei Benutzer aktiviert.

Syntax:

```
telnetcfg [Optionen]
Option:
  -en Zustand
```

Beispiel:

```
system> telnetcfg
-en 1
system>
```

Befehl "thermal"

Verwenden Sie den Befehl **thermal**, um die Richtlinie für den Temperaturmodus des Hostsystems anzuzeigen und zu konfigurieren.

Wird der Befehl **thermal** ohne Optionen ausgeführt, so wird die Richtlinie für den Temperaturmodus angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-mode	Auswahl des Temperaturmodus	normal, performance

Syntax:

```
thermal [Optionen]
Option:
  -mode Temperaturmodus
```

Beispiel:

```
system> thermal
-mode normal
system>
```

Befehl "timeouts"

Mit dem Befehl **timeouts** können Sie die Zeitlimitwerte anzeigen oder ändern. Um die Zeitlimitwerte anzuzeigen, geben Sie `timeouts` ein. Um die Zeitlimitwerte zu ändern, geben Sie die entsprechenden Optionen gefolgt von den Werten ein. Um Zeitlimitwerte ändern zu können, müssen Sie mindestens über die Berechtigung "Adapter Configuration" (Adapterkonfiguration) verfügen.

In der folgenden Tabelle sind die Argumente für die Zeitlimitwerte aufgelistet. Diese Werte entsprechen den abgestuften Pulldownoptionsskalen für Serverzeitlimits in der Webschnittstelle.

Option	Zeitlimit	Einheiten	Werte
-f	Ausschaltverzögerung	Minuten	disabled, 0.5, 1, 2, 3, 4, 5, 7.5, 10, 15, 20, 30, 60, 120
-l	Zeitlimit für das Ladeprogramm	Minuten	disabled, 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, 5, 7.5, 10, 15, 20, 30, 60, 120
-o	Zeitlimit für das Betriebssystem	Minuten	disabled, 2.5, 3, 3.5, 4

Syntax:

```
timeouts [Optionen]
Optionen:
-f Watchdogoption_für_Ausschaltverzögerung
-o Option_für_Betriebssystem-Watchdog
-l Option_für_Ladeprogramm-Watchdog
```

Beispiel:

```
system> timeouts
-o disabled
-l 3.5
system> timeouts -o 2.5
ok
system> timeouts
-o 2.5
-l 3.5
```

Befehl "usbeth"

Mit dem Befehl **usbeth** können Sie die Inbandschnittstelle "LAN over USB" aktivieren oder inaktivieren.

Syntax:

```
usbeth [Optionen]
Optionen:
-en <enabled|disabled>
```

Beispiel:

```
system>usbeth
-en : disabled
system>usbeth -en enabled
ok
system>usbeth
-en : disabled
```

Befehl "users"

Mit dem Befehl **users** können Sie auf alle Benutzerkonten und auf die zugehörigen Berechtigungsstufen zugreifen. Mit dem Befehl **users** können Sie außerdem neue Benutzerkonten erstellen und bereits vorhandene Konten ändern.

Wenn Sie den Befehl **users** ohne Optionen ausführen, werden eine Liste der Benutzer und bestimmte grundlegende Benutzerinformationen angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-Benutzer-index	Indexnummer des Benutzerkontos	1 bis 12 einschließlich oder `all` für alle Benutzer.
-n	Name des Benutzerkontos	Eindeutige Zeichenfolge, die nur Zahlen, Buchstaben, Punkte und Unterstriche enthält. Mindestens vier Zeichen; höchstens 16 Zeichen.
-p	Kennwort des Benutzerkontos	Zeichenfolge, die mindestens ein alphabetisches und ein nicht alphabetisches Zeichen enthält. Mindestens sechs Zeichen; höchstens 20 Zeichen. Mit null Zeichen wird ein Konto ohne Kennwort erstellt. Der Benutzer muss das Kennwort bei der ersten Anmeldung festlegen.

Option	Beschreibung	Werte
-a	Benutzerberechtigungsstufe	super, ro, custom Dabei gilt: • `super` (Supervisor) • `ro` (Lesezugriff) • `custom` wird gefolgt von einem Doppelpunkt und einer Liste mit Werten, die durch Pipes voneinander getrennt sind, wie im folgenden Format: `custom:am|rca`. Diese Werte können in beliebiger Kombination verwendet werden. `am` (Benutzerkontenverwaltungszugriff) `rca` (Zugriff auf ferne Konsole) `rcvma` (Zugriff auf ferne Konsole und virtuelle Datenträger) `pr` (Zugriff auf Einschalten/Neustart eines fernen Servers) `cel` (Berechtigung zum Löschen von Ereignisprotokollen) `bc` (Adapterkonfiguration - Allgemein) `nsc` (Adapterkonfiguration - Netz und Sicherheit) `rcvma` (Adapterkonfiguration - Erweitert)
-ep	Verschlüsselungskennwort (für Sicherung/ Wiederherstellung)	Gültiges Kennwort
-clear	Angegebenes Benutzerkonto entfernen	Die Indexnummer des zu entfernenden Benutzerkontos muss im folgenden Format angegeben werden: `users -clear -`*`Benutzerindex`*
-curr	Aktuell angemeldete Benutzer anzeigen	
-sauth	SNMPv3-Authentifizierungsprotokoll	HMAC-MD5, HMAC-SHA, none
-spriv	SNMPv3-Datenschutzprotokoll	CBC-DES, AES, none
-spw	SNMPv3-Datenschutzkennwort	Gültiges Kennwort
-sepw	SNMPv3-Datenschutzkennwort (verschlüsselt)	Gültiges Kennwort
-sacc	SNMPv3-Zugriffstyp	get, set
-strap	SNMPv3-Trap-Hostname	Gültiger Hostname

Option	Beschreibung	Werte
-pk	Öffentlichen SSH-Schlüssel für Benutzer anzeigen	Indexnummer des Benutzerkontos. **Anmerkung:** • Es werden jeder dem Benutzer zugeordnete SSH-Schlüssel und die jeweilige Schlüsselindexnummer angezeigt. • Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option `-pk` nach dem Benutzerindex (Option *`-Benutzerindex`*) im folgenden Format verwendet werden: `users -2 -pk`. • Alle Schlüssel weisen das OpenSSH-Format auf.
-e	Vollständigen SSH-Schlüssel im OpenSSH-Format anzeigen *(Option für öffentliche SSH-Schlüssel)*	Diese Option kann nur ohne Argumente verwendet werden. Sie muss ohne die anderen Optionen vom Typ `users -pk` verwendet werden. **Anmerkung:** Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option `-pk` nach dem Benutzerindex (Option *`-Benutzerindex`*) im folgenden Format verwendet werden: `users -2 -pk -e`.
-remove	Öffentlichen SSH-Schlüssel für Benutzer entfernen *(Option für öffentliche SSH-Schlüssel)*	Die Indexnummer des öffentlichen Schlüssels, der entfernt werden soll, muss für einen bestimmten Schlüssel mit *`-Schlüsselindex`* oder für alle dem Benutzer zugeordneten Schlüssel mit `-all` angegeben werden. **Anmerkung:** Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option `-pk` nach dem Benutzerindex (Option *`-Benutzerindex`*) im folgenden Format verwendet werden: `users -2 -pk -remove -1`.
-add	Öffentlichen SSH-Schlüssel für Benutzer hinzufügen *(Option für öffentliche SSH-Schlüssel)*	Durch Anführungszeichen begrenzter Schlüssel im OpenSSH-Format **Anmerkung:** • Die Option `-add` muss ohne die anderen Befehlsoptionen vom Typ `users -pk` verwendet werden. • Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option `-pk` nach dem Benutzerindex (Option *`-Benutzerindex`*) im folgenden Format verwendet werden: `users -2 -pk -add "AAAAB3NzC1yc2EAAAABIwAAA QEAvfnTUzRF7pdBuaBy4dO/aIFasa/Gtc+o/wlZnuC4aD HMA1UmnMyLOCiIaNOy4OOICEKCqjKEhrYymtAoVtfKApv Y39GpnSGRC/qcLGWLM4cmirKL5kxHNOqIcwbT1NPceoKH j46X7E+mqlfWnAhhjDpcVFjagM3Ek2y7w/tBGrwGgN7DP HJU1tzcJy68mEAnIrzjUoR98Q3/B9cJD77ydGKe8rPdI2 hIEpXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTBl3SAtMu cUsTkYjlXcqex1OQz4+N50R6MbNcwlsx+mTEAvvcpJhug a70UNPGhLJMl6k7jeJiQ8Xd2p XbOZQ=="`

Option	Beschreibung	Werte
-upld	Öffentlichen SSH-Schlüssel hochladen *(Option für öffentliche SSH-Schlüssel)*	Die Optionen `-i` und `-l` sind für die Angabe der Schlüsselposition erforderlich. **Anmerkung:** • Die Option `-upld` muss ohne die anderen Befehlsoptionen vom Typ `users -pk` verwendet werden (mit Ausnahme der Optionen `-i` und `-l`). • Um einen Schlüssel durch einen neuen Schlüssel zu ersetzen, müssen Sie einen *-Schlüsselindex* angeben. Wenn Sie einen Schlüssel zum Ende der Liste der aktuellen Schlüssel hinzufügen möchten, geben Sie keinen Schlüsselindex an. • Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option `-pk` nach dem Benutzerindex (Option *-Benutzerindex*) im folgenden Format verwendet werden: `users -2 -pk -upld -i tftp://9.72.216.40/ -l file.key`.
-dnld	Angegebenen öffentlichen SSH-Schlüssel herunterladen *(Option für öffentliche SSH-Schlüssel)*	Der *-Schlüsselindex* zum Herunterladen des betreffenden Schlüssels und die Optionen `-i` und `-l` zum Angeben der Speicherposition für den Download (auf einem anderen Computer als auf dem, auf dem ein TFTP-Server ausgeführt wird) sind erforderlich. **Anmerkung:** • Die Option `-dnld` muss ohne die anderen Befehlsoptionen vom Typ `users -pk` verwendet werden (mit Ausnahme von `-i`, `-l` und *-Schlüsselindex*). • Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option `-pk` nach dem Benutzerindex (Option *-Benutzerindex*) im folgenden Format verwendet werden: `users -2 -pk -dnld -1 -i tftp://9.72.216.40/ -l file.key`.
-i	IP-Adresse des TFTP/SFTP-Server zum Hoch- oder Herunterladen einer Schlüsseldatei *(Option für öffentliche SSH-Schlüssel)*	Gültige IP-Adresse **Anmerkung:** Die Option `-i` ist für die Befehlsoptionen `users -pk -upld` und `users -pk -dnld` erforderlich.
-pn	Portnummer des TFTP/SFTP-Servers *(Option für öffentliche SSH-Schlüssel)*	Gültige Portnummer (Standard 69/22) **Anmerkung:** Ein optionaler Parameter für die Befehlsoptionen `users -pk -upld` und `users -pk -dnld`.
-u	Benutzername für SFTP-Server *(Option für öffentliche SSH-Schlüssel)*	Gültiger Benutzername **Anmerkung:** Ein optionaler Parameter für die Befehlsoptionen `users -pk -upld` und `users -pk -dnld`.
-pw	Kennwort für SFTP-Server *(Option für öffentliche SSH-Schlüssel)*	Gültiges Kennwort **Anmerkung:** Ein optionaler Parameter für die Befehlsoptionen `users -pk -upld` und `users -pk -dnld`.

Option	Beschreibung	Werte
-l	Dateiname zum Hoch- oder Herunterladen einer Schlüsseldatei über TFTP oder SFTP *(Option für öffentliche SSH-Schlüssel)*	Gültiger Dateiname **Anmerkung:** Die Option `-l` ist für die Befehlsoptionen `users -pk -upld` und `users -pk -dnld` erforderlich.
-af	Verbindungen vom Host akzeptieren *(Option für öffentliche SSH-Schlüssel)*	Eine durch Kommas getrennte Liste von Hostnamen und IP-Adressen, begrenzt auf 511 Zeichen. Gültige Zeichen: alphanumerisch, Komma, Stern, Fragezeichen, Ausrufezeichen, Punkt, Bindestrich, Doppelpunkt und Prozentzeichen.
-cm	Kommentar *(Option für öffentliche SSH-Schlüssel)*	Eine durch Anführungszeichen begrenzte Zeichenfolge von bis zu 255 Zeichen. **Anmerkung:** Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option `-pk` nach dem Benutzerindex (Option *-Benutzerindex*) im folgenden Format verwendet werden: `users -2 -pk -cm "This is my comment."`.

Syntax:

```
users [Optionen]
 Optionen:
   -Benutzerindex
   -n Benutzername
   -p Kennwort
   -a Berechtigungsstufe
   -ep Verschlüsselungskennwort
   -clear
   -curr
   -sauth Protokoll
   -spriv Protokoll
   -spw Kennwort
   -sepw Kennwort
   -sacc Zustand
   -strap Hostname
users -pk [Optionen]
 Optionen:
   -e
   -remove Index
   -add Schlüssel
   -upld
   -dnld
   -i IP-Adresse
   -pn Portnummer
   -u Benutzername
   -pw Kennwort
   -l Dateiname
   -af Liste
   -cm Kommentar
```

Beispiel:

```
system> users
1. USERID Read/Write
Password Expires: no expiration
2. manu Read Only
Password Expires: no expiration
3. eliflippen Read Only
Password Expires: no expiration
```

```
4.  <not used>
5. jacobyackenovic custom:cel|ac
Password Expires: no expiration
system> users -7 -n sptest -p PASSW0RD -a custom:am|rca|cel|nsc|ac
ok
system> users
1. USERID  Read/Write
Password Expires: no expiration
2. test    Read/Write
Password Expires: no expiration
3. test2   Read/Write
Password Expires: no expiration
4. <not used>
5. jacobyackenovic custom:cel|ac
Password Expires: no expiration
6. <not used>
7. sptest  custom:am|rca|cel|nsc|ac
Password Expires: no expiration
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>
system>
```

IMM2-Steuerbefehle

Die Steuerbefehle für das IMM2 lauten wie folgt:

- „Befehl "alertentries"“
- „Befehl "batch"“ auf Seite 205
- „Befehl "clearcfg"“ auf Seite 206
- „Befehl "clock"“ auf Seite 206
- „Befehl "identify"“ auf Seite 207
- „Befehl "info"“ auf Seite 207
- „Befehl "resetsp"“ auf Seite 208
- „Befehl "spreset"“ auf Seite 208

Befehl "alertentries"

Mit dem Befehl **alertentries** können Sie Alertempfänger verwalten.

- Wird **alertentries** ohne Optionen ausgeführt, so werden alle Alerteintragseinstellungen angezeigt.
- Beim Befehl **alertentries -number -test** wird ein Testalert an die angegebene Empfängerindexnummer generiert.
- Beim Befehl **alertentries -number** (wobei für 'number' eine Zahl zwischen 0 und 12 steht) werden Alerteintragseinstellungen für die angegebene Empfängerindexnummer angezeigt oder es wird Ihnen ermöglicht, die Alerteinstellungen für diesen Empfänger zu ändern.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-number	Indexnummer des Alertempfängers, der angezeigt, hinzugefügt, geändert oder gelöscht werden soll	1 bis 12

Option	Beschreibung	Werte
-status	Alertempfängerstatus	on, off
-type	Alerttyp	email, syslog
-log	Ereignisprotokoll in Alert-E-Mail einschließen	on, off
-n	Alertempfängername	Zeichenkette
-e	E-Mail-Adresse des Alertempfängers	Gültige E-Mail-Adresse
-ip	Syslog-IP-Adresse oder Hostname	Gültige IP-Adresse oder gültiger Hostname
-pn	Syslog-Portnummer	Gültige Portnummer
-del	Angegebene Empfängerindexnummer löschen	
-test	Generiert einen Testalert an die angegebene Empfängerindexnummer	
-crt	Legt kritische Ereignisse fest, die Alerts senden	all, none, custom:te | vo | po | di | fa | cp | me | in | re | ot Benutzerdefinierte Einstellungen für kritische Alerts werden mithilfe einer Liste, in der die einzelnen Werte durch Pipe-Zeichen voneinander getrennt sind, mit Werten in der Form **alertentries -crt custom:te | vo** angegeben; benutzerdefinierte Werte sind: • te: kritischer Temperaturschwellenwert überschritten • vo: kritischer Spannungsschwellenwert überschritten • po: kritischer Netzausfall • di: Fehler beim Festplattenlaufwerk • fa: Lüfterfehler • cp: Mikroprozessorfehler • me: Speicherfehler • in: Hardwareinkompatibilität • re: Stromversorgungsredundanzfehler • ot: alle anderen kritischen Ereignisse
-crten	Alerts bei kritischen Ereignissen senden	enabled, disabled

Option	Beschreibung	Werte
-wrn	Legt Warnungsereignisse fest, die Alerts senden	all, none, custom:rp | te | vo | po | fa | cp | me | ot Benutzerdefinierte Einstellungen für Warnungsalerts werden mithilfe einer Liste, in der die einzelnen Werte durch Pipe-Zeichen voneinander getrennt sind, mit Werten in der Form **alertentries -wrn custom:rp | te** angegeben; benutzerdefinierte Werte sind: • rp: Warnung bei Stromversorgungsredundanz • te: Warnungstemperaturschwellenwert überschritten • vo: Warnungsspannungsschwellenwert überschritten • po: Warnungsnetzschwellenwert überschritten • fa: unkritischer Lüfterfehler • cp: Mikroprozessor in beeinträchtigtem Zustand • me: Speicherwarnung • ot: alle anderen Warnungsereignisse
-wrnen	Alerts bei Warnungsereignissen senden	enabled, disabled
-sys	Legt Routineereignisse fest, die Alerts senden	all, none, custom:lo | tio | ot | po | bf | til | pf | el | ne Benutzerdefinierte Einstellungen für Routinealerts werden mithilfe einer Liste, in der die einzelnen Werte durch Pipe-Zeichen voneinander getrennt sind, mit Werten in der Form **alertentries -sys custom:lo | tio** angegeben; benutzerdefinierte Werte sind: • lo: erfolgreiche Fernanmeldung • tio: Zeitlimit des Betriebssystems • ot: alle anderen Informations- und Systemereignisse • po: Stromversorgung des Systems ein/aus • bf: Bootfehler des Betriebssystems • til: Watchdog-Zeitlimitüberschreitung des Betriebssystemladeprogramms • pf: vorhergesagter Fehler (PFA - Predictive Failure Analysis) • el: Ereignisprotokoll zu 75% voll • ne: Netzänderung
-sysen	Alerts bei Routineereignissen senden	enabled, disabled

Syntax:

```
alertentries [Optionen]
   Optionen:
   -number Empfängernummer
      -status Status
      -type Alerttyp
      -log Protokollzustand_einschließen
      -n Empfängername
      -e E-Mail-Adresse
      -ip IP-Adresse_oder_Hostname
      -pn Portnummer
      -del
      -test
```

```
-crt Ereignistyp
-crten Zustand
-wrn Ereignistyp
-wrnen Zustand
-sys Ereignistyp
-sysen Zustand
```

Beispiel:

```
system> alertentries
1. test
2. <not used>
3. <not used>
4. <not used>
5. <not used>
6. <not used>
7. <not used>
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>

system> alertentries -1
-status off
-log off
-n test
-e test@mytest.com
-crt all
-wrn all
-sys none
system>
```

Befehl "batch"

Mit dem Befehl **batch** können Sie einen oder mehrere in einer Datei enthaltene CLI-Befehle ausführen.

- Kommentarzeilen in der Batchdatei beginnen mit einem #.
- Beim Ausführen einer Batchdatei werden fehlgeschlagene Befehle zusammen mit einem Fehlerrückgabecode zurückgeleitet.
- Batchdateibefehle, die nicht erkannte Befehlsoptionen enthalten, generieren möglicherweise Warnungen.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-f	Name der Batchdatei	Gültiger Dateiname
-ip	IP-Adresse des TFTP-/SFTP-Servers	Gültige IP-Adresse
-pn	Portnummer des TFTP-/SFTP-Servers	Gültige Portnummer (Standard 69/22)
-u	Benutzername für SFTP-Server	Gültiger Benutzername
-pw	Kennwort für SFTP-Server	Gültiges Kennwort

Syntax:

```
batch [Optionen]
Option:
  -f Dateiname
  -ip IP-Adresse
  -pn Portnummer
  -u Benutzername
  -pw Kennwort
```

Beispiel:

```
system> batch –f sslcfg.cli –ip 192.168.70.200
1 : sslcfg –client –dnld –ip 192.168.70.20
Command total/errors/warnings: 8 / 1 / 0
system>
```

Befehl "clearcfg"

Mit dem Befehl **clearcfg** können Sie die IMM2-Konfiguration auf die werkseitigen Voreinstellungen zurücksetzen. Sie müssen mindestens über die Berechtigung "Advanced Adapter Configuration" (Erweiterte Adapterkonfiguration) verfügen, um diesen Befehl ausgeben zu können. Nachdem die Konfiguration des IMM2 gelöscht wurde, wird das IMM2 erneut gestartet.

Befehl "clock"

Mit dem Befehl **clock** können Sie das aktuelle Datum und die aktuelle Uhrzeit entsprechend der IMM2-Uhr und der GMT-Abweichung anzeigen. Sie können das Datum, die Uhrzeit, die GMT-Abweichung und die Sommerzeiteinstellungen festlegen.

Beachten Sie Folgendes:

- Für eine GMT-Abweichung von +2, -7, -6, -5, -4 oder -3 sind besondere Einstellungen für die Sommerzeit erforderlich:
  - Für +2 gibt es folgende Optionen für die Sommerzeit: off, ee (Eastern Europe), mik (Minsk), tky (Turkey), bei (Beirut), amm (Amman), jem (Jerusalem).
  - Für -7 gibt es folgende Sommerzeiteinstellungen: off, mtn (Mountain), maz (Mazatlan).
  - Für -6 gibt es folgende Sommerzeiteinstellungen: off, mex (Mexico), cna (Central North America).
  - Für -5 gibt es folgende Sommerzeiteinstellungen: off, cub (Cuba), ena (Eastern North America).
  - Für -4 gibt es folgende Sommerzeiteinstellungen: off, asu (Asuncion), cui (Cuiaba), san (Santiago), cat (Canada - Atlantic).
  - Für -3 gibt es folgende Sommerzeiteinstellungen: off, gtb (Godthab), moo (Montevideo), bre (Brazil - East).
- Das Jahr muss von 2000 bis einschließlich 2089 angegeben werden.
- Monat, Datum, Stunden, Minuten und Sekunden können als Einzelzifferwerte angegeben werden (z. B. 9:50:25 anstatt 09:50:25).
- Die GMT-Abweisung kann im Format +2:00, +2 oder 2 (für positive Abweichungen) und im Format -5:00 oder -5 (für negative Abweichungen) angegeben werden.

Syntax:

```
clock [Optionen]
Optionen:
-d mm/tt/jjjj
-t hh:mm:ss
-g gmt offset
-dst on/off/special case
```

Beispiel:

```
system> clock
12/12/2011 13:15:23 GMT-5:00 dst on
system> clock -d 12/31/2011
ok
system> clock
12/31/2011 13:15:30 GMT-5:00 dst on
```

Befehl "identify"

Mit dem Befehl **identify** können Sie die Gehäusekennzeichnungsanzeige einschalten, ausschalten oder blinken lassen. Die Option -d kann zusammen mit -s verwendet werden, um die Anzeige nur für eine bestimmte Anzahl an Sekunden einzuschalten, die mit dem Parameter -d angegeben werden. Nachdem die Anzahl an Sekunden verstrichen ist, wird die Anzeige ausgeschaltet.

Syntax:

```
identify [Optionen]
Optionen:
-s on/off/blink
-d Sekunden
```

Beispiel:

```
system> identify
-s off
system> identify -s on -d 30
ok
system>
```

Befehl "info"

Mit dem Befehl **info** können Sie die Informationen zum IMM2 anzeigen und konfigurieren.

Wird der Befehl **info** ohne Optionen ausgeführt, so werden alle Standort- und Kontaktinformationen zum IMM2 angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-name	Name des IMM2	Zeichenkette
-contact	Name des Ansprechpartners für das IMM2	Zeichenkette
-location	IMM2-Standort	Zeichenkette
-room[1]	Raum-ID des IMM2	Zeichenkette
-rack[1]	Gehäuserahmen-ID des IMM2	Zeichenkette
-rup[1]	Position des IMM2 im Gehäuserahmen	Zeichenkette
-ruh	Höhe der Gehäuserahmeneinheit	Read only (Lesezugriff)

Option	Beschreibung	Werte
-bbay	Standort der Bladeposition	Read only (Lesezugriff)
1. Der Wert lautet "read only" und kann nicht zurückgesetzt werden, wenn sich das IMM2 auf einem IBM Flex System-Knoten befindet.		

Syntax:

```
info [Optionen]
Option:
  -name IMM-Name
  -contact Name_des_Ansprechpartners
  -location  IMM-Standort
  -room Raum-ID
  -rack Gehäuserahmen-ID
  -rup Position_der_Gehäuserahmeneinheit
  -ruh Höhe_der_Gehäuserahmeneinheit
  -bbay Bladeposition
```

Befehl "resetsp"

Mit dem Befehl **resetsp** können Sie das IMM2 erneut starten. Sie müssen mindestens über die Berechtigung "Advanced Adapter Configuration" (Erweiterte Adapterkonfiguration) verfügen, um diesen Befehl ausgeben zu können.

Befehl "spreset"

Mit dem Befehl **spreset** können Sie das IMM2 erneut starten. Sie müssen mindestens über die Berechtigung "Advanced Adapter Configuration" (Erweiterte Adapterkonfiguration) verfügen, um diesen Befehl ausgeben zu können.

Anhang A. Hilfe und technische Unterstützung anfordern

Wenn Sie Hilfe, Service oder technische Unterstützung benötigen oder einfach nur Informationen zu IBM-Produkten erhalten möchten, finden Sie bei IBM eine Vielzahl von hilfreichen Quellen.

Verwenden Sie diese Informationen, um zusätzliche Informationen zu IBM und IBM Produkten zu erhalten, um herauszufinden, was Sie bei Problemen mit Ihrem IBM System oder Ihrer Zusatzeinrichtung tun können und an wen Sie sich wenden können, wenn Sie Service benötigen.

Bevor Sie sich an den Kundendienst wenden

Stellen Sie sicher, bevor Sie sich an den Kundendienst wenden, dass Sie die folgenden Schritte durchgeführt haben, um zu versuchen, das Problem selbst zu beheben.

Wenn Sie denken, dass Sie den IBM Herstellerservice für Ihr IBM Produkt in Anspruch nehmen müssen, können die IBM Kundendiensttechniker Sie besser unterstützen, wenn Sie sich vor Ihrem Anruf beim Kundendienst vorbereiten.

- Überprüfen Sie alle Kabel und vergewissern Sie sich, dass diese angeschlossen sind.
- Prüfen Sie an den Netzschaltern, ob das System und die Zusatzeinrichtungen eingeschaltet sind.
- Überprüfen Sie, ob aktualisierte Software, Firmware und Einheitentreiber für das Betriebssystem Ihres IBM Produkts vorhanden sind. In den Bedingungen des freiwilligen IBM Herstellerservices steht, dass Sie als Eigentümer des Produkts dafür verantwortlich sind, die Software und Firmware für das Produkt zu warten und zu aktualisieren (es sei denn, dies ist durch einen zusätzlichen Wartungsvertrag abgedeckt). Der IBM Kundendiensttechniker wird Sie dazu auffordern, ein Upgrade für Ihre Software und Firmware durchzuführen, wenn in einem Software-Upgrade eine dokumentierte Lösung für das Problem vorhanden ist.
- Wenn Sie neue Hardware oder Software in Ihrer Umgebung installiert haben, überprüfen Sie unter http://www.ibm.com/systems/info/x86servers/serverproven/compat/us, ob die Hardware und Software von Ihrem IBM Produkt unterstützt werden.
- Rufen Sie die folgende Seite auf http://www.ibm.com/supportportal, um nach Informationen zu suchen, die Ihnen bei der Fehlerbehebung helfen können.
- Stellen Sie für den IBM Support folgende Informationen zusammen. Mithilfe dieser Daten findet der IBM Support schnell eine Lösung für Ihr Problem und kann sicherstellen, dass Sie genau die Servicestufe erhalten, die Sie vertraglich vereinbart haben.
  - Hardware- und Softwarewartungsvertragsnummern, falls vorhanden
  - Maschinentypnummer (vierstellige IBM Maschinenkennung)
  - Modellnummer
  - Seriennummer
  - Aktuelle UEFI- und Firmwareversionen des Systems
  - Andere relevante Informationen wie z. B. Fehlernachrichten und -protokolle

- Rufen Sie die folgende Seite auf http://www.ibm.com/support/entry/portal/Open_service_request, um eine ESR (Electronic Service Request - elektronische Serviceanforderung) zu senden. Wenn Sie eine ESR senden, beginnt der Lösungsfindungsprozess für Ihr Problem, da die relevanten Informationen dem IBM Support schnell und effizient zur Verfügung gestellt werden. IBM Kundendiensttechniker können mit der Fehlerbehebung beginnen, sobald Sie eine ESR ausgefüllt und übergeben haben.

Viele Fehler können ohne Hilfe von außen anhand der IBM Hinweise zur Fehlerbehebung in der Onlinehilfefunktion oder in der Dokumentation, die im Lieferumfang Ihres IBM Produkts enthalten ist, behoben werden. In der Begleitdokumentation der IBM Systeme sind auch die Diagnosetests beschrieben, die Sie ausführen können. Im Lieferumfang der meisten Systeme, Betriebssysteme und Programme sind eine Dokumentation zu Fehlerbehebungsprozeduren sowie Erläuterungen zu Fehlernachrichten und Fehlercodes enthalten. Wenn Sie einen Softwarefehler vermuten, finden Sie weitere Informationen dazu in der Dokumentation zum Betriebssystem oder zum Programm.

Dokumentation verwenden

Informationen zu Ihrem IBM System und, falls vorhanden, zu vorinstallierter Software sowie zu Zusatzeinrichtungen finden Sie in der mit dem Produkt gelieferten Dokumentation. Zu dieser Dokumentation können gedruckte Dokumente, Onlinedokumente, Readme-Dateien und Hilfedateien gehören.

Anweisungen zur Verwendung der Diagnoseprogramme finden Sie in den Fehlerbehebungsinformationen in der Systemdokumentation. Über die Fehlerbehebungsinformationen oder die Diagnoseprogramme erfahren Sie möglicherweise, dass Sie zusätzliche oder aktuelle Einheitentreiber oder andere Software benötigen. IBM verwaltet Seiten im World Wide Web, über die Sie nach den neuesten technischen Informationen suchen und Einheitentreiber und Aktualisierungen herunterladen können. Für den Zugriff auf diese Seiten rufen Sie http://www.ibm.com/supportportal auf.

Hilfe und Informationen über das World Wide Web anfordern

Aktuelle Informationen zu IBM Produkten und zur Unterstützung sind im World Wide Web verfügbar.

Im World Wide Web finden Sie aktuelle Informationen zu IBM Systemen, Zusatzeinrichtungen, Services und Unterstützung unter http://www.ibm.com/supportportal. Informationen zu IBM System x finden Sie unter http://www.ibm.com/systems/x. Informationen zu IBM BladeCenter finden Sie unter http://www.ibm.com/systems/bladecenter. Informationen zu IBM IntelliStation finden Sie unter http://www.ibm.com/systems/intellistation.

Vorgehensweise zum Senden von DSA-Daten an IBM

Senden Sie Ihre Diagnosedaten über das IBM Enhanced Customer Data Repository (ECuRep) an IBM.

Lesen Sie vor dem Senden von Diagnosedaten an IBM die Nutzungsbedingungen unter http://www.ibm.com/de/support/ecurep/terms.html.

Sie können eine der folgenden Methoden zum Senden von Diagnosedaten an IBM verwenden:

- **Standardupload:** http://www.ibm.com/de/support/ecurep/send_http.html
- **Standardupload mit der Seriennummer des Systems:** http://www.ecurep.ibm.com/app/upload_hw
- **Sicherer Upload:** http://www.ibm.com/de/support/ecurep/send_http.html#secure
- **Sicherer Upload mit der Seriennummer des Systems:** https://www.ecurep.ibm.com/app/upload_hw

Personalisierte Unterstützungswebseite erstellen

Durch die gezielte Angabe von IBM Produkten, an denen Sie interessiert sind, können Sie eine personalisierte Unterstützungswebseite erstellen.

Wenn Sie eine personalisierte Unterstützungswebseite erstellen möchten, rufen Sie folgende Adresse auf http://www.ibm.com/support/mynotifications. Über diese personalisierte Seite können Sie wöchentliche E-Mail-Benachrichtigungen zu neuen technischen Dokumenten abonnieren, nach Informationen und Downloads suchen und auf verschiedene Verwaltungsservices zugreifen.

Software-Service und -unterstützung

Über die IBM Support Line erhalten Sie gegen eine Gebühr telefonische Unterstützung bei Problemen mit der Nutzung, der Konfiguration und der Software von IBM Produkten.

Für weitere Informationen zur Support Line und zu anderen IBM Services rufen Sie http://www.ibm.com/services auf. Telefonnummern für Unterstützung finden Sie, wenn Sie http://www.ibm.com/planetwide aufrufen. In den Vereinigten Staaten oder in Kanada können Sie die folgende Nummer anrufen: 1-800-IBM-SERV (1-800-426-7378).

Hardware-Service und -unterstützung

Hardware-Service können Sie über den IBM Reseller oder den IBM Kundendienst erhalten.

Um nach einem Reseller zu suchen, der durch IBM zur Bereitstellung von Herstellerservice autorisiert wurde, rufen Sie http://www.ibm.com/partnerworld auf und klicken Sie rechts auf der Seite auf **Business Partner suchen**. Telefonnummern für technische Unterstützung von IBM finden Sie, wenn Sie http://www.ibm.com/planetwide aufrufen. In den Vereinigten Staaten oder in Kanada können Sie die folgende Nummer anrufen: 1-800-IBM-SERV (1-800-426-7378).

In den USA und in Kanada ist Hardware-Service und -unterstützung jederzeit rund um die Uhr erhältlich. In Großbritannien sind diese Serviceleistungen von Montag bis Freitag von 9 bis 18 Uhr verfügbar.

IBM Produktservice in Taiwan

Wenden Sie sich mithilfe dieser Informationen an den IBM Produktservice in Taiwan.

台灣 IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路 7 號 3 樓
電話：0800-016-888

Kontaktinformationen für den IBM Produktservice in Taiwan:

IBM Taiwan Corporation
3F, No 7, Song Ren Rd.
Taipei, Taiwan
Telefon: 0800-016-888

Anhang B. Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für die in diesem Handbuch beschriebenen Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieser Dokumentation ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes 2, avenue Gambetta
92066 Paris La Defense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Die auf diesen Websites verfügbaren Informationen beziehen sich nicht auf die für dieses IBM Produkt bereitgestellten Informationen. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Marken

IBM, das IBM Logo und ibm.com sind eingetragene Marken der International Business Machines Corporation. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein.

Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite http://www.ibm.com/legal/us/en/copytrade.shtml.

Adobe und PostScript sind Marken oder eingetragene Marken der Adobe Systems Incorporated in den USA und/oder anderen Ländern.

Cell Broadband Engine wird unter Lizenz verwendet und ist eine Marke der Sony Computer Entertainment, Inc. in den USA und/oder anderen Ländern.

Intel, Intel Xeon, Itanium und Pentium sind Marken oder eingetragene Marken der Intel Corporation oder ihrer Tochtergesellschaften in den USA und/oder anderen Ländern.

Java und alle auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken der Oracle Corporation und/oder ihrer verbundenen Unternehmen.

Linux ist eine eingetragene Marke von Linus Torvalds in den USA und/oder anderen Ländern.

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

UNIX ist eine eingetragene Marke von The Open Group in den USA und anderen Ländern.

Wichtige Hinweise

Die Prozessorgeschwindigkeit bezieht sich auf die interne Taktgeschwindigkeit des Mikroprozessors. Das Leistungsverhalten der Anwendung ist außerdem von anderen Faktoren abhängig.

Die Geschwindigkeit von CD- oder DVD-Laufwerken wird als die variable Lesegeschwindigkeit angegeben. Die tatsächlichen Geschwindigkeiten können davon abweichen und liegen oft unter diesem Höchstwert.

Bei Angaben in Bezug auf Hauptspeicher, realen/virtuellen Speicher oder Kanalvolumen steht die Abkürzung KB für 1.024 Bytes, MB für 1.048.576 Bytes und GB für 1.073.741.824 Bytes.

Bei Angaben zur Kapazität von Festplattenlaufwerken oder zu Übertragungsgeschwindigkeiten steht die Abkürzung MB für 1.000.000 Bytes und GB für 1.000.000.000 Bytes. Die gesamte für den Benutzer verfügbare Speicherkapazität kann je nach Betriebsumgebung variieren.

Die maximale Kapazität von internen Festplattenlaufwerken geht vom Austausch aller Standardfestplattenlaufwerke und der Belegung aller Festplattenlaufwerkpositionen mit den größten derzeit unterstützten Laufwerken aus, die IBM zur Verfügung stellt.

Zum Erreichen der maximalen Speicherkapazität muss der Standardspeicher möglicherweise durch ein optionales Speichermodul ersetzt werden.

Jede Halbleiterspeicherzelle verfügt über eine intrinsische, endliche Zahl von Schreibzyklen, welche die Zelle ausführen kann. Daher hat eine Halbleitereinheit eine maximale Anzahl von Schreibzyklen, die darauf ausgeführt werden können. Diese wird in „TBW" (total bytes written - Gesamtzahl der geschriebenen Bytes) angegeben.

Hat eine Einheit dieses Limit überschritten, antwortet sie möglicherweise nicht mehr auf vom System generierte Befehle oder kann nicht mehr beschrieben werden. IBM ist nicht für den Austausch einer Einheit verantwortlich, die ihre maximale Anzahl garantierter Programmierungs-/Löschzyklen überschritten hat, welche in den offiziellen, veröffentlichten Spezifikationen dieser Einheit dokumentiert ist.

IBM enthält sich jeder Äußerung in Bezug auf ServerProven-Produkte und -Services anderer Unternehmen und übernimmt für diese keinerlei Gewährleistung. Dies gilt unter anderem für die Gewährleistung der Gebrauchstauglichkeit und der Eignung für einen bestimmten Zweck. Für den Vertrieb dieser Produkte sowie entsprechende Gewährleistungen sind ausschließlich die entsprechenden Fremdanbieter zuständig.

IBM übernimmt keine Verantwortung oder Gewährleistungen bezüglich der Produkte anderer Hersteller. Eine eventuelle Unterstützung für Produkte anderer Hersteller erfolgt durch Drittanbieter, nicht durch IBM.

Manche Software unterscheidet sich möglicherweise von der im Einzelhandel erhältlichen Version (falls verfügbar) und enthält möglicherweise keine Benutzerhandbücher bzw. nicht alle Programmfunktionen.

Verunreinigung durch Staubpartikel

Achtung: Staubpartikel in der Luft (beispielsweise Metallsplitter oder andere Teilchen) und reaktionsfreudige Gase, die alleine oder in Kombination mit anderen Umgebungsfaktoren, wie Luftfeuchtigkeit oder Temperatur, auftreten, können für die in diesem Dokument beschriebene Einheit ein Risiko darstellen.

Zu den Risiken, die aufgrund einer vermehrten Staubbelastung oder einer erhöhten Konzentration gefährlicher Gase bestehen, zählen Beschädigungen, die zu einer Störung oder sogar zum Totalausfall der Einheit führen. Durch die in dieser Spezifikation festgelegten Grenzwerte für Staubpartikel und Gase sollen solche Beschädigungen vermieden werden. Diese Grenzwerte sind nicht als unveränderliche Grenzwerte zu betrachten oder zu verwenden, da viele andere Faktoren, wie z. B. die Temperatur oder der Feuchtigkeitsgehalt der Luft, die Auswirkungen von Staubpartikeln oder korrosionsfördernden Stoffen in der Umgebung sowie die Verbreitung gasförmiger Verunreinigungen beeinflussen können. Sollte ein bestimmter Grenzwert in diesem Dokument fehlen, müssen Sie versuchen, die Verunreinigung durch Staubpartikel und Gase so gering zu halten, dass die Gesundheit und die Sicherheit der beteiligten Personen dadurch nicht gefährdet sind. Wenn IBM feststellt, dass die Einheit aufgrund einer erhöhten Konzentration von Staubpartikeln oder Gasen in Ihrer Umgebung beschädigt wurde, kann IBM die Reparatur oder den Austausch von Einheiten oder Teilen unter der Bedingung durchführen, dass geeignete Maßnahmen zur Minimierung solcher Verunreinigungen in der Umgebung der Einheit ergriffen werden. Die Durchführung dieser Maßnahmen obliegt dem Kunden.

Tabelle 9. Grenzwerte für Staubpartikel und Gase

Verunreinigung	Grenzwerte
Staubpartikel	• Die Raumluft muss kontinuierlich mit einem Wirkungsgrad von 40 % gegenüber atmosphärischem Staub (MERV 9) nach ASHRAE-Norm 52.2[1] gefiltert werden. • Die Luft in einem Rechenzentrum muss mit einem Wirkungsgrad von mindestens 99,97 % mit HEPA-Filtern (HEPA - High-Efficiency Particulate Air) gefiltert werden, die gemäß MIL-STD-282 getestet wurden. • Die relative hygroskopische Feuchtigkeit muss bei Verunreinigung durch Staubpartikel mehr als 60 % betragen[2]. • Im Raum dürfen keine elektrisch leitenden Verunreinigungen wie Zink-Whisker vorhanden sein.
Gase	• Kupfer: Klasse G1 gemäß ANSI/ISA 71.04-1985[3] • Silber: Korrosionsrate von weniger als 300 Å in 30 Tagen

[1] ASHRAE 52.2-2008 - *Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size*. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

[2] Die relative hygroskopische Feuchtigkeit der Verunreinigung durch Staubpartikel ist die relative Feuchtigkeit, bei der der Staub genug Wasser absorbiert, um nass zu werden und Ionen leiten zu können.

[3] ANSI/ISA-71.04-1985. *Environmental conditions for process measurement and control systems: Airborne contaminants*. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

Dokumentationsformat

Die Veröffentlichungen für dieses Produkt liegen im PDF-Format vor und entsprechen den handelsüblichen Zugriffsstandards. Falls beim Verwenden der PDF-Dateien Probleme auftreten und Sie ein webbasiertes Format oder ein zugängliches PDF-Dokument für eine Veröffentlichung anfordern möchten, wenden Sie sich schriftlich an folgende Adresse:

Information Development
IBM Corporation
205/A015
3039 E. Cornwallis Road
P.O. Box 12195
Research Triangle Park, North Carolina 27709-2195
U.S.A.

Geben Sie in der Anforderung die Teilenummer und den Titel der Veröffentlichung an.

Werden an IBM Informationen eingesandt, gewährt der Einsender IBM ein nicht ausschließliches Recht zur beliebigen Verwendung oder Verteilung dieser Informationen, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Vorschriften zur Telekommunikation

Möglicherweise ist dieses Produkt in Ihrem Land nicht für den Anschluss an Schnittstellen von öffentlichen Telekommunikationsnetzen zertifiziert. Vor der Herstellung einer solchen Verbindung ist eine entsprechende Zertifizierung ggf. gesetzlich vorgeschrieben. Wenden Sie sich bei Fragen an einen IBM Ansprechpartner oder IBM Reseller.

Hinweise zur elektromagnetischen Verträglichkeit

Wenn Sie einen Bildschirm an das Gerät anschließen, müssen Sie das dazugehörige Bildschirmkabel und jede Störschutzeinheit, die im Lieferumfang des Bildschirms enthalten ist, verwenden.

Federal Communications Commission (FCC) statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that might cause undesired operation.

Industry Canada Class A emission compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Australia and New Zealand Class A statement

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

European Union EMC Directive conformance statement

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any fai-

lure to satisfy the protection requirements resulting from a nonrecommended modification of the product, including the fitting of non-IBM option cards.

Attention: This is an EN 55022 Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Responsible manufacturer:

International Business Machines Corp. New Orchard Road
Armonk, New York 10504
914-499-1900

European Community contact:

IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Deutschland
Telefon: +49 7032 15 2941
E-Mail: lugi@de.ibm.com

Deutschland - Hinweis zur Klasse A

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden: „Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem „Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)". Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV-Vorschriften ist der Hersteller:

International Business Machines Corp. New Orchard Road
Armonk, New York 10504
914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH
Technical Regulations, Abteilung M372
IBM-Allee 1, 71139 Ehningen, Deutschland
Postanschrift: 71137 Ehningen
Telefon: +49 7032 15 2941
E-Mail: lugi@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

Japan VCCI Class A statement

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI). If this equipment is used in a domestic environment, radio interference may occur, in which case the user may be required to take corrective actions.

Korea Communications Commission (KCC) statement

이 기기는 업무용(A급)으로 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

This is electromagnetic wave compatibility equipment for business (Type A). Sellers and users need to pay attention to it. This is for any areas other than home.

Russia Electromagnetic Interference (EMI) Class A statement

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать радиопомехи, для снижения которых необходимы дополнительные меры

People's Republic of China Class A electronic emission statement

中华人民共和国“A类”警告声明

声 明

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

Taiwan Class A compliance statement

警告使用者:
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Index

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z

Teilenummer: 47C9125

(1P) P/N: 47C9125