

ESMS の Web GUI (Graphical User Interface)

BMC

DIN EN ISO 9001:2008 に準拠した 認証を取得

高い品質とお客様の使いやすさが常に確保されるように、
このマニュアルは、DIN EN ISO 9001:2008
基準の要件に準拠した品質管理システムの規定を
満たすように作成されました。

cognitas. Gesellschaft für Technik-Dokumentation mbH
www.cognitas.de

著作権および商標

Copyright © 2013 Fujitsu Technology Solutions GmbH.

All rights reserved.

お届けまでの日数は在庫状況によって異なります。技術的修正の権利を有します。

使用されているハードウェア名およびソフトウェア名は、各社の商標です。

本書をお読みになる前に

お客様の安全のために

このマニュアルには、この製品を安全かつ正しくご使用いただくための重要な情報が記載されています。

この製品を使用する前に、マニュアルをよくお読みください。付属のマニュアル『Safety Notes and Regulations』をよくお読みになり、安全上の注意事項をご理解されたうえで製品を使用してください。

このマニュアルとマニュアル『Safety Notes and Regulations』は、この製品の使用中にすぐに参照できる安全な場所に保管してください。

電波妨害

この製品は、日本の情報処理装置等電波障害自主規制協議会（VCCI-A）で規定された「クラス A」の情報技術装置（ITE：Information Technology Equipment）です。この製品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。この場合にはユーザが適切な対策を取る必要のあることがあります。

アルミニウム電解コンデンサ

製品のプリント基板アセンブリとマウスおよびキーボードに使用されているアルミニウム電解コンデンサは、寿命のあるコンポーネントです。動作寿命を超えてこれらのコンポーネントを使用すると、電解質漏出や電解質減少が発生し、悪臭や煙が排出されることがあります。

ガイドラインとして、通常のオフィス環境（25°C）では、保守サポート期間（5 年）以内に動作寿命に達することはないと予想されます。ただし、製品を高温の環境で使用した場合などに、動作寿命が短くなることがあります。動作寿命を超えた交換可能なコンポーネントの交換コストはお客様にご負担いただきます。これらは単なるガイドラインですので、保守サポート期間中のトラブルフリーの動作を保証するものではありません。

高安全用途

この製品は、一般オフィス用、個人用、家庭用、一般工業用など、一般用途向けに設計および製造されています。極端に高度な安全性が要求される用途や、そのような安全性を保証できない限り生命や人体に直接および重大な危険を及ぼす用途向けに設計および製造されていません。

この製品の用途には、原子力発電所での核反応、自動飛行機の飛行制御、航空管制、公共交通機関の交通管制、生命維持用の医療機器、兵器システムのミサイル誘導コントロールなどが含まれます（以後、「高安全用途」とします）。お客様は、高安全用途に必要とされる安全性のレベルを保証するための措置が取られない限り、このような高安全用途にこの製品を使用してはなりません。高安全用途にこの製品を使用する予定がある場合は、弊社営業担当者にご相談ください。

瞬時電圧低下の測定

この製品は、雷によって生じた電源ユニットの瞬時電圧低下により影響を受ける可能性があります。瞬時電圧低下を防ぐために、AC 無停電電源装置の使用を推奨します。

（この注記は、JEITA（社団法人電子情報技術産業協会）が発行したガイドライン『パーソナルコンピュータの瞬時電圧低下対策』に従っています。）

日本の外為法、外国為替および外国貿易管理法によって規制されるテクノロジー

弊社が発行したドキュメントには、日本の外為法、外国為替および外国貿易管理法によってコントロールされるテクノロジーが含まれることがあります。このようなテクノロジーは、上記法律に従って最初に許可を受けずに、日本から国外に持ち出したり、日本の非居住者に譲渡してはなりません。

高調波電流規格

この製品は高調波電流規格 JIS C 61000-3-2 に準拠しています。

日本市場の場合のみ： SATA ハードディスクドライブについて

このサーバの SATA バージョンは、SATA/BC-SATA ストレージインタフェースを搭載したハードディスクドライブをサポートしています。ご使用のハードディスクドライブのタイプによって使用方法と動作条件が異なりますので、ご注意ください。

使用できるタイプのハードディスクドライブの使用方法と動作条件の詳細は、以下の Web サイトを参照してください。

<http://primeserver.fujitsu.com/primergy/harddisk/>

日本市場の場合のみ：



本書に記載されていても日本市場には適用されない項があります。以下のオプションおよび作業がこれに該当します。

- USB Flash Module (UFM)
- CSS (Customer Self Service)
- 標準の電源ユニットからホットプラグ電源ユニットへの変換
- DVD-RW ドライブ
- リチウムバッテリーの交換
- 他社製ラック

目次

1	ESMS の Web GUI (Graphical User Interface)	11
1.1	Web GUI の使用	11
1.2	ログイン	12
2	Dashboard	15
2.1	Device Information	16
2.2	Network Information	17
2.3	センサーの監視	18
2.4	イベントログ	18
3	サーバの情報	19
3.1	FRU Information	20
3.1.1	Basic Information	21
3.1.2	Chassis Information	21
3.1.3	Board Information	21
3.1.4	Product Information	22
3.2	Server Component	22
3.3	Server identify	24
4	Server Health Group	25
4.1	Sensor Readings	26
4.1.1	Sensor Type	27
4.1.2	Live Widget	28
4.1.3	View this Event Log	28
4.2	Event Log	29
4.2.1	Event Log Category	30

5	Configuration Group	31
5.1	Active Directory	32
5.1.1	役割グループを追加するには	35
5.1.2	役割グループを変更するには	36
5.1.3	役割グループを削除するには	36
5.2	DNS	36
5.3	LDAP/E-Directory	39
5.3.1	新しい役割グループを追加するには	42
5.3.2	役割グループを変更するには	42
5.3.3	役割グループを削除するには	43
5.4	マウスモード	43
5.5	Network	44
5.6	PEF	48
5.6.1	「Event Filter」 タブ	48
5.6.2	「Alert Policy」 タブ	51
5.6.3	「PEF Management LAN Destination」 ページ	54
5.7	RADIUS	57
5.8	Remote Session	59
5.9	SMTP	60
5.10	SOL	63
5.11	SSL	65
5.12	User Management	70
5.13	Virtual Media	75
6	Remote Control	77
6.1	Console Redirection	77
6.1.1	サポートされるクライアントオペレーティングシステムのリスト	78
6.1.2	サポートされるホストオペレーティングシステムのリスト	79
6.1.3	ブラウザの設定	79
6.1.4	Java コンソール	79
6.1.5	「Console Redirection」 メインメニュー	80
6.1.5.1	ビデオ	81
6.1.5.2	キーボード	82

1 ESMS の Web GUI (Graphical User Interface)

1.1 Web GUI の使用

BMC ファームウェアには組み込み Web サーバ機能があり、ユーザは Web ブラウザ (Microsoft Internet Explorer など) を使用して BMC も接続できます。

Web GUI には、管理中のサーバのシステム情報、システムイベント、システムステータス、およびその他のシステム関連の情報が表示されます。Web ベースの GUI は以下のブラウザでサポートされます。

- Internet Explorer 7 以降
- Firefox 2.0 以降
- Google Chrome 2.0 以降
- Safari 3.0 以降
- Opera 9.64 以降

1.2 ログイン

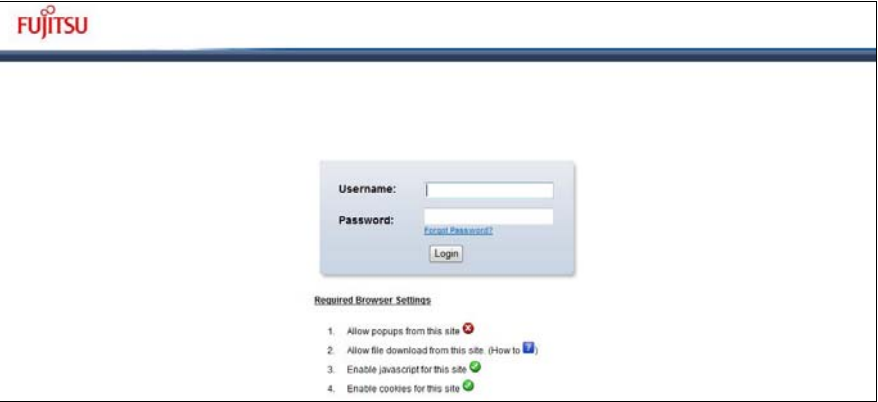
IP アドレスまたは URL（デフォルト DHCP\ 静的 IP アドレス）を Web ブラウザのアドレスバーに入力します。

BMC に接続すると、ログイン画面が表示され、ユーザ名とパスワードの入力が求められます。SSL で保護されたこの認証は、認証されていない侵入者が BMC Web サーバにアクセスするのを防ぎます。

ユーザ認証されると、役割の権限に従って、サーバを管理できます。

OEM Proprietary、Administrator、Operator 権限レベルには、Web インターフェイスにログインする権限があります。User および No Access 権限レベルでは、BMC Web GUI を通じてアクセスできません。

ログイン Web ページ



フィールド	デフォルト
Username	admin
Password	admin

表 1: デフォルトユーザ名とパスワード

メイン Web ページ


メニュー項目	説明
System Information	システム情報を表示します。
Server Health	サーバのステータスを監視します。
構成	IPMI 設定の構成
Remote Control	KVM コンソールを起動して電源を制御します。
Maintenance	ユーザはファームウェアアップデートを行うことができます。
Language	インターフェース言語を設定します。  現在、英語のみサポートしています。

表 2: メイン Web ページ

2 Dashboard

MegaRAC GUI では、「Dashboard」ページにデバイスのステータスに関する情報全般が表示されます。

「Dashboard」ページを開くには、メインメニューから「Dashboard」をクリックします。「Dashboard」ページのサンプルスクリーンショットを次に示します。

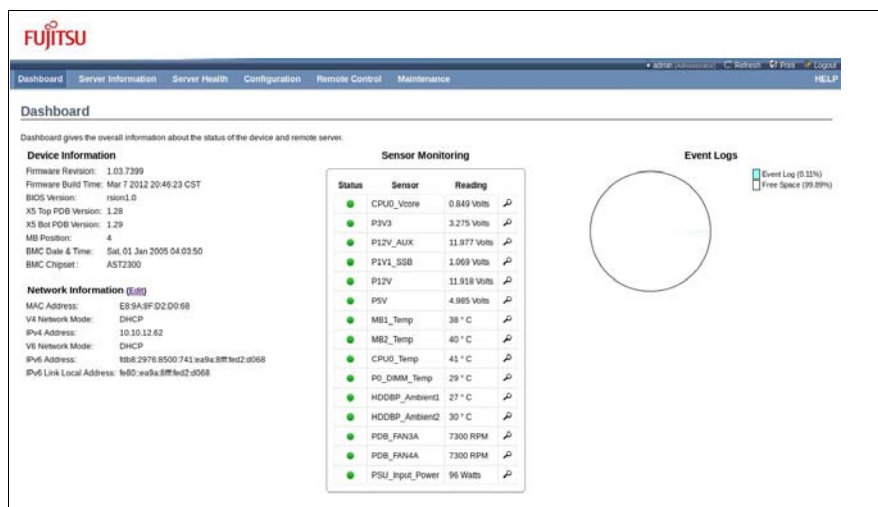


図 1: Dashboard

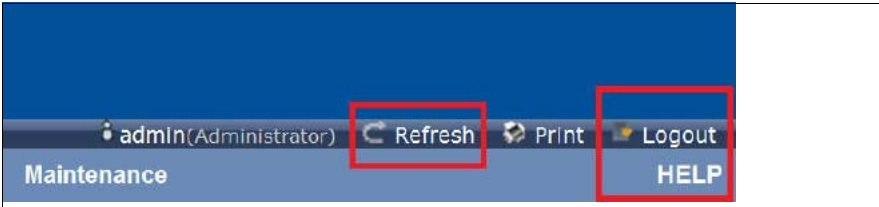
次の項で「Dashboard」ページについて簡単に説明します。

2.1 Device Information

認証に成功すると、次の Web ページが表示されます。

i デフォルトのユーザ名とパスワードは小文字です。ログインすると admin パスワードを変更するように促されます。

ご不明点がある場合はページの右隅にある「Help」ボタン、ページを更新する場合は「Refresh」ボタン、終了する場合は「Logout」ボタンをクリックします。



「Device Information」には以下の情報が表示されます。

アイテム	説明
Firmware Revision	ファームウェアのリビジョン番号。
Firmware Build Time	ファームウェアの日付けと時刻。
BIOS バージョン	BIOS のリビジョン番号。
X5 Top PDB Version	PDB (TOP) ファームウェアのリビジョン番号。
X5 Bot PDB Version	PDB (BOT) ファームウェアのリビジョン番号。
MB Position	サーバノードの位置
BMC Date & Time	現在の日付けと時刻。
BMC Chipset	このフィールドに BMC Chipset タイプが表示されます。

表 3: 「Device Information」 ページ

- i** BMC Chipset タイプのサポートリストを次に示します。
- AST2300 : 仮想 KVM 機能と関連する設定項目をサポートします。
 - 仮想 KVM を搭載しない AST2300 : 仮想 KVM 機能と関連する設定項目をサポートしません。

BMC Chipset タイプが 仮想 KVM を搭載しない AST2300 の場合は、メニュー項目の「Console Redirection」、「Mouse Mode」、「Remote Session」、「Media」が表示されません。

2.2 Network Information

デバイスの「Network Information」の以下のフィールドについて、次の表で説明します。Network Information を編集するには、「*Edit*」をクリックします。

アイテム	説明
Host Name	デバイスの DNS ホスト名を示す読み取り専用のフィールド。
MAC Address	デバイスの IP アドレスを示す読み取り専用のフィールド。
V4 Network Mode	v4 ネットワークモードのオプションは、次の無効、静的、DHCP のいずれかです。
IPv4 Address	デバイスの IPv4（静的または DHCP）。
V6 Network Mode	v6 ネットワークモードのオプションは、無効、静的、DHCP のいずれかです。
IPv6 Address	デバイスの IPv6 アドレス。

表 4: Network Information


2.3 センサーの監視

デバイスで使用可能なセンサーをすべて表示します。

デバイスのステータスカラムに、以下のようにデバイスの状態が表示されます。

ステータス（アイコン）	説明
	正常状態
	警告状態
	異常状態

表 5: ステータスアイコン

 をクリックすると、その特定のセンサーのセンサーページが表示されます。

2.4 イベントログ

さまざまなセンサーおよび占有 / 使用可能スペースによって発生したすべてのイベントが、ログにグラフィカルに表示されます。

3 サーバの情報

Server Information Group は、次の 3 つの項目で構成されます。

- FRU Information
- Server Component
- Server Identify

次のスクリーンショットは「Server Information」のメニュー項目です。

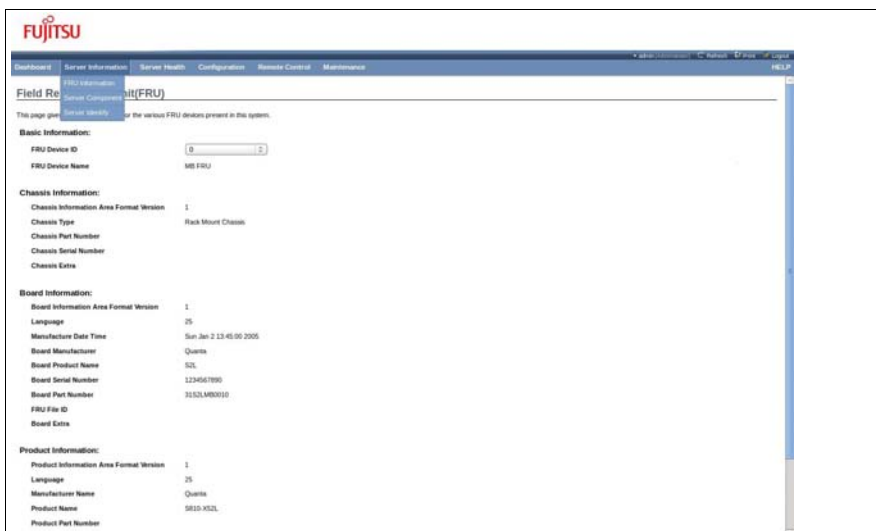


図 2: Server Information - メニュー

3.1 FRU Information

MegaRAC GUI では、「FRU Information」ページに BMC FRU ファイルの情報が表示されます。このページには、FRU デバイスの「Basic Information」、「Common Header Information」、「Chassis Information」、「Board Information」、「Product Information」が表示されます。

「FRU Information」ページを開くには、トップメニューで「*FRU Information*」をクリックします。「Basic Information」セクションの「FRU Device ID」を選択すると、選択したデバイスの詳細が表示されます。「FRU Information」ページのスクリーンショットを次に示します。



図 3: 「FRU Information」ページ

次の項で各フィールドについて簡単に説明します。

3.1.1 Basic Information

アイテム	説明
FRU device ID	デバイスの ID。
FRU Device Name	選択した FRU デバイスのデバイス名。

表 6: Basic Information

3.1.2 Chassis Information

- Chassis Information Area Format Version
- Chassis Type
- Chassis Part Number
- Chassis Serial Number
- Chassis Extra

3.1.3 Board Information

- Board Information Area Format Version
- Language
- Manufacture Date Time
- Board Manufacturer
- Board Product Name
- Board Serial Number
- Board Part Number
- FRU File ID
- Board Extra

3.1.4 Product Information

- Product Information Area Format Version
- Language
- Manufacturer Name
- Product Name
- Product Part Number
- Product Version
- Product Serial Number
- Asset Tag
- FRU File ID
- Product Extra

3.2 Server Component

「Component Information」ページには、CPU とメモリの情報が表示されます。

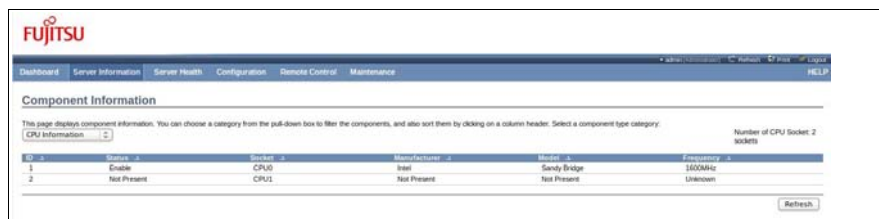


図 4: 「Component Information」ページ

アイテム	説明
CPU Information	<p>次の情報が表示されます。</p> <ul style="list-style-type: none"> – CPU ID、 – ステータス、 – ソケット、 – 製造元、 – モデル、 – 周波数
Memory Information	<p>次の情報が表示されます。</p> <ul style="list-style-type: none"> – メモリ ID、 – ステータス、 – ソケット、 – モジュールサイズ、 – モデル、 – 周波数、 – メモリタイプ*

表 7: 「Component Information」 ページ



*DDR3 ECC または NON-ECCUDIMM、RDIMM、LRDIMM メモリタイプは、公称電圧（1.5V）と低電圧（1.35V）のどちらもサポートします。

3.3 Server identify

「Server Identify」ページには、LED ランプのステータスが表示されます。
「Server Identify Operation」を選択すると、LED ランプを制御できます。



図 5: 「Server Identify」ページ

アイテム	説明
Current Server Identify Status	サーバのステータス：オンまたはオフ
Server Identify Operation	サーバの識別を示す LED の動作には次のオプションがあります。 <ul style="list-style-type: none">– ON– OFF– Blink
Server Identify Timeout	「Blink Identify Operation」を選択した場合のサーバのタイムアウト値。「Blink Operation」の場合、期間は 1 ～ 255 秒にしてください。255 秒を選択すると、点滅が継続されます。
Perform Action	選択した「Server Identify Operation」を実行します。

表 8: 「Server Identify」ページ

4 Server Health Group

Server Health Group は、次の 3 つの項目で構成されます。

- Sensor Readings
- Event Log

次の画像に示すように、Server Health のスクリーンショットで Sensor Readings または Event Log を選択することができます。

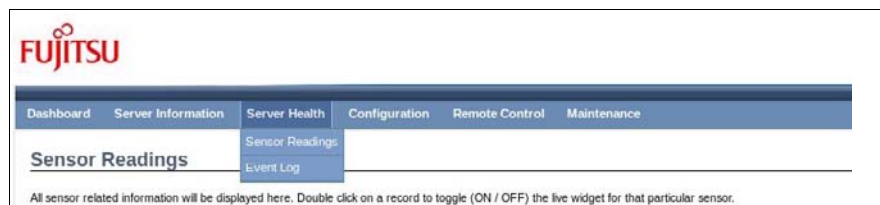


図 6: Server Health - メニュー

4.1 Sensor Readings

MegaRAC GUI では、「Sensor Readings」ページにセンサ関連のすべての情報が表示されます。

「Sensor Readings」を開くには、トップメニューの「*Server Health – Sensor Readings*」をクリックします。しきい値や、関連するすべての情報のグラフィカル表示など、特定のセンサの詳細情報を表示するには、レコードをクリックします。次の画像に「Sensor Readings」ページのスクリーンショットを示します。

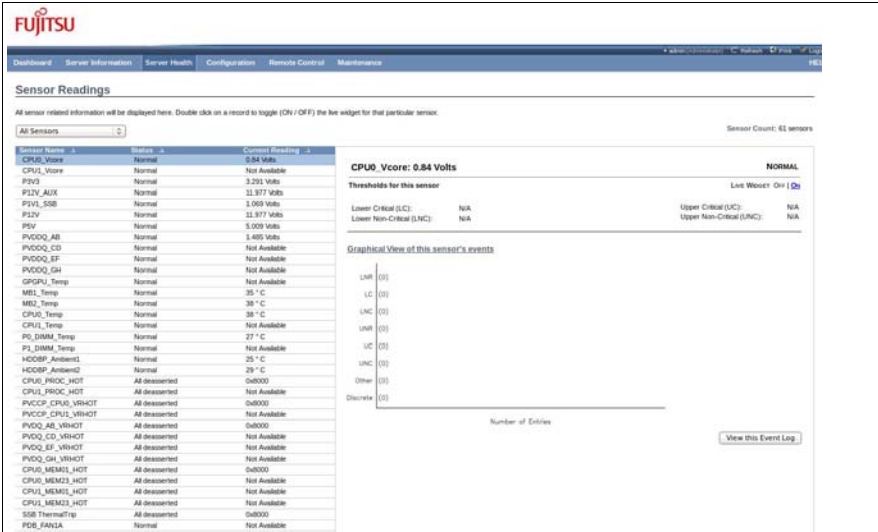


図 7: 「Sensor Readings」ページ

次の項で、「Sensor Readings」ページの各フィールドについて簡単に説明します。

4.1.1 Sensor Type

ドロップダウンメニューから特定のタイプのセンサを選択できます。センサのリストには、「Sensor Name」、「Status」、「Current Reading」が表示されます。「All Sensors」オプションで使用可能なすべてのセンサの詳細を表示して、特定タイプのセンサを選択できます。

特定タイプのセンサを選択すると、画面の右側にセンサのしきい値が表示されます。

以下の合計 4 つのしきい値を使用できます。

- Lower Critical (LC)
- Lower Non-Critical (LNC)
- Upper Critical (UC)
- Upper Non-Critical (UNC)

しきい値のステータスは、Lower Non-critical（重大でない状態の下限） - going low（下降中）、Lower Non-critical（重大でない状態の下限） - going high（上昇中）、Lower Critical（重大な状態の下限） - going low（下降中）、Lower Critical（重大な状態の下限） - going high（上昇中）、Lower Non-recoverable（回復不可能な状態の下限） - going low（下降中）、Lower Non-recoverable（回復不可能な状態の下限） - going high（上昇中）、Upper Non-critical（重大でない状態の上限） - going low（下降中）、Upper Non-critical（重大でない状態の上限） - going high（上昇中）、Upper Critical（重大な状態の上限） - going low（下降中）、Upper Critical（重大な状態の上限） - going high（上昇中）

4.1.2 Live Widget

選択したセンサのウィジェットウィンドウをオン / オフにできます。ウィジェットは、センサの測定値を動的に表示します。次の画像にウィジェットの例を示します。

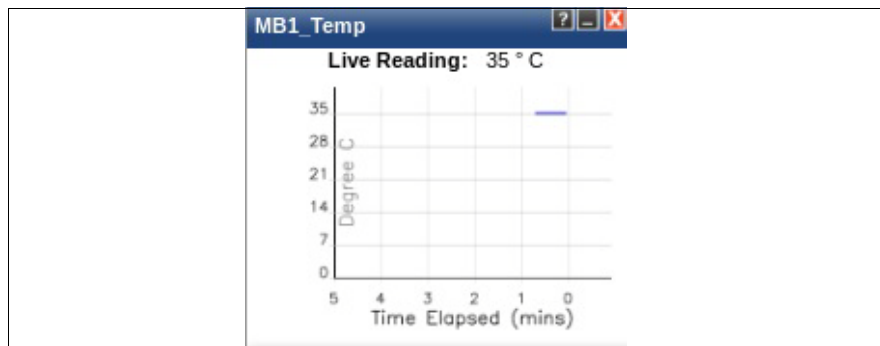


図 8: ウィジェットウィンドウ



ウィジェットは、特定センサの情報をリアルタイムに表示します。特定の時間、特定の間隔で、センサの動作を追跡できます。結果は、ウィジェットに線グラフとして表示されます。ウィジェットのデータは、ウィジェットを閉じるまでリアルタイムに更新されます。

4.1.3 View this Event Log

選択したセンサの「Event Log」ページが表示されます。

4.2 Event Log

MegaRAC GUI では、このデバイスの各種センサで発生したイベントログのリストがこのページに表示されます。エントリの詳細を表示するには、レコードをダブルクリックします。センサタイプまたはセンサ名フィルタのオプションを使用してそれらの特定のイベントを表示したり、列の見出しをクリックしてエントリのリストを並べ替えることもできます。

「Event Log」ページを開くには、トップメニューの「*Server Health – Event Log*」をクリックします。「Event Log」ページのサンプルスクリーンショットを次に示します。

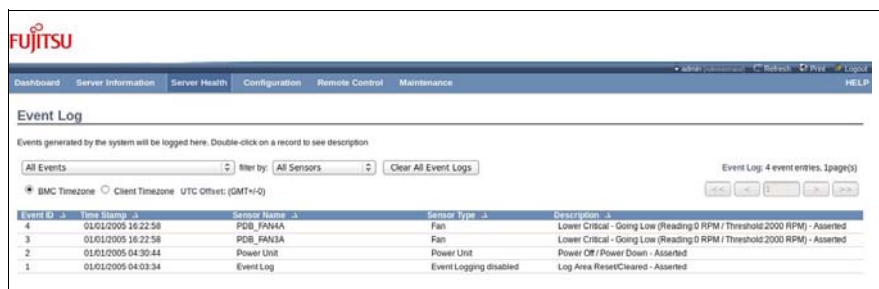


図 9: 「Event Log」 ページ

次の項で、「Event Log」ページの各フィールドについて簡単に説明します。

4.2.1 Event Log Category

カテゴリは、センサ固有のイベント、BIOS によって生成されたイベント、システム管理ソフトウェアのイベントのいずれかです。


アイテム	説明
Filter Type	リストされるフォルトのタイプ。  「Event Log Category」および「Filter Type」を選択すると、Event ID、Time Stamp、Sensor Type、Sensor Name、Description を含むイベントのリストが表示されます。
BMC Timezone	イベントの BMC UTC オフセットタイムスタンプの値。
Client Timezone	クライアントの UTC オフセットタイムスタンプのイベント。
Clear All Event Logs	すべてのセンサの既存のすべてのレコードを削除します。
Download All Event Logs	すべてのセンサの既存のすべてのレコードをダウンロードします。

表 9: Event Log Category

手順：

1. 「Event Log Category」 ドロップダウンメニューからイベントカテゴリを選択します。
2. 「Filter Type」 ドロップダウンリストからセンサ名フィルタを選択して、選択したフィルタのイベントを表示します。
3. 「BMC Timezone」 または 「Client Timezone」 を選択します。
4. リストからすべてのイベントをクリアするには、「Clear All Event Logs」 ボタンをクリックします。
5. リストからすべてのイベントをクリアするには、「Download All Event Logs」 ボタンをクリックします。

5 Configuration Group

「Configuration Group」ページでは、さまざまな構成設定にアクセスできます。次の図に「Configuration Group」メニューのスクリーンショットを示します。

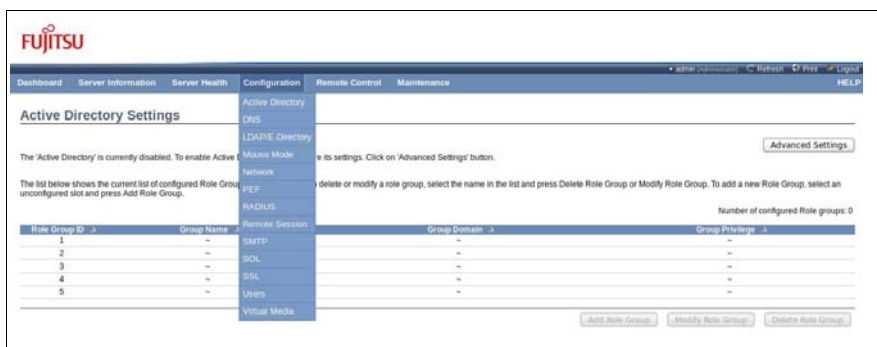


図 10: Configuration Group - メニュー

次の項で「Configuration」メニューについて詳しく説明します。

5.1 Active Directory

Active Directory（以下、AD）は、Microsoft Windows ベースのコンピュータおよびサーバで使用するディレクトリ構造体で、ネットワークやドメインの情報やデータを保存します。AD には、オブジェクトに関する情報を提供する、オブジェクトを容易に検索してアクセスできるように構造化する、エンドユーザおよび管理者へのアクセスを許可する、管理者がディレクトリのセキュリティを設定できるようにする、といったさまざまな機能があります。

次の図に示すように、MegaRAC SP-X のこの「Active Directory Settings」ページでは、Active Directory サーバの設定ができます。

「Active Directory Settings」ページを開くには、メインメニューの「*Configuration – Active Directory*」をクリックします。次のスクリーンショットに「Active Directory Settings」ページのサンプルスクリーンショットを示します。

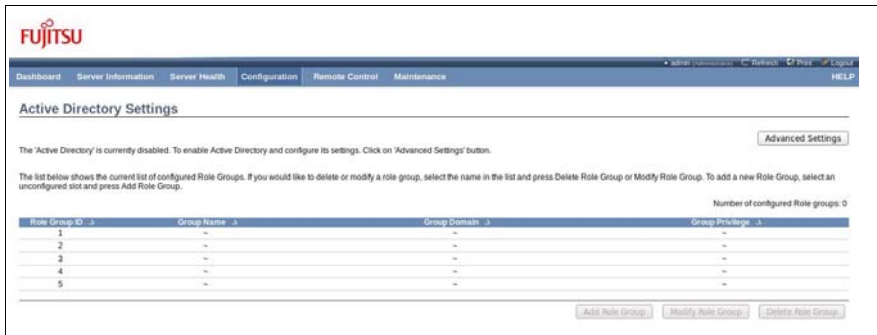


図 11: 「Active Directory Settings」ページ


アイテム	説明
Advanced Settings	Active Directory の高度な設定の設定オプションは次のとおりです。 <ul style="list-style-type: none"> – Active Directory Authentication、 – User Domain name、 – Time Out、および – 最大 3 つの Domain Controller Server Addresses を有効にします。
Role Group ID	Active Directory の役割グループを識別する名前。 <ul style="list-style-type: none"> – 役割グループ名は、255 文字の英数字の文字列です。 – 特殊記号のハイフンとアンダーバーを使用できません。
Group Name	この名前で Active Directory の役割グループを識別します。 <div>  役割グループ名は、255 文字の英数字の文字列です。特殊記号のハイフンとアンダーバーを使用できます。 </div>
Group Domain	役割グループがあるドメイン。
Group Privilege	役割グループに割り当てる権限のレベル。
Add Role Group	新しい役割グループをデバイスに追加します。
Modify role Group	役割グループを変更します。設定されたスロットをダブルクリックする方法もあります。
Delete Role Group	既存の役割グループを削除します。

表 10: Event Log Category

手順：

「Advanced Active Directory Settings」 ページへの詳細の入力

1. 「Advanced Active Directory Settings」 ページを開くには、「Advanced Settings」 をクリックします。

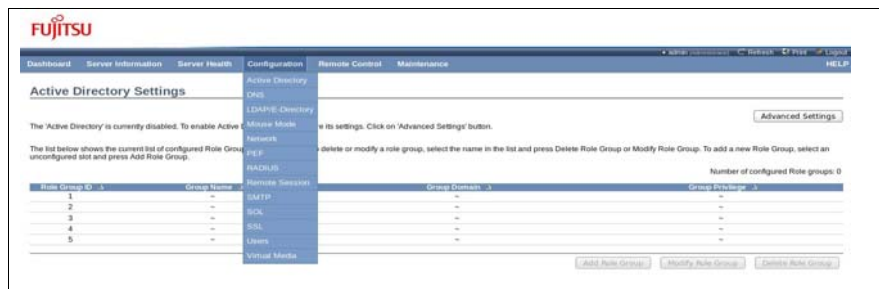


図 12: 「Advanced Active Directory」 ページ

「Active Directory Settings」 ページで、以下の詳細を有力します。

1. *Active Directory Authentication* : Active Directory を有効 / 無効にするには、「Enable」 チェックボックスをオン / オフにします。

i 「Active Directory Authentication」 を有効にした場合は、Active Directory サーバへのアクセスに必要な情報を入力します。

2. ユーザのドメイン名を、「User Domain Name」 フィールドに指定します（例：MyDomain.com）。
3. Active Directory のクエリが完了するのを待機する時間（単位：秒）を「Time Out」 フィールドに指定します。

i デフォルトのタイムアウト値は 120 秒です。
15 ~ 300 の値を指定できます。

4. 「Domain Controller Server Address1」、「Domain Controller Server Address2」、「Domain Controller Server Address3」 の IP アドレスを設定します。

i Active Directory サーバの IP アドレス：ドメインコントローラサーバのアドレスを少なくとも 1 つ設定します。

- IP アドレスは、"xxx.xxx.xxx.xxx" のように、ピリオドで区切られた 4 つの数字の組み合わせです。
- 各数字の範囲は 0 ~ 255 です。
- 先頭の数字は 0 以外でなければなりません。

ドメインコントローラサーバのアドレスは、IPv4 アドレス形式と IPv6 アドレス形式をサポートします。

5. 「Save」をクリックすると、入力した設定を保存して、「Active Directory Settings」ページに戻ります。

「Cancel」をクリックすると、入力をキャンセルして、「Active Directory Settings」ページに戻ります。

5.1.1 役割グループを追加するには

1. 下のスクリーンショットに示すように、空白行を選択して「Add Role Group」をクリックして「Add Role group」ページを開きます。

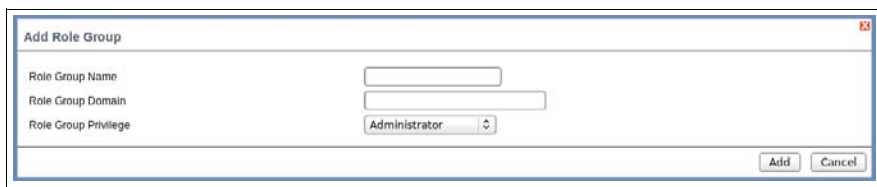


図 13: 「Add Role group」ページ

1. 「Role Group Name」フィールドに、Active Directory の役割グループを識別する名前を入力します。



役割グループ名は、255 文字の英数字の文字列です。

特殊記号のハイフンとアンダーバーを使用できます。

2. 「Role Group Domain」フィールドに、役割グループのあるドメインを入力します。



ドメイン名は、255 文字の英数字の文字列です。

特殊記号のハイフン、アンダーバー、ピリオドを使用できます。

3. 「Role Group Privilege」フィールドに、この役割グループに割り当てる権限のレベルを入力します。

4. 「Add」をクリックすると、新しい役割グループを保存して「Role Group List」に戻ります。

5. 「Cancel」をクリックすると、設定をキャンセルして「Role Group List」に戻ります。

5.1.2 役割グループを変更するには

1. 「Advanced Directory Settings」ページで変更する行を選択して、「*Modify Role Group*」をクリックします。
2. 必要な変更を行い、「*Save*」をクリックします。

5.1.3 役割グループを削除するには

1. 「Advanced Directory Settings」ページで削除する行を選択して、「*Delete Role Group*」をクリックします。

5.2 DNS

DNS（ドメインネームシステム）は、インターネットまたはプライベートネットワークに接続される、コンピュータ、サービス、または任意のリソース用の、分散階層型ネーミングシステムです。DNS は、情報を各参加者に割り当てられたドメイン名に関連付けます。最も重要なのは、デバイスを世界中で見つけてアドレスを指定するために、人間にとって意味のあるドメイン名をネットワーク機器に関連のある数値（バイナリ）識別子に変換することです。MegaRAC GUI では、「DNS Server Settings」ページを使用して、デバイスの DNS 設定を管理します。

「DNS Server Settings」ページを開くには、メインメニューの「*Configuration – DNS*」をクリックします。次のスクリーンショットに「DNS Server Settings」ページのサンプルスクリーンショットを示します。

図 14: 「DNS Server Settings」 ページ


アイテム	説明
ホストの設定	
Host Settings	「Automatic」または「Manual」での設定を選択します。
Host Name	デバイスのホスト名が表示されます。「Host Settings」で「Manual」を選択した場合は、デバイスのホスト名を指定します。
Domain Name Configuration	
Domain Settings	multiLAN チャネルへのドメインインターフェースのオプション、「Manual」、「v4」、「v6」がリストされます。  DHCP を選択した場合は、DHCP サーバに「v4」または「v6」を選択します。
Domain Name	デバイスのドメイン名が表示されます。「Domain Settings」で「Manual」を選択した場合は、デバイスのドメイン名を指定します。「Automatic」を選択すると、「Domain Name」が自動的に設定されるように設定できません。このフィールドは無効になります。

表 11: 「DNS Server Settings」 ページ

アイテム	説明
IPv4 Domain Name Server Configuration	
DNS Server Settings	デバイスの v4 DNS 設定のオプションとして、「Manual」および使用可能な LAN インターフェースがリストされます。
Preferred DNS Server	デバイスに設定される DNS（ドメインネームシステム）サーバの v4 アドレス。 <ul style="list-style-type: none"> IP アドレスは、「xxx.xxx.xxx.xxx」のように、ピリオドで区切られた 4 つの数字の組み合わせです。 各数字の範囲は 0 ～ 255 です。 先頭の数字は 0 以外でなければなりません。
Alternate DNS Server	
IPv6 Domain Name Server Configuration	
DNS Server Settings	デバイスの v6 DNS 設定のオプションとして、「Manual」および使用可能な LAN インターフェースがリストされます。「Manual」設定を選択した場合、DNS サーバの IP アドレスを設定してください。「DHCP」を選択した場合、IP アドレスを受け取るインターフェースを選択してください。IPv6 アドレスの例 - 2001:db8:0:101
Preferred DNS Server, Alternate DNS Server	デバイスに設定される DNS（ドメインネームシステム）サーバの v6 アドレスを指定します。
Save	入力した変更を保存します。
Reset	入力した変更をリセットします。

表 11: 「DNS Server Settings」ページ

手順：

1. 「Host Configuration」で「Automatic」または「Manual」を選択します。



「Automatic」の場合はホスト名は必要ありませんが、「Manual」の場合は必要です。

2. 「Manual Configuration」を選択した場合は、「Host Name」フィールドに入力します。
3. 「Register BMC」で、

1. 「*Register BMC*」オプションにチェックして、この DNS 設定で登録します。
2. 「*Direct Dynamic DNS*」オプションを選択して直接動的 DNS で登録するか、「*DHCP Client FQDN*」オプションを選択して DHCP サーバを通じて登録します。
4. 「*Domain name Configuration Settings*」で、
 1. ドロップダウンリストからドメイン設定を選択します。
 2. 「*Domain Name*」フィールドに入力します。
5. 「*IPv4 Domain Name Server Configuration*」で、
 1. ドロップダウンリストから「*DNS Server Settings*」を選択します。
 2. 「*Preferred DNS Server*」フィールドに優先 IP アドレスを入力します。
 3. 「*Alternate DNS Server*」フィールドに代替アドレスを入力します。
6. 「*IPv6 Domain Name Server Configuration*」で、
 1. ドロップダウンリストから「*DNS Server Settings*」を選択します。
 2. 「*Preferred DNS Server*」フィールドに優先 IP アドレスを入力します。
 3. 「*Alternate DNS Server*」フィールドに代替アドレスを入力します。
7. 「*Save*」をクリックするとエントリが保存されます。
8. 「*Reset*」をクリックするとエントリがリセットされます。

5.3 LDAP/E-Directory

LDAP (Lightweight Directory Access Protocol) は、IP (Internet Protocol) ネットワークで実装されるディレクトリサービスのデータにクエリや変更を行うためのアプリケーションプロトコルです。

MegaRAC GUI では、LDAP は、MegaRAC® カードがユーザの認証に使用できるインターネットプロトコルです。LDAP サーバをネットワークで設定している場合は、それを使用して、MegaRAC® カードユーザの追加、管理、認証を容易に行うことができます。これは、LDAP サーバにログインリクエストを渡すことによって行われます。つまり、MegaRAC カードを使用するときに、追加に認証メカニズムを定義する必要はありません。既存の LDAP サーバで認証を集中管理しているので、ネットワークリソースにアクセスしている人を常に認識し、ユーザまたはグループベースのポリシーを容易に定義してアクセスを制御することができます。

「LDAP Settings」ページを開くには、メインメニューの「*Configuration – LDAP*」をクリックします。次のスクリーンショットに「LDAP Settings」ページのサンプルスクリーンショットを示します。

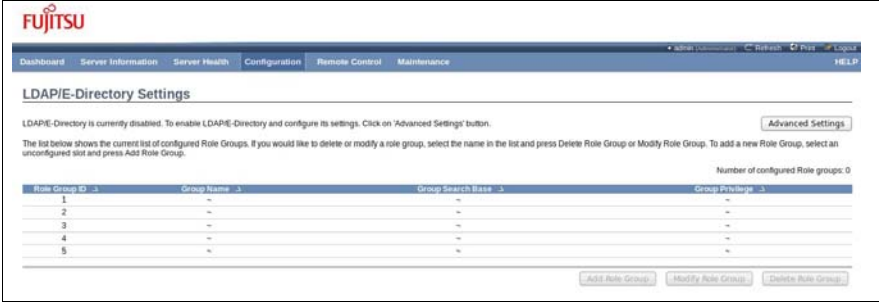


図 15: 「LDAP Settings」ページ

次に「LDAP Settings」ページのフィールドについて説明します。

アイテム	説明
Advanced Settings	「LDAP Advanced Settings」を設定します。オプションは、「Enable LDAP Authentication」、「IP Address」、「Port and Search base」です。
Add Role Group	新しい役割グループをデバイスに追加します。空きスロットをダブルクリックして、役割グループを追加することもできます。
Modify Role Group	特定の役割グループを変更します。
Delete Role Group	役割グループをリストから削除します。

表 12: 「LDAP Settings」ページ

手順：

「Advanced LDAP Settings」ページへの詳細の入力：

1. 「LDAP Settings」ページで「*Advanced Settings*」をクリックします。
「LDAP Settings」ページのサンプルスクリーンショットを次に示します。

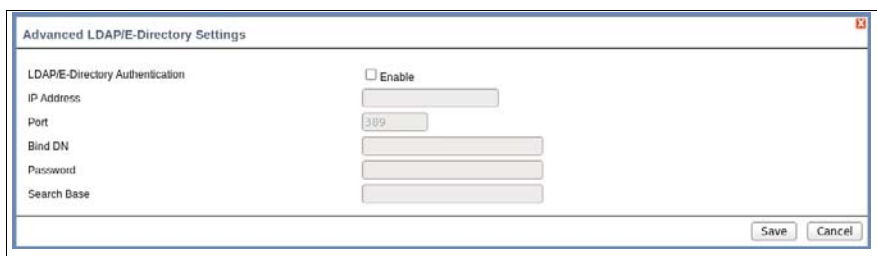


図 16: Advanced LDAP Settings

1. 「LDAP Authentication」を有効 / 無効にするには、「Enable」チェックボックスをオン / オフにします。



ログインプロンプトで、LDAP グループメンバとしてログインするためのユーザ名を入力します。

2. LDAP サーバの IP アドレスを「IP Address」フィールドに入力します。



IP アドレスは、'xxx.xxx.xxx.xxx' のように、ピリオドで区切られた 4 つの数字の組み合わせです。

- 各数字の範囲は 0 ~ 255 です。
- 先頭の数字は 0 以外でなければなりません。
- IPv4 アドレス形式と IPv6 アドレス形式をサポートします。

3. LDAP ポートを「Port」フィールドに指定します。



デフォルトポートは 389 です。セキュアな接続の場合は、デフォルトポートは 636 です。

4. 検索ベースを入力します。バインド DN は、サーバに対してクライアントを認証するバインド操作で使用します。



バインド DN は、4 ~ 64 文字の英数字の文字列です。

- 先頭はアルファベットでなければなりません。
- 特殊記号の、ピリオド (.), カンマ (,), ハイフン (-)、アンダーバー (_)、イコール (=) を使用できます。
- 例 : ou=login,dc=domain,dc=com

5. 「Save」をクリックすると、設定を保存します。
6. 「Cancel」をクリックすると、行った変更がキャンセルされます。

5.3.1 新しい役割グループを追加するには

1. 下のスクリーンショットに示すように、「LDAP Settings」ページで「*Add Role Group*」をクリックして「Add Role group」ページを開きます。



図 17: 「Add Role group」ページ

1. 「*Role Group Name*」フィールドに、役割グループを識別する名前を入力します。

i

 役割グループ名は、255 文字の英数字の文字列です。
特殊記号のハイフンとアンダーバーを使用できます。
2. 「*Role Group Search Base*」フィールドに、ベース DN までの役割グループのある場所からのパスを入力します。

i

 検索ベースは 255 文字の英数字の文字列です。
特殊記号のハイフン、アンダーバー、ピリオドを使用できます。
3. 「*Role Group Privilege*」フィールドに、この役割グループに割り当てる権限のレベルを入力します。
4. 「Add」をクリックすると、新しい役割グループを保存して「Role Group List」に戻ります。
5. 「Cancel」をクリックすると、設定をキャンセルして「Role Group List」に戻ります。

5.3.2 役割グループを変更するには

1. 「LDAP Settings」ページで変更する行を選択して、「*Modify Role Group*」をクリックします。
2. 必要な変更を行い、「Save」をクリックします。

5.3.3 役割グループを削除するには

1. 「LDAP Settings」 ページで削除する行を選択して、「Delete Role Group」 をクリックします。

5.4 マウスモード

MegaRAC GUI のコンソールリダイレクションでは、2 つの方法のいずれかで、ローカルウィンドウからリモート画面へのマウスエミュレーションを操作します。このオプションを設定するには管理者でなければなりません。

「Mouse Mode」 ページを開くには、メインメニューの「Configuration - Mouse Mode」 をクリックします。次のスクリーンショットに「Mouse Mode Settings」 ページのサンプルスクリーンショットを示します。



図 18: 「Mouse Mode Settings」 ページ

次に「Mouse Mode Settings」 ページのフィールドについて説明します。

アイテム	説明
Absolute Mode	ローカルマウスの絶対位置がサーバに送信されます。
Relative Mode	相対では、計算されたマウスの相対位置がサーバに送信されます。
Save	行った変更を保存します。
Reset	行った変更をリセットします。
Set Mode to Other	ホスト OS が絶対モードでも相対モードでもない場合。このモードを選択するには「Set Mode to Other」 オプションを選択します。

表 13: 「Mouse Mode Settings」 ページ

手順：

1. ユーザの要件に応じて次のいずれかを選択します。

- Set Mode to Absolute



Windows のすべてのバージョン、RHEL6 以降のバージョン、FC14 より後のバージョンに適用できます。

- Set Mode to Relative



Linux のすべてのバージョン、RHEL6 以降のバージョン、FC14 より前のバージョンに適用できます。

2. 「Save」 ボタンをクリックすると、行った変更が保存されます。

3. 「Reset」 をクリックすると、行った変更がリセットされます。

5.5 Network

MegaRAC GUI では、「Network Settings」 ページを使用して使用可能な LAN チャンネルのネットワーク設定を行います。

「Network Settings」 ページを開くには、メインメニューの「*Configuration – Network*」をクリックします。次のスクリーンショットに「Network Settings」 ページのサンプルスクリーンショットを示します。

FUJITSU

Dashboard Server Information Server Health **Configuration** Remote Control Maintenance

Network Settings

Manage network settings of the device.

LAN Interface:

LAN Settings: ☒ Enable

MAC Address:

IPv4 Configuration

Obtain an IP address automatically: ☒ Use DHCP

IPv4 Address:

Subnet Mask:

Default Gateway:

IPv6 Configuration

IPv6 Settings: ☒ Enable

Obtain an IP address automatically: ☒ Use DHCP

IPv6 Address:

Subnet Prefix length:

Default Gateway:

VLAN Configuration

VLAN Settings: ☐ Enable

VLAN ID:

VLAN Priority:

図 19: 「Network Settings」 ページ

次に「Network Settings」 ページのフィールドについて説明します。

アイテム	説明
LAN インタフェース	LAN インタフェースのリストを表示します。
LAN Settings	LAN の設定を有効または無効にします。
MAC Address	このフィールドには、デバイスの MAC アドレスが表示されます。読み取り専用のフィールドです。

表 14: Network Settings



アイテム	説明
IPv4 Configuration	<p>このオプションは、IPv4 の構成設定をリストします。</p> <ul style="list-style-type: none"> 「Obtain IP Address automatically」: このオプションは、DHCP (Dynamic Host Configuration Protocol) を使用して IPv4 アドレスを動的に設定します。 「IPv4 Address」、「Subnet Mask」、「Default Gateway」: これらのフィールドには、デバイスに設定する静的 IPv4 アドレス、サブネットマスク、デフォルトゲートウェイを指定します。 <p> IP アドレスは、"xxx.xxx.xxx.xxx" のように、ピリオドで区切られた 4 つの数字の組み合わせです。</p> <ul style="list-style-type: none"> 各数字の範囲は 0 ~ 255 です。 先頭の数字は 0 以外でなければなりません。
IPv6 Configuration	<p>このオプションは、次の IPv6 の構成設定をリストします。</p> <ul style="list-style-type: none"> 「IPv6 Settings」: このオプションは、デバイスの IPv6 の設定を有効にします。 「Obtain an IPv6 address automatically」: このオプションは、DHCP (Dynamic Host Configuration Protocol) を使用して IPv6 アドレスを動的に設定します。 「IPv6 Address」: デバイスに設定する静的 IPv6 アドレスを指定します。例: 2004:2010 「Subnet Prefix length」: IPv6 設定のサブネットプレフィックスの長さを指定します。 <p> 値の範囲は 0 ~ 128 です。</p> <ul style="list-style-type: none"> 「Default Gateway」: IPv6 の設定に v6 デフォルトゲートウェイを指定します。

表 14: Network Settings

アイテム	説明
VLAN Configuration	<p>VLAN 構成設定。</p> <ul style="list-style-type: none"> 「VLAN Settings」: 選択したインターフェースに対して VLAN サポートを有効 / 無効にします。 「VLAN ID」: VLAN の設定の ID。 値の範囲は 1 ~ 4095 です。 「VLAN Priority」: VLAN の設定のプライオリティ。 値の範囲は 1 ~ 7 です。 VLAN の最高プライオリティは 7 です。
Save	エントリを保存します。
Reset	行った変更をリセットします。

表 14: Network Settings

手順:

1. ドロップダウンリストから「*LAN Interface*」を選択します。
2. 「*Enable*」をオンにすると LAN の設定が有効になります。
3. 「IPv4 Configuration」で「*Use DHCP to Obtain an IP address automatically*」を有効にすると、DHCP を使用して IPv4 アドレスを動的に設定します。
4. このフィールドが無効な場合、「*IPv4 Address*」、「*Subnet Mask*」、「*Default Gateway*」の各フィールドに入力します。
5. 「IPv6 Configuration」で IPv6 の設定を有効にするには、「*Enable*」をオンにします。
6. IPv6 の設定が有効な場合、「*Use DHCP for obtaining the IP address automatically*」オプションを有効または無効にします。
7. このフィールドが無効な場合、「*IPv6 Address*」、「*Subnet Prefix length*」、「*Default Gateway*」の各フィールドに入力します。
8. 「VLAN Configuration」で VLAN の設定を有効にするには、「*Enable*」をオンにします。
9. 「*VLAN ID*」フィールドに入力します。
10. 「*VLAN Priority*」フィールドに入力します。
11. 「*Save*」をクリックするとエントリが保存されます。

12.「Reset」をクリックすると行った変更がリセットされます。

5.6 PEF

PEF (Platform Event Filtering) は、受信された、または内部で生成されたイベントメッセージに選択したアクションを行うために、BMC を設定するメカニズムを提供します。これらのアクションには、システムの電源オフ、システムのリセット、アラート生成のトリガーなどの動作があります。MegaRAC GUI では PEF Management を使用して以下の機能を設定します。

- Event Filter
- Alert Policy
- LAN Destination

「PEF Management Settings」ページを開くには、メインメニューの「*Configuration – PEF*」をクリックします。次のスクリーンショットに「PEF Management Settings」ページのサンプルスクリーンショットを示し、各タブについて説明します。

5.6.1 「Event Filter」タブ

PEF を実装して少なくとも 16 のエントリを「Event Filter」タブに入力することをお勧めします。これらのエントリのサブセットを、温度過上昇、電源システムの故障、ファンの故障イベントなどの、共通のシステム故障イベントに対してあらかじめ設定しておいてください。残りのエントリは、'OEM' または System Management Software によって設定されたイベントのために使用可能にできます。システム用に予約していることを個々のエントリにタグ付けできるので、あらかじめ設定されたエントリの、実行時に設定可能なエントリに対する割合は、必要に応じて割り当て直すことができます。

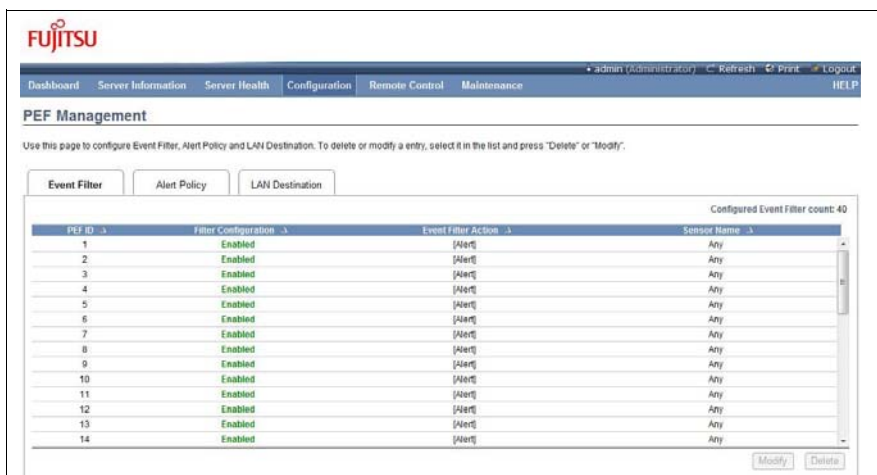


図 20: PEF Management - Event Filter

次に「PEF Management - Event Filter」タブのフィールドについて説明します。

このページには、設定された PEF のリストが表示されます。

アイテム	説明
PEF ID	このフィールドには、新しく設定した PEF エントリの ID が表示されます（読み取り専用）。
Filter configuration	このチェックボックスで PEF の設定を有効にします。
Event Filter Action	このチェックボックスで PEF のアラートアクションを有効にします。これは必須フィールドです。
Event Severity	イベントの重要度をリストから 1 つ選択します。
Sensor Name	センサリストから特定のセンサを選択します。
Modify	既存のエントリを変更します。
Cancel	変更をキャンセルして、イベントフィルタリストに戻ります。

表 15: PEF Management - Event Filter

手順：

1. 「Event Filter」タブをクリックして、使用可能なスロットにイベントフィルタを設定します。
2. PEF ID リストからいずれかを選択して「Modify」をクリックし、「Modify Event Filter Entry」ページを開きます。次のスクリーンショットに「Modify Event Filter Entry」ページのサンプルスクリーンショットを示します。

図 21: 「Modify Event Filter Entry」ページ

3. 「Event Filter Configuration」セクションの
 1. 「PEF ID」に、設定した PEF エントリの ID が表示されます（読み取り専用）。
 2. フィルタ設定でチェックボックスをオンにして PEF の設定を有効にします。
4. 「Filter Action configuration」セクションの
 1. 「Event Filter Action」は必須フィールドで、PEF アラートアクションを有効にします（読み取り専用）。デフォルトではオンです。
 2. ドロップダウンリストから、「Power down」、「Power reset」、「Power cycle」の電源アクションのいずれかを選択します。
 3. ドロップダウンリストから、設定したアラートポリシー番号のいずれかを選択します。



アラートポリシーは、「*Configuration – PEF – Alert Policy*」で設定します。

5. 「Sensor configuration」セクションで、
 1. イベントフィルタアクションをトリガーする s タイプのセンサを選択します。
 2. センサ名フィールドで、センサリストから特定のセンサを選択します。
 3. イベントオプションを「All Events」または「Sensor Specific Events」のいずれかに選択します。
6. 「*Modify*」をクリックすると、変更を受け入れて、イベントフィルタリストに戻ります。
7. 「*Reset*」をクリックすると行った変更をリセットします。
8. 「*Cancel*」をクリックすると、変更をキャンセルして、イベントフィルタリストに戻ります。

5.6.2 「Alert Policy」タブ

このページを使用して、アラートポリシーと LAN 宛先を設定します。このページの入力は、追加、削除、変更ができます。

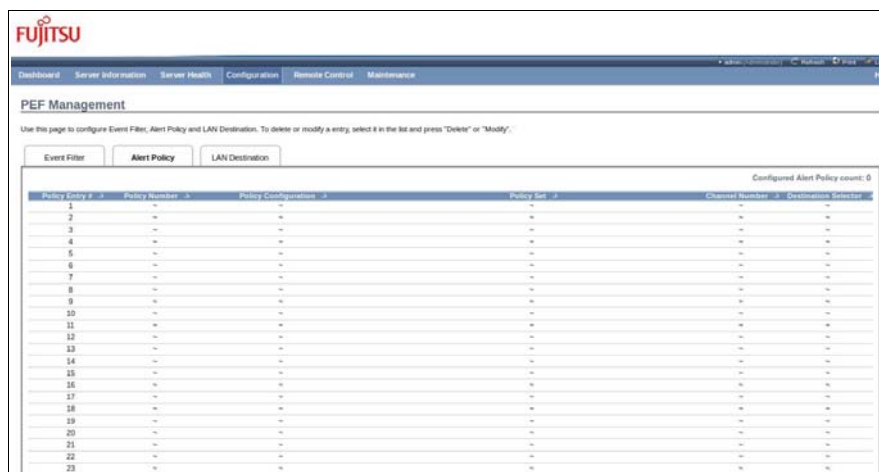


図 22: PEF Management - Alert Policy

次に「PEF Management - Alert Policy」タブのフィールドについて説明します。


アイテム	説明
Policy Entry #	新しく設定したエントリのポリシーエントリ番号を表示します（読み取り専用）。
Policy Number	設定のポリシー数を表示します。
Policy Configuration	ポリシーの設定を有効 / 無効にします。
Policy Set	<p>リストからポリシーセット値のいずれかを選択します。</p> <ul style="list-style-type: none"> 0：この宛先に常にアラートを送信。 1：前の宛先へのアラートが成功した場合は、この宛先にアラートを送信しない。このポリシーセットの次のエントリへ進む。 2：前の宛先へのアラートが成功した場合は、この宛先にアラートを送信しない。このポリシーセットのエントリはこれ以上処理しない。 3：前の宛先へのアラートが成功した場合は、この宛先にアラートを送信しない。異なるチャンネルに対する、このポリシーセットの次のエントリへ進む。 4：前の宛先へのアラートが成功した場合は、この宛先にアラートを送信しない。異なる宛先にに対する、このポリシーセットの次のエントリへ進む。
Channel Number	使用可能なチャンネルリストから特定のチャンネルを選択します。
Destination Selector	<p>設定された宛先リストから特定の宛先を選択します。</p> <div>  LAN 宛先は「<i>Configuration – PEF – LAN Destination</i>」で設定します。 </div>
Modify	既存のエントリを変更します。
Delete	アラートポリシーリストを削除するに

表 16: PEF Management - Alert Policy

手順：

1. 「Alert Policy」タブで、アラートポリシーを設定するスロットを選択します。つまり、「Event Filter Entry」ページで、アラートポリシー番号に4を選択した場合、「Alert Policy」タブで4番目のスロット（ポリシー番号4のスロット）を設定する必要があります。
2. 下のスクリーンショットに示すように、スロットをダブルクリックして「Modify」をクリックして「Add Alert Policy Entry」ページを開きます。

図 23: 「Add Alert Policy Entry」ページ

1. 「Policy Entry #」は、読み取り専用のフィールドです。
2. リストから *ポリシー番号* を選択します。
3. ポリシー設定を有効にする場合は、「Policy Configuration」フィールドで「Enable」をオンにします。
4. 「Policy Set」フィールドで、リストからポリシーセットのいずれかを選択します。
5. 「Channel Number」フィールドで、使用可能なチャネルセットから特定のチャネルを選択します。
6. 「Destination Selector」フィールドで、設定された宛先リストから特定の宛先を選択します。



LAN 宛先は、「Configuration – PEF – LAN Destination」で設定します。つまり、「Alert Policy Entry」ページの「Destination Selector」で番号4を選択した場合、「LAN Destination」タブで4番目のスロット（LAN 宛先番号4）を設定します。

7. アラートポリシーのエントリがイベント固有である場合は、「Alert String」フィールドで、チェックボックスをオンにします。
8. 「Alert String Key」フィールドで、このアラートポリシーのエントリに送信するアラート文字列を検索するために使用する値を1つ選択します。

9. 「Add」をクリックすると、新しいアラートポリシーを保存してアラートポリシーリストに戻ります。
10. 「Cancel」をクリックすると、変更をキャンセルしてアラートポリシーリストに戻ります。
11. アラートポリシーリストで設定を変更するには、変更するスロットを選択して「Modify」をクリックします。
12. 「Modify Alert Policy Entry」ページで必要な変更を行い、「Modify」をクリックします。
13. アラートポリシーページで設定を削除するには、スロットを選択して「Delete」をクリックします。

5.6.3 「PEF Management LAN Destination」ページ

このページを使用して、イベントフィルタ、アラートポリシー、LAN 宛先を設定します。「PEF Management LAN Destination」ページのサンプルスクリーンショットを次に示します。

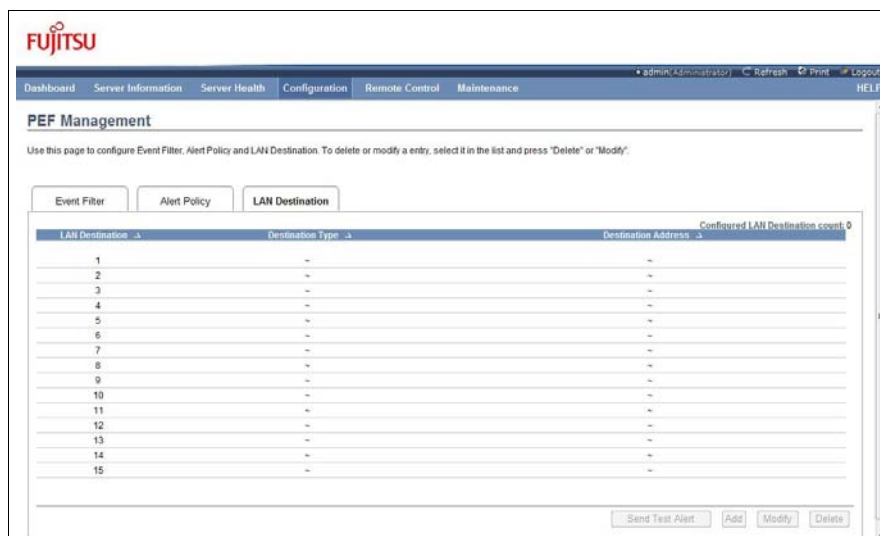


図 24: PEF Management LAN Destination

「PEF Management - LAN Destination」タブのフィールドについて説明します。

アイテム	説明
LAN Destination	新しく設定したエントリの宛先番号を表示します（読み取り専用）。
Destination Type	宛先タイプは、SNMP トラップまたは E-mail アラートのいずれかです。 <ul style="list-style-type: none"> E-mail アラートの場合は、宛先 E-mail アドレス、メッセージの件名と本文の 3 つのフィールドを入力する必要があります。また、SMTP サーバの情報も「<i>Configuration - SMTP</i>」に追します。 SNMP トラップの場合は、宛先 IP アドレスのみ入力します。
Destination Address	宛先タイプが SNMP トラップの場合、アラートを受信するシステムの IP アドレスを入力します。宛先アドレスは以下をサポートします。 <ul style="list-style-type: none"> IPv4 アドレス形式。 IPv6 アドレス形式。 宛先タイプが E-mail アラートの場合、E-mail を受信する E-mail アドレスを入力します。
Send Test Alert	宛先タイプにアラートまたは SNMP トラップを選択した場合、これらのフィールドを設定する必要があります。このフィールドはメッセージフィールドの内容で設定した宛先にテストメッセージを送信します。
Modify	既存の LAN 宛先リストを変更するに
Delete	LAN 宛先リストを削除するに


表 17: PEF Management - LAN Destination

手順

1. 「*LAN Destination*」タブで、設定するスロットを選択します。これは、「Alert Policy Entry- Destination Selector」フィールドで選択したスロットと同じでなければなりません。つまり、「Alert Policy」タブの「Alert Policy Entry」ページで「Destination Selector」を4に選択した場合、「LAN Destination」ページの4番目のスロットを設定します。
2. スロットをダブルクリックして「*Modify*」をクリックします。これで「Add LAN Destination entry」が開きます。



図 25: 「Add LAN Destination entry」ページ

1. 「*LAN Destination*」フィールドに、新しく設定したエントリの宛先が表示されます（読み取り専用のフィールド）。
2. 「*Destination Type*」フィールドで、いずれかのタイプを選択します。
3. 「*Destination Address*」フィールドに、宛先アドレスを入力します。
 宛先タイプが E-mail アラートの場合、E-mail を受信する E-mail アドレスを入力します。
4. ユーザのリストから *Username* を選択します。
5. 「*Subject*」フィールドに、件名を入力します。
6. 「*Message*」フィールドにメッセージを入力します。
7. 「Add」をクリックすると、新しい LAN 宛先を保存して LAN 宛先リストに戻ります。
8. 「Cancel」をクリックすると、変更をキャンセルして LAN 宛先リストに戻ります。
9. 「*LAN Destination*」タブで設定を変更するには、変更する行を選択して「*Modify*」をクリックします。
10. 「Modify LAN Destination Entry」ページで必要な変更を行い、「*Modify*」をクリックします。

11. 「LAN Destination」タブで設定を削除するには、スロットを選択して「Delete」をクリックします。

5.7 RADIUS

RADIUS は、モジュール式で高性能かつ機能が豊富な RADIUS スイートで、サーバ、クライアント、開発ライブラリ、およびその他数々の RADIUS ユーティリティが含まれます。

MegaRAC GUI では、このページを使用して RADIUS 認証を設定します。

「RADIUS Settings」ページを開くには、メインメニューの「Configuration – RADIUS」をクリックします。次のスクリーンショットに「RADIUS Settings」ページのサンプルスクリーンショットを示します。

図 26: 「RADIUS Settings」ページ

次に「RADIUS Settings」ページのフィールドについて説明します。

アイテム	説明
RADIUS Authentication	RADIUS 認証を有効にするオプションです。
Port	RADIUS のポート番号です。 <div data-bbox="389 1236 445 1295" data-label="Image"></div> デフォルトポートは 1812 です。

表 18: 「RADIUS Settings」ページ




アイテム	説明
Time Out	<p>タイムアウト値の単位は秒です。</p> <p> デフォルトのタイムアウト値は 3 秒です。 タイムアウト値の範囲は 3 ~ 300 です。</p>
Server Address	<p>RADIUS サーバの IP アドレス。</p> <p> IP アドレスは、"xxx.xxx.xxx.xxx" のように、ピリオドで区切られた 4 つの数字の組み合わせです。</p> <ul style="list-style-type: none"> 各数字の範囲は 0 ~ 255 です。 先頭の数字は 0 以外でなければなりません。
Secret	<p>RADIUS サーバの認証シークレットです。</p> <p> このフィールドは 31 文字以下しか設定できません。</p> <ul style="list-style-type: none"> シークレットは 4 文字以上でなければなりません。 空白は使用できません。
Save	設定を保存します。
Reset	行った変更をリセットします。

表 18: 「RADIUS Settings」 ページ

手順：

1. 「*RADIUS Authentication*」 チェックボックスをオンにして RADIUS を認証します。
2. 「*Port Number*」 フィールドにポート番号を入力します。
3. 「*Time out*」 フィールドにタイムアウト値を秒単位で入力します。
4. 「*Server Address*」 フィールドにサーバのアドレスを入力します。
5. 「*Secret*」 フィールドに RADIUS サーバの認証シークレットを入力します。
6. 「*Save*」 をクリックすると、入力した詳細を保存します。
7. 「*Reset*」 をクリックすると、入力した詳細をリセットします。

5.8 Remote Session

MegaRAC SP では、このページを使用して、次のリダイレクションセッションの仮想メディア構成設定を設定します。デフォルトでは、暗号化は無効です。

「Remote Session」ページを開くには、メインメニューの「*Configuration – Remote Session*」をクリックします。次のスクリーンショットに「Remote Session」ページのサンプルスクリーンショットを示します。



図 27: Remote Session

次に「Remote Session Settings」ページのフィールドについて説明します。


アイテム	説明
KVM Encryption	次のリダイレクションセッションの KVM データで暗号化を有効 / 無効にします。
Media Encryption	次のリダイレクションセッションのメディアデータで暗号化を有効 / 無効にします。
Virtual Media Attach Mode	2 種類の仮想メディア接続モードを使用できます。 – Attach : 起動時に即座に仮想メディアをサーバに接続します。 – Auto Attach : 仮想メディアセッションが開始されたときのみ、仮想メディアをサーバに接続します。
Save	現在の変更を保存します。 <div>  もしあれば、KVM または仮想メディアセッションのいずれかの既存のリモートリダイレクションを自動的に終了します。 </div>
Reset	行った変更をリセットします。

表 19: 「Remote Session Settings」ページ

手順：

1. 「*KVM encryption*」で、「*Enable*」オプションをオフにします。
2. 「*Media Encryption*」で、「*Enable*」オプションをオフにします。
3. 「*Virtual media Attach mode*」で、必要に応じてドロップダウンリストから「*Auto Attach*」または「*Attach*」を選択します。
4. 「*Save*」をクリックするとエントリが保存されます。
5. 「*Reset*」をクリックするとエントリがリセットされます。



- 複数の仮想 CDROM を選択しても、RHEL5 ホストの「Computer」ウィンドウには、CDROM は 1 つしか表示されません。2 つ目の CDROM をリダイレクトすると、2 つ目の CDROM デバイスが「Computer」ウィンドウに表示されます。
- 仮想ハードディスクを 3 つ以上選択しても、RHEL5 RHEL5 ホストの「Computer」ウィンドウには、ハードディスクは 2 つしか表示されません。3 つ目のハードディスクをリダイレクトすると、3 つ目のハードディスクが「Computer」ウィンドウに表示されます。

5.9 SMTP

SMTP (Simple Mail Transfer Protocol) は、IP (Internet Protocol) ネットワーク経由で E-mail (電子メール) を送信するためのインターネット標準規格です。

MegaRAC GUI を使用して、デバイスの SMTP 設定を行うことができます。

「SMTP Settings」ページを開くには、メインメニューの「*Configuration – SMTP*」をクリックします。次のスクリーンショットに「SMTP Settings」ページのサンプルスクリーンショットを示します。

図 28: 「SMTP Settings」 ページ

次に「SMTP Settings」 ページのフィールドについて説明します。

アイテム	説明
LAN Channel Number	使用可能な LAN チャンネルのリストを表示します。
Sender Address	SMTP サーバで有効な「送信元アドレス」。
Machine Name	SMTP サーバの「マシン名」。 – マシン名は、最大 15 文字の英数字の文字列です。 – 空白、特殊文字は使用できません。
Primary SMTP Server	Primary SMTP サーバ構成をリストします。
Server Address	SMTP サーバの「IP アドレス」です。必須フィールドです。 <div style="border: 1px solid black; padding: 2px; display: inline-block;">i</div> IP アドレスは、"xxx.xxx.xxx.xxx" のように、ピリオドで区切られた 4 つの数字の組み合わせです。 – 各数字の範囲は 0 ～ 255 です。 – 先頭の数字は 0 以外でなければなりません。 – IPv4 アドレス形式と IPv6 アドレス形式をサポートします。

表 20: 「SMTP Settings」 ページ




アイテム	説明
SMTP Server requires Authentication	<p>SMTP 認証を有効 / 無効にします。</p> <p> サポートされる SMTP サーバ認証のタイプを次に示します。</p> <ul style="list-style-type: none"> - CRAM-MD5 - LOGIN - PLAIN <p>SMTP サーバが上記認証タイプのいずれもサポートしない場合は、「Authentication type is not supported by SMTP Server (認証タイプが SMTP サーバでサポートされていません)」という内容のエラーメッセージが表示されます。</p>
Username	<p>SMTP アカウントにアクセスするためのユーザ名です。</p> <p> ユーザ名は、4 ～ 64 文字の英数字の文字列です。</p> <ul style="list-style-type: none"> - 先頭はアルファベットでなければなりません。 - 特殊文字の、カンマ (,)、コロン (:)、セミコロン (;)、スペース ()、バックスラッシュ (\) は使用できません。
Password	<p>SMTP ユーザアカウントのパスワードです。</p> <p> パスワードは 4 文字以上でなければなりません。</p> <ul style="list-style-type: none"> - 空白は使用できません。 - このフィールドは 64 文字以下しか設定できません。
Secondary SMTP Server	セカンダリ SMTP サーバ構成をリストします。オプションのフィールドです。プライマリ SMTP サーバが正常に動作していない場合、セカンダリ SMTP サーバ構成を使用しようとします。
Save	新しい SMTP サーバ構成を保存します。
Reset	行った変更をリセットします。

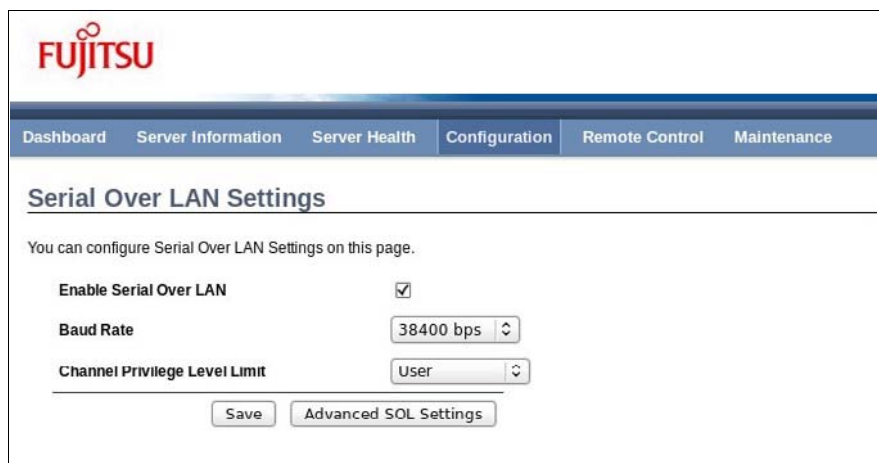
表 20: 「SMTP Settings」 ページ

手順：

1. ドロップダウンリストから「*LAN* チャネル番号」を選択します。
2. 「*Sender Address*」フィールドに入力します。
3. 「*Machine Name*」フィールドに入力します。
4. プライマリ SMTP サーバで「*Server Address*」フィールドに入力します。
5. SMTP サーバを認証する場合は、「*SMTP Server requires Authentication*」チェックボックスをオンにします。
6. 「*User name*」フィールドと「*Password*」フィールドに入力します。
7. セカンダリ SMTP サーバで「*Server Address*」フィールドに入力します。
8. SMTP サーバを認証する場合は、「SMTP Server requires Authentication」チェックボックスをオンにします。
9. 「*User name*」フィールドと「*Password*」フィールドに入力します。
10. 「*Save*」をクリックすると、入力した詳細を保存します。
11. 「*Reset*」をクリックすると、入力した詳細をアップデートします。

5.10 SOL

ここでは、SOL (Serial over LAN) 設定を行うことができます。各属性の値を選択するか変更して「*Save*」ボタンを押すと、変更が保存されます。



FUJITSU

Dashboard Server Information Server Health **Configuration** Remote Control Maintenance

Serial Over LAN Settings

You can configure Serial Over LAN Settings on this page.

Enable Serial Over LAN ☒

Baud Rate 38400 bps

Channel Privilege Level Limit User

Save Advanced SOL Settings

図 29: 「SQL Settings」 ページ

次に「SQL Settings」ページのフィールドについて説明します。

アイテム	説明
Enable Serial over LAN	オン = 有効、オフ = 無効。
Channel Privilege Level Limit	IPMI Serial over LAN の最小ユーザ権限を選択します。 <ul style="list-style-type: none"> Administrator Operator User
Save	このボタンをクリックして設定を保存します。
Advanced SOL Settings	このボタンをクリックして高度な SOL ページへ移動します。
Character Accumulate Interval	BMC が SOL 文字データパッケージの一部を転送するまで待機する時間です。1 ベースで 5ms ずつ増加。この値は 255 未満でなければなりません。
Character Send Threshold	この文字数かそれ以上が受け入れられるとすぐに、BMC は文字を含んだ SOL 文字データパッケージを送信します。1 ベース単位。この値は 255 未満でなければなりません。

表 21: 「SQL Settings」 ページ

5.11 SSL

セキュアソケットレイヤープロトコルは、Web サーバとブラウザ間のセキュアなトランザクションを保証するために、Netscape によって作成されました。このプロトコルは、サードパーティである認証局（CA：Certificate Authority）を使用して、トランザクションの片端または両端を識別します。

MegaRAC GUI を使用して、SSL 証明書を BMC に設定します。これを使用して、デバイスにセキュアモードでアクセスできます。

「SSL Certificate Configuration」ページを開くには、メインメニューの「*Configuration – SSL*」をクリックします。このページにはタブが 3 つあります。

- 「Upload SSL」オプションを使用して、証明書と秘密鍵ファイルを BMC にアップロードします。
- 「Generate SSL」オプションを使用して、設定の詳細に基づき SSL 証明書を生成します。
- 「View SSL」オプションを使用して、アップロードされた SSL 証明書を読み取り可能な形式で表示します。

次のスクリーンショットに「SSL Management」ページのサンプルスクリーンショットを示します。


図 30: SSL Certificates Configuration - Upload SSL

Certificate Configuration - Upload SSL

次に「SSL Certificate Configuration - Upload SSL」タブのフィールドについて説明します。

アイテム	説明
Current Certificate	現在の証明書の情報が表示されます（読み取り専用）。
New Certificate	証明書ファイルは PEM 形式である必要があります。
Current Privacy Key	現在の秘密鍵の情報が表示されます（読み取り専用）。
New Privacy Key	秘密鍵ファイルは PEM 形式である必要があります。
Upload	SSL 証明書と秘密鍵を BMC にアップロードします。

表 22: SSL Certificate Configuration - Upload SSL



アップロードが成功すると、HTTPs サービスが再起動して、新しくアップロードされた SSL 証明書を適用します。

SSL Certificate Configuration - Generate SSL

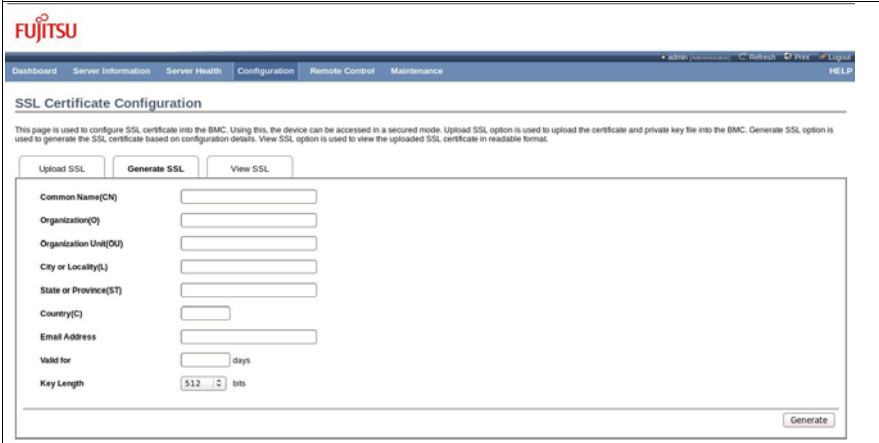


図 31: SSL Certificate Configuration - Generate SSL

次に「SSL Certificate Configuration - Generate SSL」タブのフィールドについて説明します。

アイテム	説明
Common Name (CN)	証明書が生成されるコモンネーム。 <ul style="list-style-type: none"> 最大 64 文字です。 特殊文字の '#' と '\$' は使用できません。
Organization (O)	証明書が生成される組織名。 <ul style="list-style-type: none"> 最大 64 文字です。 特殊文字の '#' と '\$' は使用できません。
Organization Unit (OU)	証明書が生成される組織全体における部門名。 <ul style="list-style-type: none"> 最大 64 文字です。 特殊文字の '#' と '\$' は使用できません。
City or Locality (L)	組織の市町村名 (必須)。 <ul style="list-style-type: none"> 最大 64 文字です。 特殊文字の '#' と '\$' は使用できません。
State or Province (ST)	組織の都道府県名 (必須)。 <ul style="list-style-type: none"> 最大 64 文字です。 特殊文字の '#' と '\$' は使用できません。
Country (C)	組織の国名 (必須)。 <ul style="list-style-type: none"> 2 文字のみ使用できます。 特殊文字は使用できません。
Email Address	組織の E-mail アドレス (必須)。
Valid for	証明書の有効期限。 <ul style="list-style-type: none"> 値の範囲は 1 ~ 3650 日です。
Key Length	証明書の鍵の長さ (ビット)。
Generate	新しい SSL 証明書を生成します。

表 23: SSL Certificate Configuration - Generate SSL



HTTPs サービスが再起動して、新しく生成された SSL 証明書を適用します。

SSL Certificate Configuration - View SSL

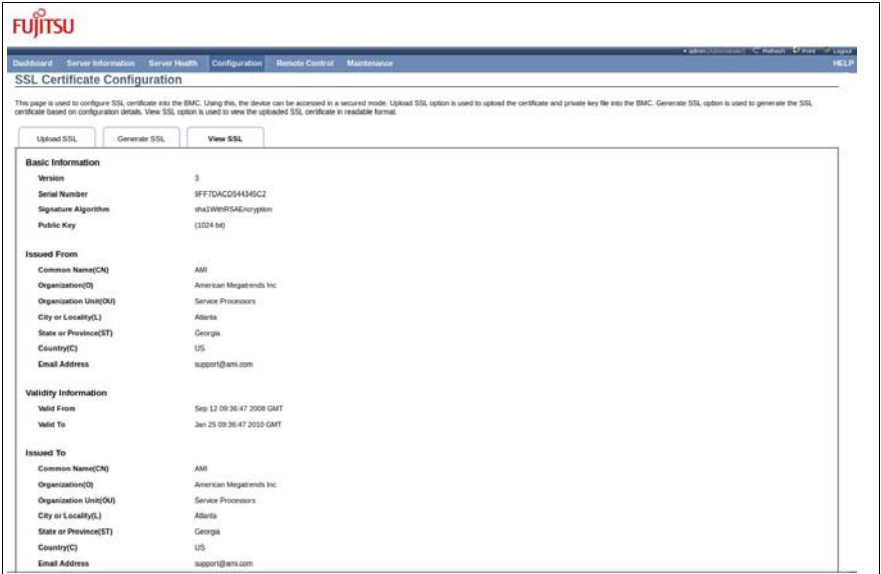


図 32: SSL Certificate Configuration - View SSL

次に「SSL Certificate Configuration - View SSL」タブのフィールドについて説明します。

アイテム	説明
基本情報	<div>このセクションには、アップロードされた SSL 証明書 の基本情報が表示されます。以下のフィールドが表示 されます。</div> <div><div>– バージョン</div><div>– Serial Number</div><div>– Signature Algorithm</div><div>– Public Key</div></div>


表 24: SSL Certificate Configuration - View SSL

アイテム	説明
Issued From	<p>このセクションには、以下の証明書発行者情報が表示されます。</p> <ul style="list-style-type: none"> – Common Name (CN) – Organization (O) – Organization Unit (OU) – City or Locality (L) – State or Province (ST) – Country (C) – Email Address
Validity Information	<p>このセクションには、アップロードされた証明書の有効期限が表示されます。</p> <ul style="list-style-type: none"> – Valid From – Valid To
Issued To	<p>このセクションには、証明書の発行者に関する情報が表示されます。</p> <ul style="list-style-type: none"> – Common Name (CN) – Organization (O) – Organization Unit (OU) – City or Locality (L) – State or Province (ST) – Country (C) – Email Address

表 24: SSL Certificate Configuration - View SSL

手順

1. 「*Upload SSL*」 タブをクリックして *新しい証明書* と *新しい秘密鍵* を表示します。
2. 「*Upload*」 をクリックして新しい証明書と新しい秘密鍵をアップロードします。
3. 「*Generate SSL*」 タブで、各フィールドに下記の詳細を入力します。
 1. 証明書が生成される *コモンネーム*。
 2. 証明書が生成される *N 組織名*。
 3. 証明書が生成される *O 組織全体* における *部門名*。

4. 組織の市町村名。
 5. 組織の都道府県名。
 6. 組織の国名。
 7. 組織の E-mail アドレス。
 8. 証明書の日数は、「Valid For」フィールドの期間有効です。
4. 証明書のキーの長さ（ビット）を選択します。
 5. 「Generate」をクリックすると証明書が生成されます。
 6. 「View SSL」タブをクリックすると、アップロードされた SSL 証明書がユーザが読み取り可能な形式で表示されます。
-  証明書をアップロード / 生成するとすぐに、HTTPS サービスが再起動します。
- これで、インターネットブラウザの IP アドレスフィールドで次の形式を使用して、Generic MegaRAC® SP にセキュアにアクセスすることができます : `https://<your MegaRAC® SP's IP address here>`
 - たとえば、MegaRAC® SP の IP アドレスが 192.168.0.30 の場合、次のように入力します :
`https://192.168.0.30`
 - `<http>` の後の `<s>` に注意してください。Generic MegaRAC® SP にアクセスする前に、証明書を承認する必要があります。

5.12 User Management

MegaRAC GUI では、「User Management」ページにサーバの現在のユーザスロットのリストを表示することができます。新しいユーザの追加、および既存のユーザの変更または削除ができます。

「User Management」ページを開くには、メインメニューの「Configuration – Users」をクリックします。次のスクリーンショットに「User Management」ページのサンプルスクリーンショットを示します。



図 33: User Management

次に「User Management」ページのフィールドについて説明します。


アイテム	説明
User ID	<p>ユーザの ID 番号を表示します。</p> <p> リストには、最大 10 名のユーザしか表示されません。</p>
User Name	ユーザの名前を表示します。
User Access	ユーザのアクセス権限を有効 / 無効にします。
Network Privilege	ユーザのネットワークアクセス権限を表示します。
SNMP Status	ユーザの SNMP ステータスが有効か無効かを表示します。
Email ID	ユーザの E-mail アドレスを表示します。
Add User	新しいユーザを追加します。Modify
User	既存のユーザを変更します。
Delete User	既存のユーザを削除します。

表 25: 「User Management」ページ

手順:



スロットのすべてのカラムで、空きスロットは "~" で示されます。

新しいユーザの追加：

1. 新しいユーザを追加するには、空きスロットを選択して「Add User」をクリックします。次のスクリーンショットに示すように、「Add User」画面が開きます。

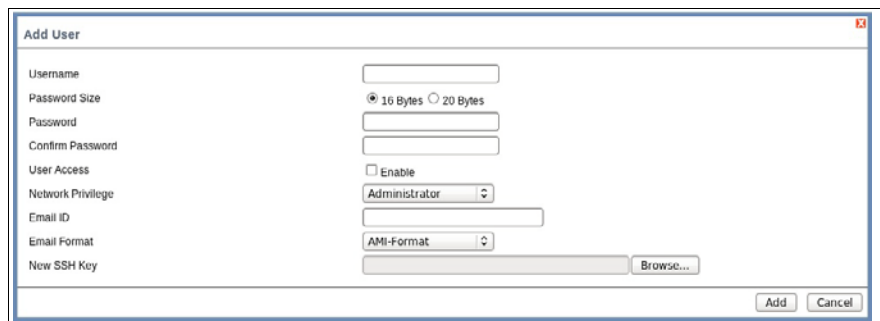


図 34: 「Add User」ページ

1. 「User Name」フィールドにユーザ名を入力します。

i

ユーザ名は、4 ～ 16 文字の英数字の文字列です。
 - － 先頭はアルファベットでなければなりません。
 - － 大文字小文字を区別します。
 - － 特殊文字の、カンマ (,), ピリオド (.), コロン (:), セミコロン (;), スペース (), スラッシュ (/), バックスラッシュ (\), 左括弧 ((), 右括弧 ()) は使用できません。
2. 「Password and Confirm Password」フィールドに、新しいパスワードを入力して確定します。

i

 - － 空白は使用できません。
 - － このフィールドは 20 文字以下しか設定できません。
3. ユーザアクセス権限を有効または無効にします。
4. 「Network Privilege」フィールドに、ユーザに割り当てられているネットワーク権限 (Administrator、Operator、User、No Access のいずれか) を入力します。
5. 「Email ID」フィールドに、ユーザの E-mail アドレスを入力します。ユーザがパスワードを忘れた場合、設定した E-mail アドレスに新しいパスワードが送信されます。

i

E-mail アドレスを送信するように SMTP サーバを設定します。

6. Email Format : 次の 2 種類の形式を使用できます。

- AMI-Format : このメール形式の件名は「Alert from (ユーザのホスト名)」です。メールの本文には、センサ情報 (センサタイプや説明など) が表示されます。
- Fixed-Subject Format : この形式では、ユーザの設定に従ってメッセージを表示します。E-mail アラート用の件名とメッセージを設定する必要があります。

7. 「*New SSK Key*」フィールドで「*Browse*」をクリックして、SSH キーファイルを選択します。



SSH キーファイルは、PUB 形式である必要があります。

8. 「*Add*」をクリックすると、新しいユーザを保存してユーザリストに戻ります。

9. 「*Cancel*」をクリックすると、変更をキャンセルしてユーザリストに戻ります。

既存のユーザの変更：

1. リストから既存のユーザを選択して「*Modify User*」をクリックします。次のスクリーンショットに示すように、「Add User」画面が開きます。

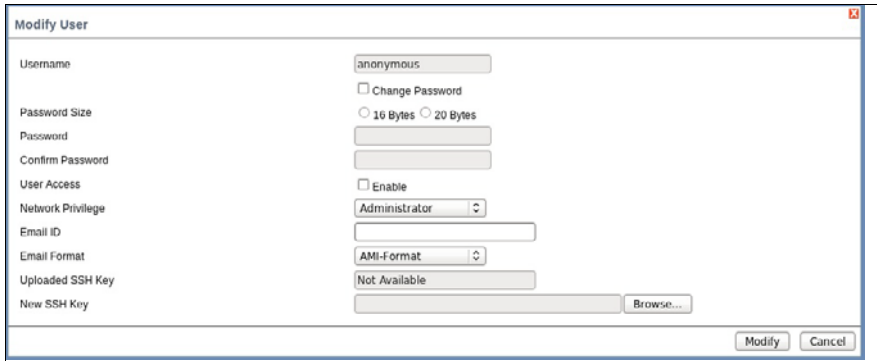


図 35: Modify User page

1. 必要なフィールドを編集します。
2. パスワードを変更するには、「*Change Password*」オプションを有効にします。
3. 編集や変更の後、「*Modify*」をクリックしてユーザリストページに戻ります。

既存のユーザの削除：

1. 既存のユーザを削除するには、リストからユーザを選択して「*Delete User*」をクリックします。



BMC ユーザとして追加 / 変更できなかった予約ユーザのリストがあります。予約ユーザのリストについては、「MEGARAC SP-X Platform Porting Guide」セクション（「Changing the Configurations in PMC File」-> 「User Configurations in PMC File」）を参照してください。

5.13 Virtual Media

MegaRAC GUI では、このページを使用して仮想メディアデバイス設定を行います。このページで仮想メディアの構成を変更する場合、「JViewer Vmedia」ダイアログに適切なデバイスが表示されます。たとえば、「Configure Virtual Media」ページで 2 つのフロッピーデバイスを選択する場合、「JViewer > Vmedia」に、2 つのフロッピーデバイスパネルを表示できます。

「Virtual Media」ページを開くには、メインメニューの「*Configuration – Virtual Media*」をクリックします。次のスクリーンショットに「User Management」ページのサンプルスクリーンショットを示します。



図 36: Configure Virtual Media Devices

このページには以下のフィールドが表示されます。

アイテム	説明
Floppy devices	仮想メディアリダイレクションをサポートするフロッピーデバイスの数。
CD/DVD devices	仮想メディアリダイレクションをサポートするCD/DVD デバイスの数。
Hard disk devices	仮想メディアリダイレクションをサポートするハードディスクデバイスの数。
Local Media Support	仮想メディアリダイレクションのローカルメディアのサポートを有効または無効にします。
Save	構成した設定を保存します。
Reset	以前保存した値にリセットします。

表 26: Configure Virtual Media Devices

手順：

1. フロッピーデバイス、CD/DVD デバイス、ハードディスクデバイスの数をドロップダウンリストから選択します。



フロッピー、CD/DVD、ハードディスクのドライブには、最大 2 つのデバイスを追加できます。

2. 必要に応じて「*Local Media Support*」を有効にします。
3. 「*Save*」をクリックして行った変更を保存するか、「*Reset*」をクリックして以前保存した値にリセットします。



各デバイスに 2 つのデバイスパネルがある場合に「*Connect*」ボタンをクリックすると、リダイレクトされたデバイスパネルが無効になります。

6 Remote Control

Remote Control は、次のメニュー項目で構成されます。

- Console Redirection
- Server Power Control

「Remote Control」メニューのサンプルスクリーンショットを次に示します。

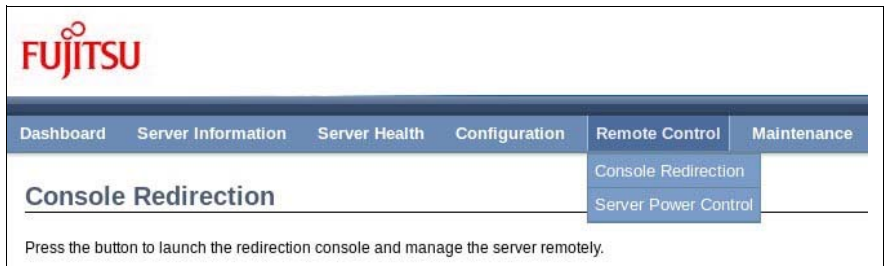


図 37: 「Remote Control」メニュー

6.1 Console Redirection

WebGUI を使用して起動するリモートコンソールアプリケーション。画面、マウス、キーボードを使用してサーバのオペレーティングシステムリモートで制御したり、ローカル CD/DVD、フロッピーディスク、ハードディスク/USB サムのドライブを、サーバに直接接続されているかのようにリダイレクトしたりします。

6.1.1 サポートされるクライアントオペレーティングシステムのリスト

- WinXP
- W2K3 - 32 bit
- W2K3 - 64 bit
- RHEL 4 - 32 bit
- RHEL 4 - 64 bit
- RHEL 5.4 - 32 bit
- RHEL 5.4 - 64 bit
- RHEL 6.0 - 64 bit
- RHEL 6.0 - 32 bit
- Ubuntu 9.10 LTS - 32
- Ubuntu 9.10 LTS - 64
- Ubuntu 8.10 -32
- Ubuntu 8.10 -64
- OpenSuse 11.2 -32
- OpenSuse 11.2 -64
- FC 9 - 32
- FC 9 - 64
- FC 10 - 32
- FC 10 - 64
- FC 12 - 32
- FC 12 - 64
- FC 13 - 32
- FC 13 - 64
- FC 14 - 32
- FC 14 - 64
- MAC -32
- MAC-64

6.1.2 サポートされるホストオペレーティングシステムのリスト

- RHEL 5
- RHEL 6
- W2K3
- W2K8
- RHEL 4
- OpenSuse 11.2
- OpenSuse 10.x
- Ubuntu 8.10
- Ubuntu 9.10
- Ubuntu 11.04

6.1.3 ブラウザの設定

KVM を起動するには、ポップアップブロックを無効にします。Internet Explorer の場合は、設定からダウンロードファイルオプションを有効にします。

6.1.4 Java コンソール

JRE を搭載した Windows および Linux で使用できる、オペレーティングシステムに依存しないプラグインです。JRE はクライアントシステムにインストールします。JRE は次のリンクからインストールできます。

<http://www.java.com/en/download/manual.jsp>

手順:

MegaRAC GUI では、次の 2 つの方法で Java コンソールを起動できます。

- 「Dashboard」ページを開いて「Remote control」セクションで「*Launch for Java Console*」をクリックします。
- 「*Remote Control – Console Redirection*」ページを開いて「*Java Console*」をクリックします。

これにより、BMC から *jnlp* ファイルがダウンロードされます。

jnlp ファイルを開くには、適切な JRE バージョン (Javaws) を使用します。

ダウンロードが完了すると「Console Redirection」ウィンドウが開きます。

6.1.5 「Console Redirection」 メインメニュー

「Console Redirection」メインメニューは、次のメニュー項目で構成されます。

- ビデオ
- キーボード
- マウス
- Options
- Media
- Keyboard Layout
- Video Record
- Active Users
- Help

これらのメニュー項目について、次に詳しく説明します。

6.1.5.1 ビデオ

このメニューには、以下のサブメニュー項目があります。

アイテム	説明
Pause redirection	このオプションを使用して、コンソールリダイレクションを一時停止します。
Resume Redirection	このオプションを使用して、セッションが一時停止の場合にコンソールリダイレクションを再開します。
Refresh Video	このオプションを使用して、「Console Redirection」ウィンドウに表示される画面を更新できます。
Full Screen	このオプションを使用して、コンソールリダイレクションをフル画面モード（最大化）で表示します。このメニューは、クライアントとホストの解像度が同じ場合のみ有効です。
Exit	このオプションを使用して、コンソールリダイレクション画面を終了します。

表 27: ビデオ

Compression Mode :

このオプションを使用して、Java コンソールで YUV 420、YUV 444、YUV 444 + 2 色 VQ、YUV 444 + 4 色 VQ などのビデオ圧縮モードを選択します。

DCT Quantization Table :

ビデオ品質を選択する 8 つのレベルがあります。

6.1.5.2 キーボード

このメニューには、以下のサブメニュー項目があります。

アイテム	説明
Hold Right Ctrl Key	このメニュー項目を使用して、コンソールリダイレクション中に、右側 <Ctrl> キーとして動作します。
Hold Right Alt Key	このメニュー項目を使用して、コンソールリダイレクション中に、右側 <Alt> キーとして動作します。
Hold Left Ctrl Key	このメニュー項目を使用して、コンソールリダイレクション中に、左側 <Ctrl> キーとして動作します。
Hold Left Alt Key	このメニュー項目を使用して、コンソールリダイレクション中に、左側 <Alt> キーとして動作します。
Left Windows Key	このメニュー項目を使用して、コンソールリダイレクション中に、左側 <Win> キーとして動作します。キーの押し方も指定できます：押したまま / 押してから放す
Right Windows Key	このメニュー項目を使用して、コンソールリダイレクション中に、右側 <Win> キーとして動作します。キーの押し方も指定できます：押したまま / 押してから放す
Alt+Ctrl+Del	このメニュー項目を使用すると、リダイレクトしているサーバで <Ctrl>, <Alt> and <Delete> キーを同時に押しているようにかのよう動作させることができます。

表 28: キーボード

コンテキストメニュー：

このメニュー項目を使用して、コンソールリダイレクション中に、コンテキストメニューキーとして動作します。

6.1.5.3 マウス

アイテム	説明
「Absolute」マウスモード	ホストオペレーティングシステムによっては（すべての Windows バージョン、RHEL6 以降の RHEL Linux バージョン）、マウスモードに「Absolute」を選択します。
「Relative」マウスモード	ホストオペレーティングシステムによっては（RHEL6 より前の RHEL Linux バージョン）、マウスモードに「Relative」を選択します。
「Other」マウスモード	「Absolute」マウスモードでも「Relative」マウスモードでもないホストオペレーティングシステムの場合。

表 29: キーボード

6.1.5.4 Options

このメニューには、以下のサブメニュー項目があります。

アイテム	説明
帯域幅	このオプションを使用して、帯域幅を手動で設定するか自動で設定するかを選択します。
Keyboard/ Mouse Encryption	このオプションを使用して、キーボード / マウス転送のデータペイロードの暗号化を有効 / 無効にします。
Zoom	このオプションを使用して、拡大 / 縮小のビデオ画面を調整します。

表 30: キーボード

6.1.5.5 Media

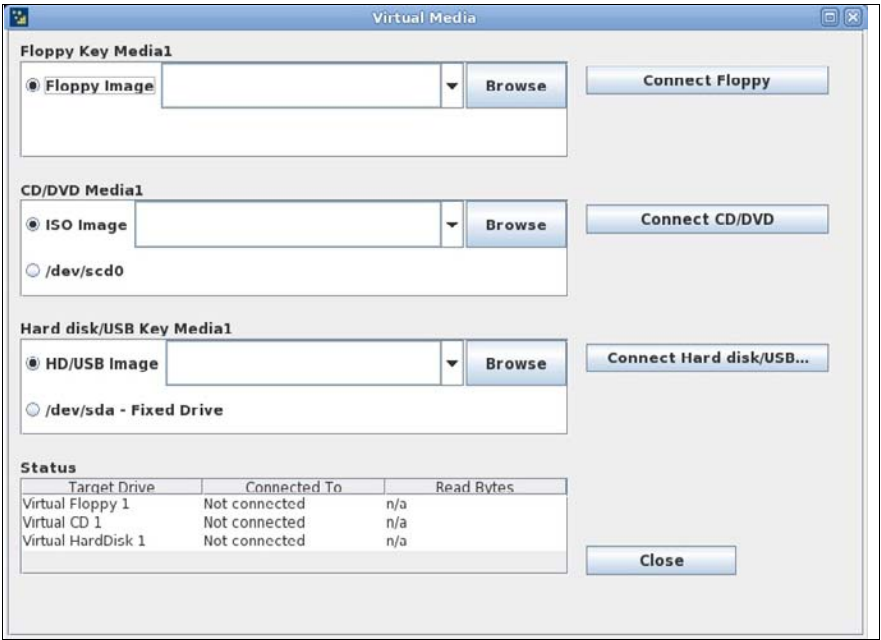


図 38: Media


アイテム	説明
Floppy Key Media	<p>このメニュー項目を使用して、物理フロッピードライブとフロッピーイメージタイプ（*.img など）のリダイレクションの開始 / 停止ができます。</p> <div> フロッピーリダイレクションは、MegaRAC SP のすべてのバージョンで使用できる機能ではありません。</div>
CD/DVD Media	<p>このメニュー項目を使用して、物理 DVD/CD-ROM ドライブと cd イメージタイプ（iso など）のリダイレクションの開始 / 停止ができます。</p>

表 31: Media

アイテム	説明
Hard disc/USB Key Media	<p>このメニュー項目を使用して、ハードディスク /USB キーイメージと USB キーイメージ (*.img など) のリダイレクションの開始 / 停止ができます。</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>i Windows クライアントの場合、物理ドライブの論理ドライブがディスマウントされた場合、論理デバイスは読み書き権限を使用してリダイレクトするか、読み取り権限のみを使用してリダイレクトされます。</p> </div> <ul style="list-style-type: none"> - MAC クライアントの場合、外付け USB ハードディスクのリダイレクションのみサポートされます。 - Linux クライアントの場合、固定ハードドライブは読み取りモードとしてのみリダイレクトされます。書き込みモードはサポートされません。 - USB キーイメージリダイレクションの場合、FAT 16、FAT 32、NTFS をサポートします。

表 31: Media

6.1.5.6 Keyboard Layout

アイテム	説明
Auto Detect	<p>このオプションを使用して、キーボードレイアウトを自動的に検出します。自動的にサポートされる言語は、英語 - 米国、フランス語 - フランス、スペイン語 - スペイン、ドイツ語 - ドイツ、日本語 - 日本です。クライアントとホストの言語が同じ場合は、上記の英語以外のすべての言語においてはこのオプションを選択して入力ミスによるエラーを回避してください。</p>

表 32: Keyboard Layout

アイテム	説明
Soft Keyboard	<p>このオプションを使用して、キーボードレイアウトを選択できます。画面キーボードと同様のダイアログが表示されます。クライアントとホストの言語が異なる場合は、上記の英語以外のすべての言語においては、JViewer に表示されるリストで適切な言語を選択し、ソフトキーボードを使用して、入力ミスによるエラーを回避してください。</p> <div><div>i</div><div>ソフトキーボードは JViewer アプリケーションにのみ適用され、クライアントシステムの他のアプリケーションには適用されません。</div></div>

表 32: Keyboard Layout

6.1.5.7 Video Record

i

このオプションは、Java コンソールを起動する場合のみ使用できます。

アイテム	説明
重要	<p>このメニューオプションを表示するには、JMF（Java Media FrameWork）をダウンロードする必要があります。JMF は次のリンクからダウンロードできます。</p> <p>http://www.oracle.com/technetwork/java/javase/download-142937.html</p>
Start Record	このオプションを使用して画面の記録を開始します。
Stop Record	このオプションを使用して記録を停止します。
設定	ビデオの記録に関する設定を行います。

表 33: Video Record

手順：

- i

記録を開始する前に、設定を入力する必要があります。
- 下のスクリーンショットに示すように、「Video Record – Settings」をクリックして設定ページを開きます。

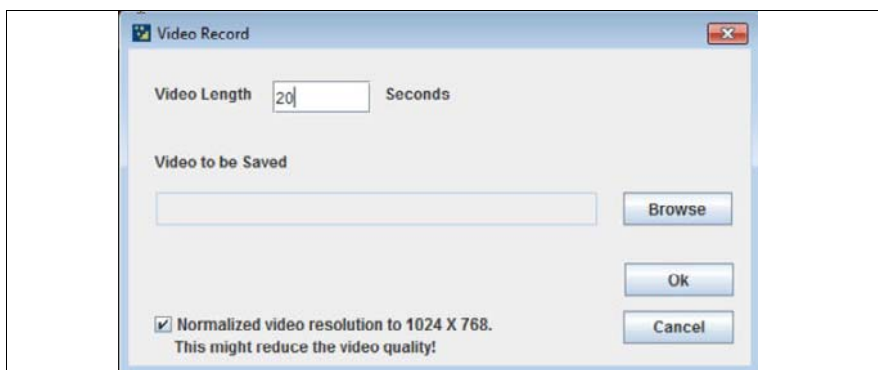


図 39: Video Record Settings page

1. 「*Video Length*」に秒単位で入力します。
2. 「*Browse*」をクリックして、ビデオの保存先を入力します。
3. 「*Normalized video resolution to 1024X768*」オプションを有効にします。
4. 「*OK*」をクリックしてエントリを保存して、コンソールリダイレクション画面に戻ります。
5. エントリを保存しない場合は、「*Cancel*」をクリックします。
6. 「Console Redirection」ウィンドウで「*Video Record – Start Record*」をクリックします。
7. 処理を記録します。
8. 記録を停止するには、「*Video Record – Stop Record*」をクリックします。

6.1.5.8 Active Users

このオプションをクリックすると、アクティブなユーザとそのシステム IP アドレスが表示されます。

6.1.5.9 Help

Jviewer：著作権情報とバージョン情報が表示されます。

6.1.5.10 クイックボタン

「Console Redirection」ウィンドウの右下に、すべてのクイックボタンが表示されます。これらのクイックボタンを使用すると、これらの機能をボタンをクリックするだけで実行できます。



このオプションは、Java コンソールを起動する場合のみ使用できません。Server Power Control。

6.1.6 Server Power Control

このページでは、サーバの電源の表示と制御ができます。

「Power Control and Status」ページを開くには、メインメニューの「*Remote Control – Server Power Control*」をクリックします。次のスクリーンショットに「Power Control and Status」ページのサンプルスクリーンショットを示します。



図 40: 「Power Control and Status」ページ


電源制御の各種オプションを次に示します。

アイテム	説明
Reset Server	このオプションで、電源をオフにせずにシステムを再起動します（ウォームブート）。
Power Off Server - Immediate	このオプションで、サーバの電源を即座に切断します。
Power Off Server - Orderly Shutdown	このオプションで、シャットダウンの前にオペレーティングシステムのシャットダウンを開始します。
Power On Server	このオプションで、サーバの電源を投入します。
Power Cycle Server	このオプションで、電源をいったん切断してからシステムを再起動します（コールドブート）。
Perform Action	このオプションをクリックして、選択した操作を実行します。

表 34: Server Power Control

手順：

アクションを選択して「*Perform Action*」をクリックすると、選択したアクションを実行します。

-  選択を確定するメッセージが表示されます。確定すると、コマンドが実行され、ステータスが通知されます。

7 Maintenance Group

このページグループでは、デバイスの保守作業を行うことができます。このメニューには、以下の項目があります。

- Firmware Update
- Preserve Configuration
- Restore Factory Defaults



図 41: Maintenance group

7.1 Firmware Update

MegaRAC GUI では、このウィザードを使用して、ファームウェアアップグレード処理を行うことができます。アップグレードが完了するかキャンセルすると、ボックスのリセットが自動的に行われます。設定を保存するためのオプションが表示されます。アップグレードを通じて構成された設定を保存するには、このオプションを有効にします。



警告！

アップデートモードウィジェットに移行すると、他の Web ページやサービスが動作しなくなることにご注意ください。開いているすべてのウィジェットは自動的に閉じます。ウィザードの途中でアップグレード処理をキャンセルすると、デバイスがリセットされます。

アップデートモードウィジェットに移行すると、他の Web ページやサービスが動作しなくなることにご注意ください。開いているすべてのウィジェットは自動的に閉じます。ウィザードの途中でアップグレード処理をキャンセルすると、デバイスがリセットされます。



ファームウェアアップグレード処理は極めて重要な操作です。この操作中は、電力損失や接続損失の可能性を最小限にしてください。

アップデートモードにしてからファームウェアフラッシュ操作のキャンセルを選択した場合は、MegaRAC® カードをリセットする必要があります。つまり、他のすべての種類の操作を行う前に、インターネットブラウザを終了して MegaRAC® カードにログオンしてください。

「Firmware Update」ページを開くには、メインメニューの「*BMC - Maintenance - Firmware Update*」をクリックします。次のスクリーンショットに「Firmware Update」ページのサンプルスクリーンショットを示します。

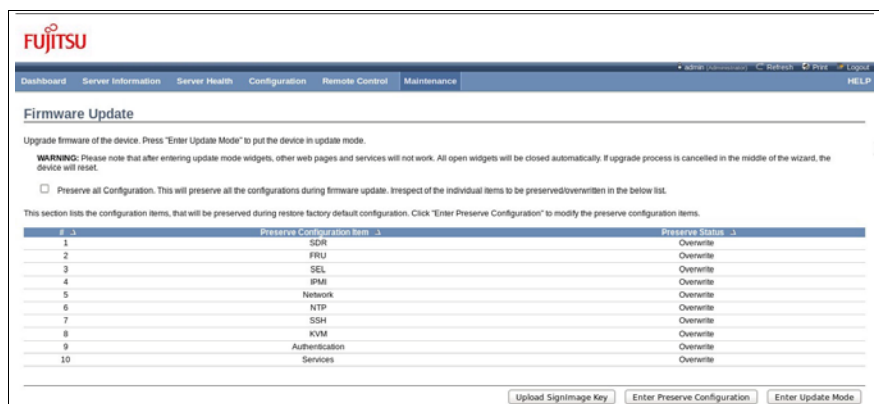


図 42: 「Firmware Update」ページ

手順:

「*Enter Update Mode*」をクリックして現在のデバイスのファームウェアをアップグレードします。次の手順に従います。

1. アクティブなすべてのクライアント要求を終了します。
2. デバイスでファームウェアアップグレードの準備をします。
3. ファームウェアイメージをアップロードします。
4. ファームウェアイメージを確認します。
5. ファームウェアイメージをフラッシュします。
6. デバイスをリセットします。



これで、後続のページの説明に従って、カードのファームウェアアップデートを成功させることができます。アップデートをキャンセルした場合、デバイスはリセットされます。また、ファームウェアアップデートが成功しても、デバイスはリセットされます。

7.2 Preserve Configuration

このページでは、構成の保存の項目を設定できます。この設定は、デフォルトの構成で上書きせずに既存の構成を保存するために「Restore Factory Defaults」で使用されます。

7.3 Restore Factory Defaults

MegaRAC GUI では、このオプションを使用してデバイスファームウェアを工場出荷時の構成に戻します。



警告！

リストアファクトリウィジェットに移行すると、他の Web ページやサービスが動作しなくなることにご注意ください。開いているすべてのウィジェットは自動的に閉じます。デバイスはリセットされ、数分以内に再起動します。

「Restore Factory Defaults」ページを開くには、メインメニューの「Maintenance – Restore Factory Defaults」をクリックします。次のスクリーンショットに「Restore Factory Defaults」ページのサンプルスクリーンショットを示します。

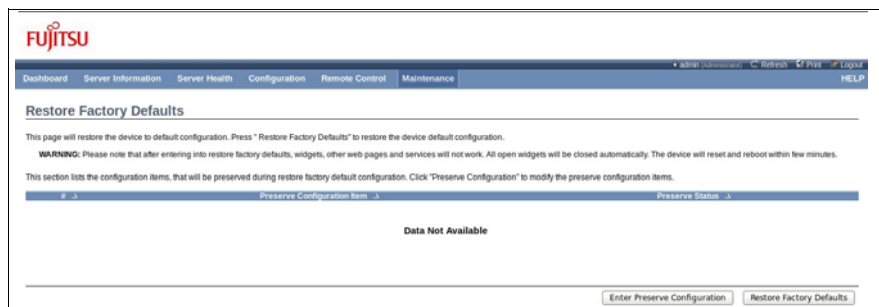


図 43: 「Restore Factory Defaults」ページ

手順：

「Restore Factory」をクリックしてデバイスファームウェアを工場出荷時の構成に戻します。

8 ログアウト

MegaRAC GUI をログアウトするには、画面の右上隅にあるログアウトリンクをクリックします。

9 ユーザ権限

Web GUI 権限リスト	IPMI と Web GUI との権限の関連正			
	Administrator	Operator	User	OEM
Web GUI から BMC へログイン、SSH	0	0	x	0
Web GUI から BMC を設定	0	x	x	x
Web GUI からユーザを設定	0	x	x	x
Web GUI からログをクリア	0	x	x	x
Web GUI からサーバの電源制御を実行	0	x	x	x
仮想 KVM リダイレクション	0	x	x	x

表 35: ユーザ権限

