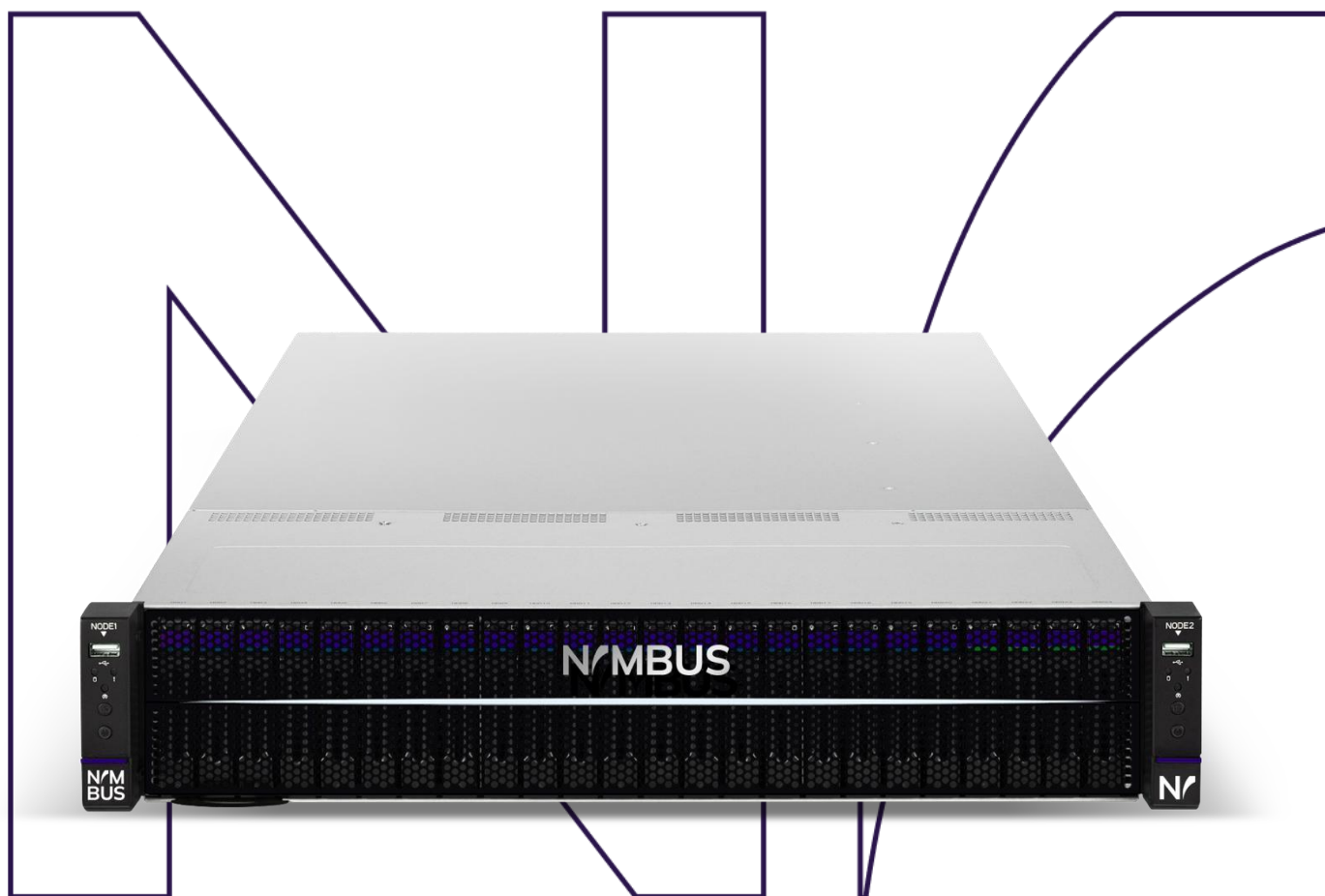




ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ВМС

+

для систем хранения данных NIMBUS
Руководство пользователя

Лист регистрации изменений

Редакция	Дата	Автор	Описание изменений
1.0	19.06.2025	Устинов Вадим	Первоначальная редакция
1.1	29.09.2026	Устинов Вадим	Добавлено содержание, обновлены шрифты и фирменной стиль

Содержание

1. Общие сведения	5
1.1 Целевая аудитория	5
1.2 Область применения	5
1.3 Соглашения, термины и обозначения	5
2. Быстрый старт	6
2.1 Параметры доступа по умолчанию	6
2.2 Первый вход в систему	6
3. Работа с веб-интерфейсом	7
3.1 Строка меню (Menu Bar)	7
3.2 Панель мониторинга (Dashboard)	8
3.3 Датчики (Sensors)	8
3.3.1 Сведения о датчике (Sensor Detail)	9
3.3.2 Настройка порогов (Threshold Settings)	9
3.4 Состав системы (System Inventory)	10
3.5 Сведения о FRU (FRU Information)	11
3.6 Журналы и отчёты (Logs & Reports)	12
3.7 Настройки (Settings)	14
3.7.1 Снимок экрана BSOD (Captured BSOD)	14
3.7.2 Дата и время (Date & Time)	15
3.7.3 Внешние службы аутентификации (External User Services)	17
3.7.4 Управление вентиляторами (Fan Management)	24
3.7.5 Настройки журналов (Log Settings)	24
3.7.6 Перенаправление носителей (Media Redirection Settings)	26
3.7.7 Сетевые настройки (Network Settings)	29
3.7.8 Порядок модулей PAM (PAM Order Settings)	35
3.7.9 Настройки SMTP (SMTP Settings)	36
3.7.10 Настройки SSL (SSL Settings)	38
3.7.11 Межсетевой экран (System Firewall)	41
3.7.12 Управление пользователями (User Management)	46
3.8 Удалённое управление (Remote Control)	50
3.9 Управление питанием (Power Control)	55
3.10 Обслуживание (Maintenance)	56
3.10.1 Резервное копирование конфигурации (Backup Configuration)	56
3.10.2 Расположение образа микропрограммы (Firmware Image Location)	58
3.10.3 Сведения о микропрограмме (Firmware Information)	59
3.10.4 Обновление микропрограммы (Firmware Update)	60
3.10.5 Сохраняемые параметры конфигурации (Preserve Configuration)	65
3.10.6 Восстановление конфигурации (Restore Configuration)	70
3.10.7 Восстановление заводских настроек (Restore Factory Defaults)	70

3.10.8 Системный администратор (System Administrator).....	71
--	----

1. Общие сведения

1.1 Целевая аудитория

Руководство предназначено для администраторов серверов, специалистов по эксплуатации ИТ-инфраструктуры и технического персонала, выполняющих управление оборудованием через контроллер BMC.

1.2 Область применения

Руководство распространяется на следующее изделие:

- Плата серверная системная ЛВГП.469539.001

1.3 Соглашения, термины и обозначения

В таблице ниже приведены основные термины и сокращения, используемые в настоящем документе.

Таблица 1. Термины и сокращения

Термин	Определение
BMC	Baseboard Management Controller — контроллер управления системной платой
IPMI	Intelligent Platform Management Interface — интеллектуальный интерфейс управления платформой
FRU	Field Replaceable Unit — сменный модуль, который можно оперативно заменить на месте эксплуатации для восстановления работоспособности системы
SDR	Sensor Data Record — запись данных датчика
SEL	System Event Log — журнал системных событий
IPMB	Intelligent Platform Management Bus — архитектура и протокол соединения интеллектуальных контроллеров через последовательную шину на базе I2C для управления платформой
NetFn	6-битное значение, определяющее функцию целевого узла, к которой выполняется обращение. Чётное значение соответствует запросу, нечётное — ответу. Например, 02h — запрос-мост (bridging request), 03h — ответ-мост (bridging response)
LUN	Младшие 2 бита байта netFn — номер логического устройства (Logical Unit Number), обеспечивающий дополнительную адресацию внутри целевого узла
KCS	Keyboard Controller Style — интерфейс в стиле контроллера клавиатуры
RMCP	Remote Management Control Protocol — протокол удалённого управления, определённый DMTF
SOL	Serial Over LAN — передача последовательной консоли по сети LAN
POST	Power On Self Test — самотестирование при включении питания
NCSI	Network Controller Sideband Interface — внеполосный (sideband) интерфейс сетевого контроллера

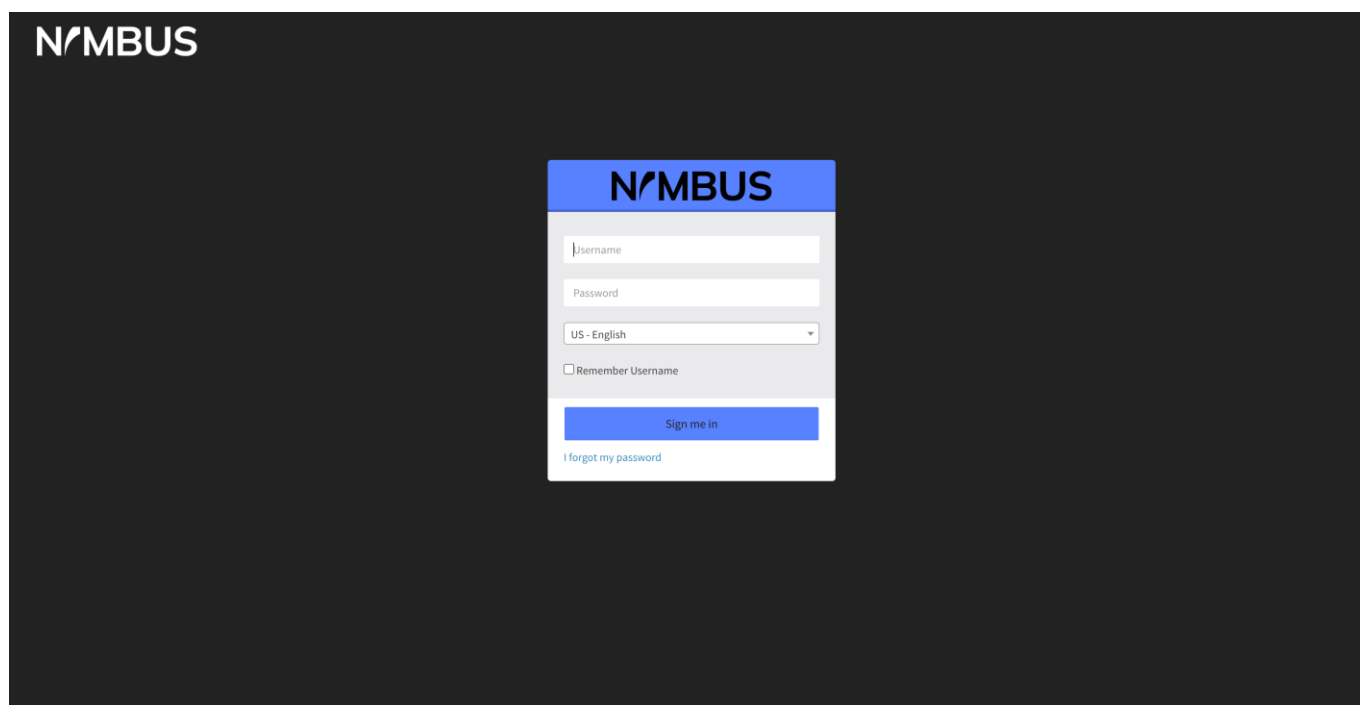
2. Быстрый старт

2.1 Параметры доступа по умолчанию

- IP-адрес по умолчанию: 192.168.1.82
- Учётные данные по умолчанию: admin/admin
- Порт: 443 (HTTPS)

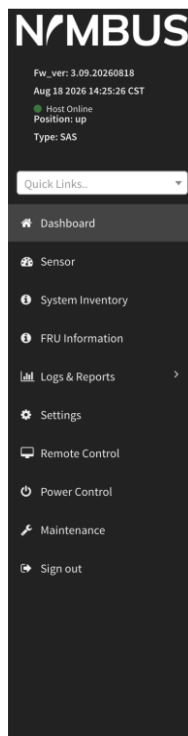
2.2 Первый вход в систему

1. Подключите рабочую станцию кабелем Ethernet к выделенному порту управления ВМС.
2. Введите IP-адрес по умолчанию в адресной строке веб-браузера.
3. Если браузер выдаст предупреждение о сертификате, подтвердите переход на страницу и выполните вход.



3. Работа с веб-интерфейсом

3.1 Строка меню (Menu Bar)



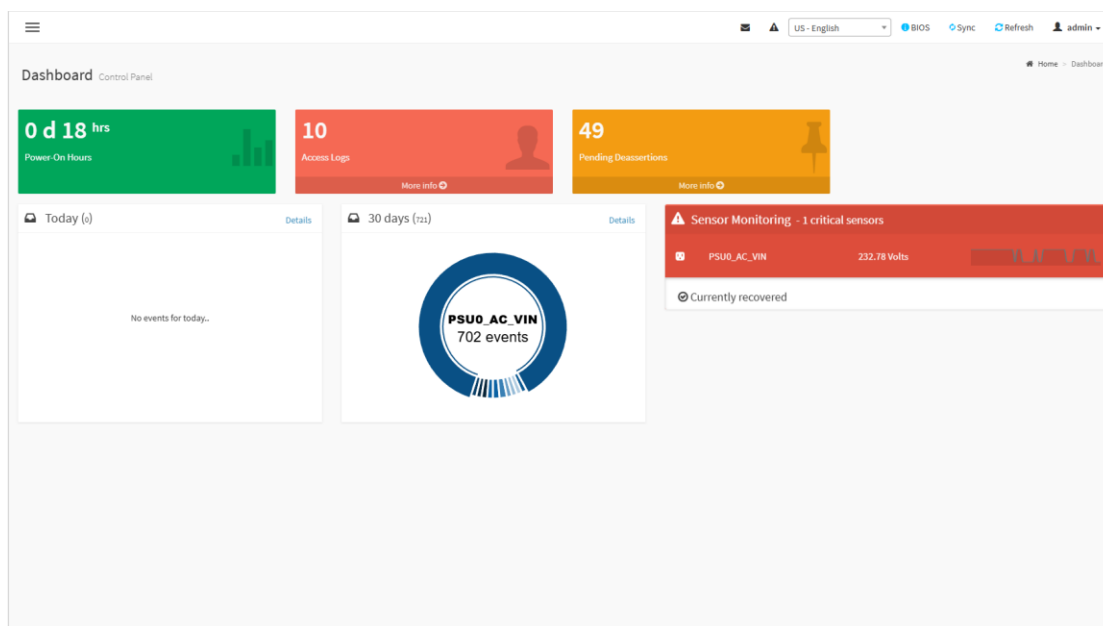
В верхней части строки меню отображается информация о микропрограмме: текущая версия, дата и время сборки. Состояние питания хоста отображается как **Host Online**. Чтобы изменить состояние питания, нажмите ссылку **Host Online**.

Также отображаются текущая позиция и тип узла.

Строка меню обеспечивает доступ к следующим функциональным разделам:

- Dashboard — панель мониторинга
- Sensor — датчики
- System Inventory — состав системы
- FRU Information — сведения о FRU
- Logs & Reports — журналы и отчёты
- Settings — настройки
- Remote Control — удалённое управление
- Power Control — управление питанием
- Maintenance — обслуживание
- Sign out — выход из системы

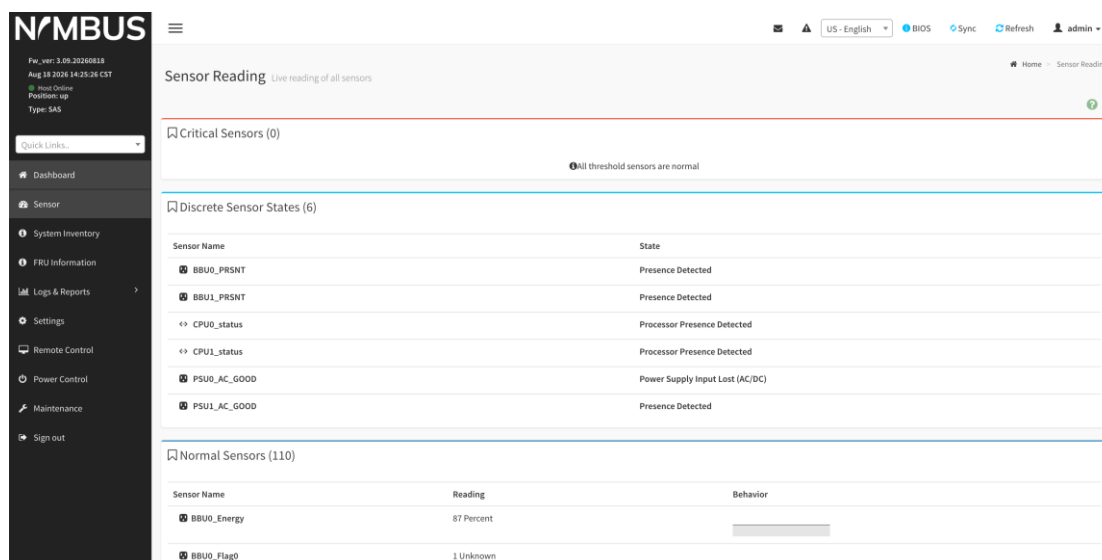
3.2 Панель мониторинга (Dashboard)



Страница **Dashboard** отображает сводную информацию о состоянии устройства. Чтобы открыть её, выберите **Dashboard** в строке меню.

На странице отображаются: время работы под питанием (Power On Hours), журнал доступа (Access Logs), неснятые события (Pending Deassertions), события за текущие сутки и за 30 дней (Today & 30 Days, Event Logs), а также данные мониторинга датчиков (Sensor Monitoring).

3.3 Датчики (Sensors)



Страница **Sensor Readings** отображает все данные, связанные с датчиками.

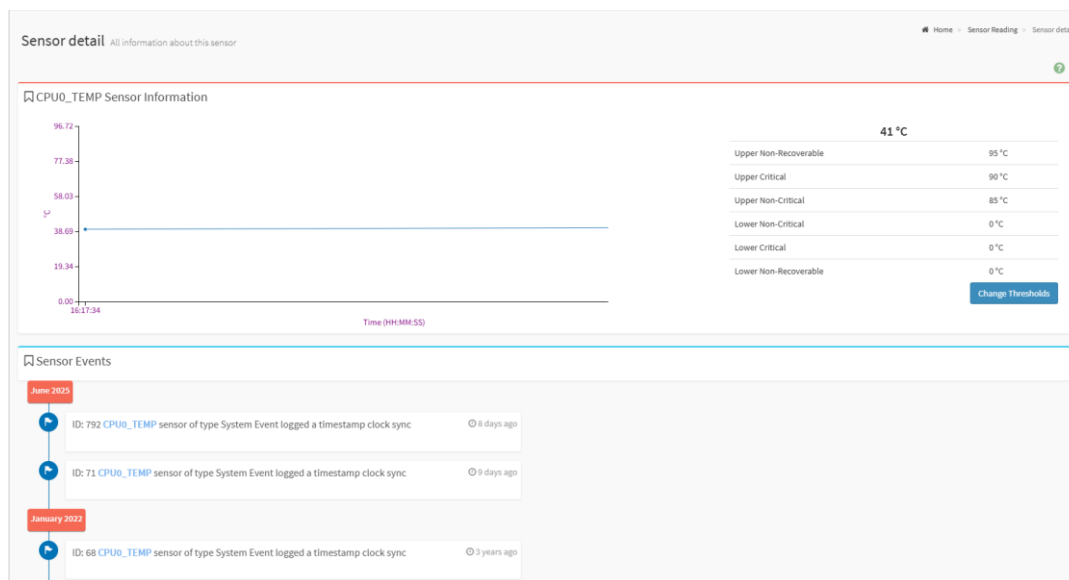
Чтобы открыть страницу, выберите **Sensor** в строке меню. При нажатии на любой датчик открывается подробная информация о нём, включая пороговые значения и график всех связанных с ним событий.

На странице **Sensor Reading** в реальном времени отображаются показания всех доступных датчиков: имя датчика (Name), состояние (Status), текущее значение

(Current Reading) и характер изменения (Behavior). Также можно выбрать из списка тип датчиков, которые требуется отобразить, например: датчики температуры, датчики вентиляторов, сторожевые датчики (Watchdog) и датчики напряжения.

3.3.1 Сведения о датчике (Sensor Detail)

Выберите датчик в списке критических (Critical Sensor) или штатных (Normal Sensor) датчиков. Для выбранного датчика отобразятся виджет текущих показаний (Live Widget) и пороговые значения (Thresholds), как показано на рисунке ниже.



Для выбранного датчика виджет отображает показания в динамике.

Предусмотрено шесть типов пороговых значений:

- Lower Non-Recoverable (LNR) — нижний неустраняемый порог
- Lower Critical (LC) — нижний критический порог
- Lower Non-Critical (LNC) — нижний некритический порог
- Upper Non-Recoverable (UNR) — верхний неустраняемый порог
- Upper Critical (UC) — верхний критический порог
- Upper Non-Critical (UNC) — верхний некритический порог

3.3.2 Настройка порогов (Threshold Settings)

Чтобы настроить пороговые значения, нажмите **Change Thresholds**. Пример страницы приведён ниже.

Введите пороговые значения и нажмите **Save**, чтобы применить их.

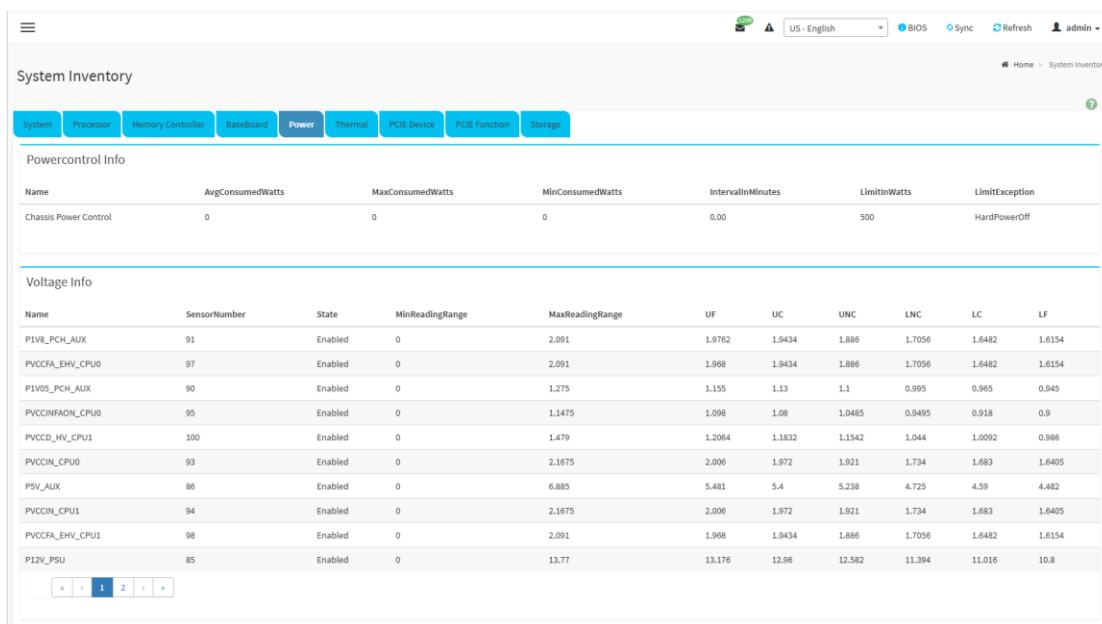
Примечание: настройка пороговых значений доступна только пользователям с правами администратора (Administrator) или оператора (Operator). Для остальных пользователей параметр **Threshold Settings** неактивен, и выполнить это действие они не могут.

3.4 Состав системы (System Inventory)

Раздел **System Inventory** веб-интерфейса BMC (Baseboard Management Controller) содержит сводные сведения об аппаратных компонентах и микропрограммах сервера, в том числе:

- Processor — процессоры
- Memory Controller — контроллер памяти
- BaseBoard (BMC) — системная плата (BMC)
- Power — электропитание
- Thermal — температурный режим
- PCIe Device — устройства PCIe
- PCIe Function — функции PCIe
- Storage — накопители

Раздел упрощает учёт оборудования, его обслуживание и поиск неисправностей, поскольку отображает конфигурацию и состояние сервера.



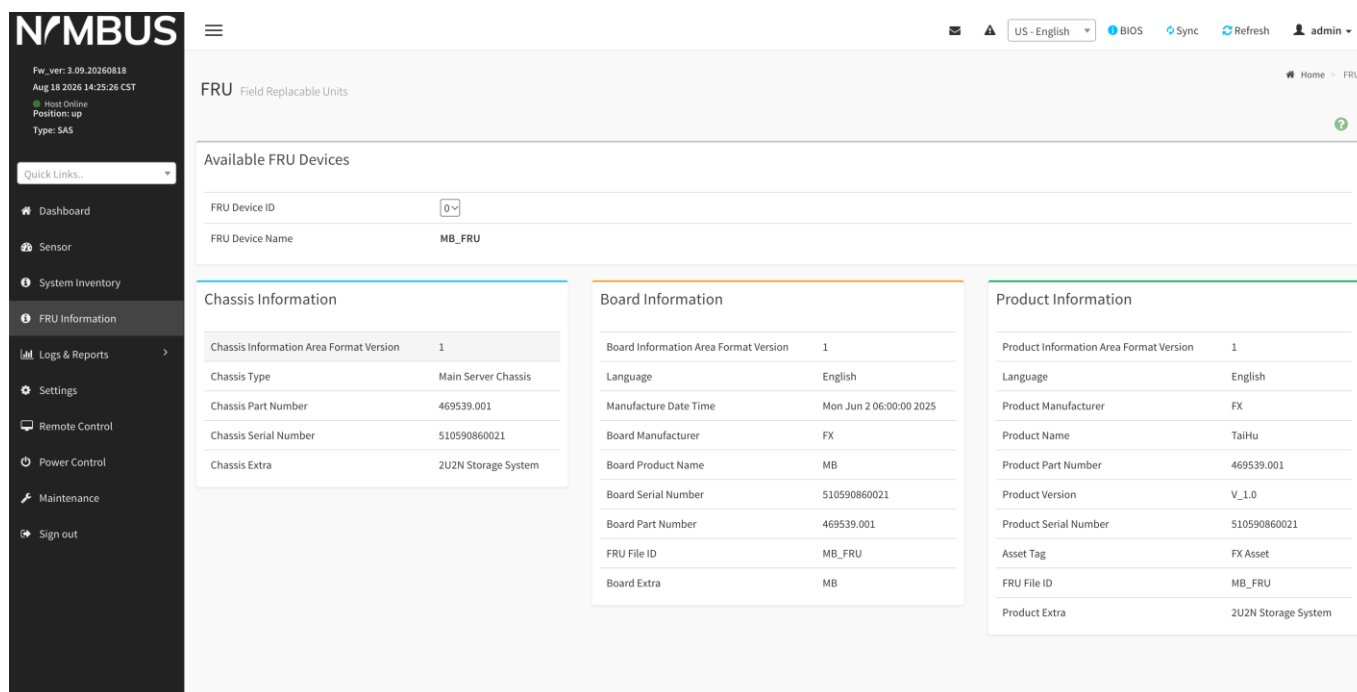
Name	AvgConsumedWatts	MaxConsumedWatts	MinConsumedWatts	IntervalInMinutes	LimitInWatts	LimitException
Chassis Power Control	0	0	0	0.00	500	HardPowerOff

Name	SensorNumber	State	MinReadingRange	MaxReadingRange	UF	UC	UNC	LNC	LC	LF
P1VB_PCH_AUX	91	Enabled	0	2.091	1.9762	1.9434	1.886	1.7056	1.6482	1.6154
PVCCFA_EHV_CPU0	97	Enabled	0	2.091	1.968	1.9434	1.886	1.7056	1.6482	1.6154
P1V95_PCH_AUX	90	Enabled	0	1.275	1.155	1.13	1.1	0.995	0.965	0.945
PVCCINFAON_CPU0	95	Enabled	0	1.1475	1.098	1.08	1.0485	0.9495	0.918	0.9
PVCCD_HV_CPU1	100	Enabled	0	1.479	1.2064	1.1832	1.1542	1.044	1.0092	0.988
PVCCIN_CPU0	93	Enabled	0	2.1675	2.006	1.972	1.921	1.734	1.683	1.6405
PSU_AUX	86	Enabled	0	6.885	5.481	5.4	5.238	4.725	4.59	4.482
PVCCIN_CPU1	94	Enabled	0	2.1675	2.006	1.972	1.921	1.734	1.683	1.6405
PVCCFA_EHV_CPU1	98	Enabled	0	2.091	1.968	1.9434	1.886	1.7056	1.6482	1.6154
P12V_PSU	85	Enabled	0	13.77	13.176	12.96	12.582	11.394	11.016	10.8

3.5 Сведения о FRU (FRU Information)

Страница **FRU Information** отображает сведения об устройствах FRU, зарегистрированных в BMC: основные сведения (Basic Information), сведения о шасси (Chassis Information), сведения о плате (Board Information) и сведения об изделии (Product Information).

Чтобы открыть страницу, выберите **FRU Information** в строке меню. Выберите идентификатор устройства в поле **FRU Device ID**, чтобы просмотреть сведения о нём. Пример страницы приведён ниже.



FRU Device ID	FRU Device Name
0	MB_FRU

Chassis Information	
Chassis Information Area Format Version	1
Chassis Type	Main Server Chassis
Chassis Part Number	469539.001
Chassis Serial Number	510590860021
Chassis Extra	2U2N Storage System

Board Information	
Board Information Area Format Version	1
Language	English
Manufacture Date Time	Mon Jun 2 06:00:00 2025
Board Manufacturer	FX
Board Product Name	MB
Board Serial Number	510590860021
Board Part Number	469539.001
FRU File ID	MB_FRU
Board Extra	MB

Product Information	
Product Information Area Format Version	1
Language	English
Product Manufacturer	FX
Product Name	TaiHu
Product Part Number	469539.001
Product Version	V_1.0
Product Serial Number	510590860021
Asset Tag	FX Asset
FRU File ID	MB_FRU
Product Extra	2U2N Storage System

Для выбранного устройства отображаются следующие поля.

Available FRU Devices — доступные устройства FRU:

- **FRU Device ID** — выберите идентификатор устройства в раскрывающемся списке;

- **FRU Device Name** — имя выбранного устройства FRU.

Chassis Information — сведения о шасси:

- Chassis Information Area Format Version — версия формата области сведений о шасси
- Chassis Type — тип шасси
- Chassis Part Number — каталожный номер шасси
- Chassis Serial Number — серийный номер шасси
- Chassis Extra — дополнительные сведения о шасси

Board Information — сведения о плате:

- Board Information Area Format Version — версия формата области сведений о плате
- Language — язык
- Manufacture Date Time — дата и время изготовления
- Board Manufacturer — изготовитель платы
- Board Product Name — наименование платы
- Board Serial Number — серийный номер платы
- Board Part Number — каталожный номер платы
- FRU File ID — идентификатор файла FRU
- Board Extra — дополнительные сведения о плате

Product Information — сведения об изделии:

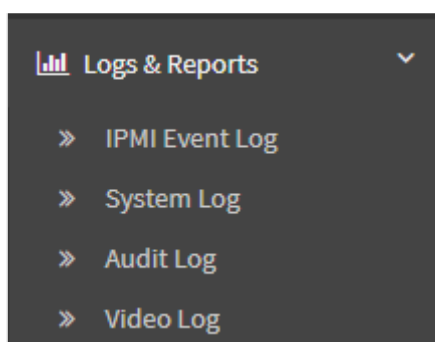
- Product Information Area Format Version — версия формата области сведений об изделии
- Language — язык
- Product Manufacturer — изготовитель изделия
- Product Name — наименование изделия
- Product Part Number — каталожный номер изделия
- Product Version — версия изделия
- Product Serial Number — серийный номер изделия
- Asset Tag — инвентарный номер
- FRU File ID — идентификатор файла FRU
- Product Extra — дополнительные сведения об изделии

3.6 Журналы и отчёты (Logs & Reports)

Страница **Logs & Reports** содержит следующие журналы:

- IPMI Event Log — журнал событий IPMI
- System Log — системный журнал
- Audit Log — журнал аудита
- Video Log — журнал видеозаписей

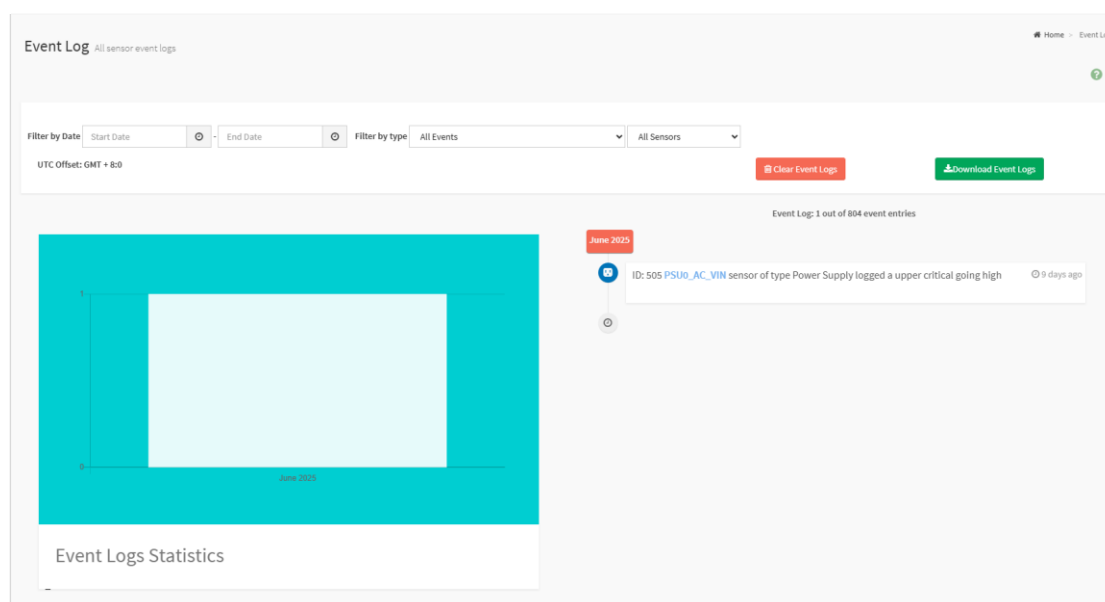
Пункты меню раздела **Logs & Reports** показаны на рисунке ниже.



Журнал событий IPMI (IPMI Event Log)

Страница отображает список событий, зарегистрированных различными датчиками устройства. Чтобы просмотреть подробности записи, дважды нажмите на неё. Для отбора событий используйте фильтры по типу или имени датчика; список также можно отсортировать, нажав на заголовок любого столбца.

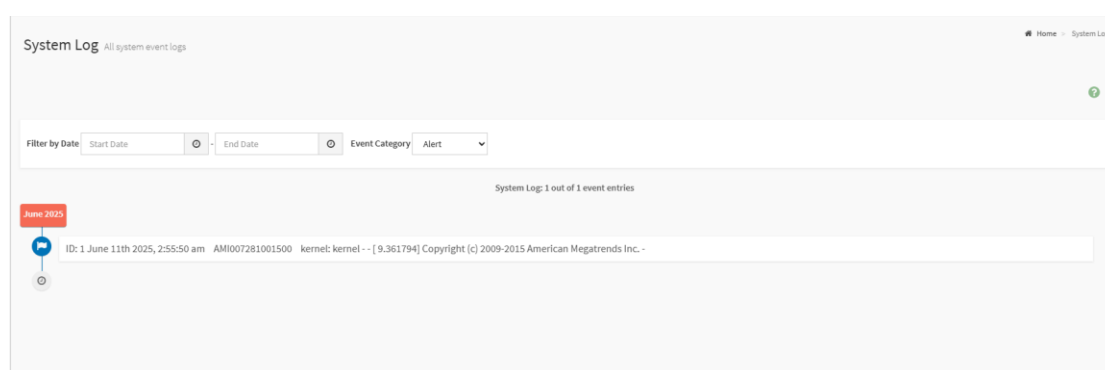
Чтобы открыть страницу, выберите в строке меню **Logs & Reports** > **Event Log**. Пример страницы приведён ниже.



Системный журнал (System Log)

Страница отображает все системные события устройства, для которых настроена регистрация.

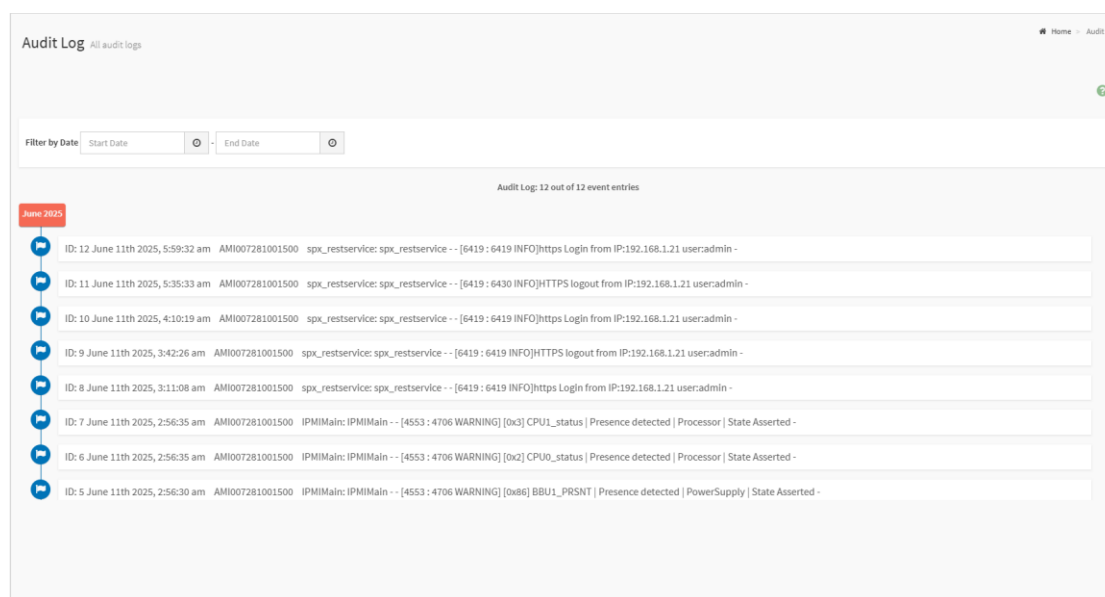
Чтобы открыть страницу, выберите в строке меню **Logs & Reports** > **System Log**.



Журнал аудита (Audit Log)

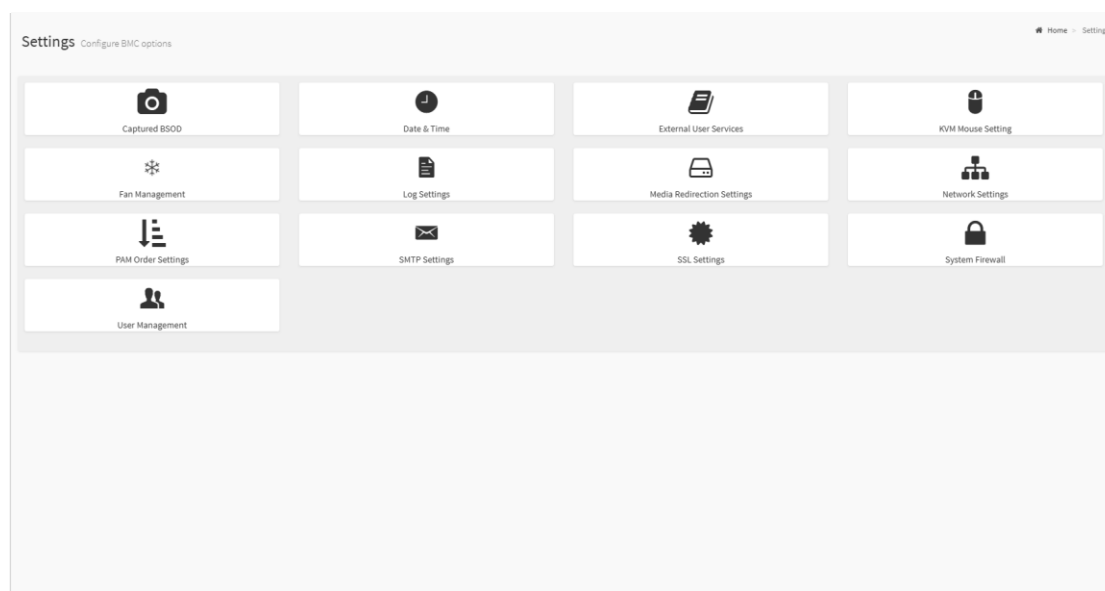
Страница отображает все события аудита устройства, для которых настроена регистрация.

Чтобы открыть страницу, выберите в строке меню **Logs & Reports > Audit Log**.



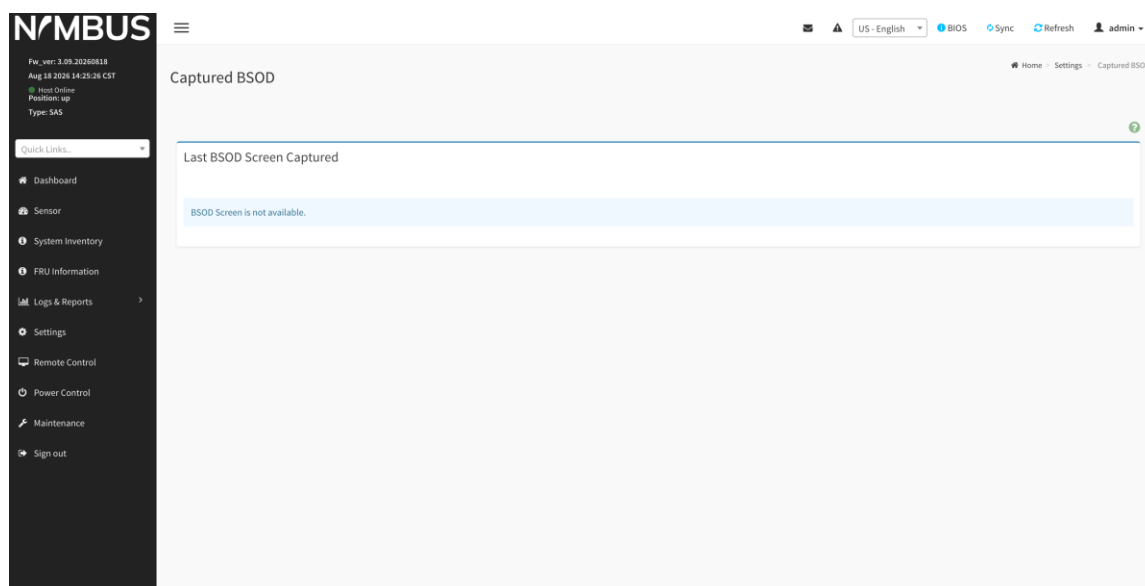
3.7 Настройки (Settings)

Раздел объединяет страницы, на которых выполняется настройка различных параметров BMC. Меню раздела показано на рисунке ниже.



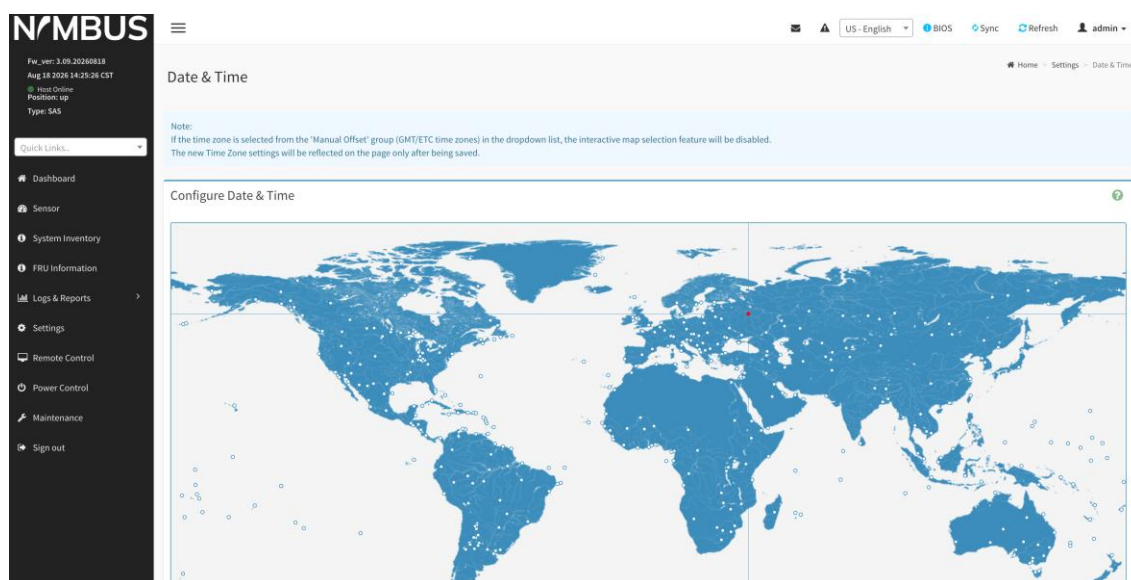
3.7.1 Снимок экрана BSOD (Captured BSOD)

Страница отображает снимок «синего экрана» (BSOD), зафиксированный в случае аварийного завершения работы операционной системы хоста после последней перезагрузки. Пример страницы приведен ниже.



3.7.2 Дата и время (Date & Time)

Страница предназначена для установки даты и времени BMC. Пример страницы приведён ниже.



Configure Date & Time — отображает список часовых поясов со смещением относительно UTC и перечнем населённых пунктов, а также карту для выбора местоположения, по которому определяется точное местное время.

Select Time Zone — выбор часового пояса, используемого при установке даты и времени BMC.

Automatic Date & Time — автоматическая синхронизация даты и времени с сервером NTP.

- **Primary NTP Server** — основной сервер NTP, используемый для автоматической установки даты и времени.
- **Secondary NTP Server** — резервный сервер NTP, используемый для автоматической установки даты и времени.

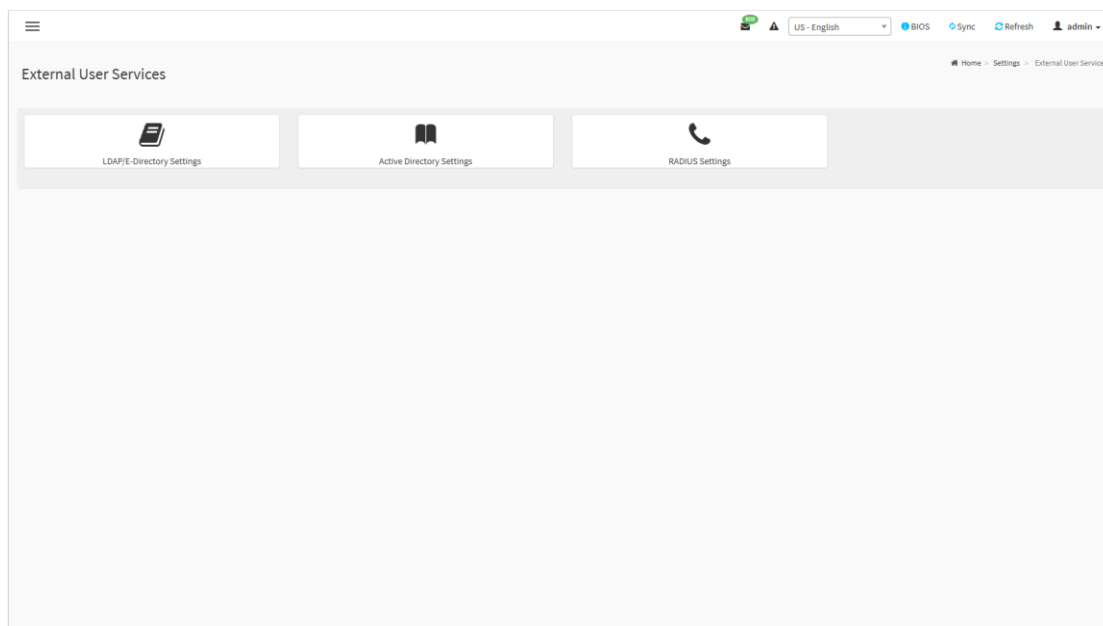
- **Automatic PTP Date & Time** — включение или отключение автоматической установки даты и времени по серверам PTP.
- **PTP Interface** — сетевой интерфейс, через который выполняется синхронизация с сервером PTP.
- **PTP Preset** — тип предустановленного профиля PTP.
- **PTP Transport** — тип транспорта PTP.
- **PTP Ipmode** — режим адресации PTP (IP mode).
- **PTP Unicast IP** — IP-адрес сервера PTP при одноадресном (unicast) режиме.
- **PTP Delay Mechanism** — механизм измерения задержки PTP.
- **PTP Inbound Latency** — входящая задержка сервера.
- **PTP Outbound Latency** — исходящая задержка сервера.
- **PTP Priority1** — приоритет часов PTP (Priority1).
- **PTP Max Master capacity** — максимальное число ведущих часов PTP (Master).
- **Panic Mode** — режим, при котором часы PTP не сбрасываются, если скачок времени превышает 1 секунду.
- **PTP Log request delay** — интервал запросов задержки PTP.

Порядок настройки

1. Выберите часовой пояс (**Timezone**) в раскрывающемся списке или на карте.
2. Включите параметр **Automatic Date & Time**, чтобы использовать серверы NTP для автоматической установки даты и времени.
 - а) В полях **Primary NTP Server** и **Secondary NTP Server** укажите адреса основного и резервного серверов NTP соответственно.

***Примечание:** поле **Secondary NTP Server** заполнять не обязательно. Резервный сервер NTP используется, если основной сервер недоступен или работает некорректно.*
3. Включите параметр **Automatic PTP Date & Time**, чтобы использовать серверы PTP для автоматической установки даты и времени.
 - а) Заполните соответствующие поля: **Interface**, **Preset**, **Transport**, **Ipmode**, **Unicast IP**, **Delay Mechanism**, **Inbound Latency**, **Outbound Latency**, **Priority1**, **Max Master capacity** и **Log request delay**.
 - б) При необходимости включите или отключите **Panic Mode** (запрет сброса часов при скачке времени более 1 секунды).
4. Нажмите **Save**, чтобы сохранить настройки.

3.7.3 Внешние службы аутентификации (External User Services)



Настройки LDAP/E-Directory (LDAP/E-Directory Settings)

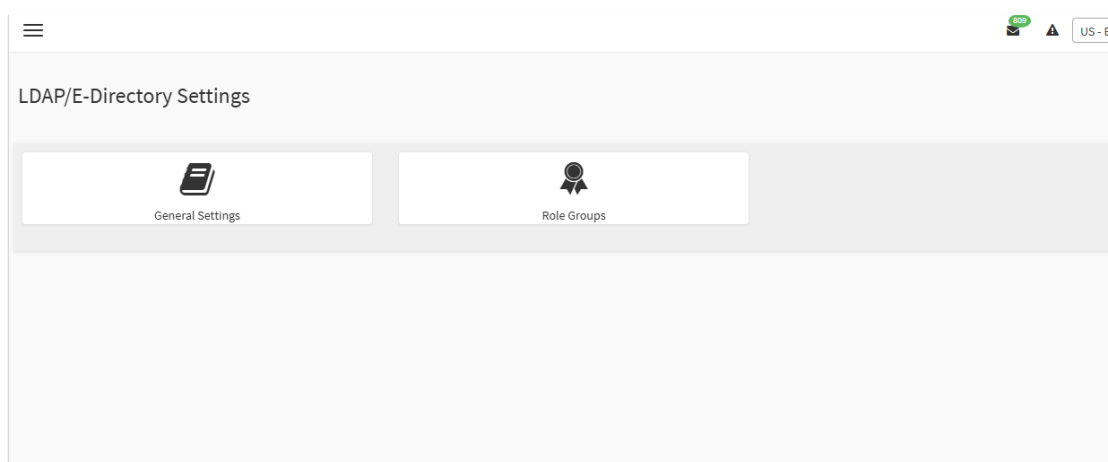
LDAP (Lightweight Directory Access Protocol) / E-Directory — прикладной протокол для запросов к службам каталогов и изменения их данных в IP-сетях.

В веб-интерфейсе BMC протокол LDAP используется для аутентификации пользователей.

Если в сети развёрнут сервер LDAP, его можно использовать для добавления, управления и аутентификации пользователей BMC: запросы на вход в систему передаются серверу LDAP.

Таким образом, при работе с BMC не требуется настраивать отдельный механизм аутентификации. Поскольку сервер LDAP обеспечивает централизованную аутентификацию, всегда известно, кто обращается к сетевым ресурсам, а политики доступа легко задать на уровне отдельных пользователей или групп.

Чтобы открыть страницу, выберите в строке меню **Settings** > **External User Services**. Пример страницы приведён ниже.



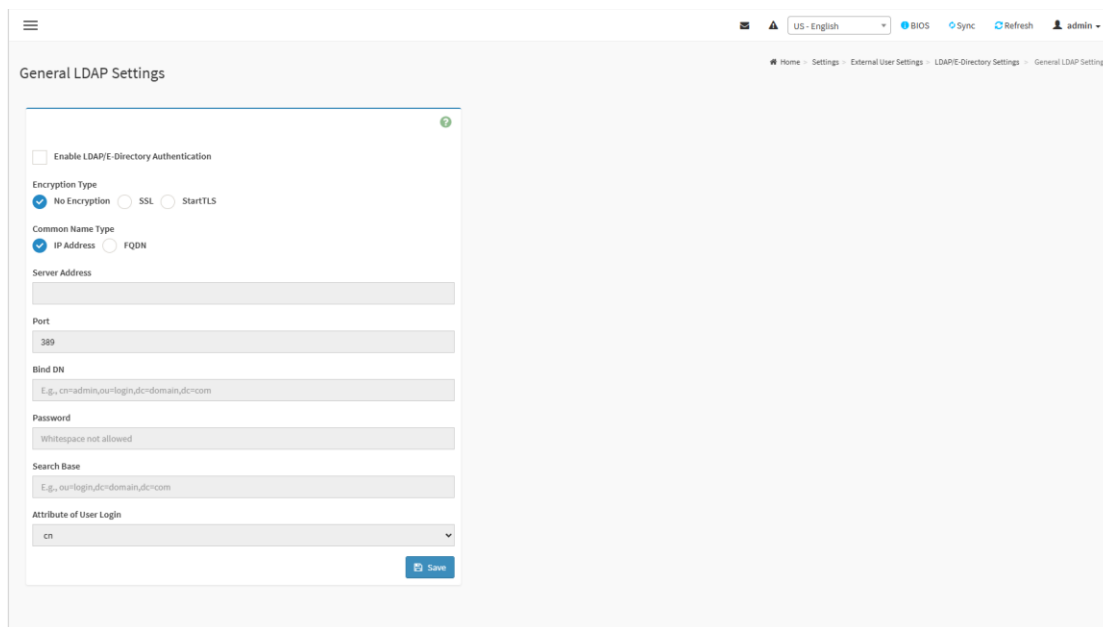
General Settings — общие настройки LDAP/E-Directory: включение аутентификации LDAP/E-Directory, IP-адрес, порт и база поиска (Search Base).

Role Groups — добавление группы ролей. Группу также можно добавить, дважды нажав на свободную строку.

Порядок настройки

Заполнение общих настроек LDAP/E-Directory:

1. На странице **LDAP/E-Directory Settings** нажмите **General Settings**. Пример страницы приведён ниже.



2. Установите флажок **Enable LDAP/E-Directory Authentication**, чтобы включить аутентификацию через LDAP/E-Directory.
3. Выберите тип шифрования в поле **Encryption Type**.
4. В поле **Common Name Type** выберите **IP Address**.
5. В поле **Server Address** введите IP-адрес сервера LDAP.
6. В поле **Port** укажите порт LDAP.
7. Укажите **Bind DN** — учётную запись, от имени которой BMC подключается к серверу LDAP при выполнении операции привязки (bind).
8. Введите пароль в поле **Password**.

Примечание: пароль должен содержать не менее 1 и не более 48 символов. Пробелы не допускаются.

9. Укажите базу поиска (**Search Base**) — ветвь дерева каталога, в которой сервер LDAP будет искать пользователей, например подразделение или группу.
10. В поле **Attribute of User Login** выберите атрибут, по которому сервер LDAP/E-Directory идентифицирует пользователя.

Примечание: поддерживаются только атрибуты *cn* и *uid*.

11. В поле **CA Certificate File** нажмите **Browse** и выберите файл сертификата доверенного удостоверяющего центра (CA).
12. В поле **Certificate File** выберите файл сертификата клиента.
13. В поле **Private Key** выберите файл закрытого ключа клиента.

Примечание: при включённом *SSL* или *StartTLS* обязательны все три файла.

14. Нажмите **Save**, чтобы сохранить настройки.

Добавление группы ролей

1. На странице **LDAP/E-Directory Settings** нажмите **Role Groups** и выберите пустую строку.
2. Нажмите **Add Role Group** или дважды нажмите на пустую строку. Откроется страница добавления группы ролей, показанная ниже.

3. В поле **Group Name** введите имя, идентифицирующее группу ролей.

Примечание: имя группы ролей — строка длиной до 255 буквенно-цифровых символов. Допускаются дефис и подчёркивание.

4. В поле **Group Domain** укажите домен, в котором находится группа ролей.

Примечание:

- имя домена — строка длиной от 4 до 64 буквенно-цифровых символов;
- имя должно начинаться с буквы;
- допускаются точка (.), запятая (,), дефис (-), подчёркивание (_) и знак равенства (=);
- пример: `cn=manager,ou=login,dc=domain,dc=com`.

5. В поле **Group Privilege** выберите уровень привилегий группы: User, Administrator, Operator или None.
6. Выберите нужные параметры (один или оба):

- **KVM Access**
- **VMedia Access**

Примечание: привилегия VMedia не распространяется на клиенты LMedia и RMedia.

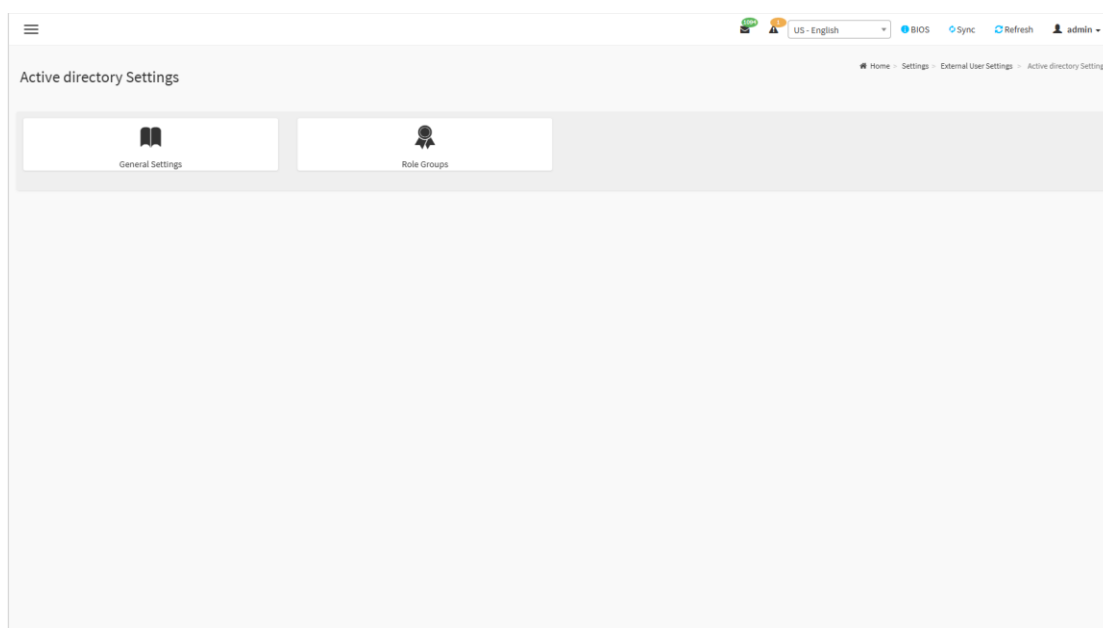
7. Нажмите **Save**, чтобы сохранить группу ролей и вернуться к списку групп.

Настройки Active Directory (Active Directory Settings)

Active Directory (AD) — служба каталогов, используемая на компьютерах и серверах под управлением Microsoft Windows для хранения сведений о сетях и доменах. Служба выполняет ряд функций, в том числе предоставляет информацию об объектах каталога.

Active Directory упорядочивает объекты для быстрого поиска и доступа, предоставляет доступ конечным пользователям и администраторам и позволяет администратору настраивать безопасность каталога.

Чтобы открыть страницу, выберите в строке меню **Settings > External User Settings > Active Directory**. Пример страницы приведён ниже.

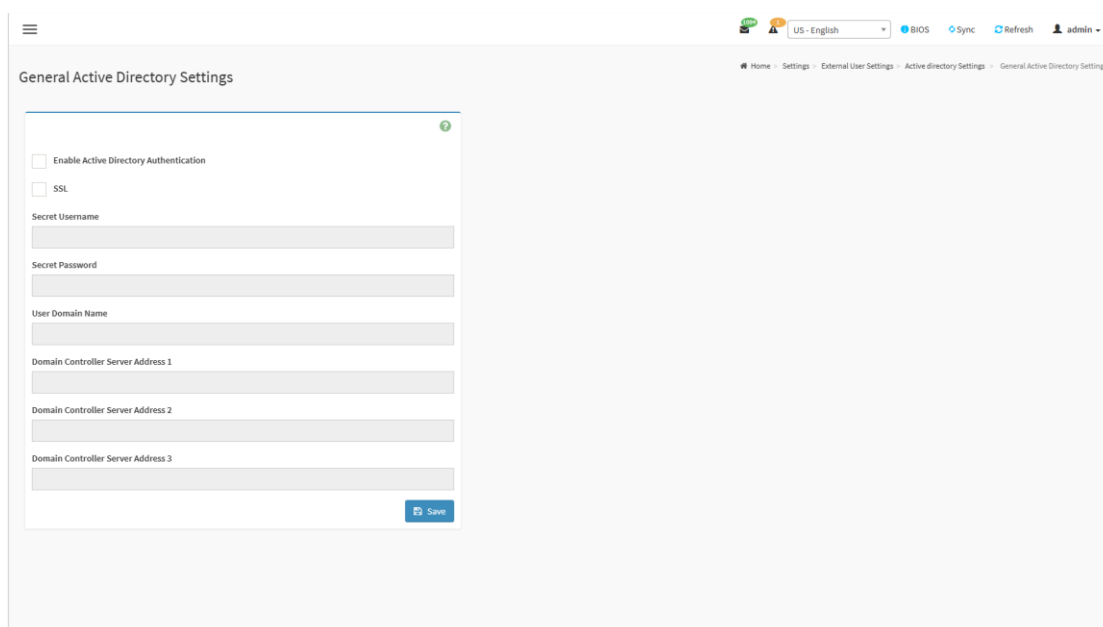


General Settings — общие настройки Active Directory: включение аутентификации через Active Directory, служебное имя пользователя (Secret User Name) и пароль (Secret Password), имя домена пользователя (User Domain Name) и до трёх адресов контроллеров домена (Domain Controller Server Address).

Role Groups — добавление группы ролей. Группу также можно добавить, дважды нажав на свободную строку.

Порядок настройки

Заполнение общих настроек Active Directory:



1. Нажмите **General Settings**, чтобы открыть страницу общих настроек Active Directory.
2. Установите или снимите флажок **Enable Active Directory Authentication**, чтобы включить или отключить аутентификацию через Active Directory.

Примечание: если аутентификация через Active Directory включена, укажите данные для подключения к серверу Active Directory.

3. **SSL** — установите или снимите флажок, чтобы включить или отключить SSL.
4. Укажите служебное имя пользователя и пароль в полях **Secret User Name** и **Secret Password**.

Примечание:

- служебные имя пользователя и пароль для AD указывать не обязательно. Если они не заданы, любая неудачная аутентификация расценивается как ошибка «Неверный пароль», и в этом случае PAM не переходит к другим методам аутентификации. Поэтому рекомендуется ставить AD последним в порядке PAM;
- имя пользователя — строка длиной от 1 до 64 буквенно-цифровых символов, начинающаяся с буквы;
- имя пользователя чувствительно к регистру;
- не допускаются: запятая, точка, двоеточие, точка с запятой, косая и обратная косая черта, квадратные и угловые скобки, вертикальная черта, знаки равенства, плюса и звёздочки, вопросительный знак, амперсанд, двойные кавычки и пробел;
- пароль должен содержать от 6 до 127 символов;
- пробелы не допускаются.

5. В поле **User Domain Name** укажите имя домена пользователя, например MyDomain.com.
6. Укажите IP-адреса контроллеров домена в полях **Domain Controller Server Address1**, **Domain Controller Server Address2** и **Domain Controller Server Address3**.

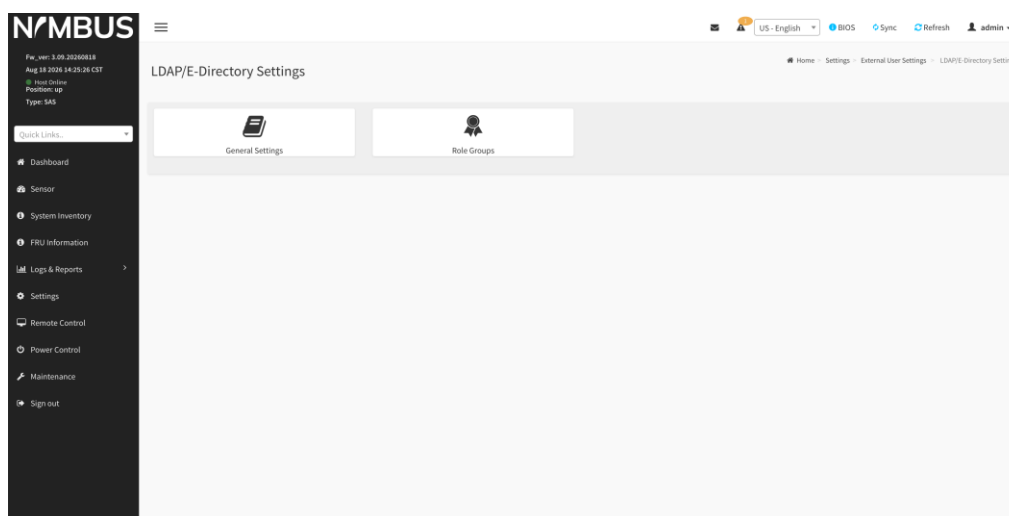
Примечание:

- необходимо указать адрес хотя бы одного контроллера домена;
- IPv4-адрес состоит из 4 чисел, разделённых точками: «xxx.xxx.xxx.xxx»;
- каждое число — от 0 до 255;
- первое число не может быть равно 0;
- поддерживаются адреса в форматах IPv4 и IPv6.

7. Нажмите **Save**, чтобы сохранить настройки и вернуться на страницу **Active Directory Settings**.

Группы ролей (Role Groups)

Чтобы открыть страницу групп ролей, выберите в строке меню **Settings > External User Settings > Active Directory > Role Groups**. Пример страницы приведён ниже.



Поля страницы:

Role Group Name — имя, идентифицирующее группу ролей в Active Directory.

Примечание: имя группы ролей — строка длиной до 64 буквенно-цифровых символов. Допускаются дефис и подчёркивание.

Group Name — имя группы ролей в Active Directory.

Примечание: имя группы ролей — строка длиной до 64 буквенно-цифровых символов. Допускаются дефис и подчёркивание.

Group Domain — домен, в котором находится группа ролей.

Примечание: имя домена — строка длиной до 255 буквенно-цифровых символов. Допускаются дефис, подчёркивание и точка.

Group Privilege — уровень привилегий, назначаемый группе ролей.

KVM Access — предоставление доступа к KVM пользователям группы, прошедшим аутентификацию в AD.

VMedia Access — предоставление доступа к VMedia пользователям группы, прошедшим аутентификацию в AD.

Добавление группы ролей

1. На странице **Active Directory Settings** выберите **Role Group** и нажмите **Add Role Group** или дважды нажмите на пустую строку. Откроется страница добавления группы ролей, показанная ниже.

2. В поле **Group Name** введите имя, идентифицирующее группу ролей в Active Directory.

Примечание: имя группы ролей — строка длиной до 64 буквенно-цифровых символов. Допускаются дефис и подчёркивание.

3. В поле **Group Domain** укажите домен, в котором находится группа ролей.

Примечание: имя домена — строка длиной до 255 буквенно-цифровых символов. Допускаются дефис, подчёркивание и точка.

4. В поле **Group Privilege** выберите уровень привилегий группы.

5. Выберите нужные параметры:

- **KVM Access**
- **VMedia Access**

Примечание: привилегия VMedia не распространяется на клиенты LMedia и RMedia.

6. Нажмите **Save**, чтобы добавить группу ролей и вернуться к списку **Role Group**.

Удаление группы ролей

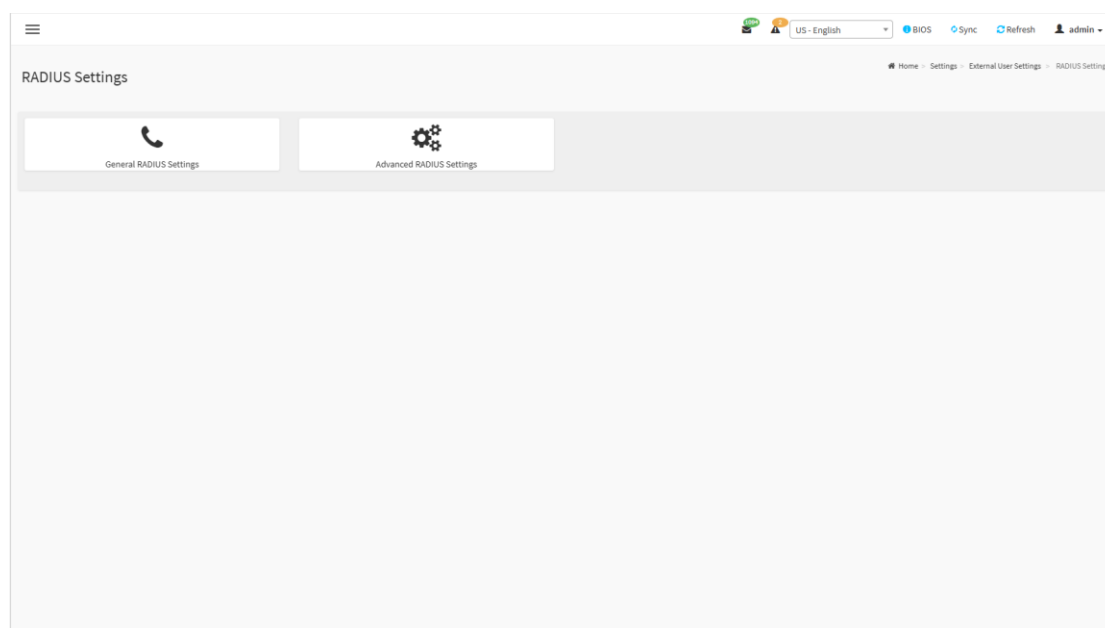
1. На странице **Role Groups** выберите строку, которую требуется удалить.

2. Нажмите **Delete Role Group**.

Настройки RADIUS (RADIUS Settings)

RADIUS — модульный высокопроизводительный комплекс программных средств с широкими возможностями, включающий сервер, клиенты, библиотеки для разработки и ряд вспомогательных утилит для работы с протоколом RADIUS.

Чтобы открыть страницу, выберите в строке меню **Settings > External User Settings > RADIUS Settings**. Пример страницы приведён ниже.



Общие настройки RADIUS (General RADIUS Settings)

Поля страницы:

Enable RADIUS Authentication — включение или отключение аутентификации через RADIUS.

Server Address — IP-адрес сервера RADIUS.

Примечание: допускаются IP-адрес (IPv4 или IPv6) и полное доменное имя (FQDN).

Port — номер порта RADIUS.

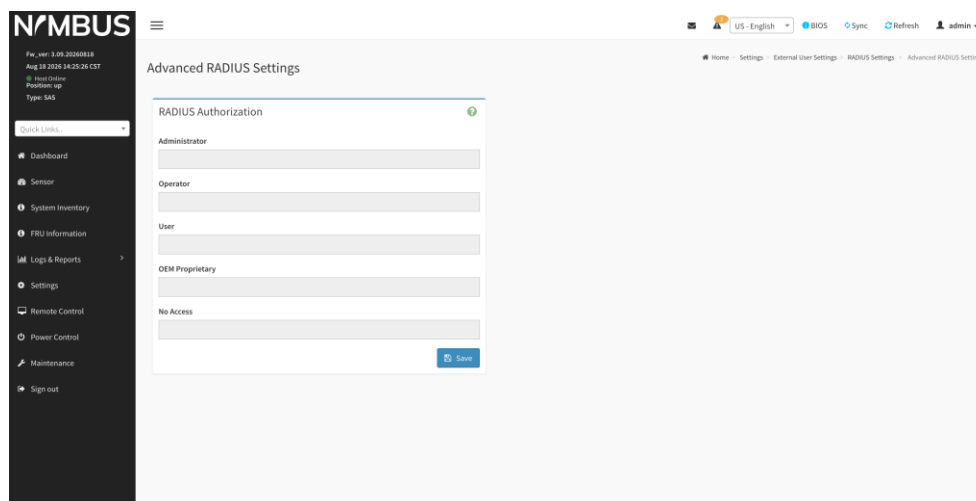
Примечание: порт по умолчанию — 1812; допустимый диапазон — от 1 до 65535.

Secret — общий секрет для аутентификации на сервере RADIUS.

Примечание: от 4 до 31 символа; пробелы не допускаются.

Порядок настройки

1. Установите флажок **Enable RADIUS Authentication**, чтобы включить аутентификацию через RADIUS.
2. Нажмите **Advanced RADIUS Settings**. Откроется окно **Radius Authorization**, показанное ниже.



Для авторизации настройте пользователя RADIUS на стороне сервера с атрибутом Vendor-Specific.

Пример 1:

```
testadmin Auth-Type :=PAP,Cleartext-Password:="admin"  
Auth-Type :=PAP, Vendor-Specific="H=4"
```

Пример 2:

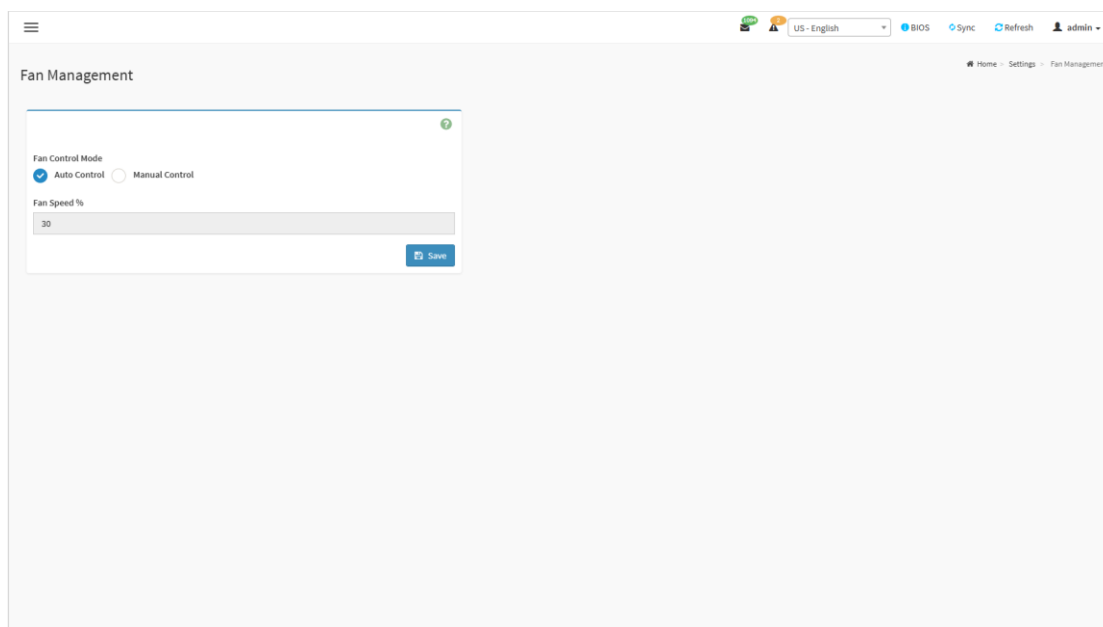
```
testoperator Auth-Type := PAP, Cleartext-Password := "operator"  
Auth-Type :=PAP, Vendor-Specific="H=3"
```

Если значение Vendor-Specific на сервере изменено, укажите такие же значения на этой странице.

3. Нажмите **Save**, чтобы сохранить изменения.

3.7.4 Управление вентиляторами (Fan Management)

Интерфейс **Fan Management** позволяет управлять вентиляторами в реальном времени. Чтобы открыть страницу, выберите в строке меню **Settings > Fan Management**. Пример страницы приведён ниже.

**Порядок настройки**

1. Выберите режим управления вентиляторами (**Fan control mode**).
2. В автоматическом режиме (**Auto mode**) поле **Fan Speed ratio** доступно только для чтения и отображает текущую скорость вращения в процентах.

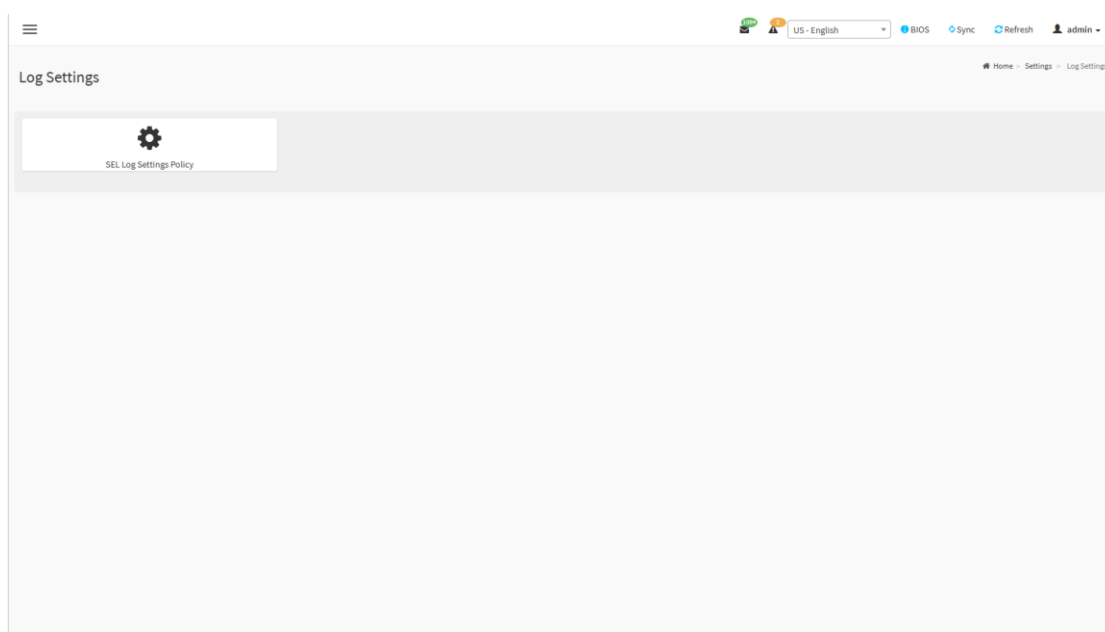
В ручном режиме (**Manual mode**) поле **Fan Speed ratio** обязательно для заполнения: укажите значение от 0 до 100.

Примечание: при питании системы от модуля резервного питания (BBU, Battery Backup Unit) максимальное значение **Fan Speed ratio** ограничивается 40 % для обеспечения сохранности данных.

3.7.5 Настройки журналов (Log Settings)

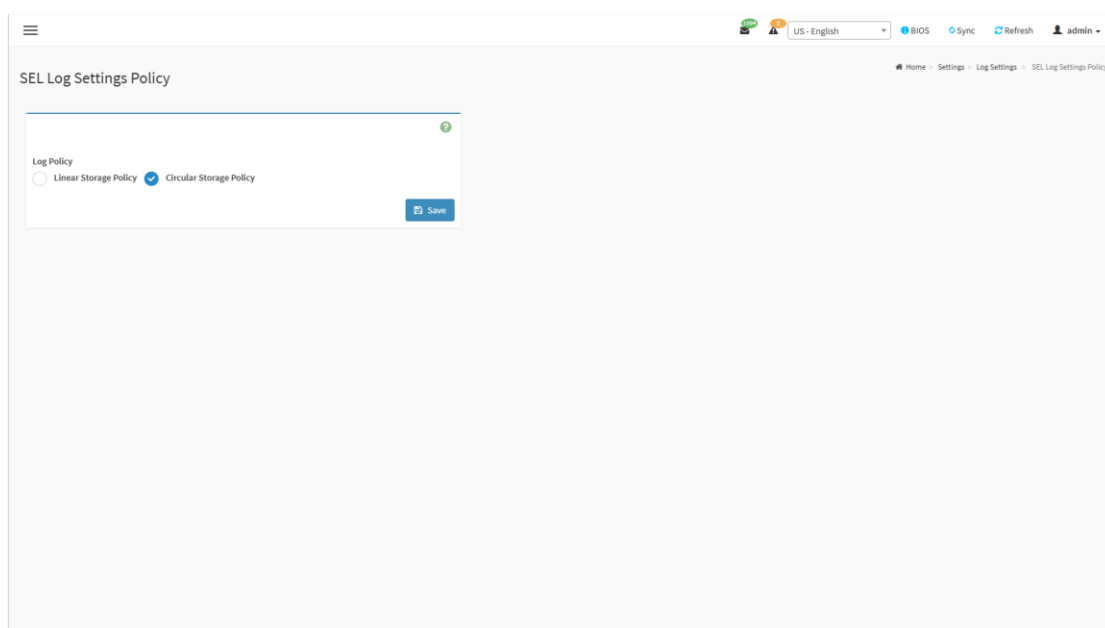
В веб-интерфейсе BMC на страницах системного журнала и журнала аудита отображаются системные события и события аудита устройства.

Чтобы открыть страницу, выберите в строке меню **Settings** > **Log Settings**. Пример страницы приведён ниже.



Политика хранения журнала SEL (SEL Log Setting Policy)

Чтобы открыть страницу, выберите в строке меню **Settings** > **Log Settings** > **SEL Log Settings Policy**. Пример страницы приведён ниже.



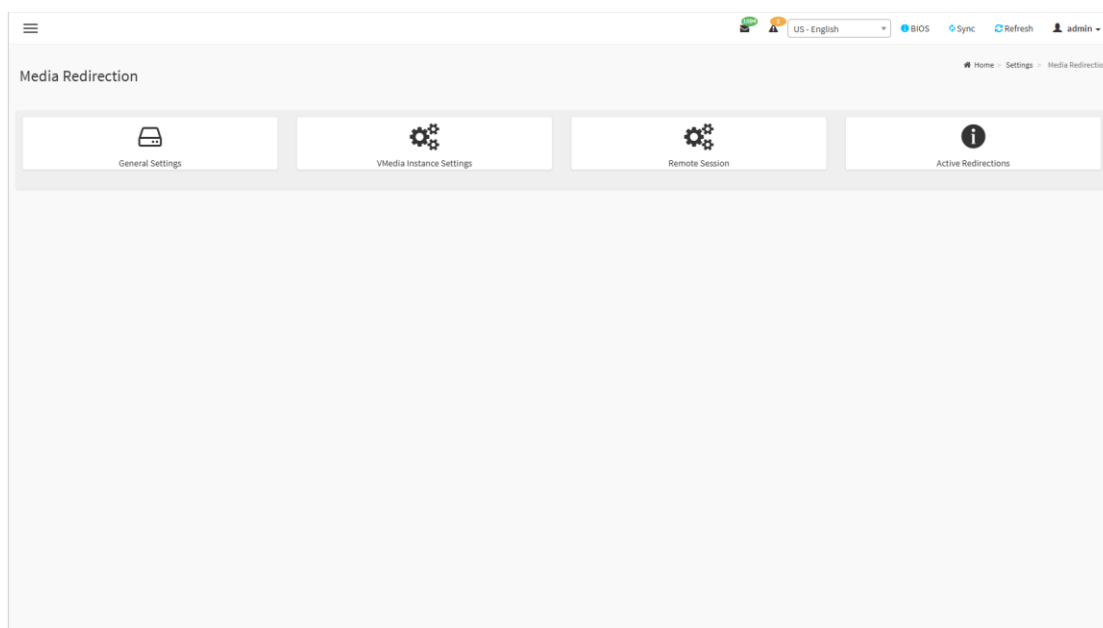
Страница используется для настройки политики хранения журнала событий. Поля страницы:

Log Policy — выбор политики хранения: линейной (**Linear Storage Policy**) или циклической (**Circular Storage Policy**).

Save — сохранение настроек.

3.7.6 Перенаправление носителей (Media Redirection Settings)

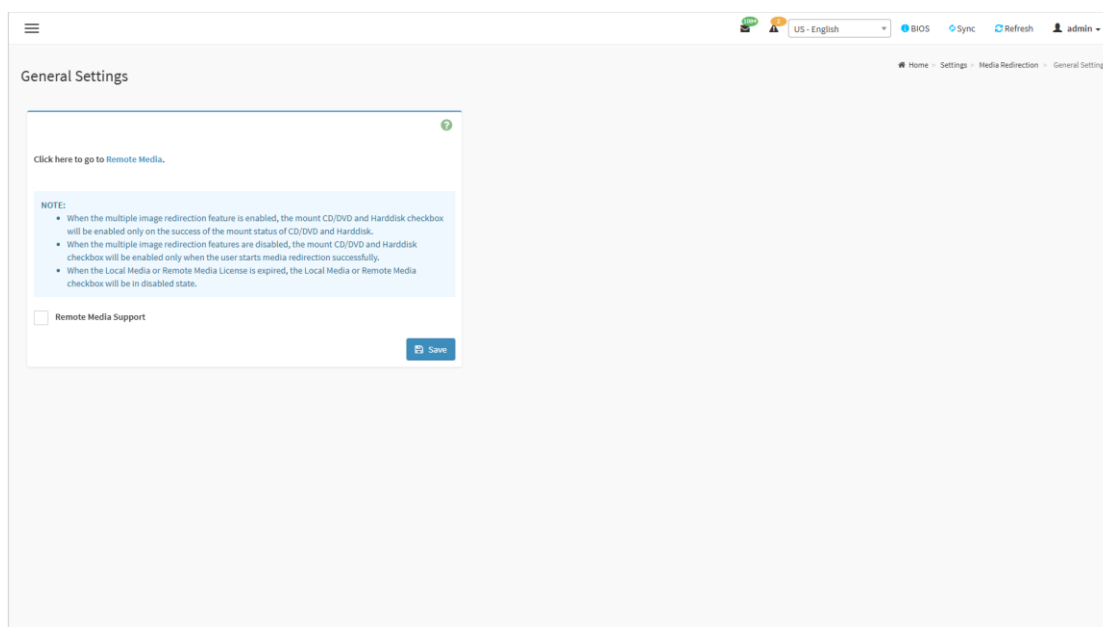
Страница используется для настройки перенаправления носителей через BMC. Чтобы открыть её, выберите в строке меню **Settings** > **Media Redirection Settings**. Пример страницы приведён ниже.



Общие настройки (General Settings)

В разделе настраиваются общие параметры перенаправления носителей.

Чтобы открыть раздел, выберите **Settings** > **Media Redirection Settings** > **General Settings**.

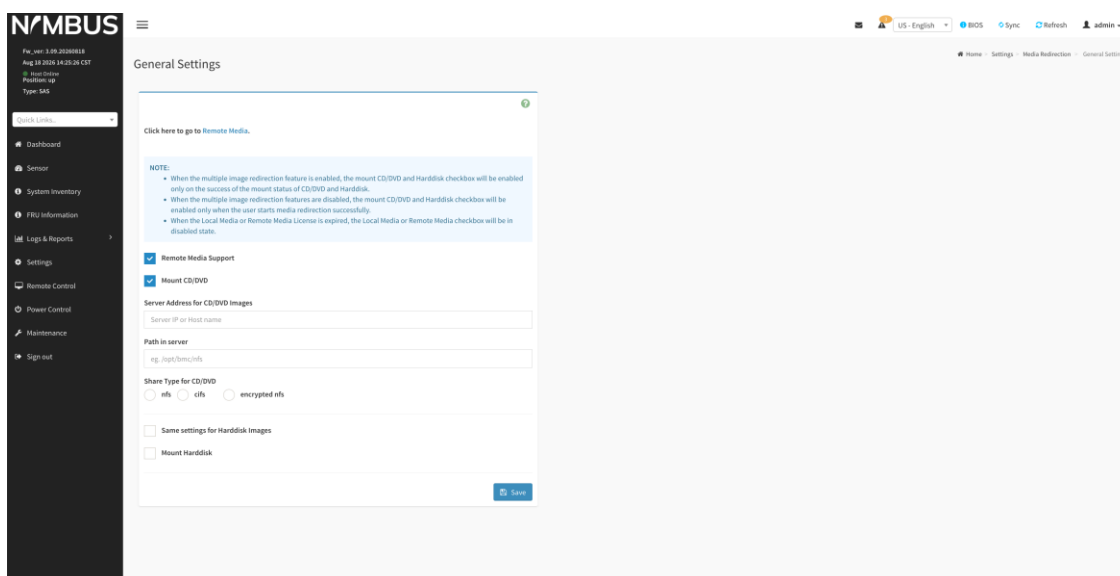


Remote Media Support — чтобы включить или отключить поддержку удалённых носителей, установите или снимите флажок **Enable**.

При включении параметра отображаются следующие типы удалённых носителей:

- Mount CD/DVD — подключение образа CD/DVD
- Mount Harddisk — подключение образа жёсткого диска

При выборе типа носителя отображаются его параметры; для каждого типа удалённого носителя их можно задать отдельно. Пример страницы приведён ниже.



Mount CD/DVD — включение или отключение подключения образов CD/DVD.

Server Address for CD/DVD Images — адрес сервера, на котором хранятся образы удалённых носителей.

Path in server — путь к образам удалённых носителей на сервере.

Примечание: путь может содержать буквы, цифры и только следующие специальные символы: «/» (косая черта), «\» (обратная косая черта), «_» (подчёркивание), «.» (точка) и «:» (двоеточие).

Share Type for CD/DVD — тип общего ресурса для CD/DVD: NFS, CIFS, HTTPS или SMBE.

Domain Name, Username, and Password — если выбран тип общего ресурса Samba (CIFS), HTTPS или SMBE (зашифрованный CIFS), укажите учётные данные для аутентификации на сервере.

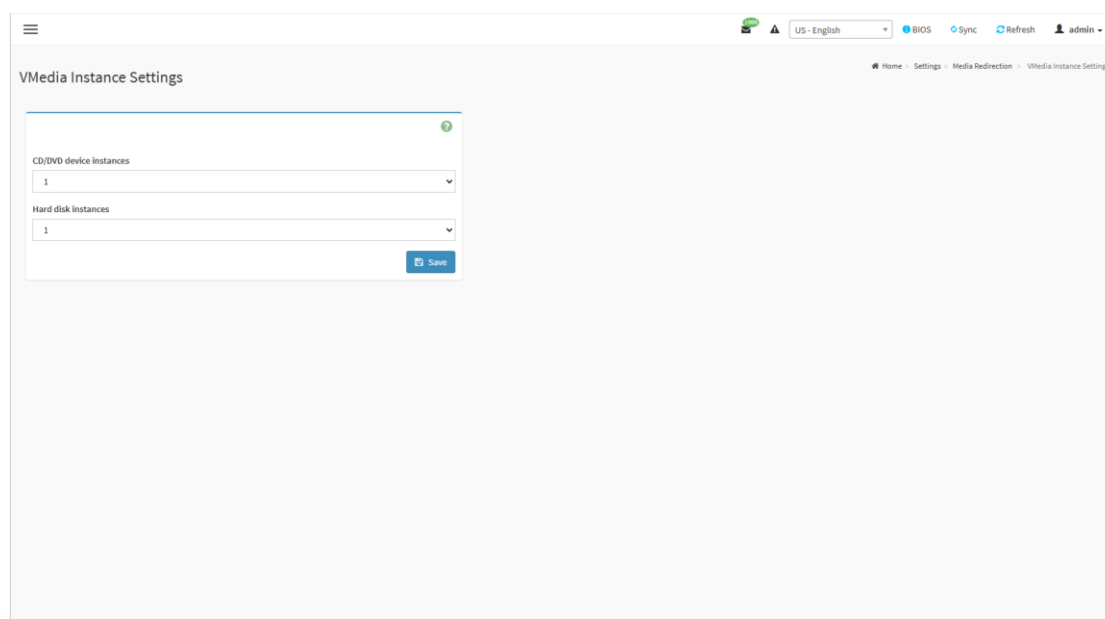
Примечание: для подключения образов с удалённых общих ресурсов к BMC (RMedia) поддерживаются протоколы NFS, CIFS, HTTPS и SMBE следующих версий:

Таблица 2. Поддерживаемые протоколы и версии

Протокол	Версии
NFS	NFSv2, NFSv3, NFSv4
CIFS	SMBv1, SMBv2.1, SMBv3.x

Экземпляры виртуальных носителей (VMedia Instance Settings)

Страница используется для настройки устройств виртуальных носителей. Чтобы открыть её, выберите в строке меню **Settings** > **Media Redirection Settings** > **VMedia Instance Settings**. Пример страницы приведён ниже.



CD/DVD device instances — количество устройств CD/DVD, доступных для перенаправления виртуальных носителей.

Harddisk instances — количество жёстких дисков, доступных для перенаправления виртуальных носителей.

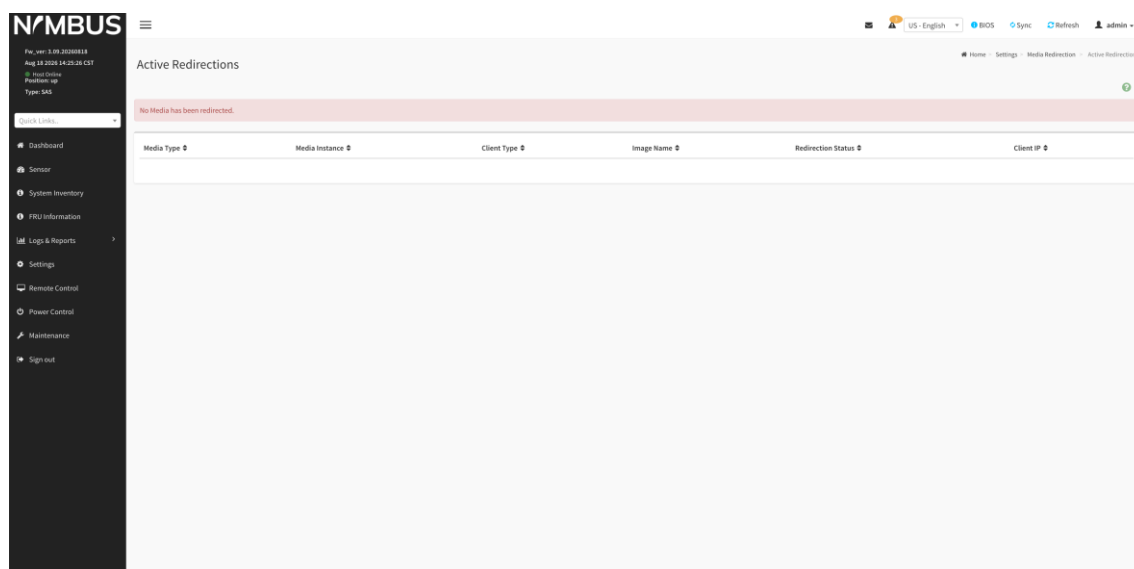
Remote KVM CD/DVD device instances — количество устройств CD/DVD, доступных для перенаправления виртуальных носителей через KVM.

Remote KVM Hard disk instances — количество жёстких дисков, доступных для перенаправления виртуальных носителей через KVM.

Примечание: изменение конфигурации виртуальных носителей приводит к перезапуску всех служб носителей. Поэтому при наличии активного перенаправления носителей изменение конфигурации заблокировано.

Активные перенаправления (Active Redirections)

Страница отображает носители, перенаправленные через JViewer, VMAPP, H5Viewer, LMedia, RMedia или VMCLI: тип и экземпляр носителя, тип клиента, имя образа, состояние перенаправления и IP-адрес клиента. Чтобы открыть страницу, выберите в строке меню **Settings** > **Media Redirection Settings** > **Active Redirections**. Пример страницы приведён ниже.



Media Type — тип носителя (CD/DVD).

Media instances — количество носителей, доступных для активного перенаправления.

Client Type — тип клиента (JViewer, VMAPP, H5Viewer, LMedia, RMedia, VMCLI), через который выполняется перенаправление.

Image Name — имя подключённого образа.

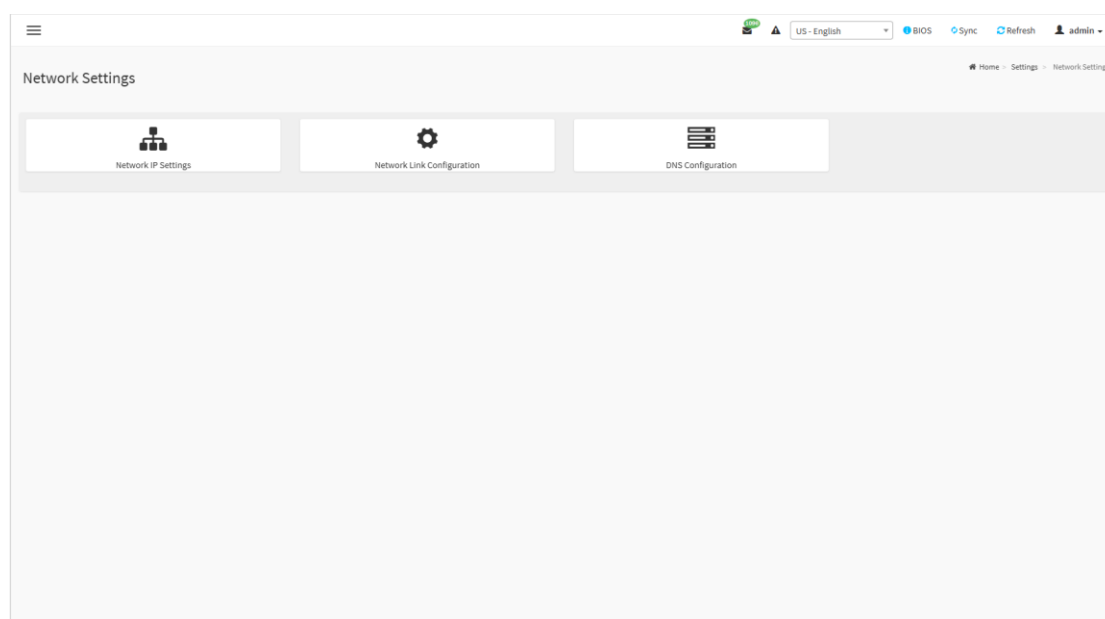
Redirection Status — состояние перенаправления.

Client IP — IP-адрес подключённого клиента.

Примечание: подключение удалённых носителей использует локальный сокет (*loopback*), поэтому для адреса *loopback* (127.0.0.1 или ::1) на странице сведений о сеансе отображается СИМВОЛ «~».

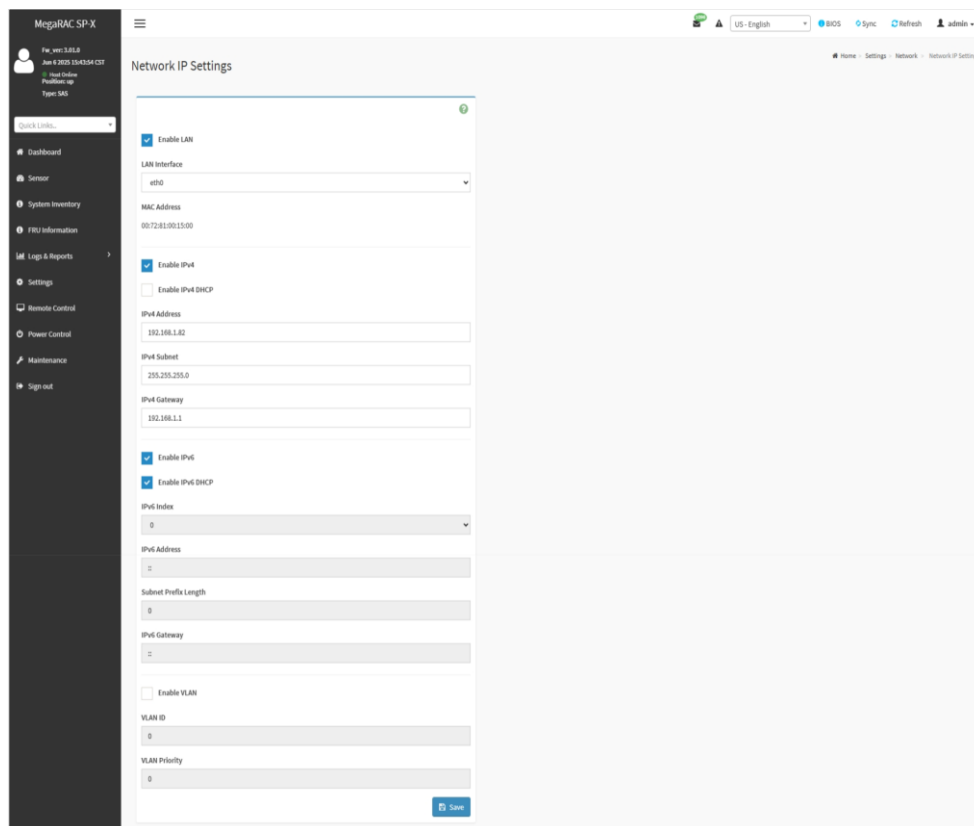
3.7.7 Сетевые настройки (Network Settings)

Страница **Network Settings** используется для настройки параметров сети для доступных каналов LAN.



Настройки IP-адресации (Network IP Settings)

Чтобы открыть страницу, выберите в строке меню **Settings** > **Network Settings** > **Network IP Settings**. Пример страницы приведён ниже.



Enable LAN — включение или отключение настроек LAN.

LAN Interface — список интерфейсов LAN.

MAC Address — MAC-адрес устройства (только для чтения).

Enable IPv4 — включение или отключение IPv4 на устройстве.

Enable IPv4 DHCP — включение получения IPv4-адреса по DHCP для выбранного интерфейса.

IPv4 Address, IPv4 Subnet Mask, IPv4 Default Gateway — статический IPv4-адрес, маска подсети и шлюз по умолчанию для устройства.

Примечание:

- IPv4-адрес состоит из 4 чисел, разделённых точками: «xxx.xxx.xxx.xxx»;
- каждое число — от 0 до 255;
- первое число не может быть равно 0.

Enable IPv6 — включение или отключение IPv6.

Enable IPv6 DHCP — включение или отключение динамического получения IPv6-адреса по протоколу DHCP (Dynamic Host Configuration Protocol).

Примечание: чтобы ввести значения в поля **IPv6 Index**, **IPv6 Address**, **Subnet Prefix length** и **IPv6 Gateway**, отключите параметр **Enable IPv6 DHCP**.

IPv6 Index — индекс статического IPv6-адреса, например 0.

IPv6 Address — статический IPv6-адрес устройства, например 2004::2010.

Subnet Prefix length — длина префикса подсети IPv6.

Примечание: допустимые значения — от 0 до 128.

Default Gateway — шлюз по умолчанию IPv6.

Clear IPv6 Address — очистка IPv6-адреса. Поле отображается, только если для выбранного индекса заданы IPv6-адрес и длина префикса подсети.

Enable VLAN — включение или отключение поддержки VLAN для выбранного интерфейса.

VLAN ID — идентификатор VLAN.

Примечание: допустимые значения — от 2 до 4094.

VLAN Priority — приоритет VLAN.

Примечание: допустимые значения — от 0 до 7; 7 — наивысший приоритет.

Save — сохранение настроек.

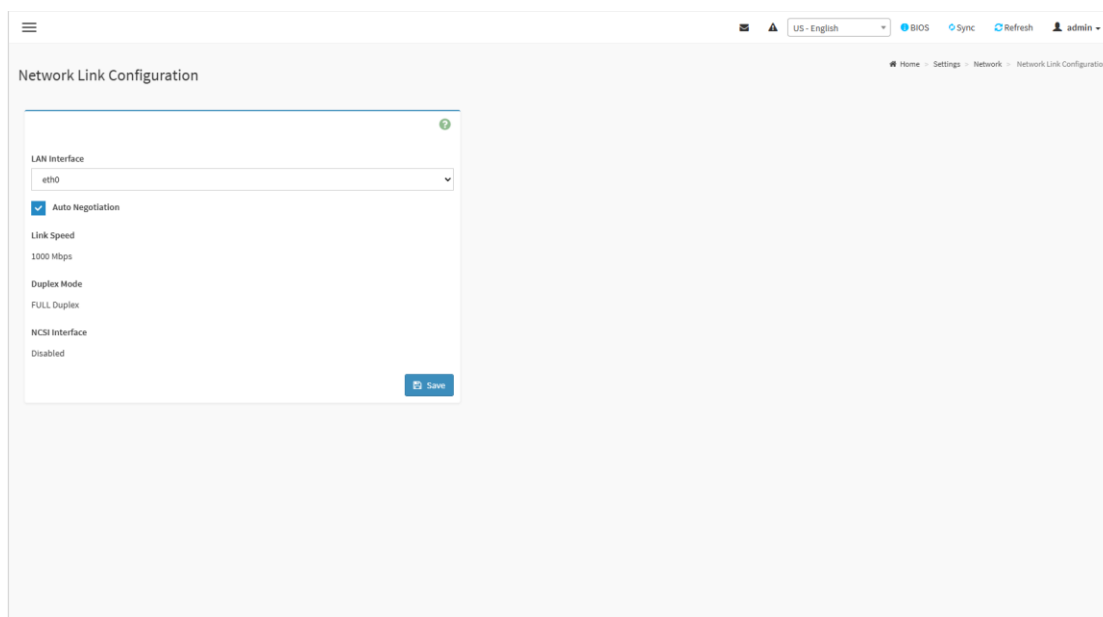
Порядок настройки

1. Установите флажок **Enable LAN**, чтобы включить LAN для выбранного интерфейса.
2. Выберите настраиваемый интерфейс в поле **LAN Interface**.
3. Установите флажок **Enable IPv4**, чтобы включить IPv4 для выбранного интерфейса.
4. Установите флажок **Enable IPv4 DHCP**, чтобы получать IPv4-адрес по DHCP.
5. Если DHCP отключён, введите значения в поля **IPv4 Address**, **IPv4 Subnet Mask** и **IPv4 Default Gateway**.
6. Чтобы включить IPv6, в разделе IPv6 Configuration установите флажок **Enable IPv6**.
7. Если IPv6 включён, включите или отключите параметр **Enable IPv6 DHCP**.
8. Если DHCP для IPv6 отключён, введите значения в поля **IPv6 Address**, **Subnet Prefix length** и **IPv6 Index**.
9. Чтобы включить VLAN, в разделе VLAN Configuration установите флажок **Enable VLAN**.
10. Введите идентификатор в поле **VLAN ID**.
11. Введите приоритет в поле **VLAN Priority**.
12. Нажмите **Save**, чтобы сохранить настройки.

Параметры сетевого соединения (Network Link)

Страница используется для настройки параметров соединения доступных сетевых интерфейсов.

Чтобы открыть страницу, выберите в строке меню **Settings > Network Settings > Network Link**. Пример страницы **Network Link Configuration** приведён ниже.



LAN Interface — сетевой интерфейс, для которого настраиваются скорость соединения и режим дуплекса.

Auto Negotiation — автосогласование: устройство автоматически выбирает оптимальный режим работы соединения (скорость и дуплекс).

Link Speed — скорость соединения из числа поддерживаемых интерфейсом: 10, 100 или 1000 Мбит/с.

Примечание: скорость 1000 Мбит/с недоступна при отключённом автосогласовании.

Duplex Mode — режим дуплекса: полудуплекс (Half Duplex) или полный дуплекс (Full Duplex).

NCSI Interface — состояние интерфейса NCSI для выбранного интерфейса LAN: включён (Enabled) или отключён (Disabled).

Порядок настройки

1. Выберите интерфейс в раскрывающемся списке **LAN Interface**.
2. Для параметра **Auto Negotiation** выберите **Enable** или **Disable**.

Примечание: поля **Link Speed** и **Duplex Mode** доступны, только если автосогласование отключено.

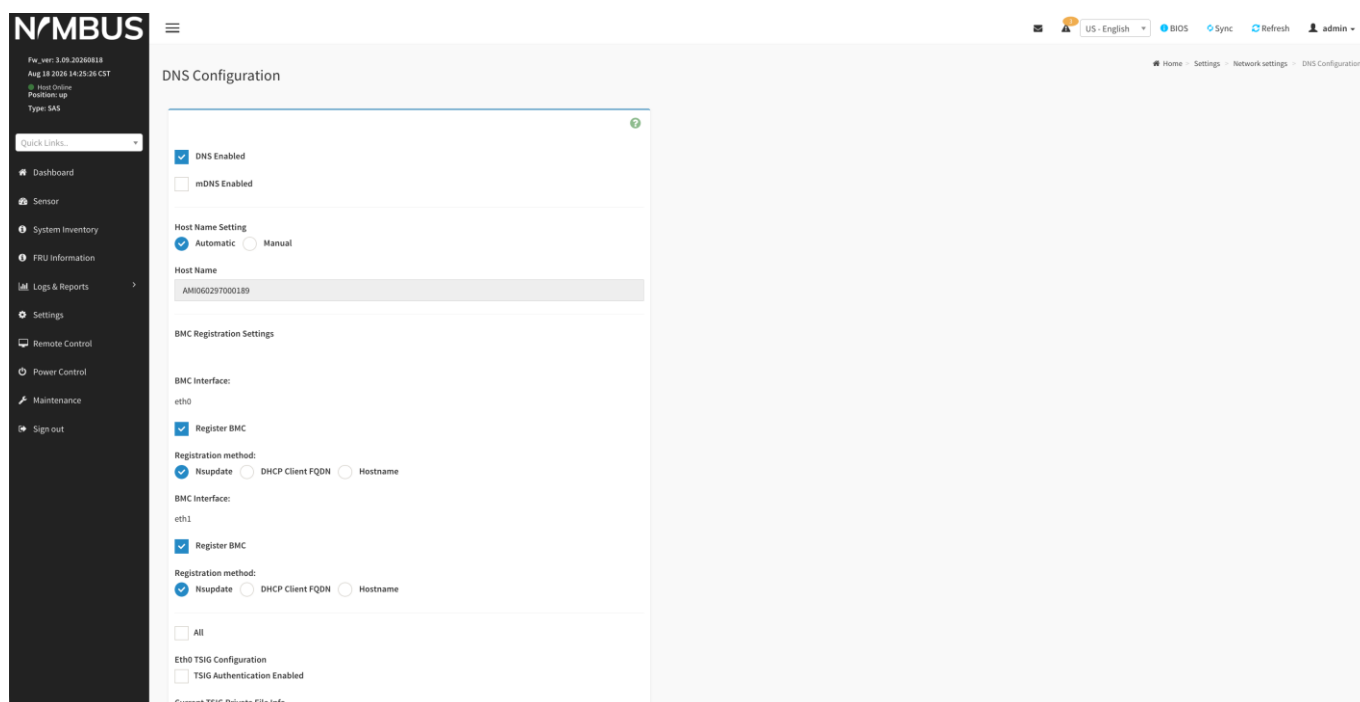
3. Выберите скорость в раскрывающемся списке **Link Speed**.
4. Выберите режим дуплекса в поле **Duplex Mode**: Full duplex или Half duplex.
5. Нажмите **Save**, чтобы сохранить настройки.

Настройка DNS (DNS Configuration)

DNS (Domain Name System) — распределённая иерархическая система имён для компьютеров, служб и других ресурсов, подключённых к интернету или частной сети. Она сопоставляет сведения с доменными именами участников сети и, прежде всего, преобразует понятные человеку доменные имена в числовые идентификаторы сетевого оборудования, необходимые для его обнаружения и адресации.

Страница **DNS Server Settings** используется для управления настройками DNS устройства.

Чтобы открыть страницу, выберите в строке меню **Settings > Network Settings > DNS Configuration**. Пример страницы приведён ниже.



Настройка службы доменных имён (Domain Name Service Configuration)

DNS Enabled — включение или отключение всех настроек службы DNS.

mDNS Enable — включение или отключение поддержки mDNS.

Host Name Settings — способ задания имени хоста: автоматически (Automatic) или вручную (Manual).

Host Name — имя хоста устройства. При выборе ручного режима укажите имя хоста.

Примечание:

- от 1 до 64 буквенно-цифровых символов;
- допускаются дефис (-) и подчёркивание (_);
- имя не может начинаться или заканчиваться дефисом. Браузеры Internet Explorer работают некорректно, если имя хоста содержит символ подчёркивания (_).

Регистрация BMC (BMC Registration Settings)

BMC Interface — интерфейсы, через которые регистрируется BMC (eth0 и eth1).

Register BMC — регистрация BMC выбранным способом.

Способ регистрации (Registration Method)

BMC регистрируется с помощью NS Update, DHCP Client FQDN или Hostname.

Настройка TSIG (TSIG Configuration)

Both — установите флажок, чтобы изменить настройки аутентификации TSIG сразу для обоих интерфейсов.

Eth 0&1:

- **TSIG Authentication Enabled** — включение аутентификации TSIG при регистрации в DNS через nsupdate. Для каждого интерфейса LAN можно загрузить отдельный файл TSIG.

- **Current TSIG Private File** — сведения о текущем закрытом файле TSIG и дата/время его загрузки (только для чтения).
- **New TSIG Private File** — выбор нового закрытого файла TSIG.

Примечание: файл TSIG должен быть закрытого (private) типа.

Domain Setting — способ задания доменного интерфейса: вручную или автоматически.

- **Automatic** — имя домена задаётся автоматически, поле недоступно для ввода.
- **Manual** — укажите имя домена устройства вручную.

Примечание: при выборе Automatic отображается параметр Domain Interface, при выборе Manual — поле Domain name.

- **Domain Name** — имя домена устройства.

Настройка DNS-серверов (Domain Name Server Setting)

Automatic — при выборе автоматического режима укажите интерфейс в поле DNS Interface.

Manual — укажите адреса DNS-серверов для BMC вручную.

IP Priority:

- при приоритете **IPv4** используются 2 DNS-сервера IPv4 и 1 DNS-сервер IPv6;
- при приоритете **IPv6** используются 2 DNS-сервера IPv6 и 1 DNS-сервер IPv4.

Примечание: не применяется при ручной настройке.

DNS Server 1, 2 & 3

Адреса DNS-серверов, используемых BMC.

Примечание:

- адреса IPv4 указываются в десятичном формате с точками;
- поддерживаются адреса IPv6; они должны быть глобальными одноадресными (global unicast).

Поддерживаются адреса DNS-серверов в форматах IPv4 и IPv6.

Save — сохранение изменений.

Порядок настройки

1. В разделе **Domain Name Service Configuration** включите службу DNS: установите флажок **DNS Enabled**, чтобы включить все настройки службы DNS.
2. Выберите способ задания имени хоста в поле **Host Name Setting**: Automatic или Manual.

Примечание: при выборе Automatic имя хоста вводить не нужно, при выборе Manual — необходимо.

3. При ручной настройке введите имя в поле **Host Name**.
4. В разделе **Register BMC** выберите сетевой порт BMC для регистрации в DNS:
 - установите флажок **Register BMC**, чтобы зарегистрировать BMC в DNS;
 - **Nsupdate** — регистрация на DNS-сервере с помощью утилиты nsupdate;
 - **DHCP Client FQDN** — регистрация на DNS-сервере с помощью опции DHCP 81;
 - **Hostname** — регистрация на DNS-сервере с помощью опции DHCP 12.

Примечание: выбирайте Hostname, если сервер DHCP не поддерживает опцию DHCP Client FQDN.

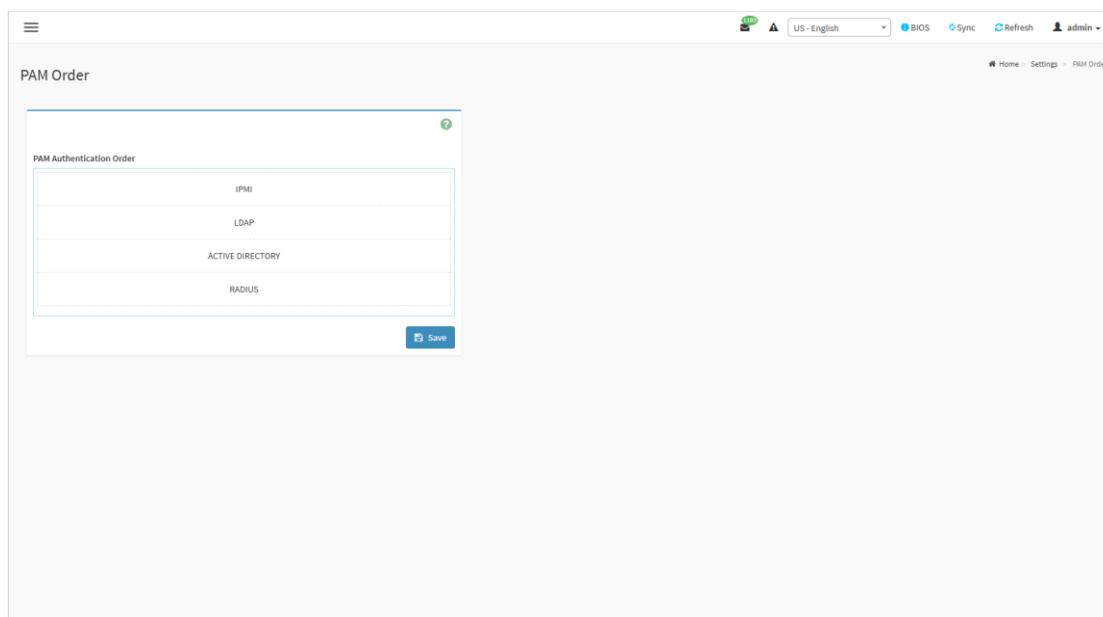
5. Установите флажок **Both**, чтобы изменить настройки аутентификации TSIG для обоих интерфейсов (eth0 и eth1).

6. В разделе **Eth 0&1 TSIG Configuration** установите или снимите флажок **TSIG Authentication Enabled**, чтобы включить или отключить аутентификацию TSIG при регистрации в DNS через nsupdate:
 - имя текущего файла отображается в поле **Current TSIG Private file**;
 - чтобы загрузить новый файл, нажмите **New TSIG private file** и выберите закрытый файл TSIG.
7. В разделе **Domain Settings**:
 - выберите способ задания домена (Automatic или Manual);
 - при выборе Manual введите имя домена в соответствующее поле.
8. В разделе **Domain Name Server Setting**:
 - выберите способ задания DNS-серверов (**DNS Name Server Setting**);
 - выберите приоритет IP: IPv4 или IPv6;
 - введите адреса DNS-серверов.
9. В полях **DNS Server1**, **DNS Server2** и **DNS Server3** укажите адреса серверов для BMC.
10. Нажмите **Save**, чтобы сохранить настройки.

3.7.8 Порядок модулей PAM (PAM Order Settings)

Страница используется для настройки порядка модулей PAM при аутентификации пользователей в BMC.

Чтобы открыть страницу, выберите в строке меню **Settings > PAM Order Settings**. Пример страницы приведён ниже.



PAM Module — список модулей PAM, поддерживаемых BMC.

Примечание:

- не рекомендуется использовать одинаковые имена пользователей в разных модулях PAM;
- аутентификация может завершиться ошибкой из-за неверного имени пользователя или неверного пароля;
- при ошибке аутентификации RADIUS невозможно определить, что именно неверно — имя пользователя или пароль. Поэтому такая ошибка всегда расценивается как «Неверное имя пользователя», и PAM переходит к другим методам аутентификации;

- по той же причине RADIUS должен стоять последним в порядке PAM. В противном случае для пользователей, вошедших через другие службы аутентификации, будет отображаться идентификатор пользователя RADIUS;
- если для AD не заданы служебные имя пользователя и пароль, любая неудачная аутентификация расценивается как ошибка «Неверный пароль», и PAM не переходит к другим методам. Поэтому при включённой аутентификации RADIUS рекомендуется ставить AD перед RADIUS, а при отключённой — последним в порядке PAM.

Порядок настройки

1. Выберите нужный модуль PAM и перетащите его вверх или вниз, чтобы изменить порядок.
2. Нажмите **Save**, чтобы сохранить изменения.

Примечание: после любого изменения настроек веб-сервер автоматически перезапускается, а текущий сеанс завершается.

3.7.9 Настройки SMTP (SMTP Settings)

SMTP (Simple Mail Transfer Protocol) — стандартный протокол передачи электронной почты в IP-сетях.

В веб-интерфейсе BMC можно настроить параметры SMTP устройства.

Чтобы открыть страницу, выберите в строке меню **Settings > SMTP Settings**. Пример страницы приведён ниже.

The screenshot shows the 'SMTP Settings' page in the NIMBUS web interface. On the left is a dark sidebar with navigation links: Dashboard, Sensor, System Inventory, FRU Information, Logs & Reports, Settings, Remote Control, Power Control, Maintenance, and Sign out. The main content area has a top header with 'NIMBUS' and a hamburger menu icon. Below this, the 'SMTP Settings' title is followed by a green status icon. The settings are organized into a form with the following fields: 'LAN Interface' (dropdown menu showing 'eth0'), 'Sender Email ID' (text input), 'Primary SMTP Support' (checkbox, checked), 'Primary Server Name' (text input), 'Primary Server IP' (text input), 'Primary SMTP port' (text input with '25' entered), 'Primary Secure SMTP port' (text input with '465' entered), 'Primary SMTP Authentication' (checkbox, unchecked), 'Primary Username' (text input), 'Primary Password' (text input), 'Primary SMTP SSL/TLS Enable' (checkbox, unchecked), 'Primary SMTP STARTTLS Enable' (checkbox, unchecked), and 'Secondary SMTP Support' (checkbox, unchecked). A blue 'Save' button is located at the bottom right of the form.

LAN Interface — список доступных каналов LAN.

Sender Email ID — действительный адрес отправителя, от имени которого BMC отправляет письма.

Primary Server Name — имя компьютера (Machine Name) BMC, с которого отправляются письма.

Примечание: имя компьютера — строка длиной до 15 буквенно-цифровых символов; пробелы и специальные символы не допускаются.

Primary SMTP Support — включение или отключение поддержки SMTP для BMC.

Primary SMTP Port — обычный порт SMTP.

Primary Secure SMTP Port — защищённый порт SMTP.

Примечание: порт **Primary SMTP Port** по умолчанию — 25, порт **Primary Secure SMTP Port** по умолчанию — 465; допустимый диапазон — от 1 до 65535.

Primary Server IP — IP-адрес сервера SMTP (обязательное поле).

Примечание:

- IPv4-адрес состоит из 4 чисел, разделённых точками: «xxx.xxx.xxx.xxx»;
- каждое число — от 0 до 255;
- первое число не может быть равно 0;
- поддерживаются адреса в форматах IPv4 и IPv6.

Primary SMTP Authentication — включение или отключение аутентификации SMTP.

Примечание: поддерживаются типы аутентификации CRAM-MD5, LOGIN и PLAIN. Если сервер SMTP не поддерживает ни один из них, выводится сообщение об ошибке «Authentication type is not supported by SMTP Server».

Primary Username — имя пользователя учётной записи SMTP.

Примечание: от 4 до 64 символов: буквы, цифры, точка (.), дефис (-) и подчёркивание (_); имя должно начинаться с буквы; другие специальные символы не допускаются.

Primary Password — пароль учётной записи SMTP.

Примечание: от 4 до 64 символов; пробелы не допускаются.

Primary SMTP STARTTLS Enable — включение поддержки STARTTLS для клиента SMTP:

- **Upload SMTP CA Certificate File** — файл сертификата доверенного удостоверяющего центра (CA) в формате PEM;
- **Upload SMTP Certificate File** — файл сертификата клиента в формате PEM;
- **Upload SMTP Private Key** — файл закрытого ключа клиента в формате PEM.

Примечание: для включения STARTTLS должна быть включена соответствующая поддержка SMTP.

Secondary SMTP Support — настройки резервного сервера SMTP (необязательно). Резервный сервер используется, если основной сервер SMTP недоступен или работает некорректно.

Примечание: параметры резервного сервера аналогичны параметрам основного (Primary SMTP Support).

Save — сохранение новой конфигурации сервера SMTP.

Порядок настройки

1. Выберите интерфейс в раскрывающемся списке **LAN Interface**.
2. Введите адрес отправителя в поле **Sender Email ID**.
3. Установите флажок **Primary SMTP Support**, чтобы включить поддержку SMTP для BMC.
4. Введите имя компьютера сервера SMTP в поле **Primary Server Name**.
Примечание: имя компьютера — строка длиной до 15 буквенно-цифровых символов; пробелы и специальные символы не допускаются.
5. Введите IP-адрес сервера SMTP в поле **Primary Server IP** (обязательное поле).
6. Введите номер порта в поле **Primary SMTP Port**.
7. Введите номер защищённого порта в поле **Primary Secure SMTP Port**.

8. Установите флажок **Primary SMTP Authentication**, если сервер SMTP требует аутентификации.
9. Введите имя пользователя и пароль в поля **Primary User name** и **Primary Password**.
10. Установите флажок **Primary SMTP SSLTLS Enable**, чтобы передавать данные через защищённый порт.
Примечание: при выборе этого параметра параметр **STARTTLS** и обычный порт скрываются.
11. Установите флажок **Secondary SMTP Support**, чтобы включить резервный сервер SMTP для BMC.
12. Введите значения в поля **Secondary Server Name**, **Secondary Server IP**, **Secondary SMTP Port** и **Secure Port**.
13. Установите флажок **SMTP Server Authentication**, если резервный сервер SMTP требует аутентификации.
14. Введите имя пользователя и пароль в поля **Secondary User name** и **Password**.
15. Установите флажок **Secondary SMTP SSLTLS**, чтобы передавать данные через защищённый порт.
Примечание: при выборе этого параметра параметр **STARTTLS** и обычный порт скрываются.
16. Нажмите **Save**, чтобы сохранить настройки.

3.7.10 Настройки SSL (SSL Settings)

Протокол SSL (Secure Socket Layer) разработан компанией Netscape для защиты обмена данными между веб-серверами и браузерами. Для подтверждения подлинности одной или обеих сторон протокол использует третью сторону — удостоверяющий центр (CA, Certificate Authority).

В веб-интерфейсе BMC можно установить в BMC сертификат SSL, чтобы обращаться к устройству в защищённом режиме.

Чтобы открыть страницу **SSL Certificate Configuration**, выберите в строке меню **Settings > SSL Settings**. Страница содержит три вкладки:

- **Upload SSL Certificate** — загрузка сертификата и файла закрытого ключа в BMC;
- **Generate SSL Certificate** — формирование сертификата SSL по заданным параметрам;
- **View SSL Certificate** — просмотр загруженного сертификата SSL в удобочитаемом виде.

Загрузка сертификата SSL (Upload SSL Certificate)

Пример страницы приведён ниже.

Upload SSL Certificate

Current Certificate
Sat Jan 1 05:00:32 2022

New Certificate

Current Private Key
Sat Jan 1 05:00:31 2022

New Private Key

☒ Trusted CA Support

Current trusted CA certificate
Sat Jan 1 05:00:32 2022

Trusted CA Certificates

Save

Current Certificate — текущий сертификат и дата/время его загрузки (только для чтения).

New Certificate — файл нового сертификата в формате PEM.

Current Private Key — сведения о текущем закрытом ключе (только для чтения).

New Private Key — файл нового закрытого ключа в формате PEM.

Trusted CA Certificates — сертификаты доверенных удостоверяющих центров в формате PEM.

Примечание: после успешной загрузки служба HTTPS перезапускается, чтобы начать использовать новый сертификат SSL.

Формирование сертификата SSL (Generate SSL Certificate)

Generate SSL Certificate

Common Name (CN)

Organization (O)

Organization Unit (OU)

City or Locality (L)

State or Province (ST)

Country (C)

Email Address

Valid for
in days

Key Length
2048 bits

Save

Common Name (CN) — общее имя, для которого формируется сертификат: до 64 буквенно-цифровых символов, символы «#» и «\$» не допускаются.

Organization (O) — наименование организации: до 64 буквенно-цифровых символов, символы «#» и «\$» не допускаются.

Organization Unit (OU) — наименование подразделения организации: до 64 буквенно-цифровых символов, символы «#» и «\$» не допускаются.

City or Locality (L) — город или населённый пункт организации (обязательное поле): до 128 буквенно-цифровых символов, символы «#» и «\$» не допускаются.

State or Province (ST) — регион организации (обязательное поле): до 64 буквенно-цифровых символов, символы «#» и «\$» не допускаются.

Country (C) — код страны организации (обязательное поле): ровно два символа, специальные символы не допускаются.

Email Address — адрес электронной почты организации (обязательное поле).

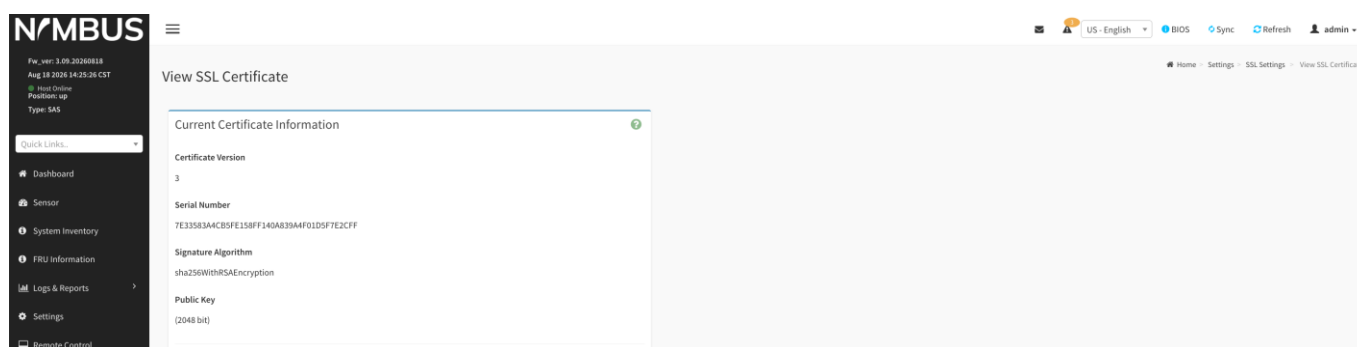
Valid for — срок действия сертификата: от 1 до 3650 дней.

Key Length — длина ключа сертификата в битах.

Save — формирование нового сертификата SSL.

Примечание: после формирования служба HTTPS перезапускается, чтобы начать использовать новый сертификат SSL.

Просмотр сертификата SSL (View SSL Certificate)



Basic Information — основные сведения о загруженном сертификате SSL. Отображаются следующие поля:

- Version Serial Number — версия и серийный номер
- Signature Algorithm — алгоритм подписи
- Public Key — открытый ключ
- Issuer Common Name (CN) — общее имя издателя
- Issuer Organization (O) — организация издателя
- Issuer Organization Unit (OU) — подразделение издателя
- Issuer City or Locality (L) — город издателя
- Issuer State or Province (ST) — регион издателя
- Issuer Country (C) — страна издателя
- Issuer E-mail Address — адрес электронной почты издателя
- Valid From — действителен с
- Valid Till — действителен до

Порядок настройки

1. На вкладке **Upload SSL Certificate** нажмите **Browse** и выберите новый сертификат (**New Certificate**) и новый закрытый ключ (**New Private key**).

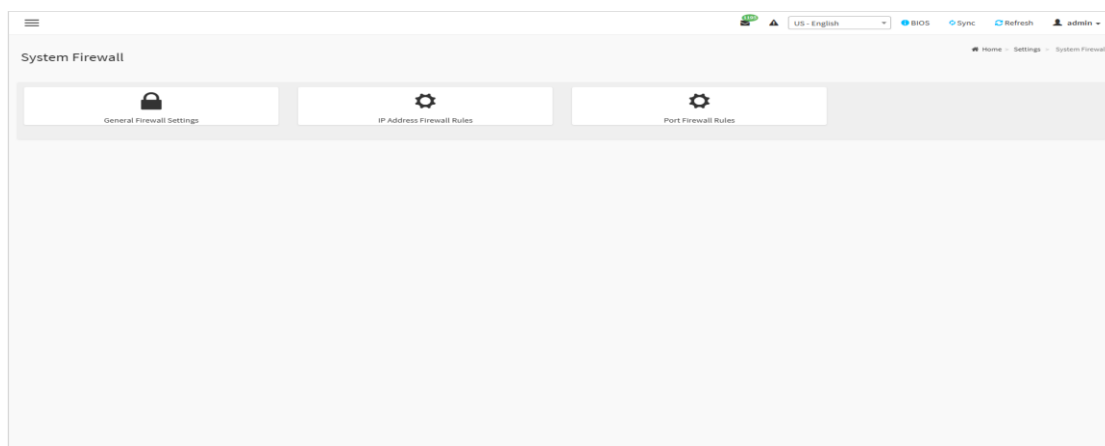
2. Нажмите **Upload**, чтобы загрузить новый сертификат и закрытый ключ.
3. На вкладке **Generate SSL Certificate** заполните поля:
 - общее имя, для которого формируется сертификат;
 - наименование организации;
 - наименование подразделения;
 - город или населённый пункт организации;
 - регион организации;
 - страна организации;
 - адрес электронной почты организации;
 - срок действия сертификата в днях (поле **Valid For**).
4. Выберите длину ключа сертификата (**Key Length**).
5. Нажмите **Save**, чтобы сформировать сертификат.
6. Откройте вкладку **View SSL Certificate**, чтобы просмотреть загруженный сертификат в удобочитаемом виде.

Примечание: после загрузки или формирования сертификата перезапускается только служба HTTPS.

3.7.11 Межсетевой экран (System Firewall)

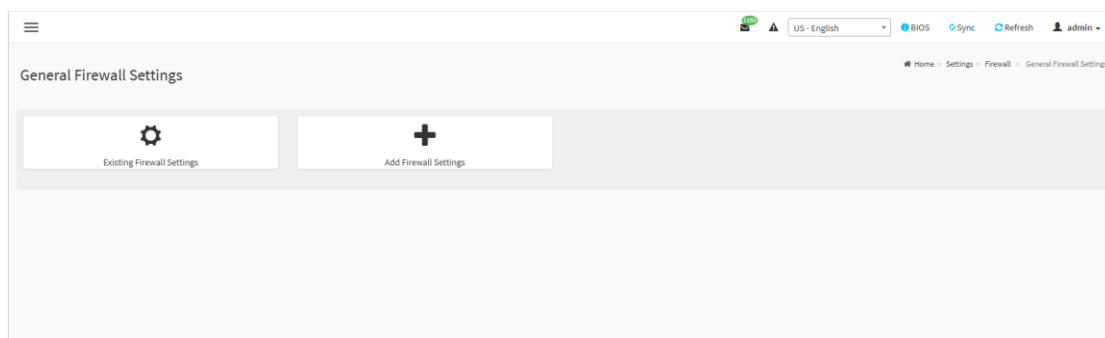
Страница **System Firewall** веб-интерфейса BMC используется для настройки межсетевого экрана. Правила можно задавать для отдельного IP-адреса, диапазона IP-адресов или номеров портов. Для просмотра страницы требуются права не ниже оператора (Operator); добавлять и удалять правила могут только администраторы.

Чтобы открыть страницу, выберите в строке меню **Settings > System Firewall**.



Общие настройки межсетевого экрана (General Firewall Settings)

Откройте страницу **General Firewall Settings**. Пример страницы приведён ниже.

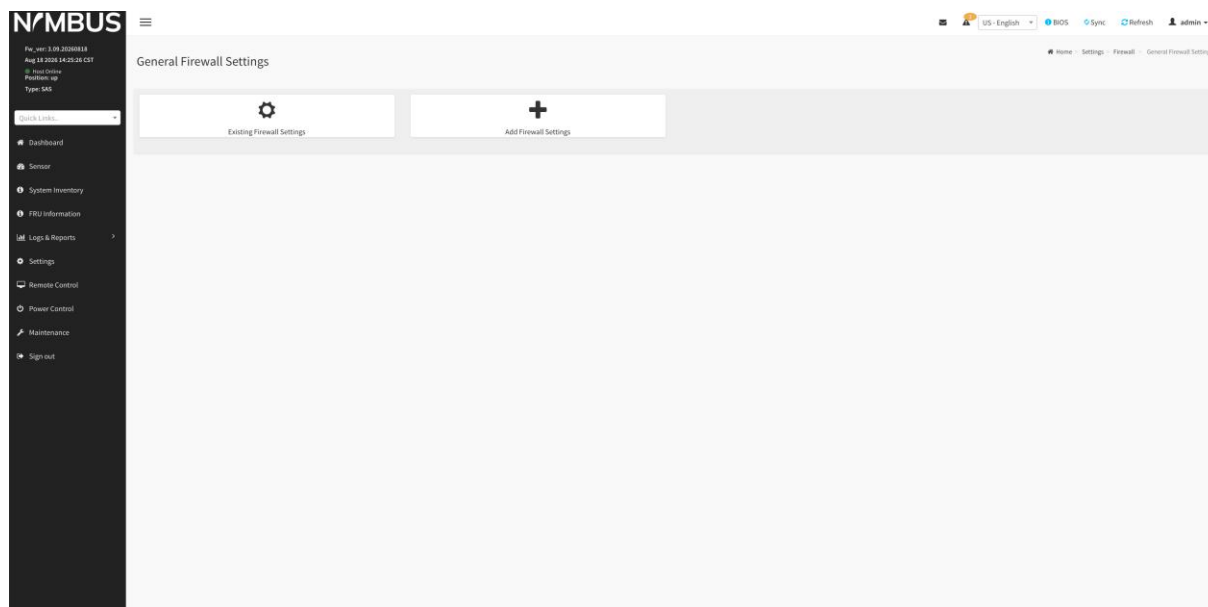


Существующие настройки (Existing Firewall Settings)

Если настройки в разделе **Add Firewall Settings** ещё не добавлялись, откроется пустая страница. В этом случае добавьте настройки по ссылке **Add Firewall Settings**.

Просмотр существующих настроек

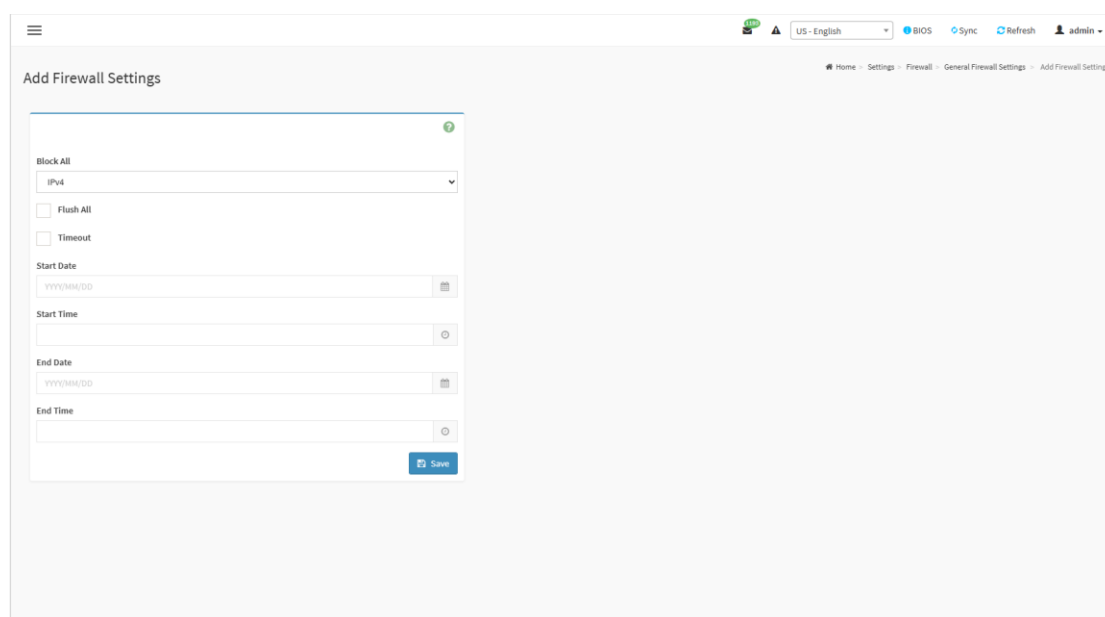
1. Выберите **General Firewall Settings > Existing Firewall Settings**. Пример страницы приведён ниже.



- **Block All** — просмотр заблокированных входящих IP-адресов и портов.
- **Flush All** — сброс всех правил межсетевого экрана (только для чтения).
- **Timeout** — включение или отключение ограничения правил по времени.
- **Time Out** — отображение даты и времени начала и окончания действия правила.
- **Delete** — удаление правил межсетевого экрана.

Добавление настроек межсетевого экрана

1. Выберите **General Firewall Settings > Add Firewall Settings**. Откроется страница, показанная ниже.



2. Выберите **Block All**, чтобы заблокировать все входящие IP-адреса и порты.
3. Выберите **Flush All**, чтобы сбросить все правила межсетевого экрана.
4. Выберите **Timeout**, чтобы включить или отключить ограничение правил по времени.
5. В поле **Start Time** укажите время начала действия правила.
6. В поле **End Time** укажите время окончания действия правила.

Примечание: время указывается в формате *dd-mm-yy:hh-mm*.

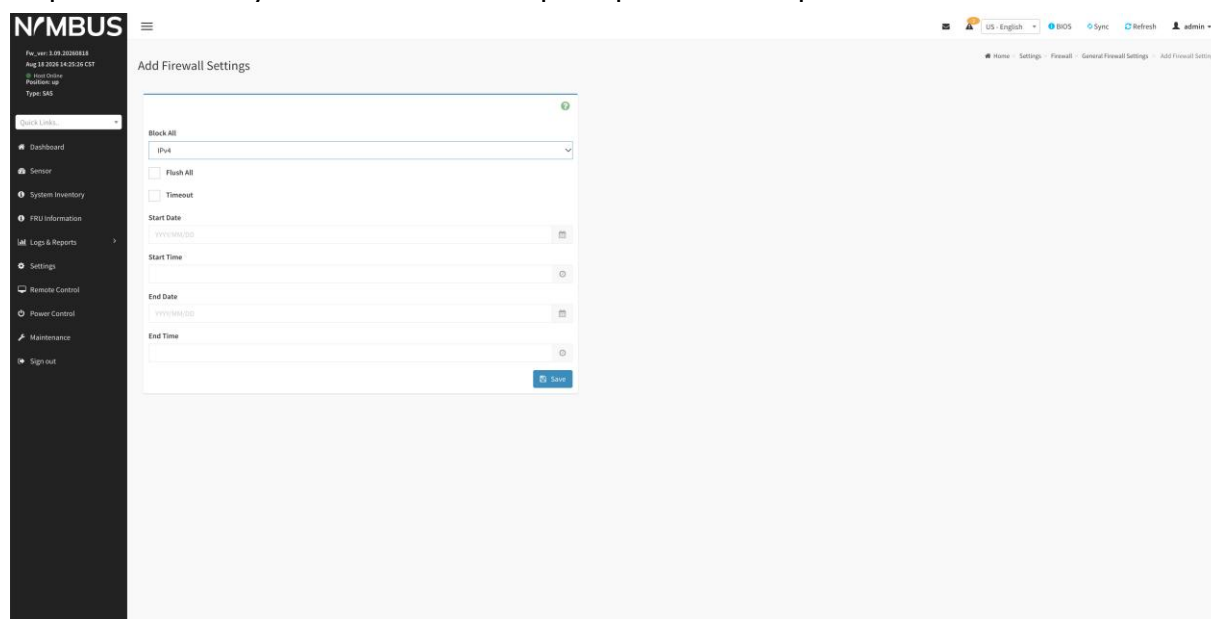
7. Нажмите **Save**, чтобы сохранить изменения, или **Cancel**, чтобы вернуться на предыдущую страницу.

Правила для IP-адресов (IP Address Firewall Rules)

Если правила в разделе **Add IP Rule** ещё не добавлялись, при просмотре существующих правил для IP-адресов и диапазонов откроется пустая страница. В этом случае добавьте правило по ссылке **Add IP Rule**.

Просмотр правил для IP-адресов

1. Выберите **Settings > System Firewall > IP Address Firewall Rules > Existing IP Rules**. Если правила не добавлялись, откроется пустая страница; добавленные правила отображаются на странице **Existing IP Rules**.
2. Откройте вкладку **IP Addresses**. Пример вкладки приведён ниже.



IP Single (or) Range Start — IP-адрес или начало диапазона IP-адресов.

IP Range End — конец диапазона IP-адресов.

Enable Timeout — включение или отключение ограничения по времени.

Start Date — дата начала действия правила.

Start Time — время начала действия правила.

End Date — дата окончания действия правила.

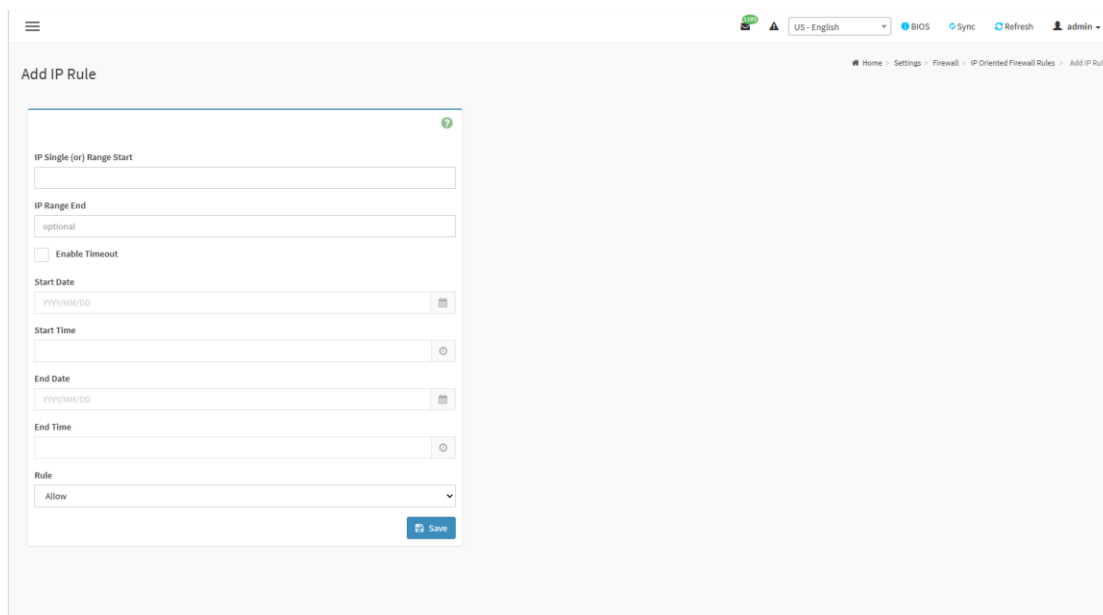
End Time — время окончания действия правила.

Rule — действие правила: разрешить (Allow) или заблокировать (Block).

Delete — удаление выбранной записи.

Добавление IP-адреса или диапазона IP-адресов

1. Выберите **Settings > System Firewall > IP Address Firewall Rules > Add New IP Rule**, чтобы добавить IP-адрес или диапазон IP-адресов.



2. На странице **Add new rule** введите IP-адрес или начало диапазона в поле **IP Single or IP Range Start**.

Примечание:

- поддерживаются только адреса IPv4;
- IPv4-адрес состоит из 4 чисел, разделённых точками: xxx.xxx.xxx.xxx;
- каждое число — от 0 до 255;
- первое число не может быть равно 0;
- IPv6-адрес состоит из 8 групп по 4 шестнадцатеричные цифры, разделённых двоеточиями: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx.

3. Введите конец диапазона в поле **IP Range End**.
4. Включите **Timeout**, чтобы ограничить действие правила по времени.
5. В поле **Start Date** укажите дату начала действия правила.
6. В поле **End Date** укажите дату окончания действия правила.
7. В поле **Start Time** укажите время начала действия правила.
8. В поле **End Time** укажите время окончания действия правила.

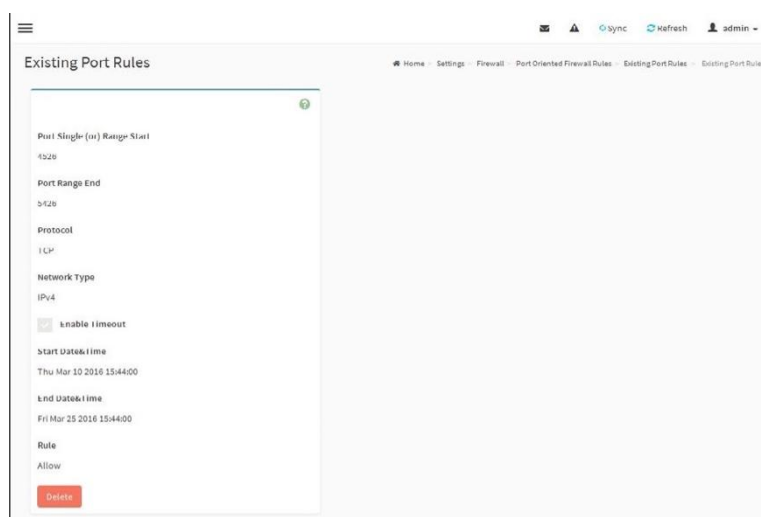
Примечание: дата указывается в формате YYYY/MM/DD, время — в формате hh-mm.

9. Выберите действие правила: заблокировать или разрешить.
10. Нажмите **Save**, чтобы сохранить изменения.

Правила для портов (Port Firewall Rules)

Просмотр правил для портов

1. Выберите **Settings > System Firewall > Port Firewall Rules > Existing Port Rules**. Если правила в разделе **Add New port Rule** не добавлялись, откроется пустая страница; добавленные правила отображаются на странице **Existing Port Rules**.
2. Откройте **Existing Port Rules**. Пример вкладки приведён ниже.



Port Single (or) Range Start — порт или начало диапазона портов.

Port Range End — конец диапазона портов.

Protocol — протокол для порта или диапазона портов.

Network Type — тип сети, на который распространяется правило для порта или диапазона портов.

Enable Timeout — включение или отключение ограничения правила по времени.

Start Date — дата начала действия правила.

Start Time — время начала действия правила.

End Date — дата окончания действия правила.

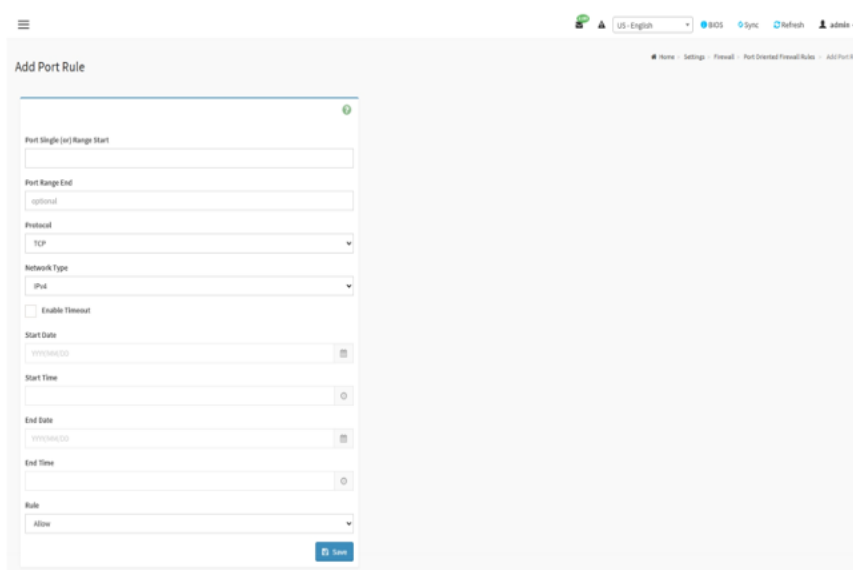
End Time — время окончания действия правила.

Rule — действие правила: разрешить (Allow) или заблокировать (Block).

Delete — удаление записи из списка правил.

Добавление порта или диапазона портов

1. Нажмите **Add**, чтобы добавить новый порт или диапазон портов.



- В окне **Add new rule for Port** введите номер порта или начало диапазона в поле **Port Single (or) Range Start**.

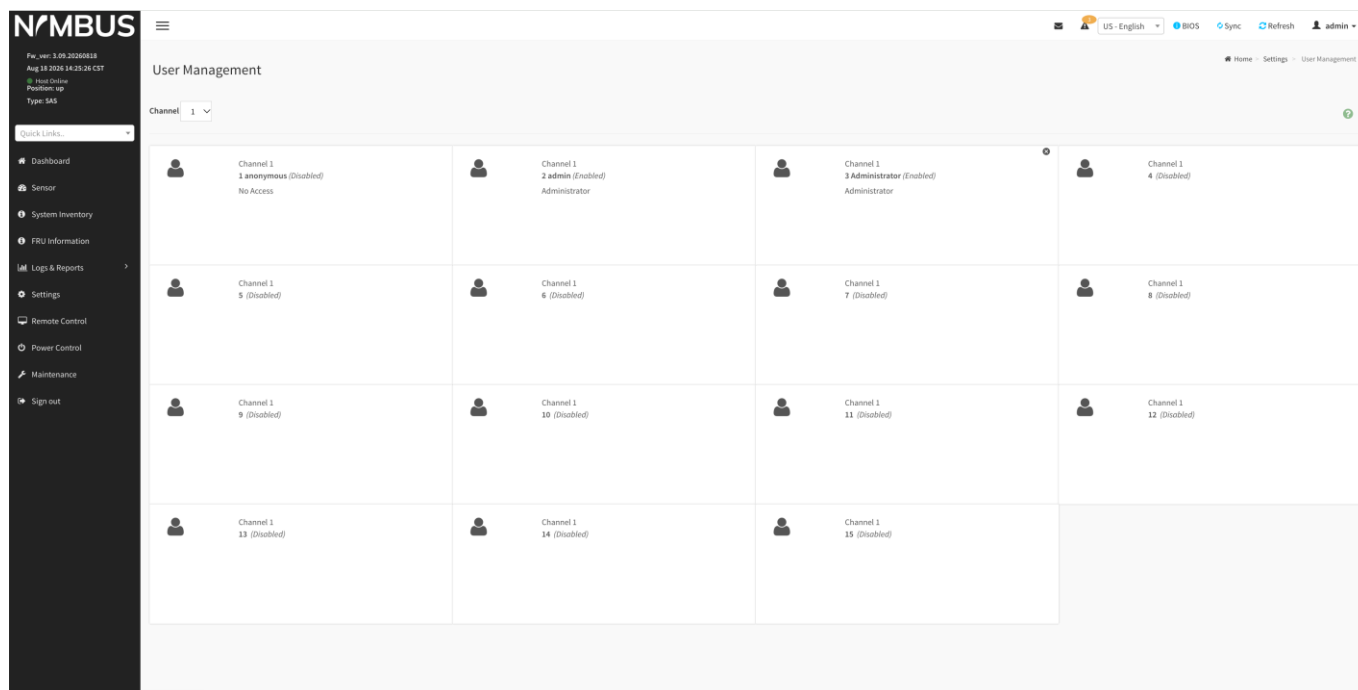
Примечание: допустимые значения — от 1 до 65535.

- Введите конец диапазона в поле **Port Range End**.
 - Выберите протокол в поле **Protocol**: TCP, UDP или Both.
 - Выберите тип сети в поле **Network Type**: IPv4, IPv6 или Both.
 - Выберите **Timeout**, чтобы включить или отключить ограничение правила по времени.
 - В поле **Start Time** укажите время начала действия правила.
 - В поле **Start Date** укажите дату начала действия правила.
 - В поле **End Date** укажите дату окончания действия правила.
 - В поле **End Time** укажите время окончания действия правила.
- Примечание:** дата и время указываются в формате YYYY/MM/DD:hh-mm.
- В поле **Rule** выберите действие правила: Block или Allow.
 - Нажмите **Save**, чтобы сохранить изменения.

3.7.12 Управление пользователями (User Management)

Страница **User Management** веб-интерфейса BMC отображает текущий список учётных записей пользователей сервера. На ней можно добавлять новых пользователей, а также изменять и удалять существующих.

Чтобы открыть страницу, выберите в строке меню **Settings > User Management**. Пример страницы приведён ниже.



Чтобы добавить пользователя, на главной странице **User Management** нажмите значок пользователя и выберите любую свободную строку.

Чтобы удалить запись из списка, нажмите значок удаления (x) в правом верхнем углу.

Примечание: свободные строки отображаются со значением «Disabled» во всех столбцах.

Поля страницы:

Channel — выбор канала из списка доступных.

User ID — идентификатор пользователя.

Примечание: список может содержать не более 15 пользователей.

User Name — имя пользователя.

User Access — включение или отключение доступа пользователя.

Network Privilege — уровень сетевых привилегий пользователя.

SNMP Status — состояние SNMP для пользователя: включено или отключено.

E-mail ID — адрес электронной почты пользователя.

Add User — добавление пользователя.

Delete User — удаление пользователя.

Добавление пользователя

1. Выберите свободную строку и нажмите на неё. Откроется окно добавления пользователя, показанное ниже.

2. Введите имя пользователя в поле **User Name**.

Примечание:

- имя пользователя — строка длиной от 1 до 16 буквенно-цифровых символов, начинающаяся с буквы;
- имя чувствительно к регистру;
- допускаются дефис (-), подчёркивание (_) и знак «@»;
- при длине пароля 20 байт сеанс LAN не устанавливается.

3. Задайте допустимую длину пароля в поле **Password Size**.

4. Введите новый пароль в поле **Password** и повторите его в поле **Confirm Password**.

Примечание:

- пароль должен содержать буквы, цифры, специальные символы и прописные буквы;
- пробелы не допускаются;
- максимальная длина — 16 или 20 символов в зависимости от значения поля **Password Size**;

- пароль не может содержать символы, приведённые в таблице ниже;
- при установке пароля командой «`ipmitool user set password`» пароль должен передаваться строкой.

Таблица 3. Недопустимые символы в пароле

Hex	Символ	Hex	Символ
0	NUL '\0'	11	DC1 (device control 1)
1	SOH (start of heading)	12	DC2 (device control 2)
2	STX (start of text)	13	DC3 (device control 3)
3	ETX (end of text)	14	DC4 (device control 4)
4	EOT (end of transmission)	15	NAK (negative ack.)
5	ENQ (enquiry)	16	SYN (synchronous idle)
6	ACK (acknowledge)	17	ETB (end of trans. blk)
7	BEL '\a' (bell)	18	CAN (cancel)
8	BS '\b' (backspace)	19	EM (end of medium)
9	HT '\t' (horizontal tab)	1A	SUB (substitute)
0A	LF '\n' (new line)	1B	ESC (escape)
0B	VT '\v' (vertical tab)	1C	FS (file separator)
0C	FF '\f' (form feed)	1D	GS (group separator)
0D	CR '\r' (carriage ret)	1E	RS (record separator)
0E	SO (shift out)	1F	US (unit separator)
0F	SI (shift in)	20	SPACE
10	DLE (data link escape)	7F	DEL

5. Установите флажок **Enable User Access**, чтобы предоставить пользователю сетевой доступ.

Примечание:

- включение доступа пользователя к каналу (*Channel User Access*) назначает пользователю этого канала привилегию обмена сообщениями IPMI;
- при создании пользователя через IPMI рекомендуется включить для него обмен сообщениями IPMI, чтобы активировать параметр User Access.

6. В поле **Enable Channel Access** выберите каналы, для которых предоставляется сетевой доступ.

7. В поле **Privilege** выберите уровень привилегий пользователя: Administrator, Operator, User, OEM или None. По умолчанию привилегии канала отображаются в зависимости от его доступности.

Примечание: привилегия *Callback* отображается в поле **Privilege**, только если она назначена через другие интерфейсы. По умолчанию назначить её через веб-интерфейс, как другие привилегии, нельзя.

8. Установите флажок **KVM Access**, чтобы предоставить пользователю доступ к KVM.

Примечание: при изменении доступа к KVM пользователем, выполнившим вход, появится сообщение о необходимости завершить текущий сеанс для применения изменений.

9. Установите флажок **VMedia Access**, чтобы предоставить пользователю доступ к VMedia.

Примечание:

- под VMedia понимаются клиенты H5Viewer, JViewer, VMap и VMCLI;
- доступ к KVM и VMedia рекомендуется предоставлять только пользователям с уровнем ADMIN, но не USER и OPERATOR. Администратор может предоставить этот доступ пользователям уровней USER и OPERATOR на свой риск;
- привилегия VMedia ограничивает только запуск перенаправления носителей. Если устройство уже перенаправлено и подключено к хосту, на хосте оно отображается как обычное устройство и доступно во всех сеансах KVM, в том числе в сеансах только с привилегией KVM;
- при изменении доступа к KVM и VMedia пользователем, выполнившим вход, появится сообщение о необходимости завершить текущий сеанс для применения изменений.

- 10.** Установите флажок **SNMP Access**, чтобы предоставить пользователю доступ по SNMP.

Примечание: при включённом SNMP поле пароля обязательно для заполнения.

- 11.** Выберите уровень доступа SNMP в раскрывающемся списке **SNMP Access level:** Read Only (только чтение) или Read Write (чтение и запись).

- 12.** Выберите протокол аутентификации SNMP в раскрывающемся списке **SNMP Authentication Protocol:** SHA или MD5.

Примечание: при изменении протокола аутентификации поле пароля обязательно для заполнения.

- 13.** Выберите алгоритм шифрования SNMP в раскрывающемся списке **SNMP Privacy protocol:** AES или DES.

- 14.** В поле **Email ID** введите адрес электронной почты пользователя. Если пользователь забудет пароль, новый пароль будет отправлен на этот адрес.

Примечание: для отправки писем должен быть настроен сервер SMTP.

Email Format — доступны два формата писем:

AMI-Format — тема письма «Alert from (имя хоста)»; в тексте приводятся сведения о датчике, например тип датчика и описание.

Fixed-Subject Format — письмо формируется по настройкам пользователя; тему и текст оповещения необходимо задать.

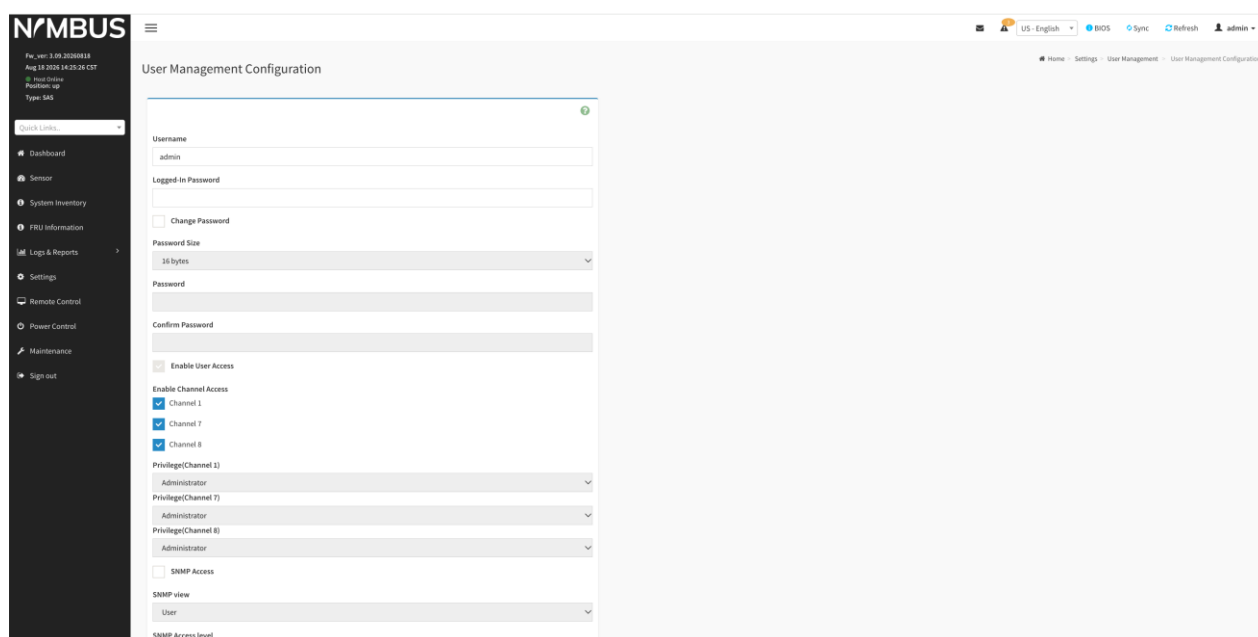
- 15.** В поле **Upload SSH Key** нажмите **Browse** и выберите файл ключа SSH.

Примечание: файл ключа SSH должен иметь формат PUB.

- 16.** Нажмите **Save**, чтобы сохранить пользователя и вернуться к списку пользователей.

Изменение пользователя

- 1.** Нажмите на строку существующего пользователя. Откроется окно, показанное ниже.



2. Введите имя пользователя в поле **Username**.

3. В поле **Logged-In Password** введите пароль, с которым выполнен вход в систему.

Примечание: для подтверждения необходимо повторно ввести пароль текущего сеанса. Изменение пользователя возможно только при успешной проверке пароля, в противном случае выводится сообщение об ошибке.

4. Установите флажок **Change Password**, если требуется изменить пароль.

5. Выполните шаги 3–15 из порядка добавления пользователя.

6. Нажмите **Save**, чтобы сохранить изменения и вернуться к списку пользователей.

7. Чтобы удалить пользователя, нажмите **Delete**.

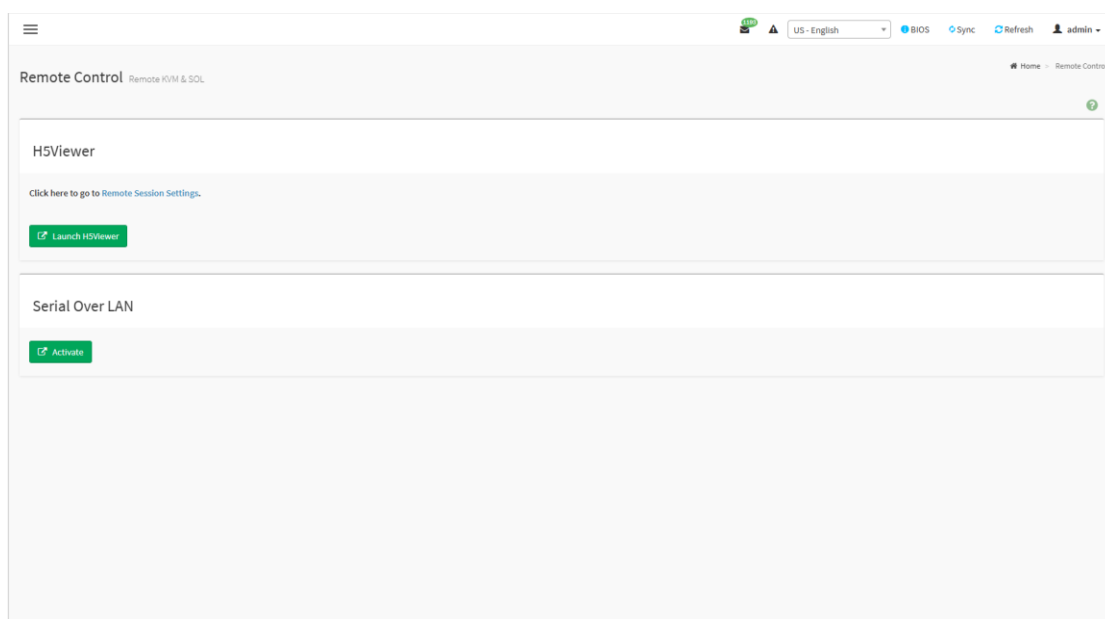
Важно. Зарезервированные имена: следующие имена пользователей зарезервированы и не могут использоваться для пользователей BMC:

- sysadmin
- daemon
- sshd
- ntp
- root

3.8 Удалённое управление (Remote Control)

Страница **Remote Control** содержит перечисленные ниже функции. Пример страницы приведён ниже.

- Launch H5Viewer — запуск консоли H5Viewer
- SOL Activate — активация Serial over LAN



Запуск H5Viewer (Launch H5Viewer)

Требования к системе и браузеру для удалённого управления:

Системные требования

- Клиентский компьютер с 8 ГБ ОЗУ.
- При объёме ОЗУ 4 ГБ и менее возможны задержки при перенаправлении видео, клавиатуры, мыши и носителей.

Поддерживаемые браузеры

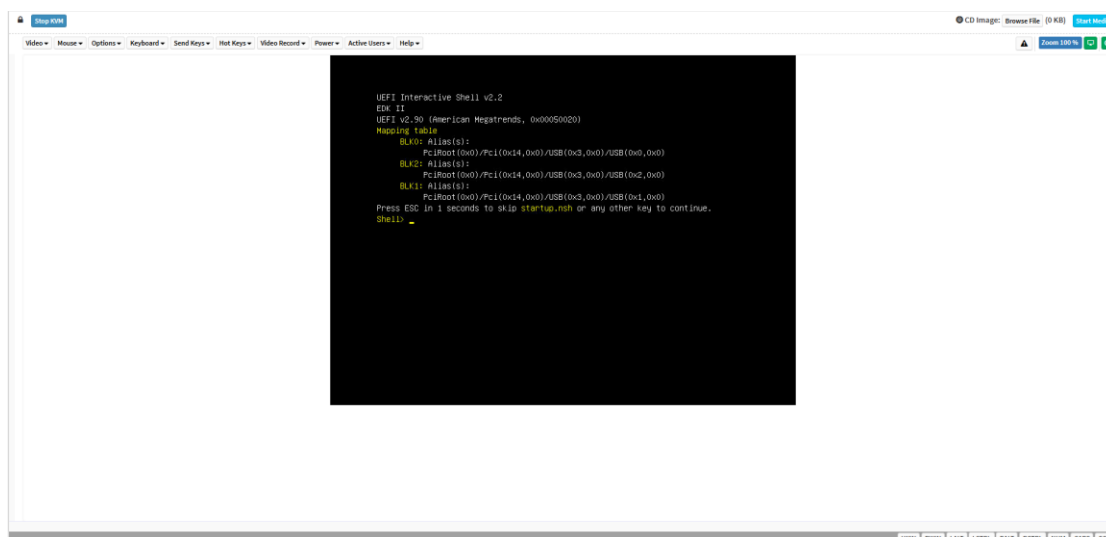
- Chrome последней версии.
- Firefox (с ограниченной поддержкой).
- Microsoft Edge на базе Chromium.
- Safari (только на Mac).

Чтобы открыть страницу, выберите **Remote Control** в строке меню.

На странице **Remote Control** нажмите **Launch H5Viewer**. Откроется страница удалённой консоли KVM.

Запуск KVM

1. Нажмите **Launch H5Viewer**, чтобы открыть страницу удалённой консоли KVM. Пример страницы приведён ниже.



2. Чтобы остановить перенаправление видео H5Viewer, нажмите **Stop KVM**.

Запуск и остановка перенаправления носителей

1. Нажмите **Browse** и выберите образ CD. После выбора образа установите или снимите флажок ускорения носителей (**media boost**).
2. Нажмите **Start Media**, чтобы перенаправить выбранный образ CD на хост.

Примечание: в режиме *media boost* процессы перенаправления носителей получают более высокий приоритет, чем остальные процессы. Это повышает производительность носителей, но ограничивает доступ других процессов к ресурсам процессора. Если экземпляр CD/DVD запущен в режиме *media boost*, следующий экземпляр CD/DVD запускается без всплывающего сообщения.

3. Чтобы остановить перенаправление образа CD, нажмите **Stop Media**.

Ниже приведено описание пунктов меню консоли.

Видео (Video)

Меню содержит следующие пункты:

Pause Video — приостановка перенаправления консоли.

Resume Video — возобновление приостановленного перенаправления консоли.

Refresh Video — обновление изображения в окне перенаправления консоли.

Capture Screen — снимок экрана хоста с сохранением на клиентском компьютере.

Мышь (Mouse)

Show Client Cursor — отображение или скрытие локального курсора мыши в окне удалённой консоли.

Mouse Mode — способ эмуляции мыши при передаче из локального окна на удалённый экран. Изменять этот параметр может только администратор (Administrator).

- **Absolute mouse mode** — на сервер передаются абсолютные координаты локального курсора.
- **Relative mouse mode** — на сервер передаётся вычисленное относительное смещение курсора.
- **Other mouse mode** — клиентский курсор устанавливается в центр окна, а на хост передаётся отклонение от центра. Режим предназначен для установки SUSE Linux.

Параметры (Options)

Zoom — масштаб:

- **Normal** — исходный масштаб (выбран по умолчанию);
- **Zoom In** — увеличение изображения от 100 до 150 % с шагом 10 %;
- **Zoom Out** — уменьшение изображения от 100 до 50 % с шагом 10 %.

Block Privilege Request — включение или отключение запросов на получение привилегий доступа.

Compression Mode* — режим сжатия передаваемых видеоданных.

DTC Quantization Table* — выбор качества видео.

Примечание: * — только для SoC AST.

Клавиатура (Keyboard)

Keyboard Layout — функция полностью совместима, если на хосте и клиенте используется одинаковая раскладка клавиатуры. При разных раскладках некоторые специальные символы передаются некорректно.

Раскладки физической клавиатуры хоста, поддерживаемые в SPX H5Viewer:

1. Английская (США).
2. Немецкая.
3. Японская.

Отправка клавиш (Send Keys)

Меню используется для отправки сочетаний клавиш и содержит следующие пункты:

- Hold Down — удержание клавиши
- Press and Release — нажатие и отпускание

Удержание (Hold Down)

Меню содержит следующие пункты:

Right Ctrl Key — правая клавиша <CTRL> в режиме перенаправления консоли.

Right Alt Key — правая клавиша <ALT> в режиме перенаправления консоли.

Right Windows Key — правая клавиша <WIN> в режиме перенаправления консоли.

Left Ctrl Key — левая клавиша <CTRL> в режиме перенаправления консоли.

Left Alt Key — левая клавиша <ALT> в режиме перенаправления консоли.

Left Windows Key — левая клавиша <WIN> в режиме перенаправления консоли. Можно выбрать способ нажатия: удержание (Hold Down) или нажатие и отпускание (Press and Release).

Нажатие и отпускание (Press and Release)

Ctrl+Alt+Del — одновременное нажатие клавиш <CTRL>, <ALT> и <DEL> на сервере, консоль которого перенаправлена.

Left Windows Key — левая клавиша <WIN> в режиме перенаправления консоли. Можно выбрать способ нажатия: удержание (Hold Down) или нажатие и отпускание (Press and Release).

Right Windows Key — правая клавиша <WIN> в режиме перенаправления консоли.

Context Menu Key — клавиша контекстного меню в режиме перенаправления консоли.

Print Screen Key — клавиша Print Screen в режиме перенаправления консоли.

Hot Keys — добавление пользовательских сочетаний клавиш для отправки на хост. Настроенные сочетания сохраняются в BMC.

Меню содержит следующие пункты:

- **Add Hot Keys** — добавление макросов. Нажмите **Add**, чтобы добавить макрос.

Запись видео (Video Record)

Меню содержит следующие пункты:

Record Video — начало записи экрана.

Stop Recording — остановка записи.

Record Settings — длительность записи и степень сжатия видео. Длительность записи — от 1 до 1800 секунд; степень сжатия — от 0,1 (низкое качество изображения) до 0,9 (высокое качество изображения).

Normalized video resolution to 1024 X 768 (*только для SoC AST) — видео хоста при записи масштабируется до разрешения 1024 × 768. Включение параметра повышает производительность записи на стороне клиента в H5Viewer.

Отключите параметр, чтобы записывать видео в разрешении хоста. В этом случае качество захвата зависит от производительности клиентского компьютера, и записанный файл может отличаться от ожидаемого (например, его длительность может не совпадать с заданной).

Примечание:

- максимальный размер видеофайла — около 40 МБ. При достижении предельного размера записанный файл загружается на клиентский компьютер, а запись продолжается до истечения заданного времени. Файл сохраняется под именем вида `video_дата-месяц-год_ч-мин-сек_номерчасти`;
- сохранение видеофайлов в разных браузерах пользователь контролирует самостоятельно;
- если окно H5Viewer теряет фокус во время записи, запись останавливается с уведомлением, а записанный файл удаляется;
- из-за ограничений браузера при потере фокуса окна срабатывание таймеров задерживается, видеосервер перестаёт передавать видеопакеты в H5Viewer, и запись останавливается.

Питание (Power)

Меню используется для управления питанием. Выберите нужный пункт, чтобы выполнить операцию:

Reset Server — перезагрузка системы без отключения питания («тёплая» перезагрузка).

Immediate Shutdown — немедленное отключение питания.

Orderly Shutdown — штатное завершение работы сервера с отключением питания.

Power ON Server — включение питания сервера.

Power Cycle Server — отключение питания с последующим включением («холодная» перезагрузка).

Активные пользователи (Active Users)

Отображает активных пользователей и IP-адреса их компьютеров.

При наличии нескольких сеансов KVM активный сеанс может быть завершён из главного сеанса (Master, сеанс KVM с полными привилегиями).

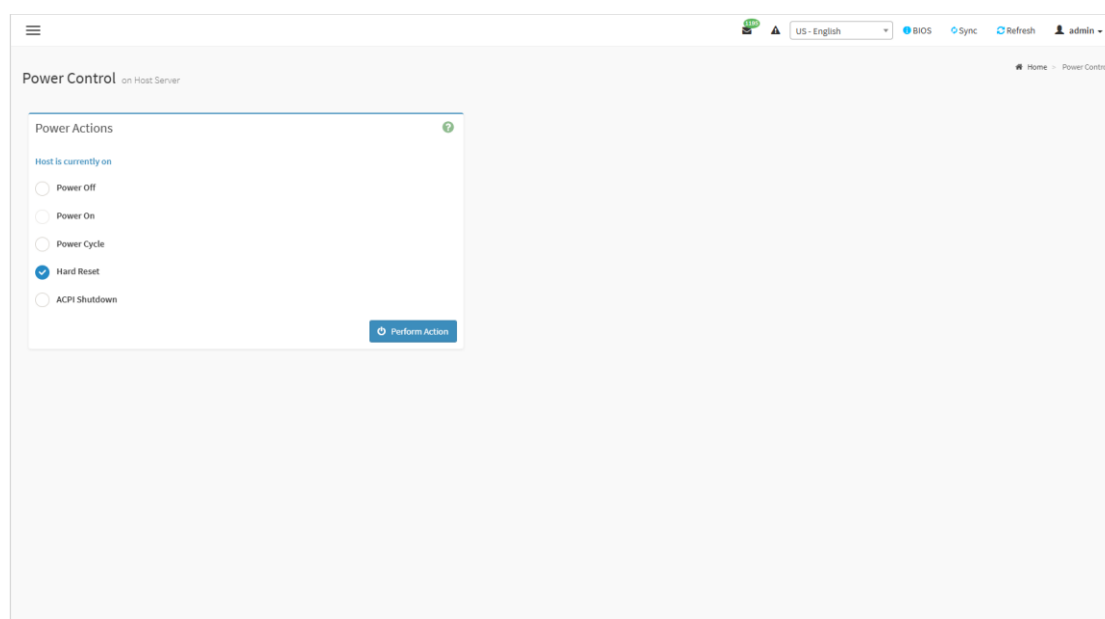
Справка (Help)

Отображает сведения о H5Viewer: версию утилиты удалённой консоли KVM и версию подключаемого модуля.

3.9 Управление питанием (Power Control)

Страница используется для просмотра состояния питания сервера и управления им.

Чтобы открыть страницу, выберите **Power Control** в строке меню. Пример страницы приведён ниже.



Power Off — немедленное отключение питания сервера.

Power On — включение питания сервера.

Power Cycle — отключение питания с последующей перезагрузкой системы («холодная» перезагрузка).

Hard Reset — перезагрузка системы без отключения питания («тёплая» перезагрузка).

ACPI Shutdown — штатное завершение работы операционной системы перед отключением питания.

Perform Action — выполнение выбранной операции.

Порядок действий

Выберите операцию и нажмите **Perform Action**.

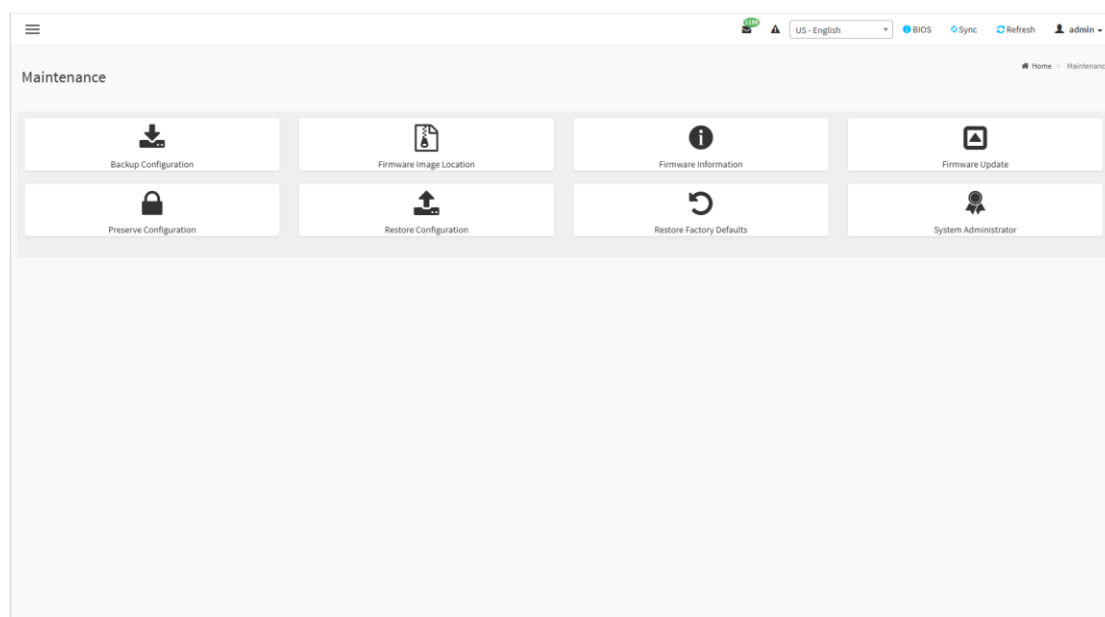
Примечание: при выполнении будет запрошено подтверждение. После подтверждения через несколько минут отобразится результат операции.

3.10 Обслуживание (Maintenance)

Раздел объединяет страницы для выполнения операций обслуживания устройства. Меню содержит следующие пункты:

- Backup Configuration — резервное копирование конфигурации
- Firmware Image Location — расположение образа микропрограммы
- Firmware Information — сведения о микропрограмме
- Firmware Update — обновление микропрограммы
- Preserve Configuration — сохраняемые параметры конфигурации
- Restore Configuration — восстановление конфигурации
- Restore Factory Defaults — восстановление заводских настроек
- System Administrator — системный администратор

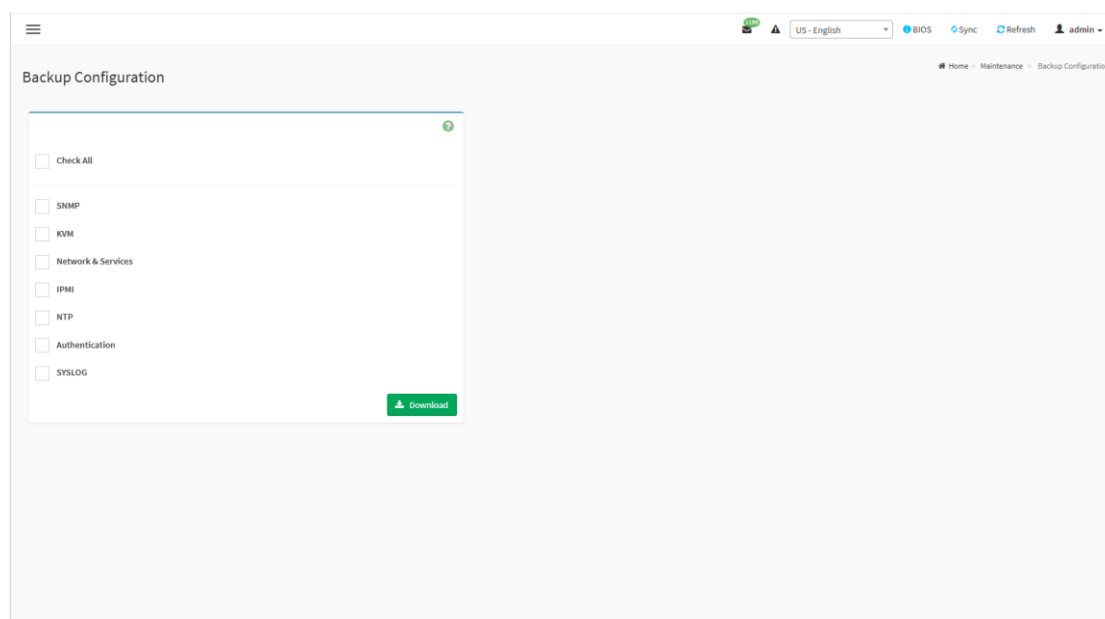
Пример страницы приведён ниже.



3.10.1 Резервное копирование конфигурации (Backup Configuration)

Страница используется для выбора параметров конфигурации, включаемых в резервную копию.

Чтобы открыть страницу, выберите в строке меню **Maintenance > Backup Configuration**. Пример страницы приведён ниже.



Check All — выбор всех параметров конфигурации.

Download Config — загрузка резервной копии файлов конфигурации из BMC на клиентский компьютер.

Примечание: в целях безопасности при резервном копировании конфиденциальные данные отфильтровываются и в резервную копию не попадают. Если после восстановления конфигурации войти в систему не удаётся, войдите под пользователем по умолчанию и заново задайте пароль.

Порядок резервного копирования

1. Нажмите **Check All**, чтобы включить в резервную копию все параметры, или выберите нужные параметры вручную. Страница будет выглядеть, как показано на рисунке выше.

Примечание: сетевые настройки связаны с настройками IPMI, поэтому при выборе раздела «Network and Services» настройки IPMI выбираются автоматически.

2. Нажмите **Download Config**, чтобы сохранить файл резервной копии на клиентском компьютере.

3. Нажмите **OK**, чтобы выполнить резервное копирование. Файл резервной копии будет сохранён на клиентском компьютере.

4. Нажмите **Cancel**, чтобы отменить резервное копирование.

Примечание: если для хранения резервной копии выбран *sd/emmc*, перед резервным копированием создайте в разделе *sd/emmc* каталог */confbkup*.

Настройка сервера TFTP (TFTP Server Configuration)

Сервер TFTP используется для выгрузки файла резервной копии.

Примечание: убедитесь, что другие серверы TFTP не запущены; при наличии удалите их вместе со всеми файлами конфигурации. Вход под «суперпользователем» означает вход под пользователем *root*.

Настройка сервера TFTP по умолчанию

1. Установите необходимые пакеты:

```
>apt-get install xinetd tftp tftpd
```

2. Отредактируйте файл конфигурации TFTP:

```
>vi /etc/xinetd.d/tftp
```

Приведите файл к следующему виду:

```
service tftp
{
  protocol = udp
  port = 69
  socket_type = dgram
  wait = yes
  user = nobody
  server = /usr/sbin/in.tftpd
  server_args = <DIR to which the file to be access>
  disable = no
}
#EOF
#example:server_args = /tftpboot
```

Примечание: в параметре `server_args` не указывается ничего, кроме каталога.

```
>vi /etc/xinetd.conf
```

Добавьте в файл:

```
defaults
{
  # Please note that you need a log_type line to use log_on_success and log_on_failure.
  The default is the following :
  # log_type = SYSLOG daemon info
}
includedir /etc/xinetd.d
```

3. Перезапустите сервер:

```
>/etc/init.d/xinetd restart
```

4. Предоставьте доступ к каталогу всем пользователям:

```
>mkdir <DIR>
>chmod -R 777 <DIR>
>chown -R nobody <DIR>
```

Например:

```
mkdir /tftpboot
chmod -R 777 /tftpboot
chown -R nobody /tftpboot
```

5. Чтобы принять файл, создайте его командой `touch` и предоставьте доступ всем пользователям:

```
> touch <DIR>/conf.bak
> chmod 777 <DIR>/conf.bak
```

6. Если после выполнения всех шагов сохраняется ошибка тайм-аута:

- В файле `/etc/xinetd.d/tftp` раскомментируйте строку EOF (удалите символ «#» только перед EOF).
- Перезапустите сервер.

3.10.2 Расположение образа микропрограммы (Firmware Image Location)

Страница используется для указания расположения образа микропрограммы ВМС (TFTP).

Чтобы открыть страницу, выберите в строке меню **Maintenance > Firmware Image Location**. Пример страницы приведён ниже.

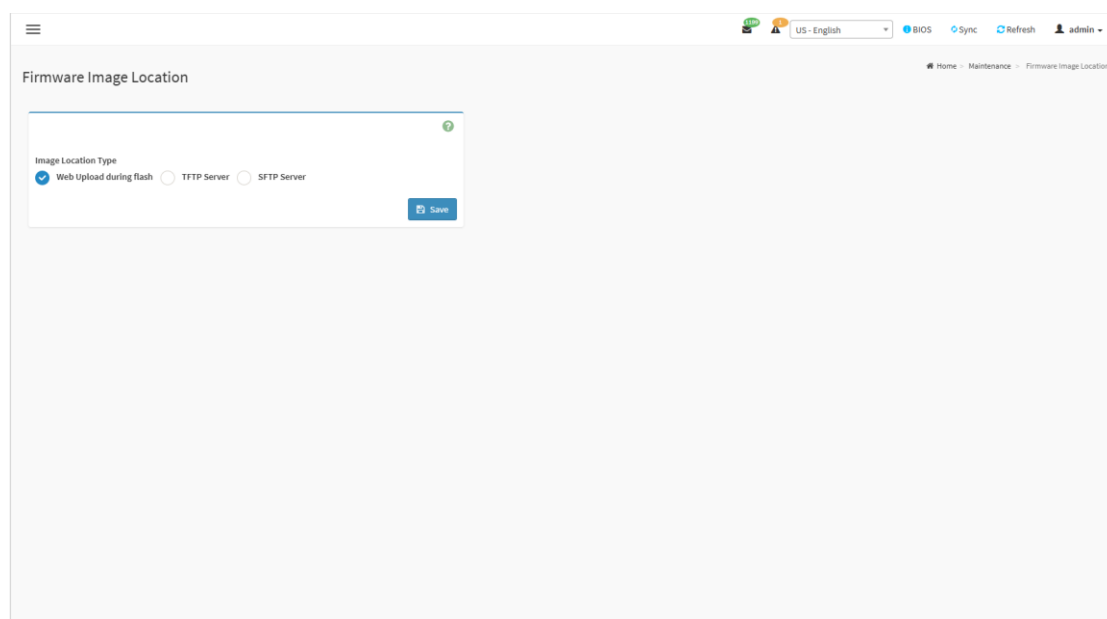


Image Location Type — способ передачи образа микропрограммы в BMC: **Web Upload during Flash** (загрузка через веб-интерфейс при прошивке), **TFTP Server** или **SFTP Server**.

Server Address — адрес сервера, на котором хранится образ микропрограммы.

Примечание: сервер поддерживает адреса IPv4 и IPv6:

- IPv4-адрес состоит из 4 чисел, разделённых точками: «xxx.xxx.xxx.xxx»;
- каждое число — от 0 до 255;
- первое число не может быть равно 0;
- IPv6-адрес состоит из 8 групп по 4 шестнадцатеричные цифры, разделённых двоеточиями: «xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx»;
- шестнадцатеричные цифры указываются строчными буквами.

Image Name — полный путь к файлу образа микропрограммы на сервере TFTP/SFTP, включая имя файла.

Retry Count — количество повторных попыток при ошибке передачи: от 0 до 255.

Save — сохранение настроек.

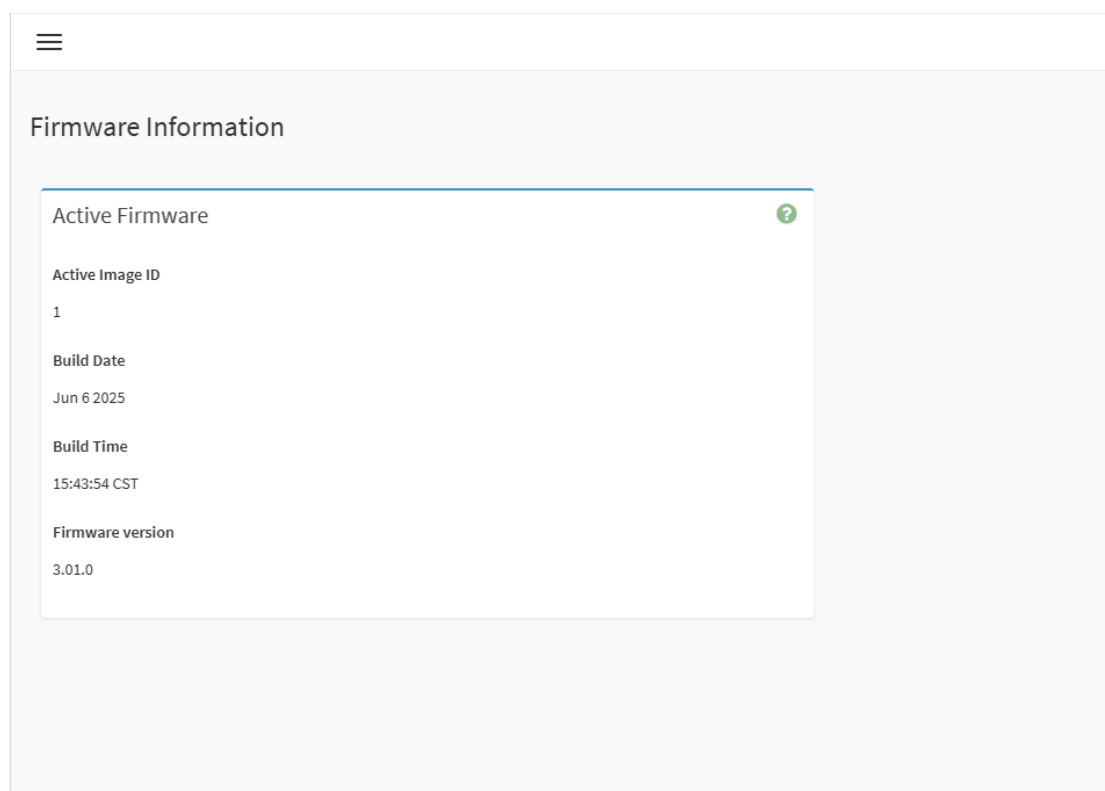
Порядок настройки

1. Выберите способ передачи в поле **Image Location Type**: **Web Upload during flash**, **TFTP Server** или **SFTP Server**.
2. Если выбран TFTP или SFTP, введите IP-адрес сервера в поле **Server Address**.
3. Введите путь к образу в поле **Image Name**.
4. Введите количество повторных попыток в поле **Retry Count**.
5. Нажмите **Save**, чтобы сохранить изменения.

3.10.3 Сведения о микропрограмме (Firmware Information)

Страница отображает сведения о микропрограмме BMC.

Чтобы открыть страницу, выберите в строке меню **Maintenance** > **Firmware Information**. Пример страницы приведён ниже.



Build Date — дата сборки активного образа BMC.

Build Time — время сборки активного образа BMC.

Firmware version — версия микропрограммы активного образа BMC.

3.10.4 Обновление микропрограммы (Firmware Update)

Мастер обновления последовательно проводит пользователя через процесс обновления микропрограммы и позволяет выполнять все операции обновления: обновление микропрограммы (Firmware Update), обновление HPM (HPM Firmware Update) и обновление двух образов (Dual Firmware Update).

Для текущей версии BMC поддерживается обновление микропрограмм следующих устройств:

- BMC (bin, два образа)
- BIOS (bin, два образа)
- CPLD (hpm)

Обновление BMC (Update BMC)

После завершения или отмены обновления устройство автоматически перезагружается. Чтобы сохранить текущие настройки при обновлении, включите параметр **Preserve All Configuration**.

Предупреждение: после перехода в режим обновления виджеты, остальные веб-страницы и службы перестают работать, все открытые виджеты автоматически закрываются. Если отменить обновление до завершения работы мастера, устройство будет перезагружено.

Примечание:

– обновление микропрограммы — критическая операция. Перед её выполнением минимизируйте риск отключения питания или потери связи;

- если после перехода в режим обновления отменить прошивку, BMC необходимо перезагрузить: закройте браузер и снова войдите в BMC, прежде чем выполнять другие операции;
- если в конфигурации проекта отключена обработка команд IPMI во время прошивки (*Enable IPMI Command handling during flashing*), то после начала обновления через веб-интерфейс штатные команды IPMI в целях безопасности не принимаются.

Порядок обновления

1. Нажмите **Browse** и выберите образ микропрограммы.

Примечание: при загрузке по HTTP/HTTPS отображается окно выбора файла; при использовании TFTP файл загружается автоматически с отображением хода загрузки.

2. Нажмите **Start firmware update**, чтобы загрузить сведения об обновлении. В поле **Image to be Updated** выберите образ, который требуется обновить. Пример экрана приведён ниже.

Note:
Following are the Firmware update methods and components supported in this page.

- Dual Firmware update.
- HPM Firmware update supports the following components.
 - BOOT and APP
 - BIOS
 - CPLD
- BIOS Firmware update

Select Firmware Image
Taihu_BMC_v2_5_20250320.ima

Start firmware update

Protocol Type: HTTPS

The dual image formation to be used for firmware update is displayed as follows. To configure Image to be booted from upon Reset, choose 'Dual Image Configuration' under Maintenance.

Current Active Image	Image-1
Image to be Updated	
Inactive Image	
Inactive Image	
Image 1	
Image 2	
Both Images	

All configuration items below will be preserved as default during the restore configuration operation. Click "Edit Preserve Configuration" to modify the Preserve status settings.

[Edit Preserve Configuration](#)

S.No	Preserve Configuration Item	Preserve Status
1	SDR	Overwrite
2	FRU	Overwrite
3	SEL	Overwrite
4	IPMI	Overwrite
5	NETWORK	Overwrite
6	NTP	Overwrite
7	SNMP	Overwrite

3. Нажмите **Preserve all Configuration**, чтобы сохранить всю конфигурацию:

- **Preserve all Configuration** — сохранение всей конфигурации;
- **Edit Preserve Configuration** — изменение перечня сохраняемых параметров.

Этот шаг необязателен: при полной прошивке (full flash) сохранять конфигурацию не требуется.

Примечание: при восстановлении конфигурации все параметры будут сохранены или перезаписаны значениями по умолчанию.

4. Нажмите **Proceed to Flash** — появится предупреждение. Нажмите **OK**, чтобы начать обновление микропрограммы.

The dual image formation to be used for firmware update is displayed as follows. To configure image to be booted from upon Reset, Maintenance.

Current Active Image Image-1

Image to be Updated Image 1

☐ Preserve all Configuration. This will preserve all the configuration settings during the firmware update - irrespective of the individual items marked as preserve/overwrite in the table below.

All configuration items below will be preserved as default during the restore configuration operation. Click "Edit Preserve Configuration" to modify the Preserve status settings.

[Edit Preserve Configuration](#)

S.No	Preserve Configuration Item	Preserve Status
1	SDR	Overwrite
2	FRU	Overwrite
3	SEL	Overwrite
4	IPMI	Overwrite
5	NETWORK	Overwrite
6	NTP	Overwrite
7	SNMP	Overwrite
8	SSH	Overwrite
9	KVM	Overwrite
10	AUTHENTICATION	Overwrite
11	SYSLOG	Overwrite
12	WEB	Overwrite
13	REDFISH	Overwrite
14	AUTOMATIONENGINE	Overwrite

Proceed to Flash

5. Обновление выполняется в следующем порядке:

- Завершение всех активных клиентских запросов.
- Подготовка устройства к обновлению микропрограммы.
- Загрузка образа микропрограммы.
- Проверка образа микропрограммы.

При обновлении по разделам (Section Based Firmware Update) можно выбрать разделы образа для прошивки. Отметьте нужные разделы и нажмите **Proceed**.

Если требуется прошить все разделы, выберите **Full Flash**.

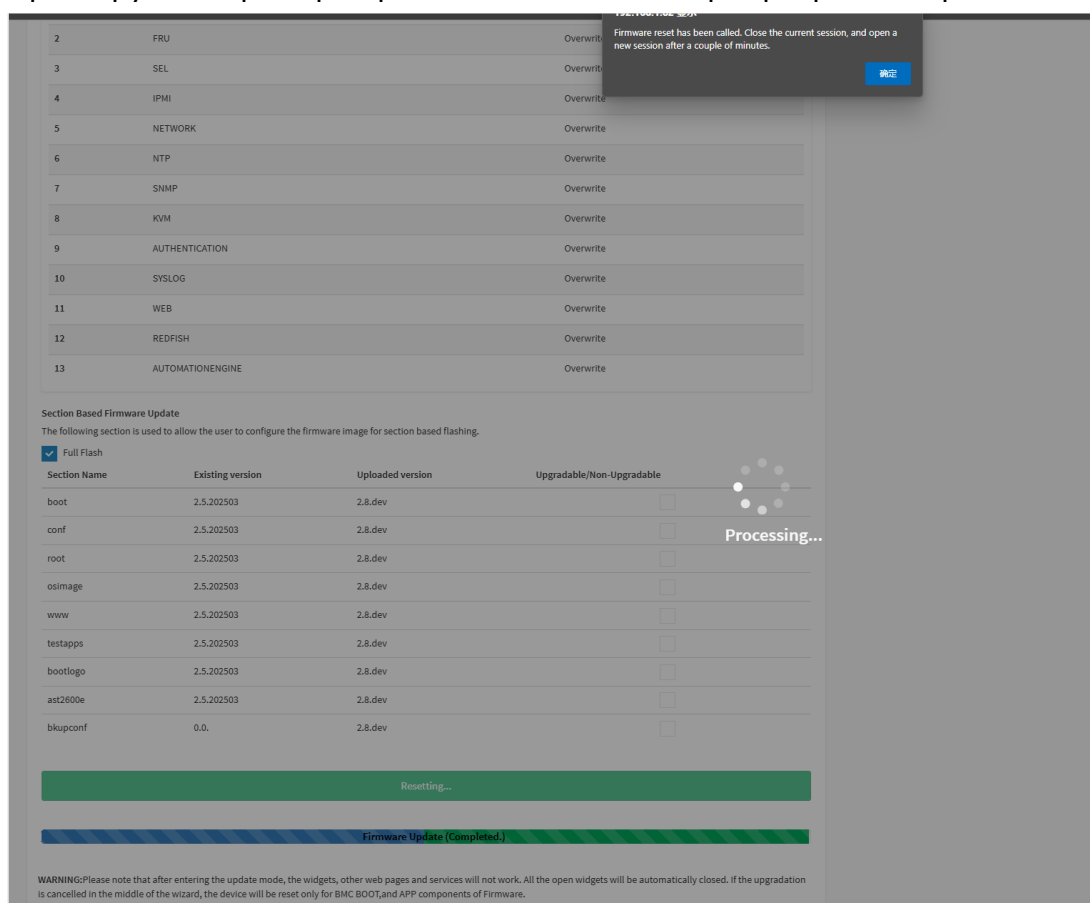
При выборе **Version Compare Flash** сравниваются версии, расположение FMH и размер модулей текущего и загруженного образов:

- если размер и расположение модулей различаются, выполняется принудительное обновление;
- если версии всех модулей совпадают, BMC перезагружается с сообщением о совпадении версий;
- если различаются версии только некоторых модулей, прошиваются только они.

Примечание: обновляются только выбранные разделы микропрограммы, остальные пропускаются. Перед прошивкой рекомендуется проверить совместимость разделов образа.

- Прошивка образа микропрограммы.

f) Перезагрузка. Пример экрана обновления микропрограммы приведён ниже.

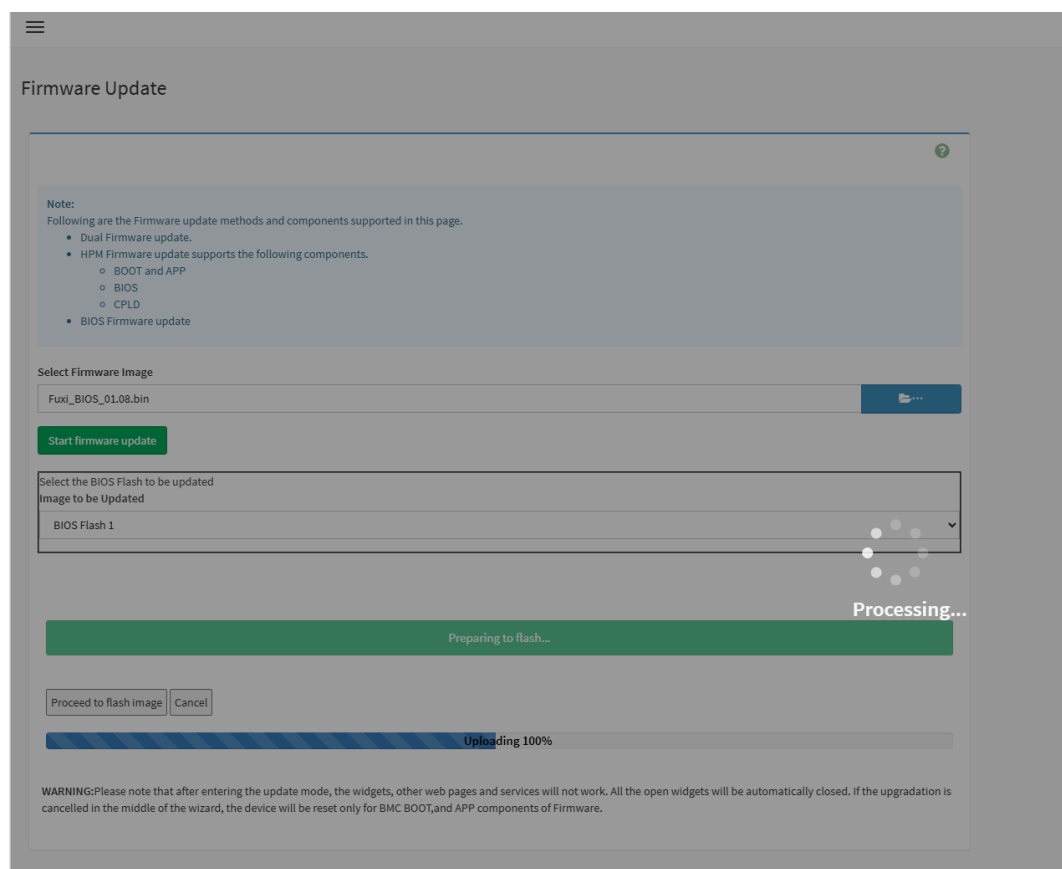
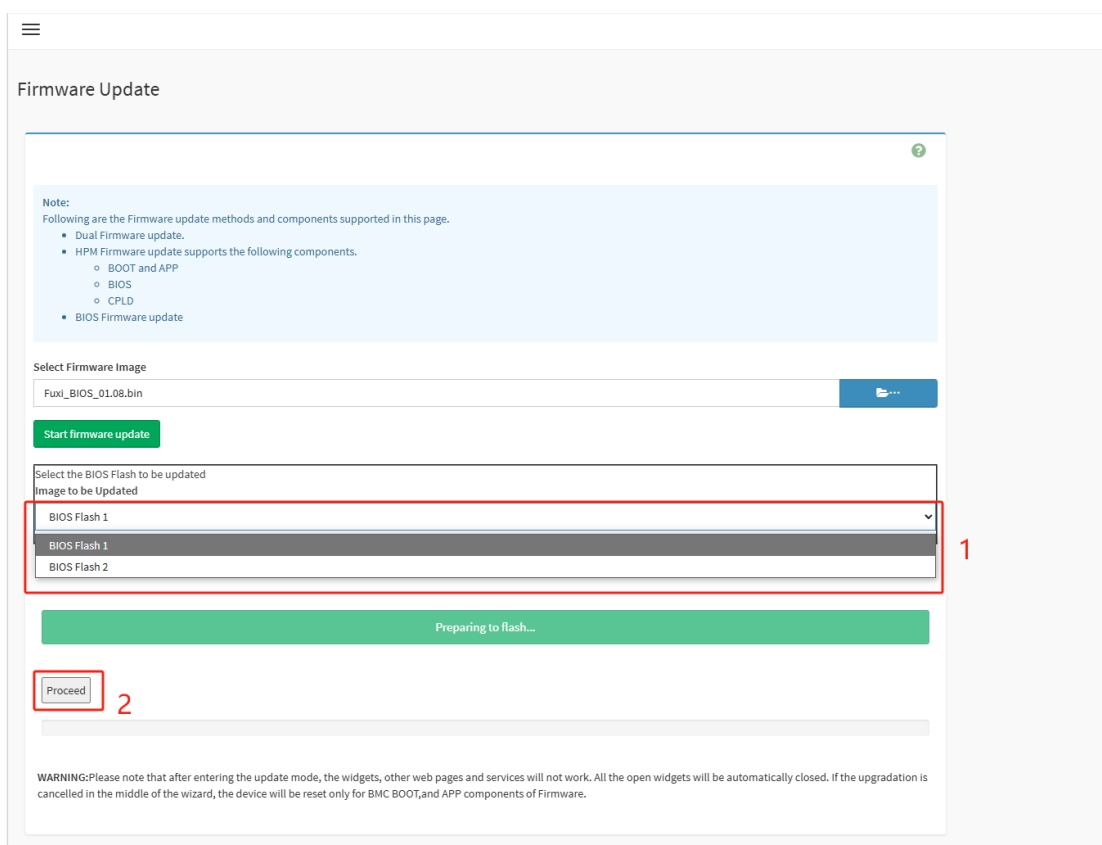


Обновление BIOS (Update BIOS)

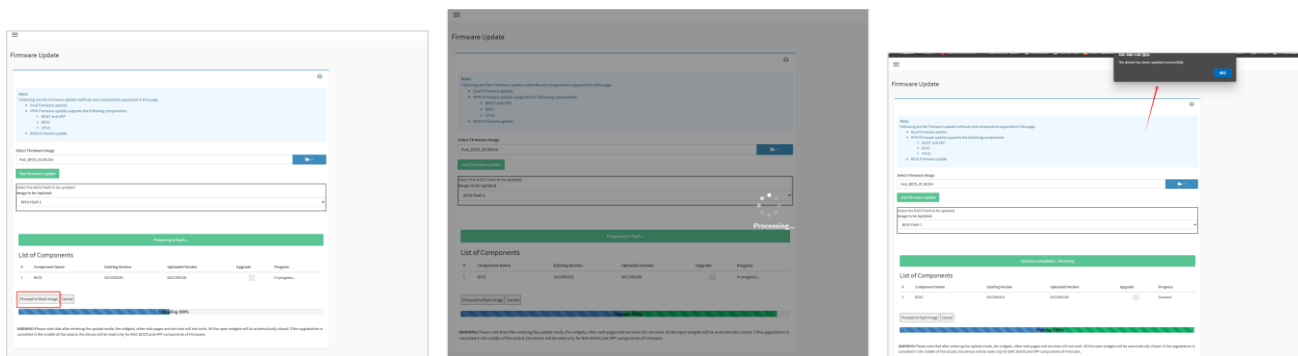
Обновите микропрограмму BIOS в указанном ниже порядке, заранее подготовив двоичный файл микропрограммы.

Настоятельно рекомендуется выполнять обновление BIOS при выключенном хосте или после полной загрузки ОС хоста. Не обновляйте BIOS во время загрузки BIOS.

1. Нажмите **Browse** и выберите файл микропрограммы BIOS.
2. Выберите флеш-память BIOS, которую требуется обновить. Нажмите **Proceed** и подтвердите действие. Дождитесь окончания загрузки микропрограммы в BMC.



3. Нажмите **Proceed to flash image** и дождитесь окончания обновления.



Обновление CPLD (Update CPLD)

Обновите микропрограмму CPLD в указанном ниже порядке, заранее подготовив двоичный файл микропрограммы.

Обновление обязательно выполнять при выключенном хосте. Во время обновления CPLD возможна нестабильная работа оборудования; после обновления обязателен полный цикл отключения и включения питания системы.

1. Нажмите **Browse** и выберите файл микропрограммы CPLD.
2. Выберите устройство CPLD, соответствующее выбранному файлу. Нажмите **Proceed** и подтвердите действие — будет выполнено обновление.

Внимательно проверяйте соответствие микропрограммы и выбранного устройства CPLD: прошивка несовместимой микропрограммы может привести к необратимому повреждению CPLD.

В СХД NIMBUS поддерживается обновление следующих устройств CPLD до актуальной версии:

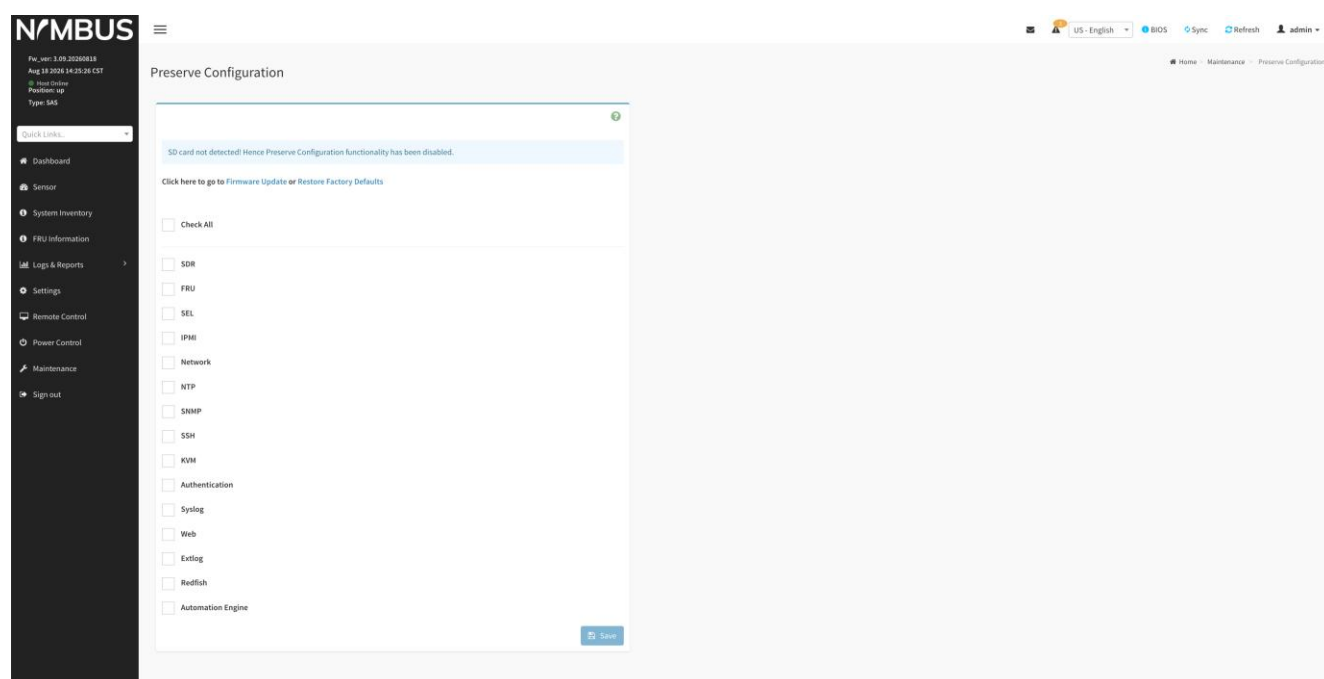
- CPLD системной платы (MB_CPLD)
- CPLD промежуточной платы (MP_CPLD)
- CPLD объединительной платы (BP_CPLD)

3.10.5 Сохраняемые параметры конфигурации (Preserve Configuration)

Страница используется для выбора параметров конфигурации, которые сохраняются при восстановлении заводских настроек и при обновлении микропрограммы, то есть не перезаписываются значениями по умолчанию.

Чтобы открыть страницу, выберите в строке меню **Maintenance > Preserve Configuration**. Пример страницы приведён ниже.

Примечание: со страницы можно перейти к страницам **Firmware Update** и **Restore Factory Defaults** по соответствующим ссылкам.



Click here to go to Firmware Update или **Restore Factory Defaults** — переход на страницу обновления микропрограммы или восстановления заводских настроек, для которых применяются сохраняемые параметры.

Check All — выбор всех параметров конфигурации.

Save — сохранение изменений.

***Примечание:** заданный перечень используется при восстановлении заводских настроек.*

Сохраняемые файлы

SDR

Сохраняются следующие файлы:

SDR.dat — записи данных датчиков (Sensor Data Record), используемые IPMI.

Зависимые параметры — нет.

FRU

Сохраняются следующие файлы:

FRU.bin — логические данные сменных модулей (FRU), используемые IPMI.

Зависимые параметры — SDR.

SEL

Если параметр Delete SEL reclaim space отключён, сохраняется файл:

SEL.dat — журнал системных событий, регистрируемых IPMI.

Если параметр Delete SEL reclaim space включён, сохраняются:

Selreclaiminfo.ini — сведения о хранилище SEL;

SEL folder — каталог с несколькими файлами журналов событий.

Зависимые параметры — IPMI.

IPMI

При выборе IPMI автоматически выбирается параметр Network, и наоборот. В конфигурации IPMI сохраняются следующие файлы:

IPMI.conf — настройки IPMI: размер хранилищ SEL и SDR, параметры интерфейсов, включение/отключение, основной/резервный, номер шины IPMB и др.

dcmi.conf — параметры спецификации DCMI 1.5: DHCP Timing1, DHCP Timing2, DHCP Timing3. Файл сохраняется, только если функция DCMI 1.5 включена в конфигурации проекта MDS.

pwdEncKey — ключи для расшифровки паролей. Файл сохраняется, если в конфигурации проекта MDS включён параметр паролей пользователей.

Зависимые параметры — Network.

Network

Для сохранения сетевых настроек, связанных с IPMI (IP-адрес LAN или настройки DHCP), при выборе IPMI автоматически выбирается Network, и наоборот. После восстановления конфигурации сетевые настройки сохраняются. Также сохраняются следующие файлы:

dhcp.conf — настройка имени хоста в формате FQDN.

dns.conf — способ регистрации в DNS и DNS-сервер для интерфейса.

hostname — имя хоста BMC.

hostname.conf — способ задания имени хоста BMC: вручную или автоматически.

Vlaninterfaces — включение интерфейса VLAN для интерфейса LAN.

vlansetting.conf — идентификатор и приоритет VLAN для интерфейса VLAN.

bond.conf — включение агрегированного интерфейса (bond) для указанных интерфейсов LAN.

Interfaces — IPv4/IPv6-адреса интерфейсов LAN (статические или по DHCP).

activeslave.conf — активный интерфейс агрегированного интерфейса; зависит от bond.conf.

hosts — сопоставление имён хостов и IP-адресов.

hosts.allow — список хостов, которым разрешён доступ к системе.

hosts.deny — список хостов, которым запрещён доступ к системе.

resolv.conf — сервер имён и имя домена для регистрации имени хоста.

dhcp6c-script — имя домена, IPv6-адрес DNS-сервера и адрес NTP.

dhcp6c.conf — параметры IPv6 для клиентов DHCPv6.

ncsicfg.conf — настройки NCSI.

nsupdate.conf — идентификаторы канала и пакета для интерфейса NCSI.

phycfg.conf — скорость соединения, режим дуплекса и MTU для интерфейса.

dhcp.preip_4 — предыдущий IPv4-адрес; файл создаётся во время работы.

ncml.conf — параметры служб.

Зависимые параметры — IPMI.

NTP

Сохраняются следующие файлы:

ntp.conf — параметры демона NTP: источники синхронизации, узлы и связанные сведения.

ntp.stat — тип синхронизации времени по сети: автоматический или ручной.

adjtime — данные для синхронизации системных часов.

Localtime — системная ссылка на файл местного времени или на нужный часовой пояс в системном каталоге часовых поясов.

Зависимые параметры — IPMI.

SNMP

Сохраняются следующие файлы:

snmp_users.conf — настройки пользователей SNMP: имена пользователей и механизмы шифрования паролей.

snmpcfg.conf — уровни привилегий пользователей SNMP (ro и rw).

Зависимые параметры — нет.

SSH

Сохраняются следующие файлы:

sshd_config — параметры конфигурации в виде пар «ключ — значение»: Address family, AcceptEnv, Allow users, authorized key files и др.

ssh_host_dsa_key, ssh_host_rsa_key — закрытые части ключей хоста.

ssh_host_dsa_key.pub, ssh_host_rsa_key.pub — открытые части ключей хоста.

Зависимые параметры — нет.

KVM & Media

Сохраняются следующие файлы:

vmedia.conf — режимы носителей (cd, hd) и флаги включения серверов lmedia, rmedia и sd.

adviserd.conf — режим мыши и раскладка физической клавиатуры хоста, заданные в конфигурации проекта MDS.

autorecord.conf — максимальные размер, количество и длительность файлов видеозаписи, а также путь на удалённом компьютере, если он задан в конфигурации проекта MDS.

usermacro.conf — пользовательские макросы JViewer.

rmedia.conf — имя образа и сведения об удалённом компьютере: IP-адрес, имя пользователя, пароль, имя домена и тип общего ресурса.

Зависимые параметры — нет.

Authentication

Сохраняются следующие файлы:

activedir.conf — параметры Active Directory: sslenable, timeout, racdomain, adtype, adfilterdc1, adfilterdc2, adfilterdc3, имя пользователя, пароль, а также сведения о группах ролей (имя, домен, привилегии).

openLdapGroup.conf — сведения о группах ролей OpenLDAP: имя, домен и привилегии.

nsswitch.conf — источники сведений службы имён по категориям и порядок их опроса.

pam_withinix — порядок модулей PAM: IPMI, LDAP, RADIUS и UNIX.

pam_wounix — порядок модулей PAM: IPMI, LDAP и RADIUS.

group — группы Linux: хранит сведения о группах пользователей.

passwd — сведения об учётных записях пользователей Linux.

shadow — зашифрованные пароли пользователей.

ldap.conf — параметры сервера LDAP: binddn, bindpw, pam_password, nss_reconnect_tries, основной и резервный порт, основной и резервный хост.

radius.conf — IP-адрес, порт, общий секрет, тайм-аут, привилегии сервера RADIUS и др.

Зависимые параметры — нет.

Syslog

Сохраняются следующие файлы:

- syslog.conf
- rotate.conf
- rsyslog.conf

Файлы содержат настройки системного журнала для различных категорий событий: оповещения, критические события, ошибки и др.

Зависимые параметры — нет.

Web

Сохраняется следующий файл:

updatefirmware.conf — расположение образа микропрограммы для обновления.

Зависимые параметры — нет.

Extlog

Сохраняет события расширенного журнала SEL (Extended SEL).

Зависимые параметры — IPMI.

Примечание: параметр Extlog отображается на странице *Preserve Configuration*, только если соответствующая функция включена.

Порядок настройки

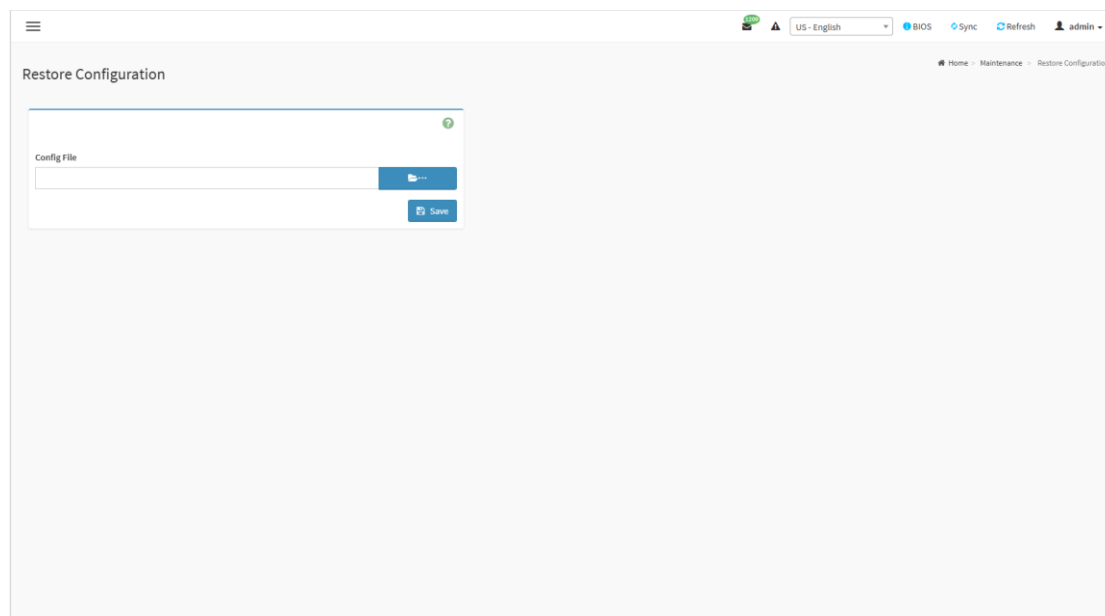
1. Нажмите ссылку **Firmware Update** или **Restore Configuration**, чтобы перейти на соответствующую страницу.

2. Выберите сохраняемые параметры, установив нужные флажки, или выберите все параметры с помощью **Check All**.
3. Нажмите **Save**, чтобы сохранить изменения.

3.10.6 Восстановление конфигурации (Restore Configuration)

Страница используется для восстановления файлов конфигурации в BMC с клиентского компьютера.

Чтобы открыть страницу, выберите в строке меню **Maintenance > Restore Configuration**. Пример страницы приведён ниже.



Поля страницы:

Config File — выбор ранее сохранённого файла резервной копии.

Upload — загрузка файла резервной копии для восстановления конфигурации.

Порядок восстановления

1. Нажмите **Browse** и выберите файл резервной копии конфигурации.
2. Нажмите **Upload**, чтобы восстановить конфигурацию из резервной копии.
3. Нажмите **OK**, чтобы загрузить файл конфигурации и выполнить восстановление.

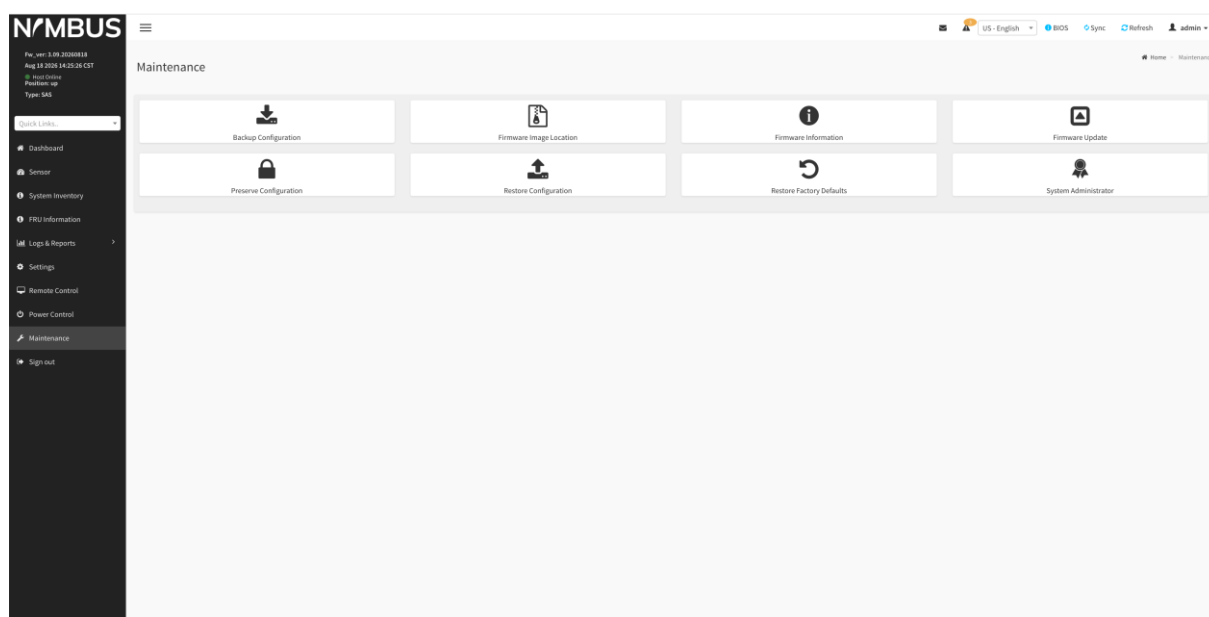
3.10.7 Восстановление заводских настроек (Restore Factory Defaults)

Функция используется для восстановления заводских настроек микропрограммы устройства.

При восстановлении заводских настроек сохраняются параметры конфигурации, выбранные на странице **Preserve Configuration**.

Предупреждение: после перехода в режим восстановления заводских настроек остальные веб-страницы и службы перестают работать, все открытые виджеты автоматически закрываются. Через несколько минут устройство будет сброшено и перезагружено.

Чтобы открыть страницу, выберите в строке меню **Maintenance > Restore Factory Defaults**. Пример страницы приведён ниже.



Порядок действий

1. Нажмите **Preserve Configuration**, чтобы перейти на страницу выбора параметров, которые не должны перезаписываться значениями по умолчанию.
2. Нажмите **Restore Factory Defaults**, чтобы восстановить заводские настройки микропрограммы устройства.

Примечание: после восстановления заводских настроек в журнале могут присутствовать события. Это могут быть новые события — проверить это можно по их отметкам времени.

3.10.8 Системный администратор (System Administrator)

Страница используется для настройки учётной записи системного администратора.

Чтобы открыть страницу, выберите в строке меню **Maintenance > System Administrator**. Пример страницы приведён ниже.

Username — имя системного администратора (только для чтения).

Enable User Access — включение доступа для системного администратора.

Change Password — изменение пароля пользователя.

Примечание: пароль должен содержать от 8 до 64 символов; пробелы не допускаются.

Save — сохранение новых настроек системного администратора.

Порядок настройки

1. Установите флажок **Enable User Access**, чтобы включить доступ для системного администратора.
2. Включите параметр **Change Password**, чтобы изменить пароль. Станут доступны поля для ввода пароля.
3. Введите новый пароль в поле **Password**.
4. Повторите пароль в поле **Confirm Password**.
5. Нажмите **Save**, чтобы сохранить изменения.