D-Link D-View8 / DV-800

Network Management System

ユーザマニュアル

D-Link®
Building Networks for People

安全にお使いいただくために

このたびは、弊社製品をお買い上げいただきありがとうございます。
本書は、製品を正しくお使いいただくための取扱説明書です。
必要な場合には、いつでもご覧いただけますよう大切に保管してください。
また、必ず本書、設置マニュアル、および弊社 WEB に掲載された製品保証規程をよくお読みいただき、内容をご理解いただいた上で、記載事項に従ってご使用ください。

製品保証規定は以下を参照ください。
https://www.dlink-jp.com/support/info/product-assurance-provision.html

- 本書の記載内容に逸脱した使用の結果発生した、いかなる障害や損害において、弊社は一切の責任を負いません。あらかじめご了承ください。
- 弊社製品の日本国外でご使用の際のトラブルはサポート対象外になります。
- 弊社は、予告なく本書の全体または一部を修正・改訂することがあります。
- 弊社は改良のため製品の仕様を予告なく変更することがあります。

なお、本製品の最新情報やファームウェアなどを弊社ホームページにてご提供させていただく場合がありますので、ご使用の前にご確認ください。
製品保証、保守サービス、テクニカルサポートご利用について、詳しくは弊社ホームページのサポート情報をご確認ください。
https://www.dlink-jp.com/support

警告 本書の内容の一部、または全部を無断で転載したり、複写することは固くお断りします。

目次

はじめに 5

本マニュアルの対象者 6
表記規則について 6

第 1 章　本製品のご利用にあたって 7

D-View8 の概要 7
D-View8 の機能 8
ライセンスの種類 10
90 日間無料トライアル 10
システム要件 11
ネットワーク管理システム 12
サポートされる製品 13
デバイスグループによる管理 14
D-View8 管理ユーザの認証の種類 14
ネットワークデバイス検出の準備 15
D-View8 による管理の開始 15

第 2 章　製品のインストール 16

インストール要件 16
D-View8 サーバのインストール（Windows サーバ / スタンドアロン構成） 16
D-View8 サーバのインストール（Windows サーバ / クラスタ構成）※エンタープライズ版のみ 25
D-View8 プローブのインストール（Windows サーバ） 42
（参考）D-View8 サーバのインストール（Linux サーバ / スタンドアロン構成） 45
（参考）D-View8 サーバのインストール（Linux サーバ / クラスタ構成）※エンタープライズ版のみ 47
（参考）D-View8 プローブのインストール（Linux サーバ） 62
D-View8 ソフトウェアのアップグレード 65
D-View8 ソフトウェアのアンインストール 65
D-View7 から D-View8 へのソフトウェアの移行 66

第 3 章　D-View8 の利用を開始する 80

Web GUI の起動とログイン 80
Web ダッシュボードについて 83
ユーザパスワードの変更 91
通知用の電子メールサーバの設定 92
通知センターの設定 93

第 4 章　ネットワークとデバイスの検出・管理 96

ネットワークの検出 96
ネットワークデバイスの管理 102
デバイスグループの管理 110
SNMP 設定 113
バッチ構成による複数ネットワークの管理 117

第 5 章　ネットワークの監視 120

デフォルトダッシュボードの表示 120
ダッシュボードのカスタマイズ 123
レポートの表示とエクスポート 128
レポート設定の管理 129
ファームウェアバージョンの表示 131
D-View8 通知の表示 132
複数のネットワークの監視 133

第 6 章　デバイス構成とファームウェア / コンフィグレーションの管理 136

タスクとプロファイルの作成 137
タスクの管理 142
デバイスのファームウェアアップグレード 144
コンフィグレーションファイルのバックアップとリストア 147
ネットワークファイル管理 151

第 7 章　アラームと通知 160

アラームの表示と管理 161
トラップログと Syslog の表示 162
トラップエディタ機能 163
Syslog エディタ機能 164
アラームおよび監視の管理 165
通知の管理 168

第 8 章　アーキテクチャトポロジの管理 173

ネットワークトポロジの表示と管理 173
トポロジビューの作成 176

第 9 章　ラックグループの管理 180

ラックグループの追加 180
ラックグループの表示と変更 183

第 10 章　sFlow の管理 188

sFlow 監視の設定 188
sFlow 監視の管理 193
sFlow 構成テンプレートのカスタマイズ 194
sFlow ネットワークの監視 195
sFlow 監視結果の表示とエクスポート 197

第 11 章　テンプレート機能 198

デバイステンプレートの生成 198
デバイスベンダとデバイスタイプの管理 199
パネルテンプレートの生成 199
監視テンプレートの生成 200
設定テンプレートの生成 201

第 12 章　レポート機能 204

レポートの管理 204
スケジュールレポートとマイレポートの作成 209
スケジュールレポート / マイレポートの表示と削除 212

第 13 章　ユーザとセキュリティプロファイルの管理 213

ユーザ役割の種類と機能毎のアクセス権限 213
認証の資格情報 216
ユーザプロファイルの管理 218

第 14 章　グローバル設定の管理 220

組織の設定 220
メールサーバ設定 221
トラップ転送の設定 222
Syslog 転送の設定 223
REST API キーの生成 224
接続プロトコルの認証情報の設定 225
sFlow 設定のセットアップ 230
システム環境設定 235
スケジュール機能 236
ライセンス管理 238
D-View8 ログ 243

第 15 章　各種ツール 244

MIB ブラウザ 244
MIB コンパイラツール 246
ICMP Ping の実行 248
SNMP テストの実行 249
Trace Route の実行 251
CLI からのネットワーク管理の設定 252
コンフィグレーションファイルの比較 254

第 16 章　付録 255

付録 A：クラスタ構成のインスト―ルシナリオ（Windows サーバ 5 台構成） 255

はじめに

本ユーザマニュアルは、D-View8 の機能と設定方法について記載しています。

「第 1 章　本製品のご利用にあたって」
- 本製品の概要、機能、動作環境について説明します。

「第 2 章　製品のインストール」
- 製品のインストールとデータベースの構成手順について説明します。

「第 3 章　D-View8 の利用を開始する」
- WebUI へのログイン方法やアカウント情報 / パスワード設定の変更手順などについて説明します。

「第 4 章　ネットワークとデバイスの検出・管理」
- ネットワークの検出、デバイス / デバイスグループの管理方法について説明します。

「第 5 章　ネットワークの監視」
- 各種ダッシュボード、ログ等の表示について説明します。

「第 6 章　デバイス構成とファームウェア / コンフィグレーションの管理」
- タスク管理やファームウェアの更新、コンフィグレーションバックアップ / リストア機能などについて説明します。

「第 7 章　アラームと通知」
- アラームやログの表示、設定について説明します。

「第 8 章　アーキテクチャトポロジの管理」
- ネットワークを階層表示するトポロジマップについて説明します。

「第 9 章　ラックグループの管理」
- ラックグループの設定、表示について説明します。

「第 10 章　sFlow の管理」
- sFlow の設定について説明します。

「第 11 章　テンプレート機能」
- デバイスの構成に使用する各種テンプレートについて説明します。

「第 12 章　レポート機能」
- レポートの管理やスケジュール設定などについて説明します。

「第 13 章　ユーザとセキュリティプロファイルの管理」
- ユーザプロファイルの管理、ユーザの種類に応じたアクセス権限について説明します。

「第 14 章　グローバル設定の管理」
- 組織情報、メールサーバ、Syslog、REST API などの設定について説明します。

「第 15 章　各種ツール」
- MIB ブラウザ / コンパイラ、Ping、トレースルート、ファイル比較などの機能について説明します。

「第 16 章　付録」
- 設定 / 監視に関する制限事項、クラスタ構成のインストールシナリオ（5 台構成）について説明します。

本マニュアルの対象者

本マニュアルは、本製品の操作方法についての情報を記載しています。また、ネットワーク管理の概念や用語に十分な知識を持っているネットワーク管理者、システム管理者、または IT 技術者を対象としています。

表記規則について

本項では、本マニュアル中での表記方法について説明します。

注意 注意では、使用にあたっての注意事項について説明します。

警告 設定の組み合わせ、イベントや手順によりネットワークの接続状態やセキュリティなどに悪影響を及ぼす恐れのある事項について説明します。

メモ 特長や技術についての詳細情報を説明します。

本マニュアル中での字体、・記号についての表記規則を表します。

字体・記号	解説	例
「」	メニュータイトル、ページ名、ボタン名。	「Submit」をクリックして設定を確定してください。
青字	参照先。	「ご使用になる前に」を参照してください。
太字	画面遷移。	**System** > **About** 画面

第 1 章　本製品のご利用にあたって

本章では、以下のトピックについて説明します。

- 「D-View8 の概要」
- 「D-View8 の機能」
- 「ライセンスの種類」
- 「90 日間無料トライアル」
- 「システム要件」
- 「ネットワーク管理システム」
- 「サポートされる製品」
- 「デバイスグループによる管理」
- 「D-View8 管理ユーザの認証の種類」
- 「ネットワークデバイス検出の準備」
- 「D-View8 による管理の開始」

D-View8 の概要

D-View8 は、Server & Probe アーキテクチャ設計の有線 / 無線デバイスの統合ネットワーク管理ツールです。本製品は、ネットワークのトラブルシューティング、設定、パフォーマンス監視、セキュリティをサポートします。また、D-Link およびサードパーティ製デバイスの管理機能を提供し、IT ストラクチャのエンドツーエンド管理、システムアーキテクチャのスケーラビリティ、新しいテクノロジとインフラストラクチャへの適応をサポートします。

D-View8 の「スタンダード」「エンタープライズ」ライセンスオプションにより、SMB からエンタープライズ展開までの異なるネットワーク要件に対応します。「エンタープライズ」ライセンスでは、複数サーバ及び複数 Probe をサポートし、より高度な機能を提供しています。

メモ　ライセンスの詳細は、P.10 の「ライセンスの種類」を参照してください。

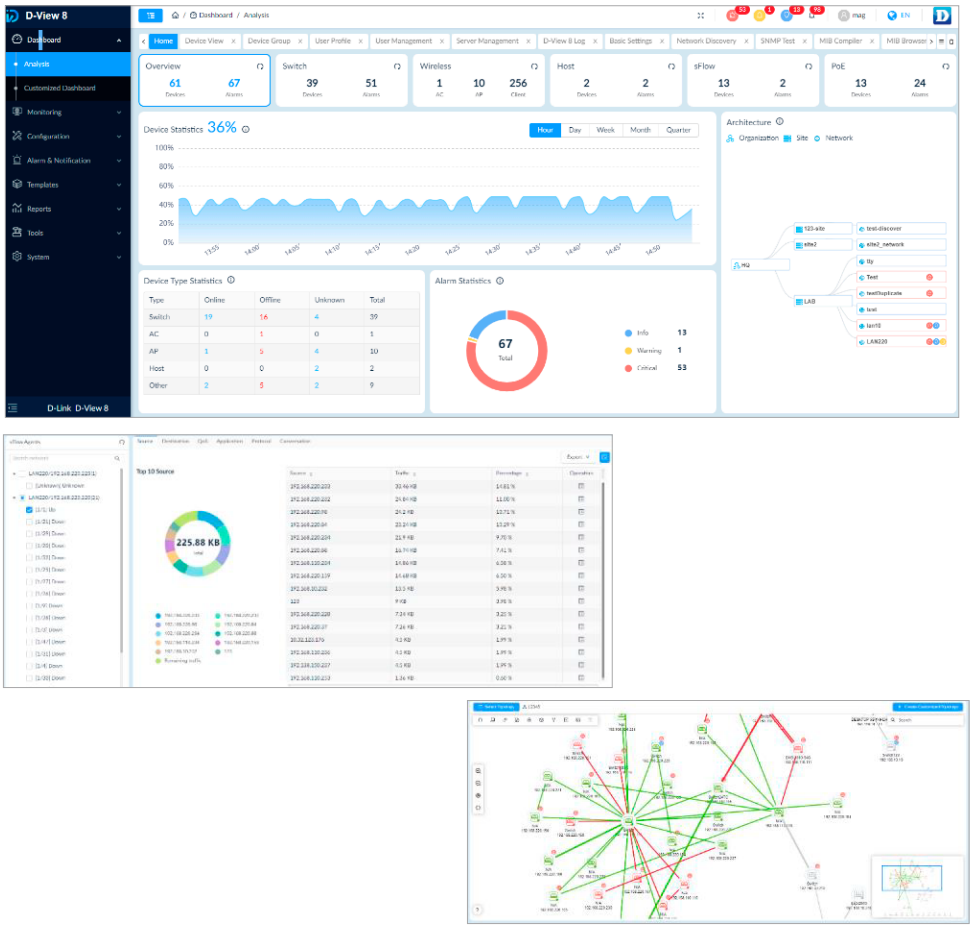


図 1-1　D-View8 の Web インタフェース

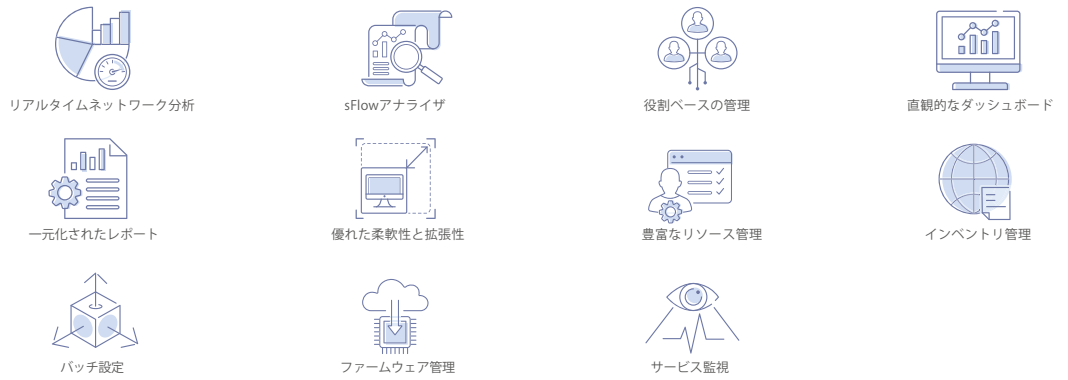
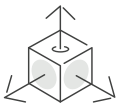


図 1-2　D-View8 の機能

D-View8 の機能

D-View8 は、以下の機能をサポートしています。

メニュー		説明
	リアルタイムネットワーク分析	リアルタイムネットワーク分析は、ネットワークの可視性を提供します。 D-View8 を使用すると、管理対象デバイスの重要なアラーム、応答時間、CPU/ メモリ使用率、帯域使用状況などの統計情報を、すばやく視覚的に把握することができます。
	sFlow アナライザ	D-View8 では、特にネットワークが大規模で複雑な環境において、sFlow アナライザを使用して組織内のネットワーク異常を検出することができます。デバイスから sFlow データを収集し、統計レポートを生成するのに役立ちます。 補足　本機能はエンタープライズ版でのみサポートされます。
	役割ベースの管理	ユーザ認証には、Windows Active Directory や RADIUS といった一般的な認証システムを利用することができます。また、オペレータ毎に管理対象ネットワークや役割の設定が可能です。役割により、利用可能な機能が制限されます。
	直感的なダッシュボード	D-View8 はユーザフレンドリなダッシュボードを提供します。ネットワークデバイスの概要、デバイス統計、アラーム統計、CPU/ メモリ使用率、応答時間、温度など、管理者のニーズに合わせてカスタマイズできます。
	一元化されたレポート	様々なパフォーマンス情報のレポートテンプレートが用意されています。 ネットワークデバイスの正常性、トラップ、Syslog などに関するレポートの設定を行います。取得データや間隔などの設定オプションを、簡単にカスタマイズすることができます。また、レポートのスケジュール設定を行うことも可能です。
	優れた柔軟性と拡張性	D-View8 は、管理ネットワークの規模に応じた機能や展開オプションに対応しています。
	充実したリソース管理	包括的なネットワークインベントリに対応した、ネットワークの探索とトポロジ機能を提供します。レイヤ 2/ レイヤ 3 や VLAN の情報が含まれます。
	インベントリ管理	マルチベンダのデバイスについて、統合的な管理機能を提供します。デバイスの詳細画面では、パフォーマンス情報のリアルタイムデータや接続クライアント情報などの主要なデータを監視することができます。

メニュー		説明
	バッチ設定	タスクを設定すると、複数のデバイスに対して同時に設定を行うことができます。スケジュールを定義することも可能です。
	ファームウェア管理	複数のデバイスのファームウェアを管理・アップグレードできます。
	サービス監視	プローブを介して、一般的なネットワークサービスの可用性と応答性を監視します。プローブは、ローカルおよびリモートの D-View8 ソフトウェアエージェントとして配備され、サーバやデバイスの接続性をチェックします。

メモ　D-View8 の最新情報については、弊社ホームページの D-View8 製品ページを参照してください。

メモ　管理デバイスの新機能やバグ修正を含む最新ファームウェア情報については、弊社ホームページの各製品ページを参照してください。

ライセンスの種類

D-View8 は、規模や利用機能に応じて 2 種類のライセンスを用意しています。

ライセンスタイプ	スタンダード（DV-800S）	エンタープライズ（DV-800E）
サポートノード数	最大 5,000 台	最大 5,000 台
サーバと Probe	1 サーバ、1Probe HA 未サポート	2 サーバ、20 Probe HA サポート
Probe タイプ	ローカルのみ	ローカル、リモート
組織	1 組織	1 組織
sFlow アナライザ	―	○
MIB ブラウザ / コンパイラ	―	○
REST API	―	○

※ Probe サーバ 1 台当たり最大 500 ノードまでとなります。

ライセンスの適用期間とサポートについて

最初にご購入いただくスタンダード版またはエンタープライズ版ライセンスには、1 年間のフリーメンテナンスサポートが付いています。フリーメンテナンスサポート期間（1 年間）が過ぎると、管理ノードは 30 台に制限されます。スタンダード版またはエンタープライズ版のメンテナンスサポート（上限管理数までの D-View8 機能サポートおよび製品サポート）を継続して利用するには、追加ライセンス（1 年 /2 年 /3 年 /4 年 /5 年のメンテナンスサポートから選択）をご購入いただく必要があります。スタンダード版ライセンスを適用している場合、別途アップグレードライセンスを購入いただくことで、エンタープライズ版へのアップグレードが可能です。

メモ　各ライセンスの詳細は、データシートをご確認ください。

メモ　D-View7 でご利用のリモート Probe を引き続き利用する場合は、D-View8 エンタープライズ版をご購入ください。これにより、リモート Probe の D-View8 へのアップグレードとメンテナンスが可能になります。

90 日間無料トライアル

D-View8 アプリケーションをダウンロードし、90 日間無料でお試しいただくことができます。最新のアプリケーションは D-Link Japan のホームページをご確認ください。

無料トライアルでは、「エンタープライズ」ライセンスと同等の機能を使用することが可能です。

ライセンスの適用について

トライアル期間終了後、アクティベーションの情報が表示されます。D-View8 を継続してご利用いただくにはライセンスを購入し、アクティベーションを行う必要があります。なお、90 日間トライアルをご利用いただいた後、同じコンピュータ上で再度トライアルをご利用いただくことはできません。

メモ　アクティベーション手順については、P.16 の「D-View8 サーバのインストール（Windows サーバ / スタンドアロン構成）」を参照してください。

システム要件

本製品が動作するには、以下のハードウェア要件を満たしている必要があります。

■ D-View8 サーバのシステム要件

ハードウェア条件	
CPU	Quad Core3.5GHz 以上
メモリ	16GB 以上
ハードディスク容量	200GB 以上
ソフトウェア条件	
OS	Windows10 Professional Edition 以上（64bit） Windows Server 2016 Standard Edition 以上（64bit） Windows Server 2019 Standard Edition 以上（64bit） Ubuntu 18.04 以上（64bit）※1 Debian 10 以上（64bit）※1
データベース	MongoDB 4.0 以上※2

※ 1 サポート予定
※ 2 既存の MongoDB を利用、もしくは D-View8 サーバのインストール時に新規で MongoDB をインストール

■ D-View8 リモート Probe のシステム要件

ハードウェア条件	
CPU	Dual Core3.0GHz 以上
メモリ	4GB 以上
ハードディスク容量	200GB 以上
ソフトウェア条件	
OS	Windows10 Professional Edition 以上（64bit） Windows Server 2016 Standard Edition 以上（64bit） Windows Server 2019 Standard Edition 以上（64bit） Ubuntu 18.04 以上（64bit）※1 Debian 10 以上（64bit）※1
管理キャパシティ	
管理ノード	最大 500

※ 1 サポート予定

■ D-View8 クライアントのシステム要件

クライアント条件	
CPU	Dual Core3.0GHz 以上
メモリ	4GB 以上
ハードディスク容量	100GB 以上
ブラウザ	Chrome、Firefox、Safari、Edge

ネットワーク管理システム

本アプリケーションは、ローカルエリアネットワーク（LAN）上の静的 IP アドレスを持つ D-View8 サーバで稼働し、ネットワーク上の D-Link 及びサードパーティ製デバイスを管理します。

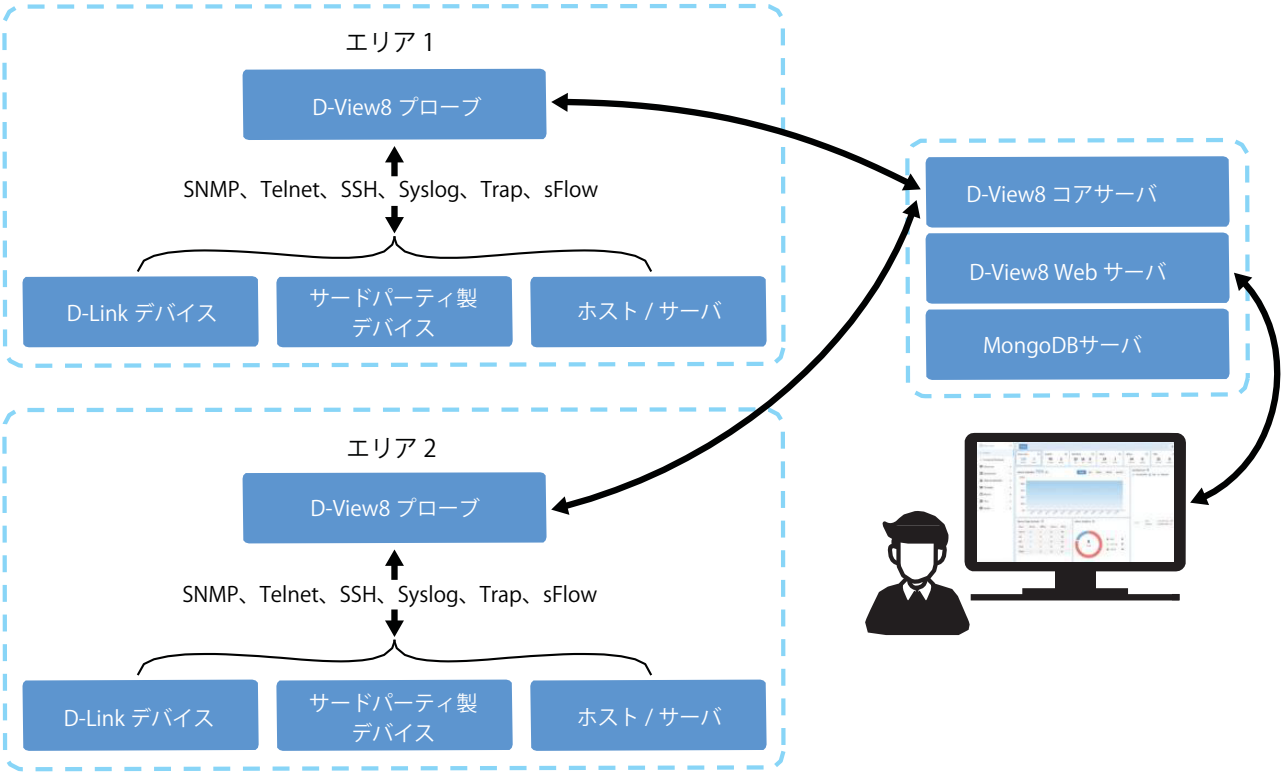


図 1-3　ネットワーク管理システム

D-View8 アプリケーションには、Web ブラウザを介してアクセスします。
サーバの IP アドレスにローカル接続できない場合は、最初にネットワークへのアクセスを許可する必要があります。

本アプリケーションは、以下のデバイスを検出、管理することができます。

- SNMP プロトコルをサポートする D-Link デバイス

サポートされる製品

以下の D-Link 製品について、D-View による管理がサポートされます。対応する H/W バージョン、F/W バージョンにご注意ください。

注意 D-View8 でサポートしている製品であっても、すべての機能を使用できるわけではありません。本マニュアルの各章やセクションに記載の注意書きをご確認ください。

■ スイッチ製品

シリーズ	製品名	H/W バージョン	F/W バージョンの最小要件
DXS-3610	DXS-3610-54T	A1	1.01.B031
	DXS-3610-54S	A1	1.01.B031
DXS-3400	DXS-3400-24TC	A1	3.00.B019
DGS-3630	DGS-3630-28TC	A1/A2	2.25.B025
	DGS-3630-28PC	A2	2.25.B025
	DGS-3630-28SC	A1/A2	2.25.B025
	DGS-3630-52TC	A1/A2	2.25.B025
	DGS-3630-52PC	A2	2.25.B025
DGS-1520	DGS-1520-28	A1	1.00.B037
	DGS-1520-28MP	A1	1.00.B037
	DGS-1520-52	A1	1.00.B037
	DGS-1520-52MP	A1	1.00.B037
DGS-3000	DGS-3000-10L	B1	4.00.B023
	DGS-3000-20L	B1	4.00.B023
	DGS-3000-28L	B1	4.00.B023
	DGS-3000-28X	B1	4.00.B023
	DGS-3000-28LP	B1	4.00.B023
	DGS-3000-28XMP	B1	4.00.B023
	DGS-3000-28XS	B1	4.00.B023
	DGS-3000-52L	B1	4.00.B023
	DGS-3000-52X	B1	4.00.B023
	DGS-3000-52X	B3	4.16.B007
DGS-1510	DGS-1510-20	A1	1.70.B015
	DGS-1510-28	A1	1.70.B015
	DGS-1510-28X	A1	1.70.B015
	DGS-1510-28P	A1	1.70.B015
	DGS-1510-28XMP	A1	1.70.B015
	DGS-1510-52	A1	1.70.B015
	DGS-1510-52X	A1/A2/A3	1.70.B015
DXS-1210	DXS-1210-10TS	B1	2.01.B012
	DXS-1210-12TC	B1	2.01.B012
	DXS-1210-12SC	B1	2.01.B012
	DXS-1210-28T	A1	1.00.B029
	DXS-1210-28S	A1	1.00.B029
DGS-1250	DGS-1250-28X	A1	2.03.B010
	DGS-1250-28XMP	A1	2.03.B010
	DGS-1250-52X	A1	2.03.B010
	DGS-1250-52XMP	A1	2.03.B010
DGS-1210	DGS-1210-10	F1	6.30.B022
	DGS-1210-10MP	F1	6.30.B022
	DGS-1210-10MP	F3	6.31.B038
	DGS-1210-20	F1	6.30.B022
	DGS-1210-28	F1/F2/F3	6.30.B022
	DGS-1210-28MP	F1/F2/F3/F4	6.30.B022
	DGS-1210-52	F1/F2/F3	6.30.B022
DMS-1100	DMS-1100-10TS	A1	1.10.017
	DMS-1100-10TP	A1	1.10.017

シリーズ	製品名	H/W バージョン	F/W バージョンの最小要件
DGS-1100V2	DGS-1100-05V2	A1	1.00.B006
	DGS-1100-05PDV2	A1	1.00.B006
	DGS-1100-08V2	A1	1.00.B006
	DGS-1100-08PV2	A1	1.00.B006
	DGS-1100-08PV2	A4	1.01.B005
DIS-200G	DIS-200G-12SW	A1	1.20.B012
	DIS-200G-12PSW	A1/A2	1.20.B012

■ **無線製品**

シリーズ	製品名	H/W バージョン	F/W バージョンの最小要件
DAP シリーズ	DAP-X2850	A1	1.10r027
	DAP-X2810	A1	1.20r032
	DAP-2610	A1	2.06B06r097
	DAP-2680	A1	2.00B08r051

デバイスグループによる管理

D-VView8 では、デバイスグループ機能を使用することでネットワーク管理（ファームウェアアップグレードなど）を簡素化することができます。管理者は、サイト、ネットワーク、場所、デバイスタイプなどでデバイスを分類し、グループ化して管理することができます。

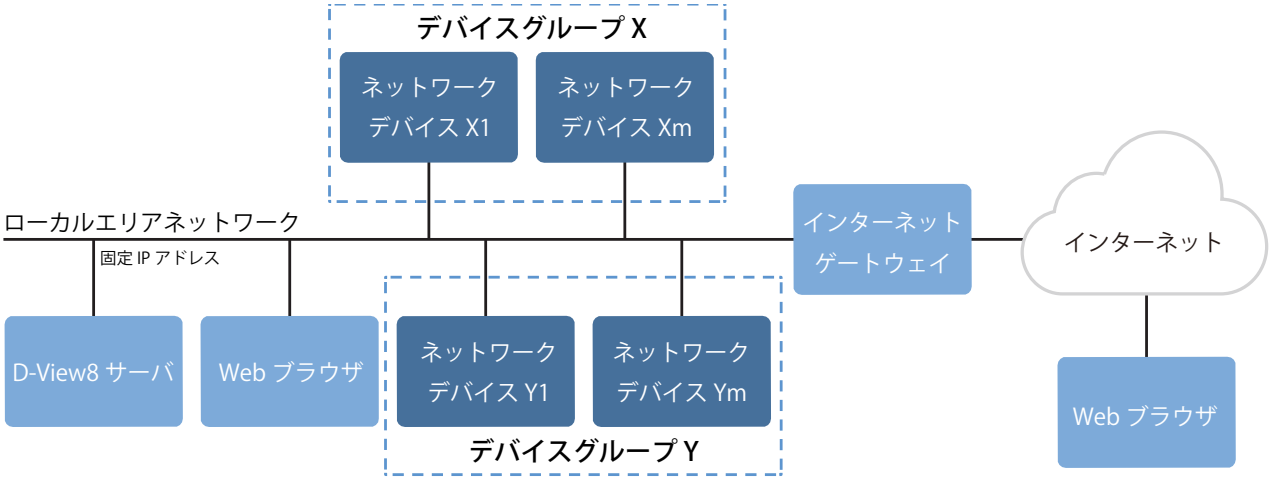


図 1-4　デバイスグループによる管理

D-View8 管理ユーザの認証の種類

D-View8 アプリケーションでは、認証プロファイルをユーザに関連付けることで、特定のネットワークにのみユーザがアクセスできるように権限を付与することができます。サポートされる認証は以下の 3 種類です。

- ローカル：ローカルシステムで認証されるユーザアカウント。
- RADIUS：RADIUS（Remote Authentication Dial-In User Service）によって認証されるユーザアカウント。
- Active Directory：Microsoft 管理コンソールによって認証されるユーザアカウント。

ネットワークデバイス検出の準備

ネットワーク上のデバイスを適切に管理するためのセットアップを行います。

ネットワーク検出対象のデバイスについて、以下の設定を確認してください。
- SNMP が有効であり、コミュニティ名および関連する読み取り / 書き込み権限が設定されていること。
- ネットワーク上のデバイスに有効な IPv4 アドレスが設定されていること。

D-View8 による管理の開始

D-View8 コンポーネントのインストール、および基本的なシステム設定とデバイス検出手順については、以下の章を参照してください。

- 「第 2 章　製品のインストール」
- 「第 3 章　D-View8 の利用を開始する」

第 2 章　製品のインストール

D-View8 ソフトウェアは、Windows または Linux※オペレーティングシステムへのインストールをサポートしています。
※サポート予定

本章では、以下のトピックについて説明します。

- 「インストール要件」
- 「D-View8 サーバのインストール（Windows サーバ / スタンドアロン構成）」
- 「D-View8 サーバのインストール（Windows サーバ / クラスタ構成）※エンタープライズ版のみ」
- 「D-View8 プローブのインストール（Windows サーバ）」
- 「（参考）D-View8 サーバのインストール（Linux サーバ / スタンドアロン構成）」
- 「（参考）D-View8 サーバのインストール（Linux サーバ / クラスタ構成）※エンタープライズ版のみ」
- 「（参考）D-View8 プローブのインストール（Linux サーバ）」
- 「D-View8 ソフトウェアのアップグレード」
- 「D-View8 ソフトウェアのアンインストール」
- 「D-View7 から D-View8 へのソフトウェアの移行」

インストール要件

D-View8 をインストールするためのハードウェアおよびソフトウェア要件は、P.11 の「システム要件」を参照してください。

D-View8 サーバのインストール（Windows サーバ / スタンドアロン構成）

1. D-Link Japan のサイトから D-View8 インストールパッケージをダウンロードします。
2. D-View8 のインストーラをダブルクリックし、セットアップウィザードを開始します。
   「Next >」をクリックします。

図 2-1　　セットアップウィザードの開始

3. 使用許諾画面が表示されます。
「I Agree」をクリックし、使用許諾に同意します。

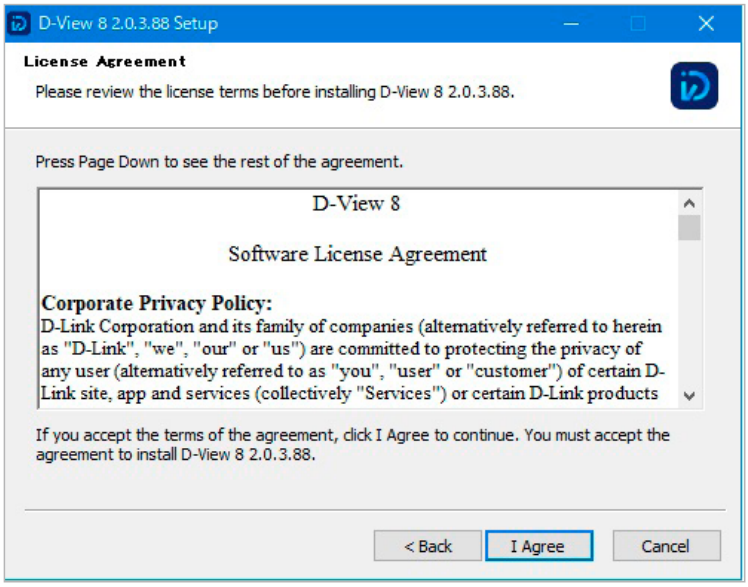


図 2-2　使用許諾への同意

4. D-View8 のインストールディレクトリを指定します。
「Next >」をクリックします。

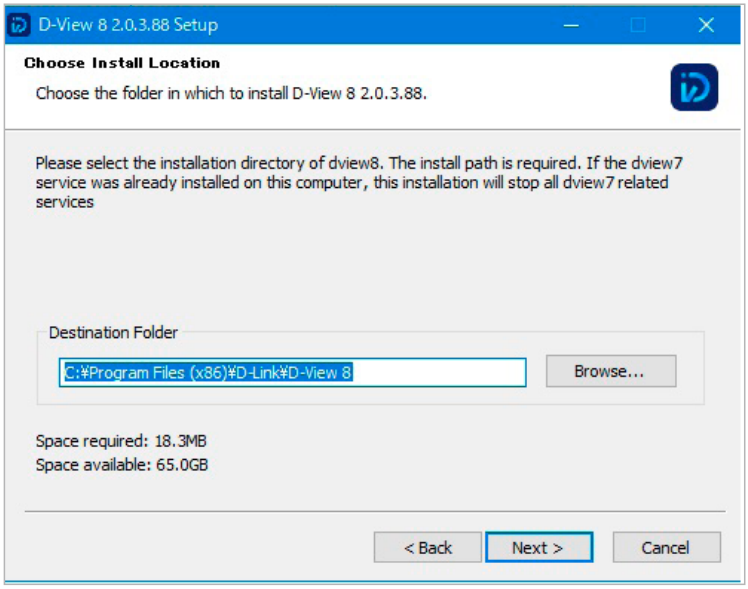


図 2-3　インストールディレクトリの選択

5. 以下の項目を確認、設定し、「Next >」をクリックします。

- 「MongoDB Type」：ここでは「Standalone（スタンドアロン）」を選択します。
- 「Server IP」：サーバのローカル IP アドレスを選択します。
- 「Check」：サービスポートが利用可能かどうかをテストします。緑色の「Check Pass!」メッセージが表示された場合、ポートが利用可能です。

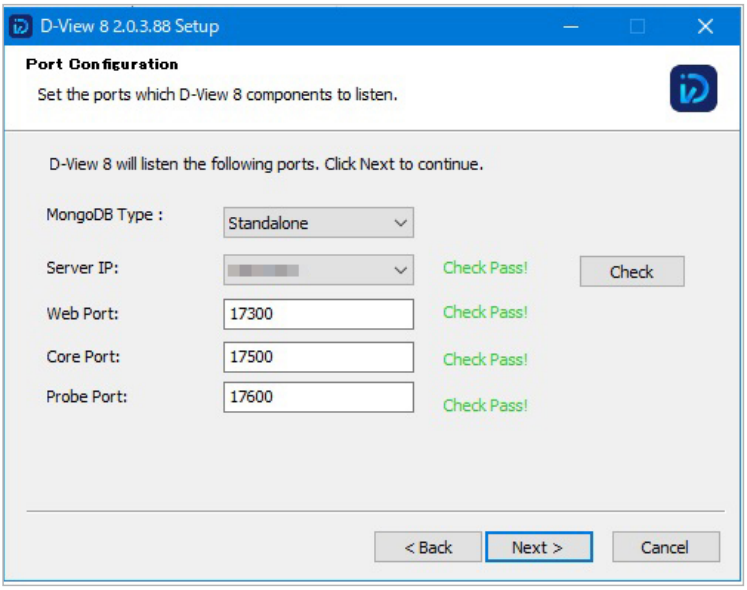


図 2-4　　ポート構成

6. D-View8 を使用するには、MongoDB をインストールする必要があります。新規にインストールするか、既存のデータベースを利用することができます。以下のいずれかのオプションを選択し、「Next >」をクリックします。

- 「Install a new MongoDB」：新規の MongoDB サービスをインストールします。
- 「Use an existing MongoDB」：既存の MongoDB を利用します。

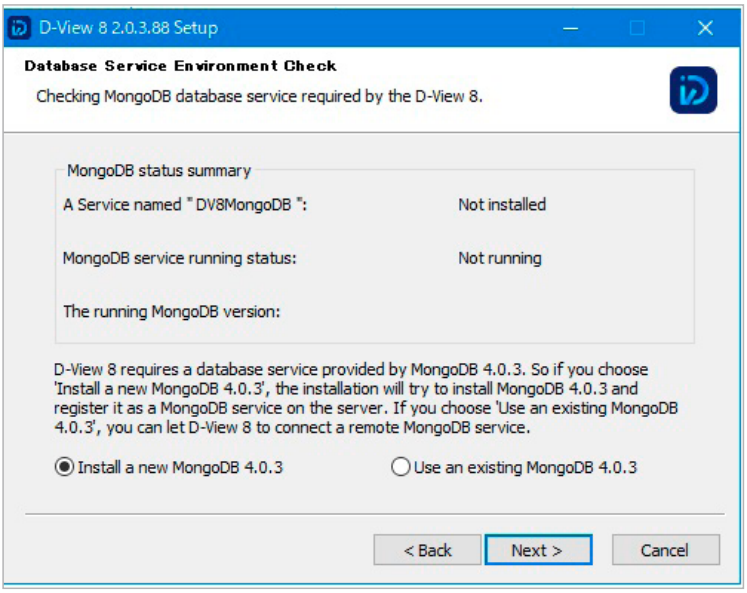


図 2-5　　データベースサービスのステータス確認

7. MongoDB の設定を行います。

新規で MongoDB サービスをインストールする場合：

(1) 「MongoDB Port」欄に、データベースへのアクセス用ポートを入力します。
(2) データベース認証用のユーザ名とパスワードを入力します。
(3) 「Next >」をクリックします。

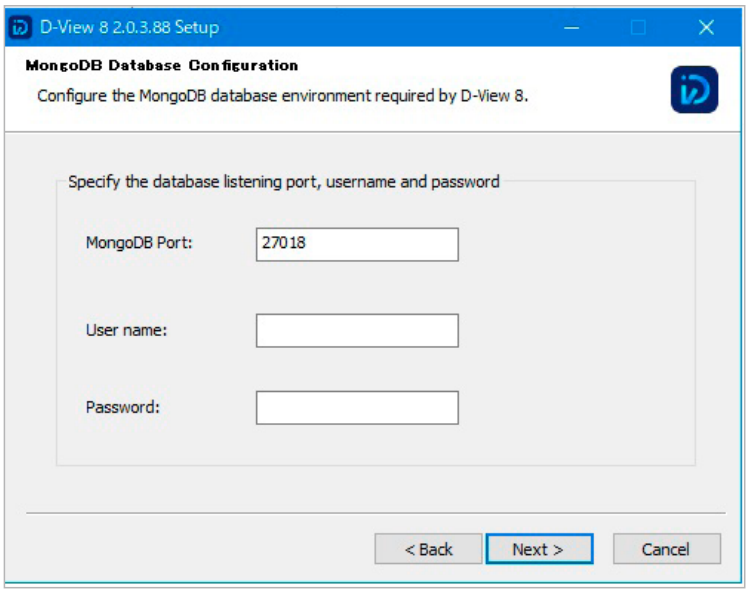


図 2-6　MongoDB データベース構成（新規インストール）

既存の MongoDB サービスを利用する場合：

(1) 「MongoDB Address」欄に、データベースのアドレスとポートを入力します。
(2) データベースへのアクセスにユーザ名とパスワードが必要な場合は、「Password Authentication」にチェックを入れます。
(3) データベースにアクセスする権限を持つアカウントのユーザ名とパスワードを入力します。
(4) 「Check Connection」をクリックして、接続をテストします。
入力が完了すると、「Next >」ボタンが有効になります。
接続チェックが失敗する場合は、設定内容を見直してください。
(5) 「Next >」をクリックします。

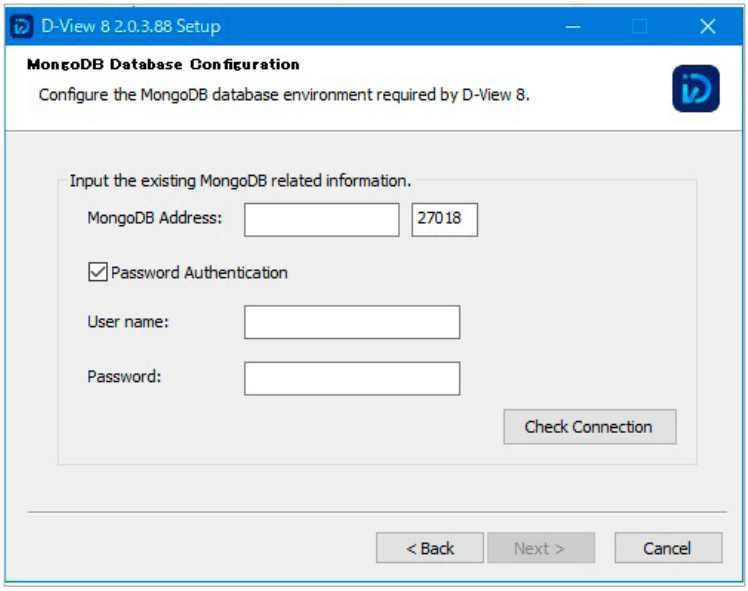


図 2-7　データベース構成（既存データベース使用）

8. D-View8 のインストールが開始され、進捗状況が表示されます。

9. インストール完了後、「Next >」をクリックします。

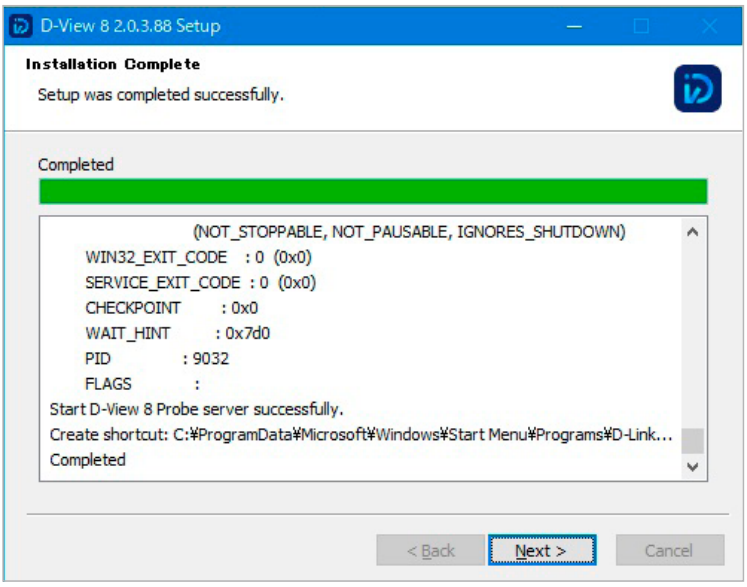


図 2-8　　インストール完了

10. 「Launch D-View8」にチェックを入れたまま「Finish」をクリックし、セットアップウィザードを終了します。

図 2-9　　セットアップウィザードの終了

セットアップウィザードが終了すると、Web ブラウザが起動し D-View8 のログイン画面が表示されます。

11. ユーザ名 /Email アドレスとパスワードを入力し、「Sign in」をクリックします。初期値は以下のとおりです。
- 「Username or email」初期値 : admin
- 「Password」初期値 : admin

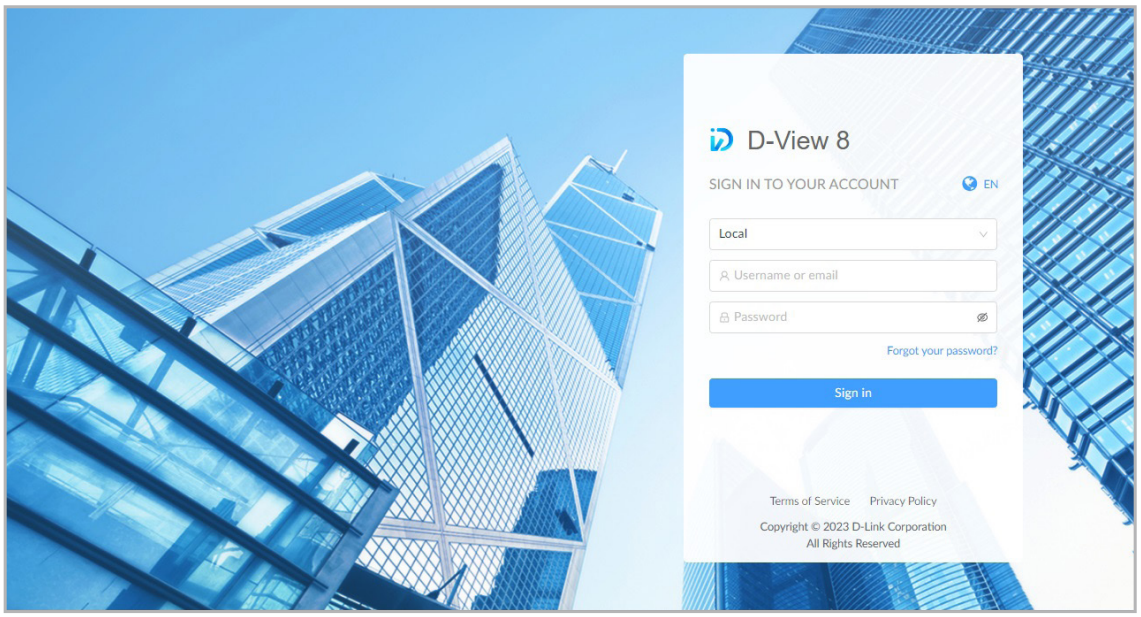


図 2-10　サインイン画面

デフォルトでは、「Account Type」フィールドに「Local」と表示されます。
初回ログイン時に、ライセンスのアクティベーションコードを入力するか、試用（Trial）アカウントを使用するかを選択できます。

12. 「Choose Activation Mode（アクティベーションモードの選択）」画面で、ライセンスのアクティベーション方法を選択するか、「Start Trial」をクリックして試用ライセンスをアクティブ化します。

- 「Online Activation（オンラインアクティベーション）」: 本製品をアクティブ化するためのライセンスキーを入力します。この機能でライセンスを認証するには、サーバがインターネットに接続されている必要があります。
- 「Offline Activation（オフラインアクティベーション）」: 提供されているアクティベーションファイルを使用して、本製品をアクティブ化します。サーバがインターネットに接続されていないときに利用できます。
- 「Start Trial」: アプリケーションの 90 日間の試用バージョンを試します。

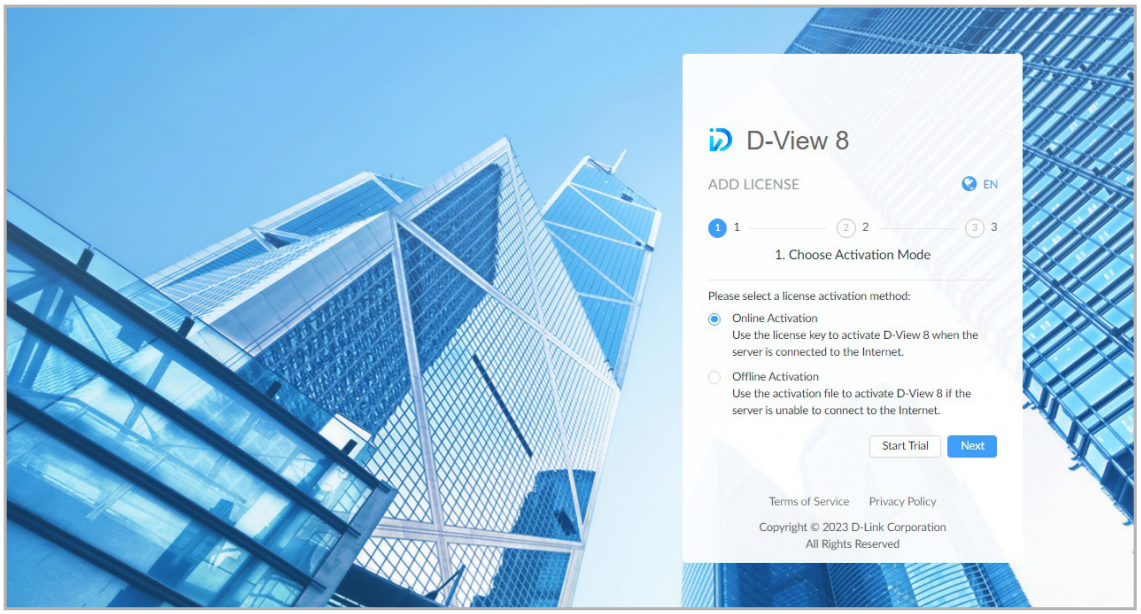


図 2-11　アクティベーションモードの選択

13. 「Next」をクリックして先へ進みます。

14. オンラインアクティベーションの場合はライセンスキーを入力します。
オフラインアクティベーションの場合はアクティベーションファイルをアップロードします。

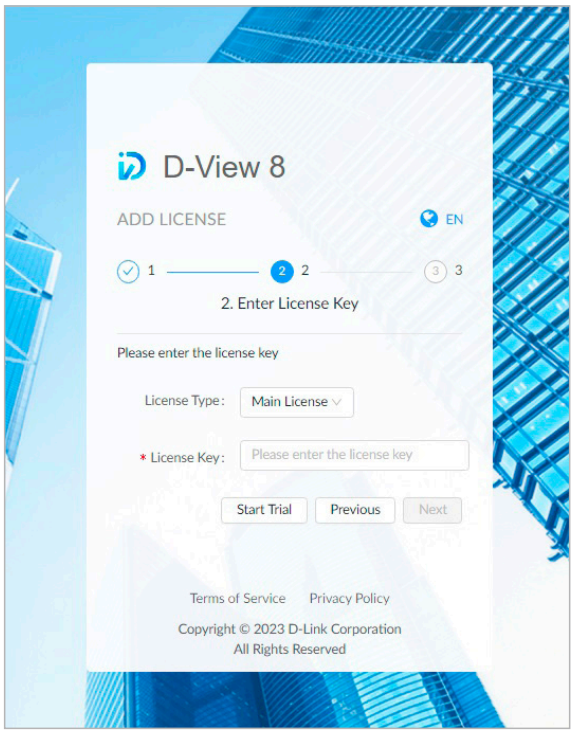


図 2-12　オンラインアクティベーション

図 2-13　オフラインアクティベーション

15. 「Next」をクリックします。

16. 「Home」をクリックします。

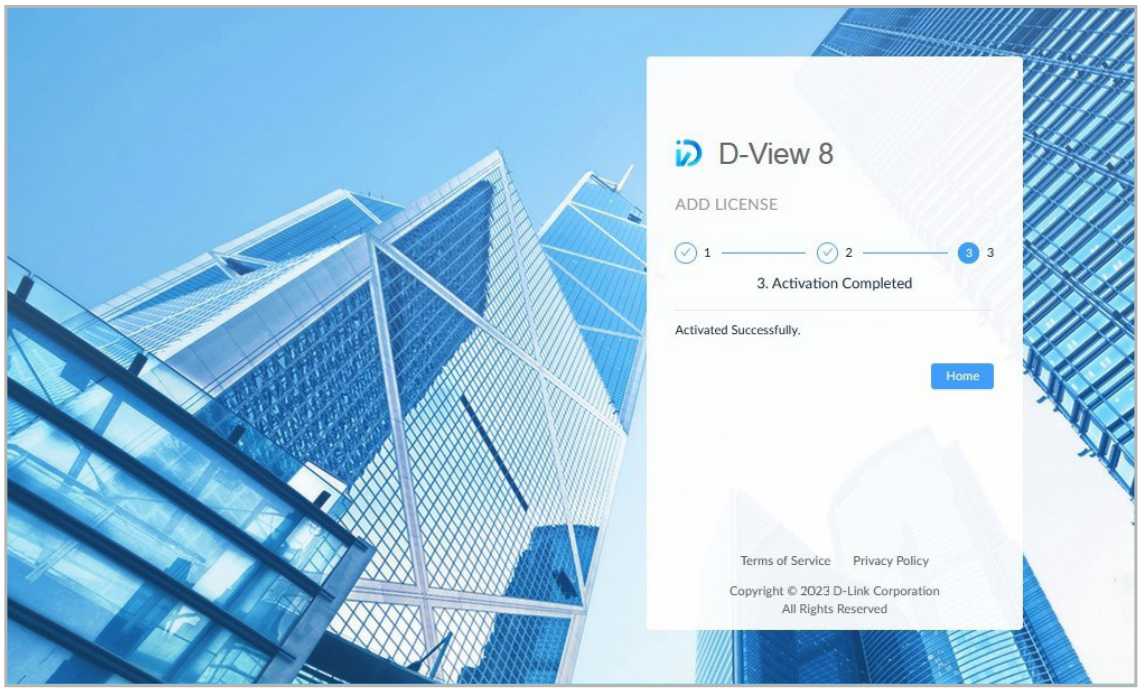


図 2-14　アクティベーションの完了

17. パスワードの変更画面が表示されます。新しいパスワードを 2 回入力し、「Set and Sign In」をクリックします。

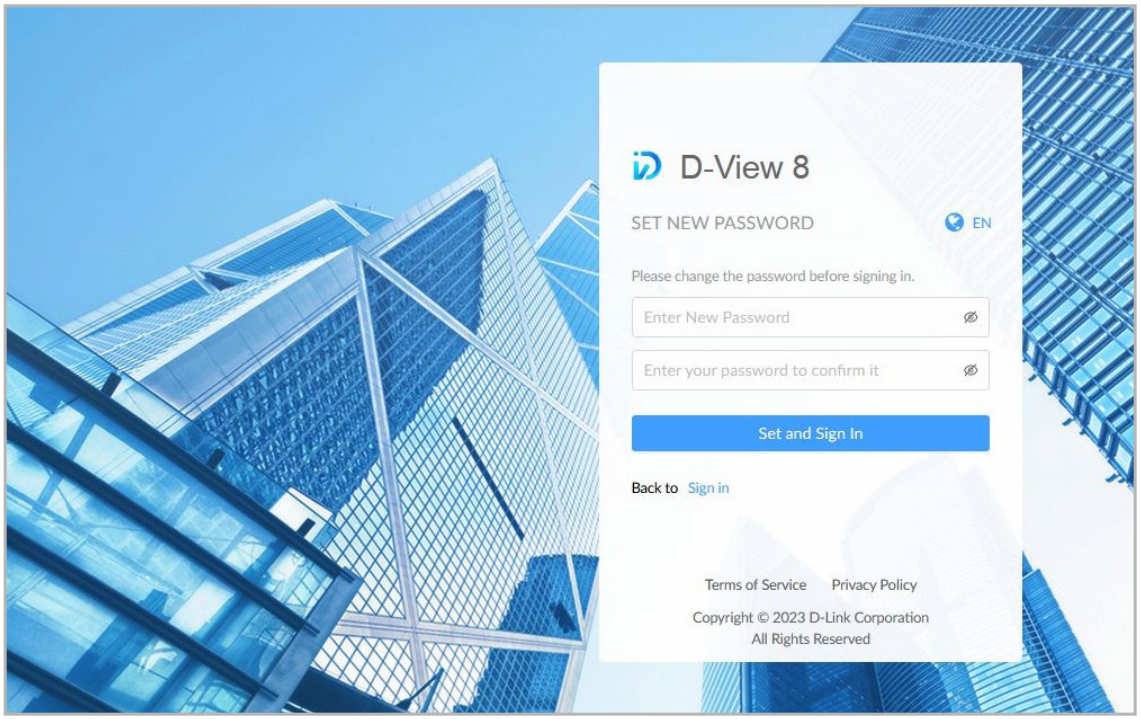


図 2-15　パスワードの変更

18. 初回ログイン時には、設定ウィザードが表示されます。

- 「D-View7 Upgrade」: このオプションを使用すると、D-View7 データベースとプローブを現在のアプリケーションに移行できます。
- 「Discovery」: このオプションでは、ネットワークおよびデバイスの検出を行うことができます。
- 「Monitoring」: このオプションでは、トポロジ / ラックシミュレーション / ダッシュボードを作成して、ネットワークのモニタリングに役立てることができます。
- 「Alarm」: このオプションでは、通知とアラームを設定できます。

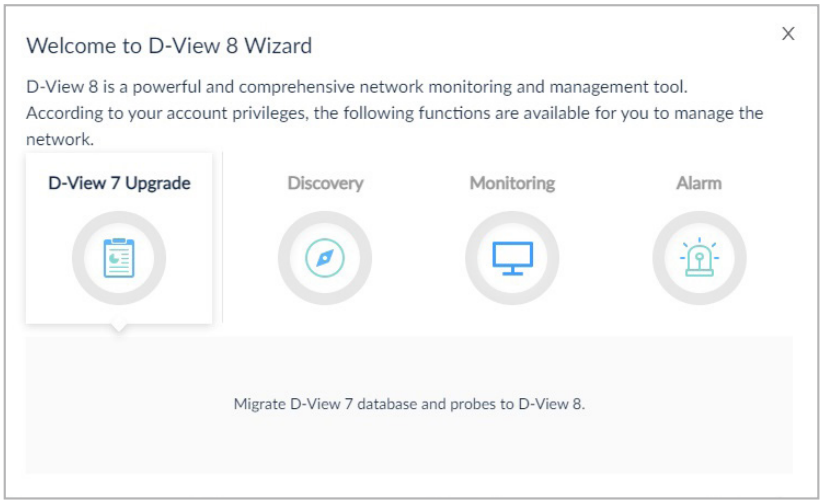


図 2-16　D-View8 ウィザードの開始

19. いずれかのカテゴリを選択すると、最初に国および組織の設定が表示されます。ウィザードに従って設定を行います。

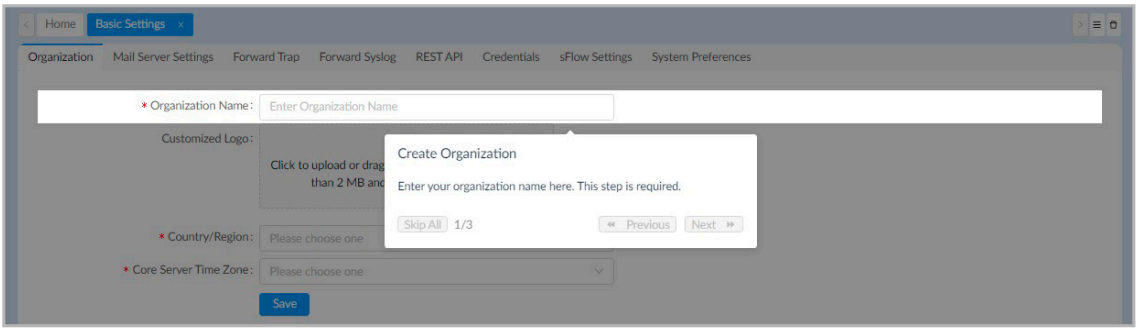


図 2-17　Wizard

メモ　国と組織以外の設定はスキップ可能です。ネットワーク検出を適切に実行するためには、組織の設定が必要です。

セットアップが完了すると、D-View8 が使用できるようになります。

D-View8 サーバのインストール（Windows サーバ / クラスタ構成）※エンタープライズ版のみ

クラスタアーキテクチャ

D-View8 は、冗長性とロードバランシング機能をサポートしています。

次の図は、クラスタアーキテクチャの説明図です。

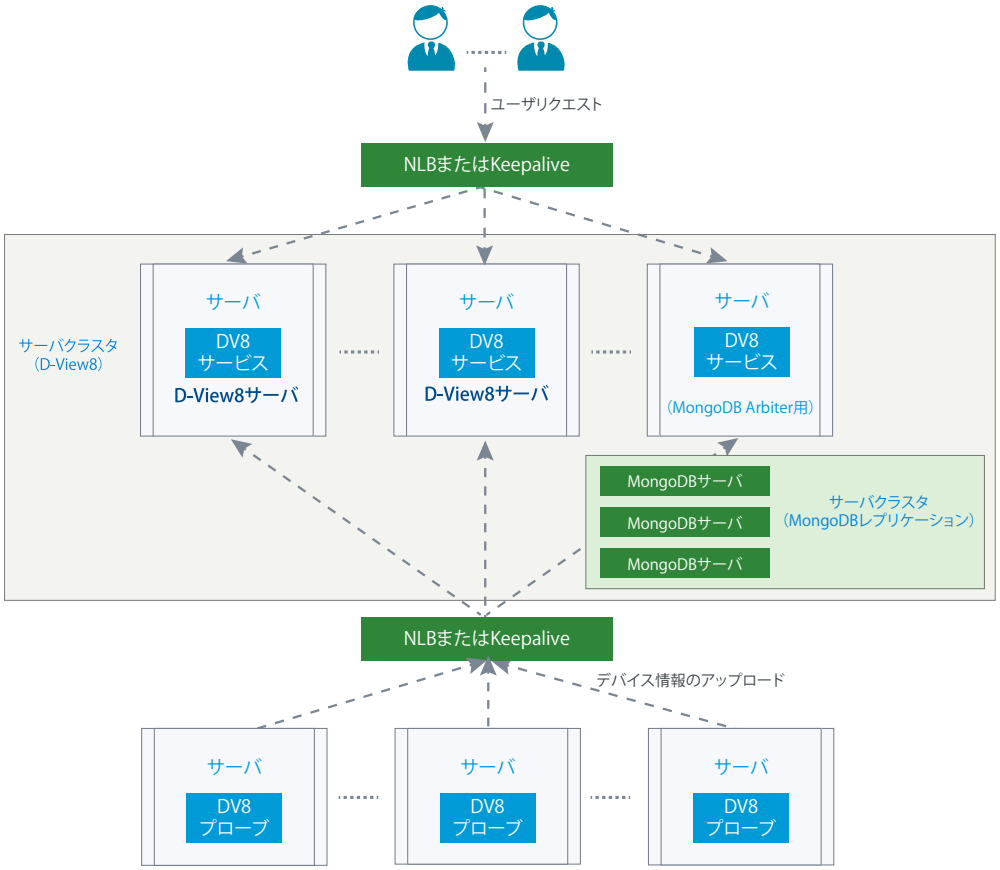


図 2-18　クラスタアーキテクチャ

次の図は、D-View8 と MongoDB のストラクチャ（構造）を示しています。ストラクチャには、プライマリ、セカンダリ、およびアービターが含まれます。D-View8 アプリケーションはプライマリとセカンダリデータベースに接続します。セカンダリデータベースがプライマリに選出され、プライマリデータベースがセカンダリに降格する場合もあります。デフォルトでは、クライアントはプライマリから読み取りを行いますが、セカンダリデータベースからの読み取りを許可する設定にすることもできます。

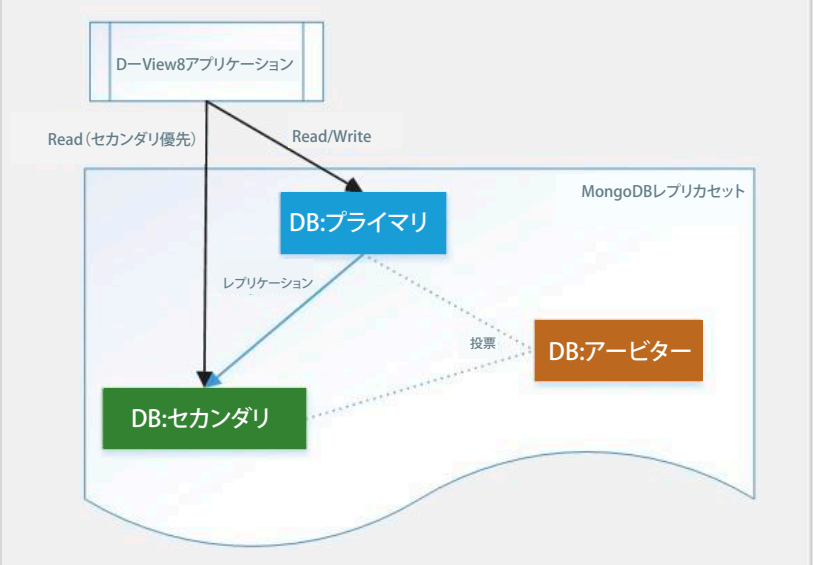


図 2-19　MongoDB ストラクチャ

クラスタの構築手順（概要）

クラスタ構築手順を以下の概略図で示します。

データ冗長性のサポート：

1. 3 台の Windows サーバを用意し、MongoDB をインストールします。

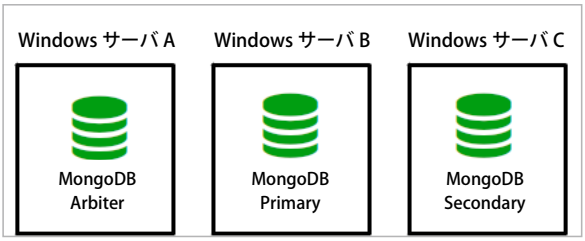


図 2-20　複数サーバの準備

2. 追加のサーバに D-View8 をインストールし、当該アプリケーションを MongoDB クラスタに接続します。

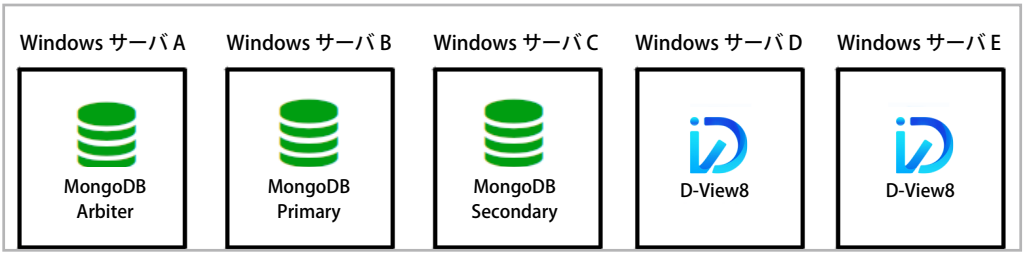


図 2-21　MongoDB クラスタへの接続

サーバ負荷分散のサポート：

3. Windows サーバに NLB をインストールします。

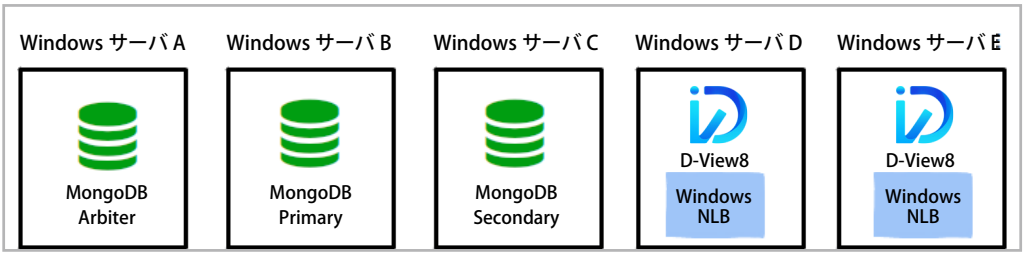


図 2-22　NLB のインストール

メモ　プライマリ / セカンダリデータベースとして設定したサーバに D-View8 をインストールすることもできます。サーバ 3 台構成については、次ページ以降の図と手順を参照してください。

4. 追加のデバイスを管理するには、追加サーバにプローブをインストールし、NLB による負荷分散が設定された D-View8 サーバに接続します。

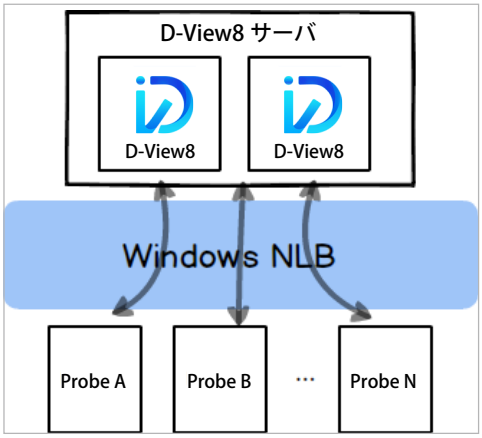


図 2-23　NLB アーキテクチャ

クラスタ構築手順

クラスタ構築手順について説明します。

- 「データ冗長性のサポート：MongoDB クラスタの構成」
- 「データ冗長性のサポート：複数サーバへの D-View8 インストール」
- 「サーバ C での NLB 管理」

メモ　本セクションでは、Windows サーバを 3 台使用したクラスタ構成の設定手順について説明しています。MongoDB レプリカセットのうち、2 台のサーバに D-View8 server サービスをインストールします。

メモ　Windows サーバを 5 台使用した場合のインストール手順については、P.255 の「付録 A：クラスタ構成のインストールシナリオ（Windows サーバ 5 台構成）」を参照してください。

Windows サーバ構成例

項目	サーバ A	サーバ B	サーバ C
IP アドレス	192.168.1.203	192.168.1.201	192.168.1.202
OS ※	Windows 10 Windows Server 2016 Windows Server 2019	Windows Server 2016 Windows Server 2019	Windows Server 2016 Windows Server 2019
MongoDB レプリカセット役割	Arbiter	Primary	Secondary
NLB 設定	—	仮想 IP：192.168.1.200	仮想 IP：192.168.1.200

※いずれかの OS を想定

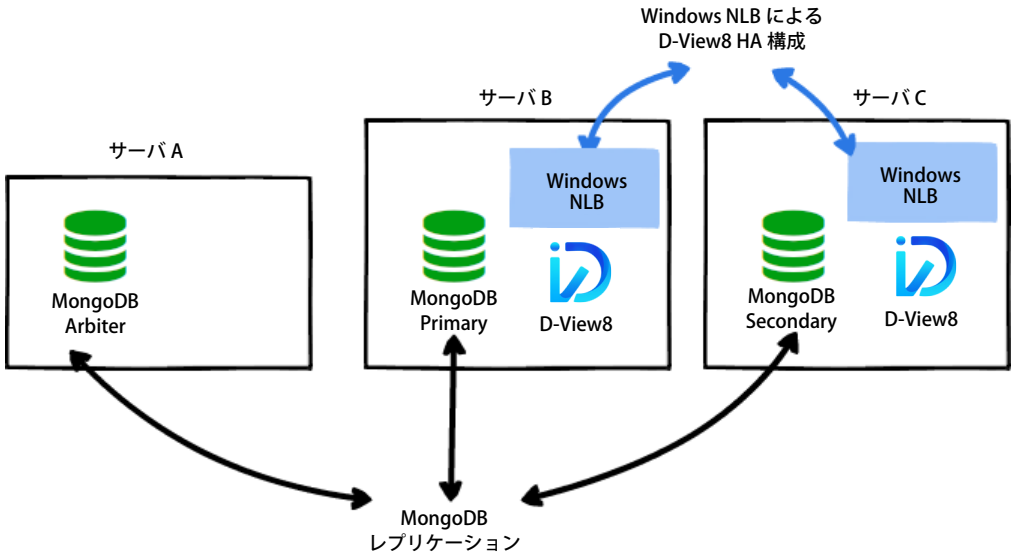


図 2-24　クラスタ構成図

データ冗長性のサポート：MongoDB クラスタの構成

以下の手順に従い、サーバ A、サーバ B、サーバ C にそれぞれ MongoDB をインストールします。

1. D-Link Japan のサイトから D-View8 MongoDB インストールパッケージをダウンロードします。
2. D-View8 MongoDB のインストーラをダブルクリックし、セットアップウィザードを開始します。
「Next >」をクリックします。

図 2-25　セットアップウィザードの開始

3. 使用許諾画面が表示されます。
「I Agree」をクリックし、使用許諾に同意します。

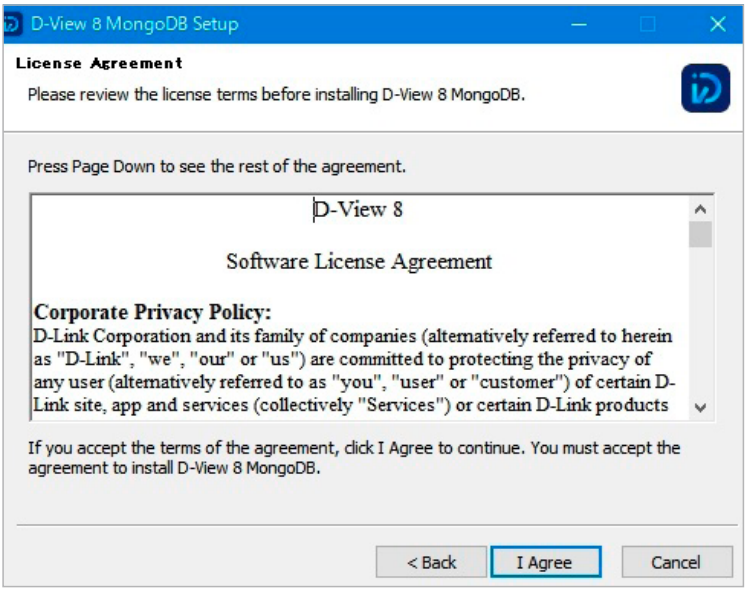


図 2-26　使用許諾への同意

4. 「Connection Configuration」画面で、MongoDB の設定を行います。

(1) 以下のパラメータを設定します。
- 「MongoDB Type」:「Replication」を選択します。
- 「MongoDB」: サーバ接続用に設定される MongoDB ポート番号を入力します。

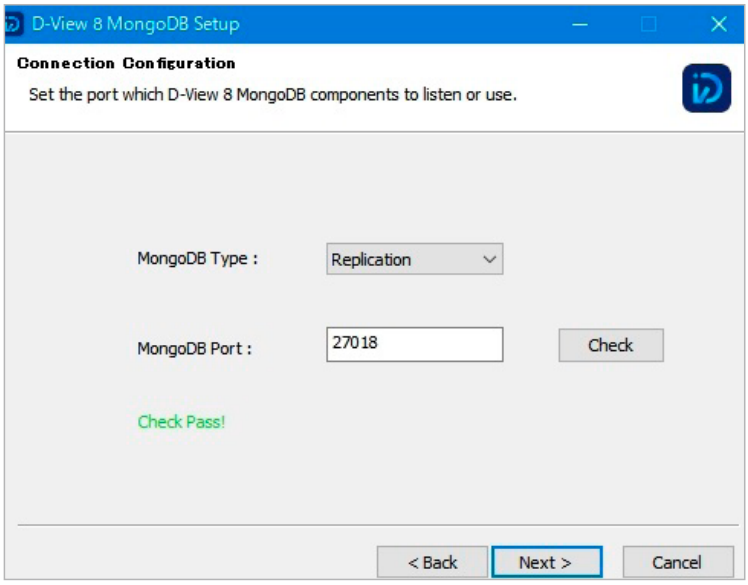


図 2-27　接続設定（MongoDB タイプの設定）

(2) 設定をテストするには、「Check」をクリックします。
正しく設定されている場合は、「Check Pass!」が表示されます。テストが失敗した場合は、ポート設定を見直してください。

(3) 「Next >」をクリックして先へ進みます。

5. インストールディレクトリを指定し、「Install」をクリックします。

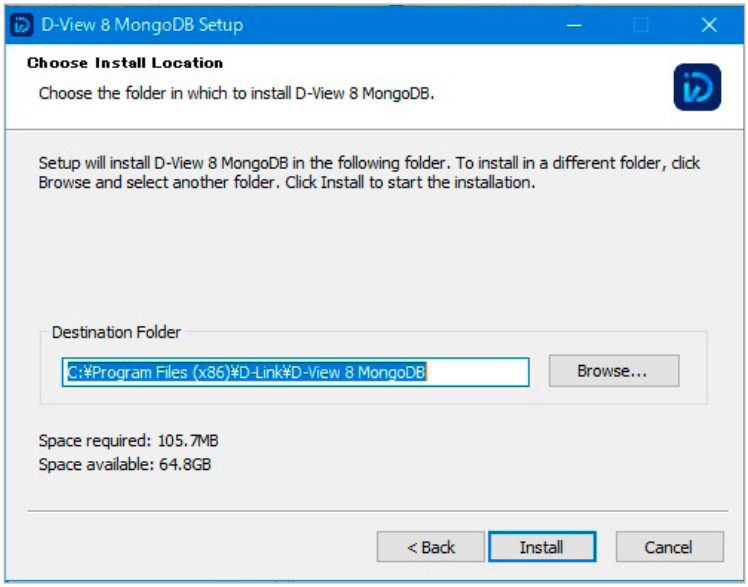


図 2-28　インストールディレクトリの選択

6. D-View8 MongoDB のインストールが開始され、進捗状況が表示されます。

7. インストール完了後、「Close」をクリックします。

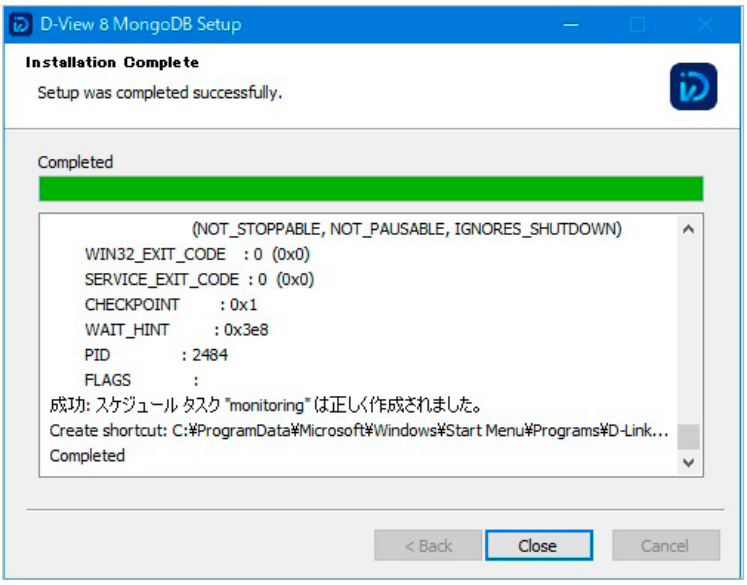


図 2-29　インストール完了

データ冗長性のサポート：複数サーバへの D-View8 インストール

以下の手順に従い、サーバ B、サーバ C にそれぞれ D-View8 アプリケーションをインストールし、それらを MongoDB クラスタに接続します。

1. D-Link Japan のサイトから D-View8 インストールパッケージをダウンロードします。
2. D-View8 のインストーラをダブルクリックし、セットアップウィザードを開始します。
「Next >」をクリックします。

図 2-30　セットアップウィザードの開始

3. 使用許諾画面が表示されます。
「I Agree」をクリックし、使用許諾に同意します。

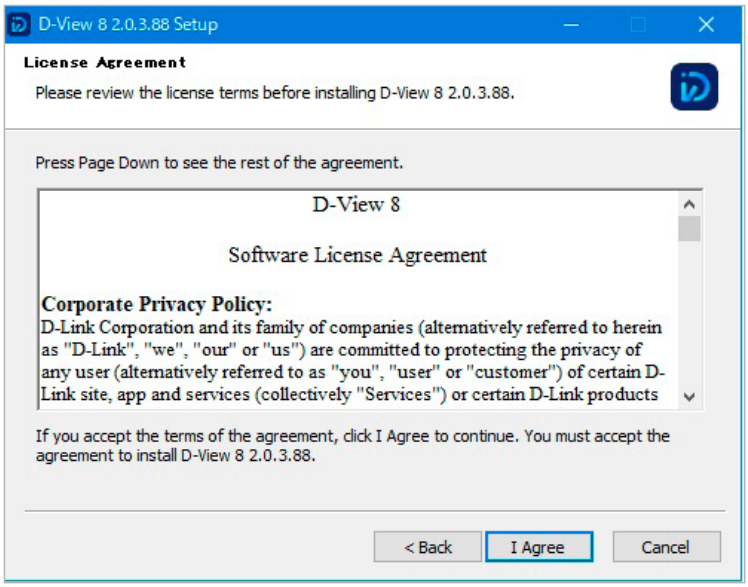


図 2-31　使用許諾への同意

4. D-View8 のインストールディレクトリを指定します。
「Next >」をクリックします。

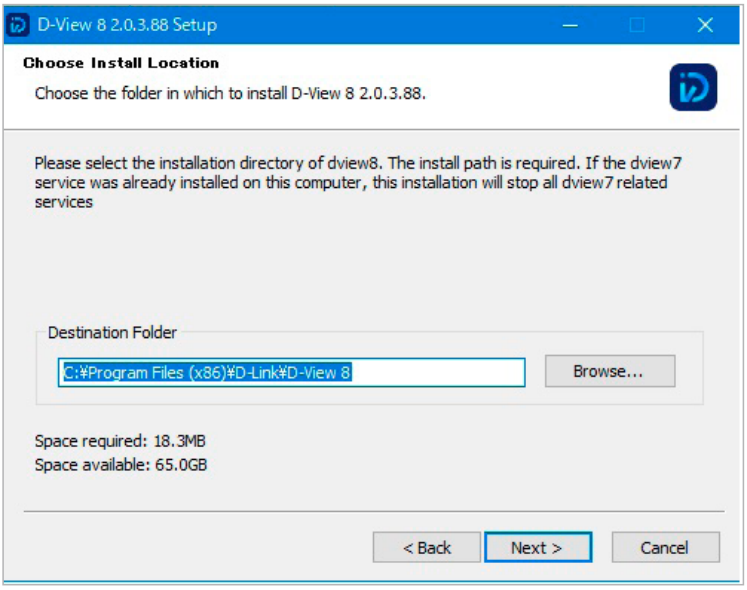


図 2-32　インストールディレクトリの選択

5. 「Connection Configuration」画面で、MongoDB の設定を行います。

(1) 以下のパラメータを設定します。
- 「MongoDB Type」:「Replication」を選択します。
- 「Server IP」:当該サーバの IP アドレスを入力します。
- 「Web Port」:Web アクセス用のポート番号を入力します。
- 「Core Port」:コアサーバのポート番号を入力します。
- 「Probe Port」:プローブ接続用のポート番号を入力します。

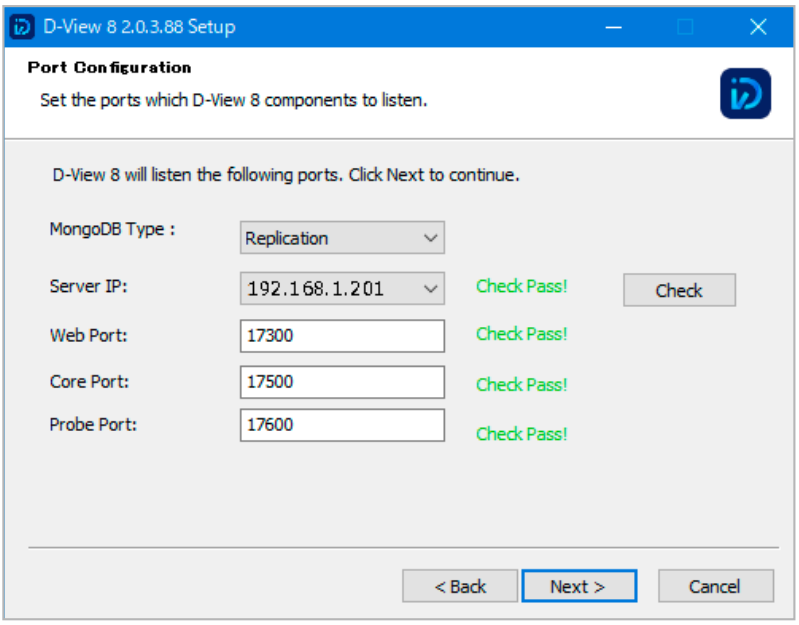


図 2-33　ポート構成（サーバ B の例）

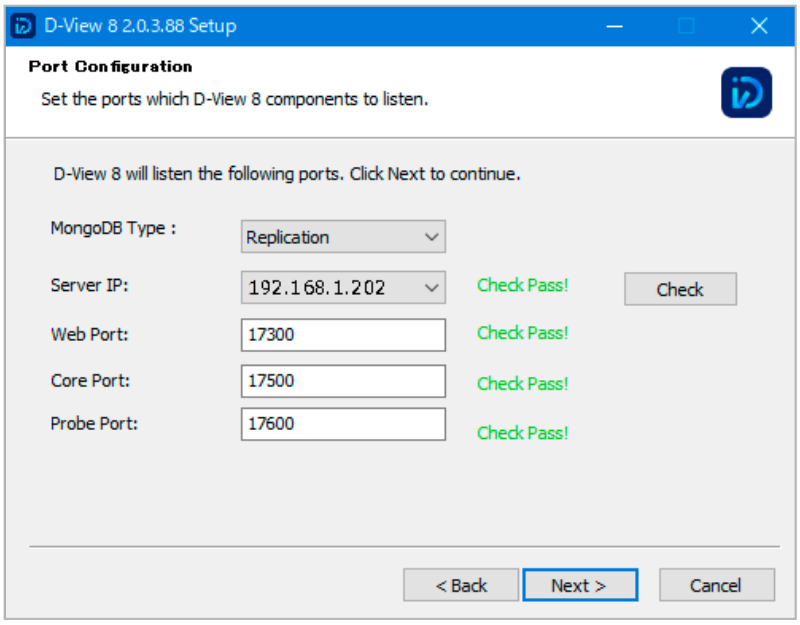


図 2-34　ポート構成（サーバ C の例）

(2)　設定をテストするには、「Check」をクリックします。
正しく設定されている場合は、「Check Pass!」が表示されます。テストが失敗した場合は、設定内容を見直してください。

(3)　「Next >」をクリックして先へ進みます。

6.　「MongoDB Database Configuration」画面で、MongoDB レプリカセットとの接続設定を行います。

(1)　以下のパラメータを設定します。
- 「Primary/Secondary/Arbiter」：MongoDB レプリカセットとなる各サーバの IP アドレスとポート番号を入力します。

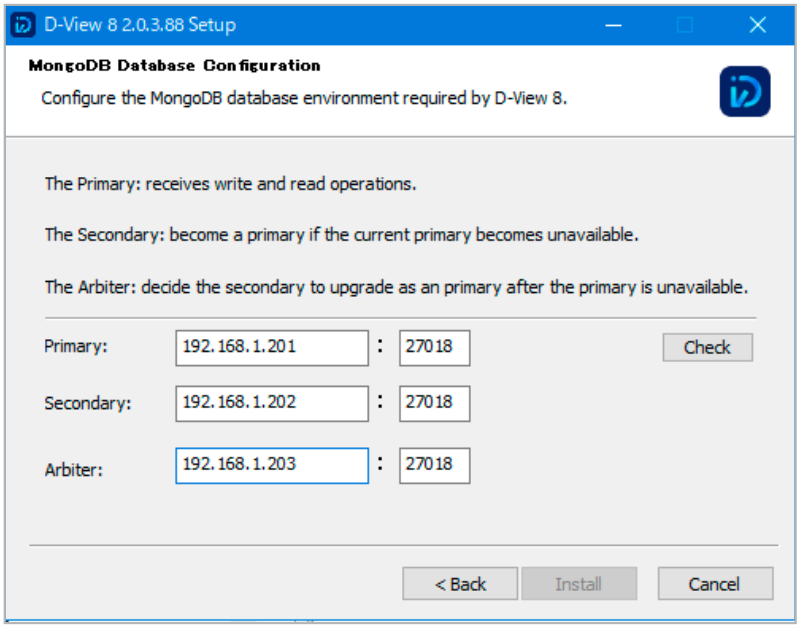


図 2-35　MongoDB 設定

(2)　設定をテストするには、「Check」をクリックします。
正しく設定されている場合は、「Check Pass!」が表示されます。テストが失敗した場合は、設定内容を見直してください。

(3)　「Install」をクリックしてインストールを開始します。

7.　「Finish」をクリックし、セットアップウィザードを終了します。

以上の設定により、Web ブラウザから D-View8 サーバにアクセスできるようになります。

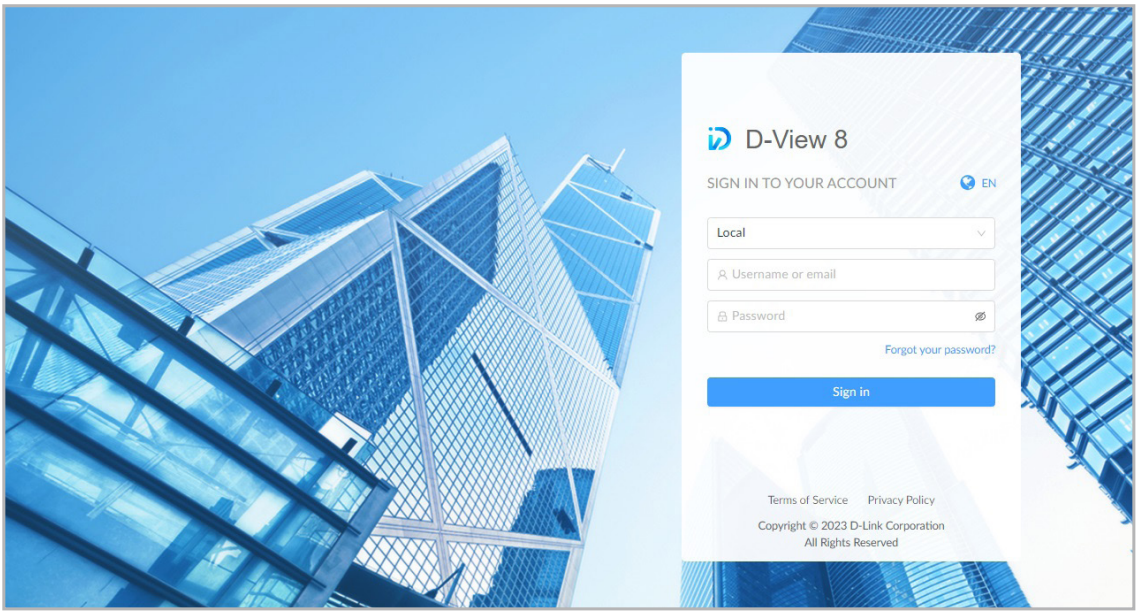


図 2-36　D-View8 ログイン画面

サーバ負荷分散のサポート：NLB のインストール

本アプリケーションでは、サーバのロードバランシング（負荷分散）がサポートされています。
同じサブネット内で 2 台のサーバを負荷分散用に構成します。本セクションでは、3 台のサーバ構成のうち、2 台の D-View8 サーバ上で NLB を設定する手順を説明します。

1. サーバ B とサーバ C に、Windows のサーバーマネージャーから「ネットワーク負荷分散マネージャー」をインストールします。

■ NLB の設定（サーバ B）

2. 「ネットワーク負荷分散クラスター」を右クリックして、「新しいクラスター」を選択します。

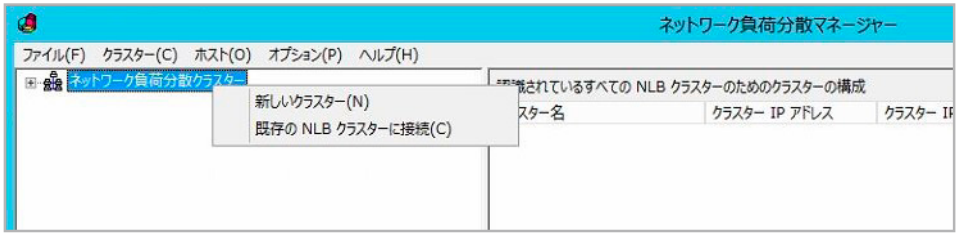


図 2-37　ネットワーク負荷分散マネージャー

3. 「新しいクラスター：接続」画面で、以下の設定を行います。
「ホスト」にサーバ B の IP アドレス（例：192.168.1.201）」を入力し、「接続」をクリックします。

図 2-38　新しいクラスタ接続のセットアップ

4. 「新しいクラスター：ホスト パラメーター」画面で、「次へ >」をクリックして先へ進みます。

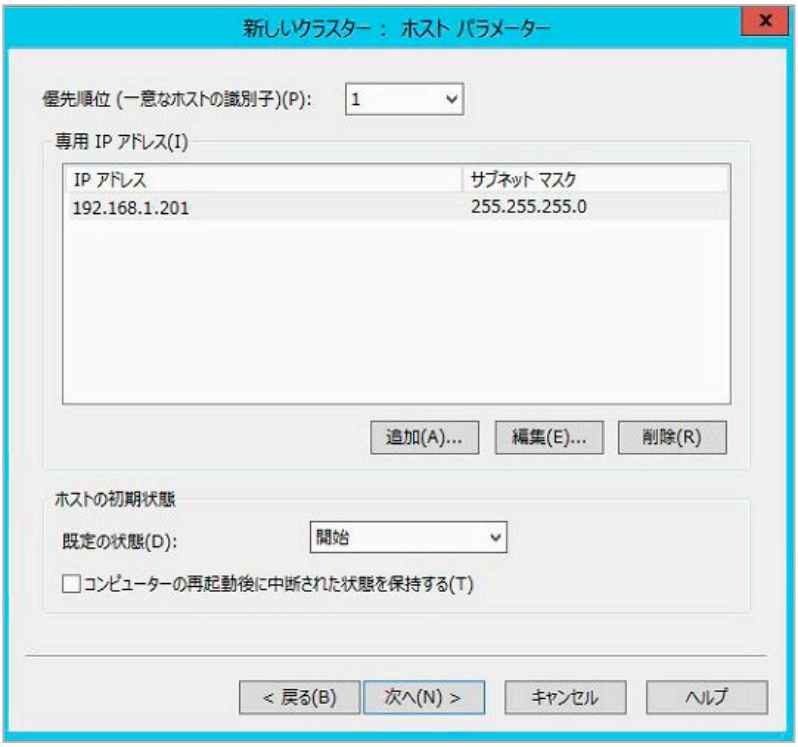


図 2-39　ホストパラメーターの設定

5. 「新しいクラスター：クラスター IP アドレス」画面で、「追加 ...」ボタンをクリックします。
「IP アドレスの追加」画面で、クラスタ IP およびネットマスクとして使用する仮想 IP アドレスとネットマスクを入力します。

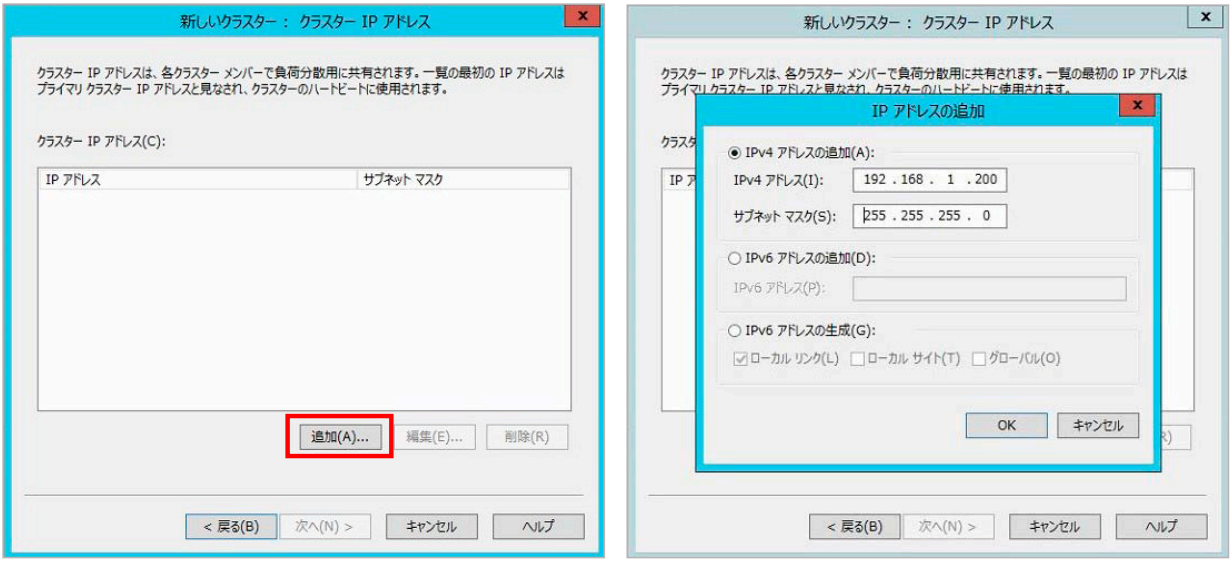


図 2-40　クラスタ IP の設定

6. 「新しいクラスター：クラスター パラメーター」画面で、以下の設定を行い「次へ >」をクリックします。
   - 「クラスタ操作モード」:「マルチキャスト」を選択し、パフォーマンスを最適化します。

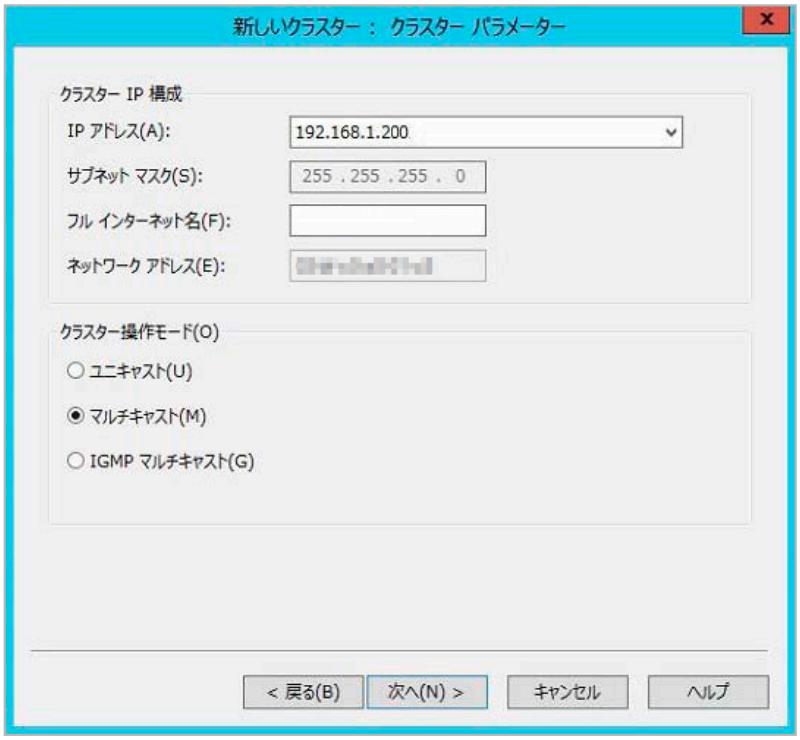


図 2-41　クラスターパラメータの設定

7. 「新しいクラスター：ポートの規則」で定義済みのポートの規則を選択し、「編集 ...」をクリックします。
   「ポートの規則の追加と編集」画面で、「フィルターのモード」に「複数ホスト」を選択し、「アフィニティ」を「なし」に指定します。

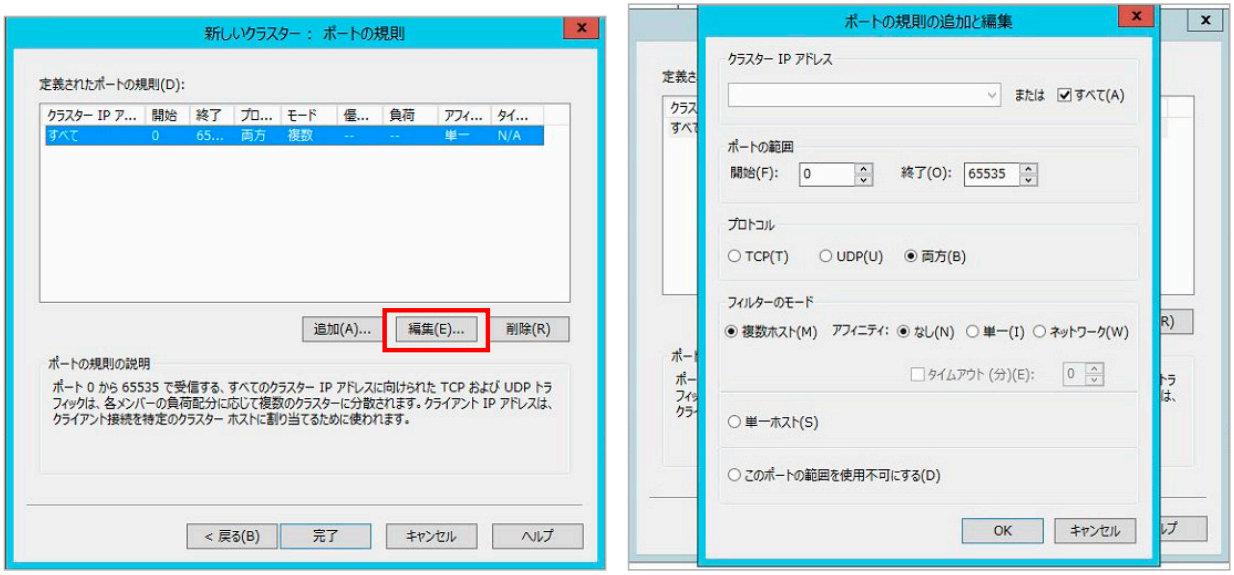


図 2-42　ポートの規則

8. 「OK」→「完了」をクリックして、クラスタの編集を完了します。

以上の手順により、NLB クラスタが作成されます。

図 2-43　ポートの規則

次に、このクラスタにサーバ C を追加します。

9. クラスタノードを右クリックして、「ホストをクラスターに追加」をクリックします。

図 2-44　ホストをクラスタに追加

10. 「ホストをクラスターに追加：接続」画面で、「ホスト」にサーバ C の IP アドレス（例：192.168.1.202）を入力し、「接続」をクリックします。

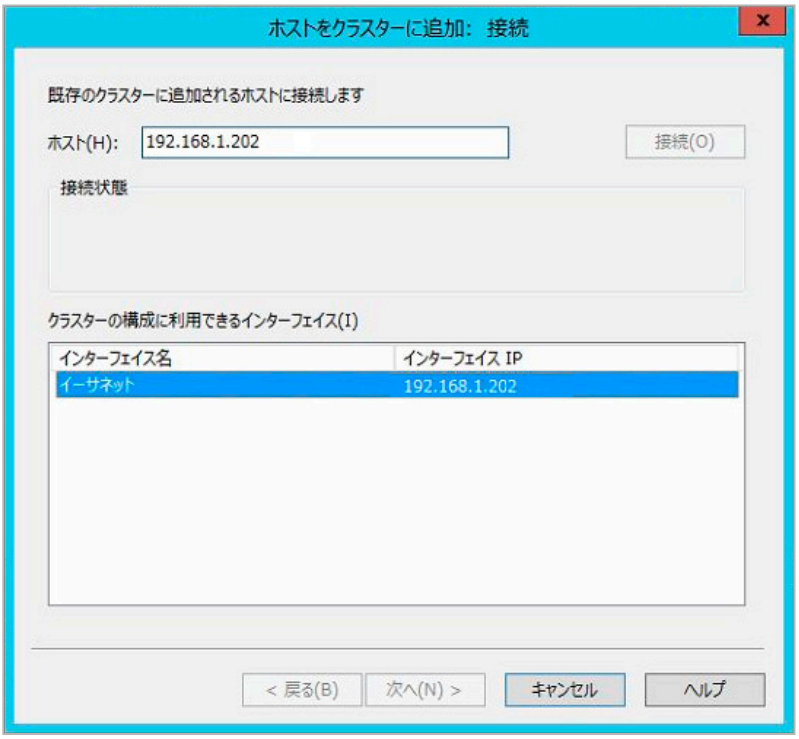


図 2-45　ホストをクラスタに追加

11.「ホストをクラスターに追加：ホスト パラメーター」画面で、「次へ >」をクリックして先へ進みます。

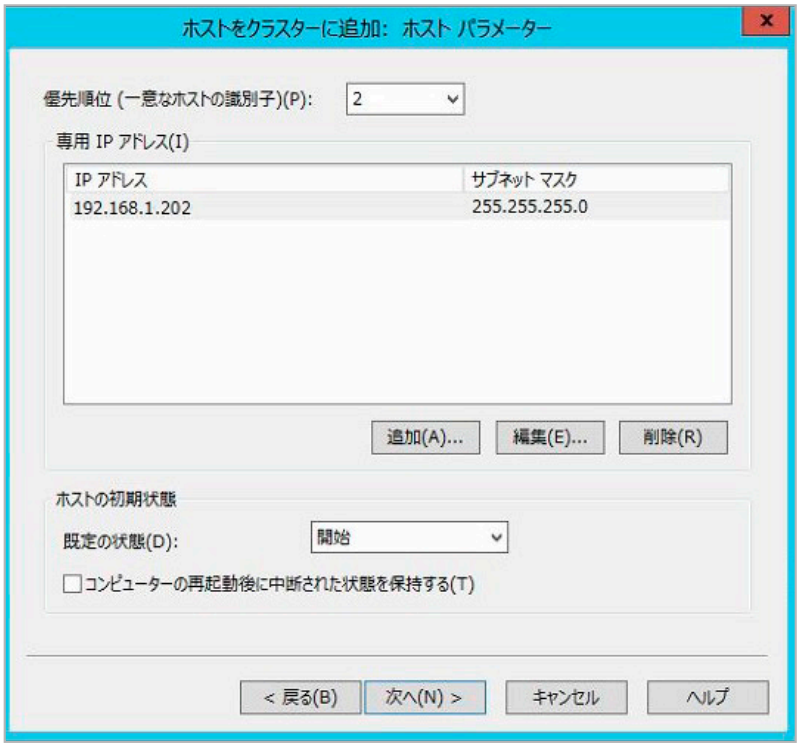


図 2-46　ホストパラメーターの設定

12.「ホストをクラスターに追加：ポートの規則」画面で、「完了」をクリックします。

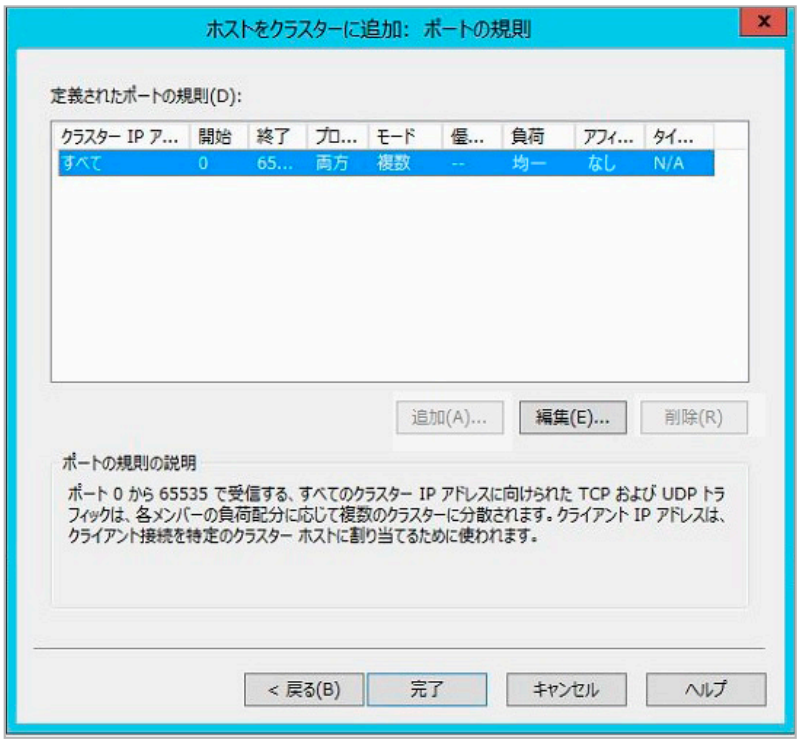


図 2-47　ポートの規則

以上の設定により、サーバ B とサーバ C で構成されるクラスタが作成されます。

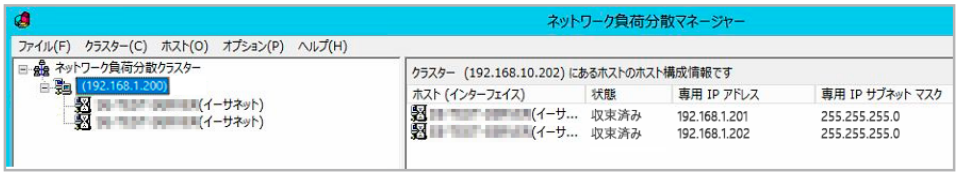


図 2-48　ネットワーク負荷分散クラスタ

仮想 IP アドレスを使用して D-View8 にアクセスすることができます。

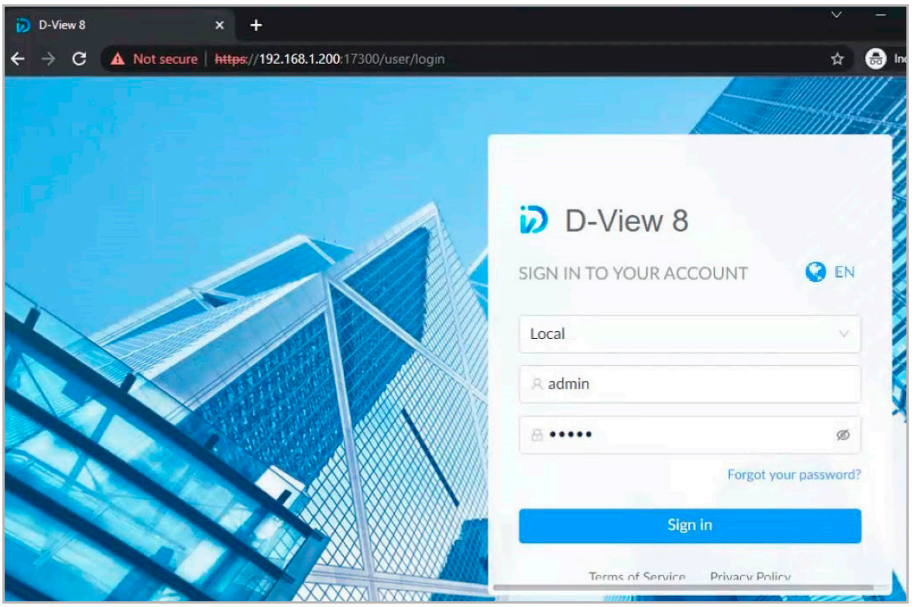


図 2-49　D-View8 ログイン画面

■ サーバ C での NLB 管理

サーバ C で NLB クラスタを管理する場合は、次の手順を実行します。

1. 「ネットワーク負荷分散クラスター」を右クリックして、「既存の NLB クラスターに接続」を選択します。

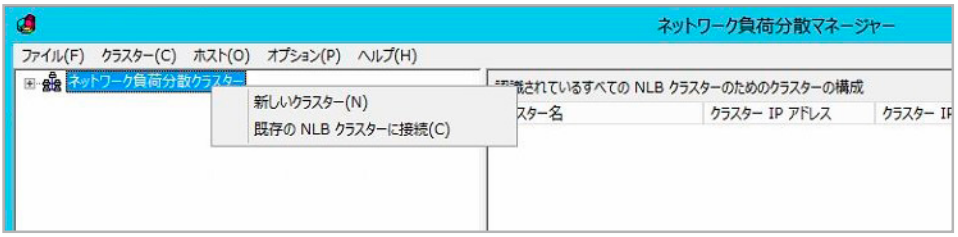


図 2-50　ネットワーク負荷分散マネージャー

2. 「既存のクラスターに接続：接続」画面で、NLB クラスタ IP（例：192.168.1.200）を入力し、「接続」ボタンをクリックします。

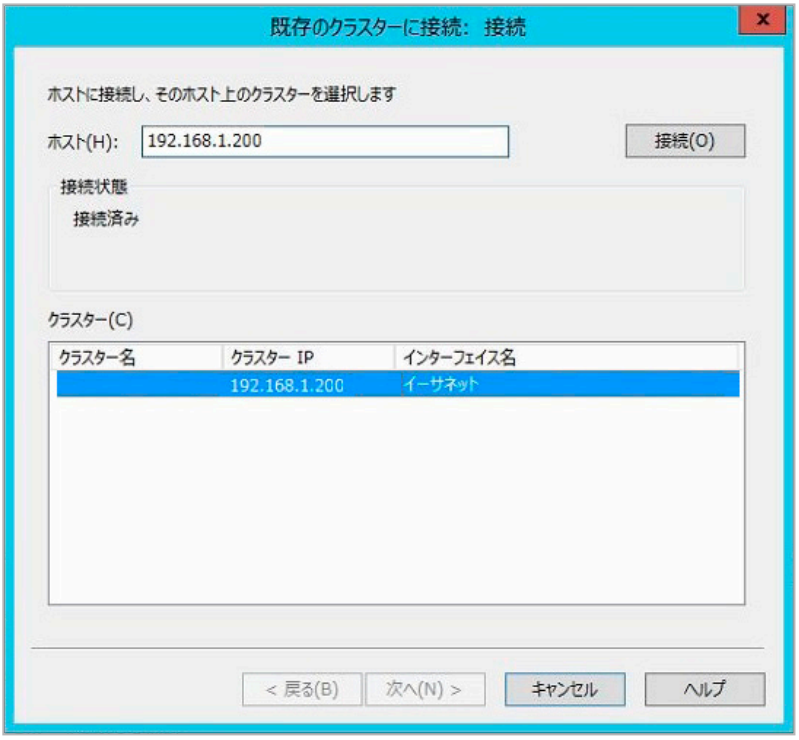


図 2-51　既存のクラスタに接続

- サーバ C で NLB クラスタ情報を確認できます。

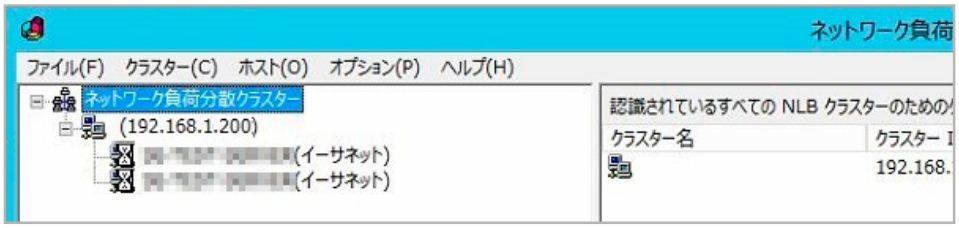


図 2-52　ネットワーク負荷分散クラスタ

■ NLB の動作確認

1. クラスタサーバノードのいずれかでネットワークアダプタを無効にします。（例：192.168.1.201）
2. 仮想 IP（例：192.168.1.200）、他のサーバの IP（例：192.168.1.202）を使用し、Web ブラウザからアプリケーションにアクセスします。
3. 仮想 IP と他のサーバの IP が接続可能であることを確認します。
   切断したサーバには接続できなくなります。

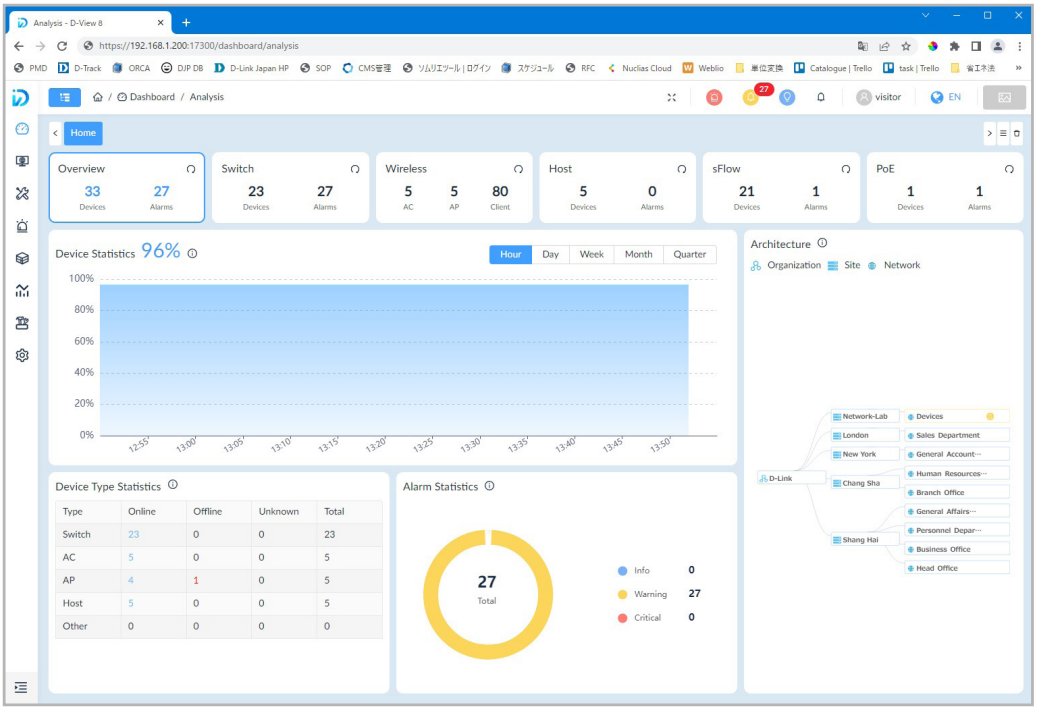


図 2-53　接続確認（192.168.1.200）

D-View8 プローブのインストール（Windows サーバ）

Windows サーバにプローブをインストールします。プローブには以下の 2 種類があります。

- 「Local Probe（ローカルプローブ）」：コアサーバと同じ IP アドレスを使用して D-View8 Core サービスに接続します。D-View8 サーバインストール時にデフォルトで同サーバ上にインストールされます。
- 「Remote Probe（リモートプローブ）」：D-View8 Core サーバとは異なる IP アドレスを持ちます。Probe インストールパッケージを使用してインストールします。

HA/ 冗長構成における動作

プローブは、NLB による HA（High Availability）機能および負荷分散機能で動作することも可能です。
HA 構成に組み込まれる場合、リモートプローブは仮想 IP およびポート 17500（D-View8 サーバのデフォルトポート）を使用してサーバクラスタに接続します。HA で動作しない場合、リモートプローブは物理 IP アドレスを使用して D-View8 サーバに直接接続します。

プローブのインストール手順

セットアップウィザードを使用して、D-View8 プローブのインストールを行うことができます。インストールを開始する前に、すべてのアプリケーションを閉じて、システムを再起動せずに関連するシステムファイルの更新を行うことができるようにすることをお勧めします。

1. D-Link Japan のサイトから D-View8 プローブのインストールパッケージをダウンロードします。
2. D-View8 プローブのインストーラをダブルクリックし、セットアップウィザードを開始します。
3. 「Next >」をクリックします。

図 2-54　セットアップウィザードの開始

4. 使用許諾画面が表示されます。
「I Agree」をクリックし、使用許諾に同意します。

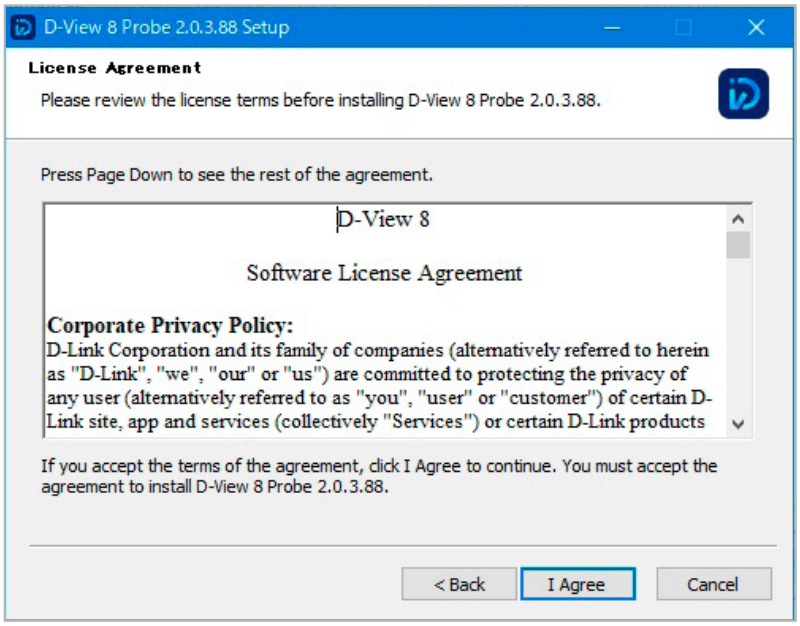


図 2-55　使用許諾への同意

5. 「Browse」をクリックして、インストールフォルダを選択します。
「Next >」をクリックします。

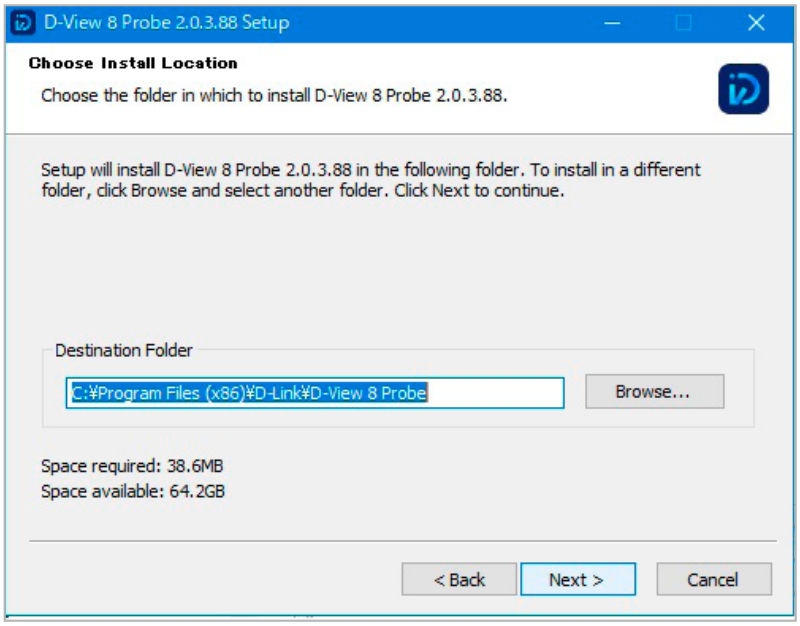


図 2-56　インストールフォルダの選択

6. プローブコンポーネントの設定を行います。
   - 「Local IP」：ローカル IP アドレスを選択します。
   - 「Probe Port」：Probe 通信を許可するポート番号を入力します。
   - 「Core Server IP」：コアサーバの IP アドレスを入力します。
   - 「Core Server Port」：コアサーバのポート番号を入力します。
   - 「Check」：設定を検証します。ローカル IP が正しく設定されている場合は、「Check Pass!」メッセージが表示されます。それ以外の場合は、設定内容を見直してください。

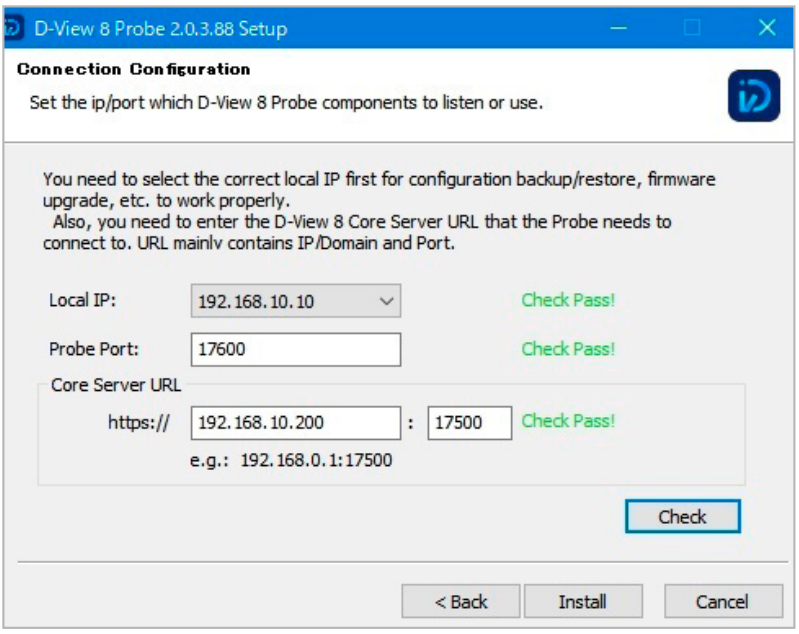


図 2-57　Core サーバへの接続設定

7. 「Install」をクリックしてインストール処理を開始します。

8. インストール完了後、「Close」をクリックしてインストールプロセスを終了します。
   プローブのセットアップ処理が完了すると、以下の項目が Windows メニューに生成されます。
   - 「D-View 8 Service Management Tool」
   - 「Uninstall」

「D-View8 Service Management Tool（D-View8 サービス管理ツール）」により、プローブの管理を行うことができます。

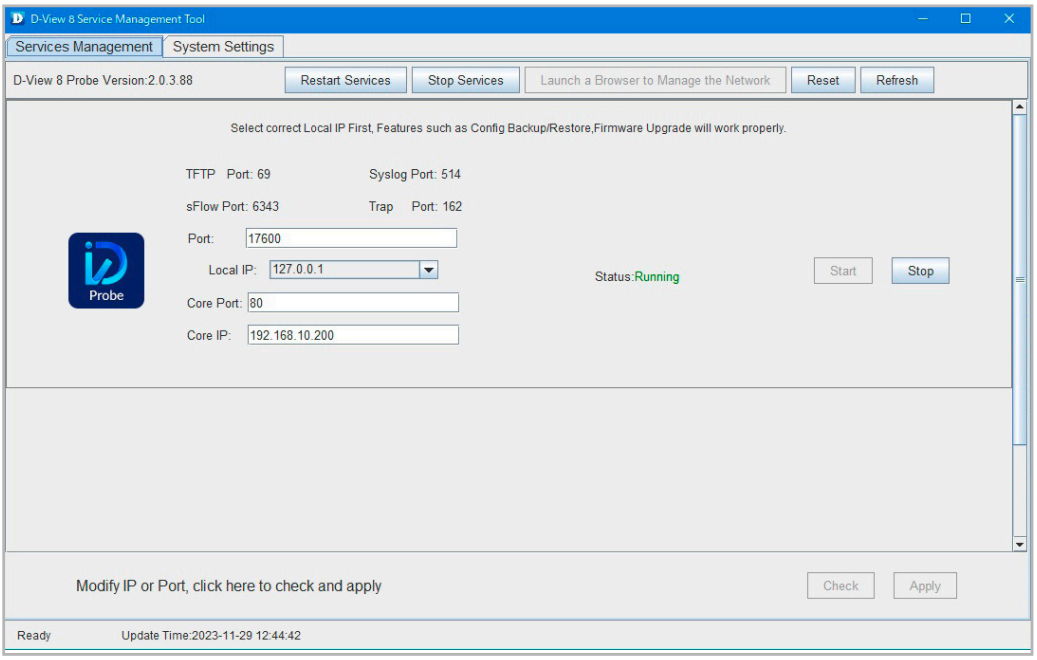


図 2-58　サービス管理ツールの表示

（参考）D-View8 サーバのインストール（Linux サーバ / スタンドアロン構成）

注意 Linux サーバへの D-View8 のインストールは未サポートです。

1. D-Link Japan のサイトから D-View8 インストールパッケージをダウンロードします。
2. 次のコマンドを入力して、ダウンロードしたパッケージのインストールプロセスを開始します。

```
dpkg -i D-View_8_2.0.3.88_Installation.deb
```

注意 上記はコマンドの実行例です。パッケージ名の部分には、ダウンロードしたファイル名を指定してください。

3. プロンプトの指示に従い、ローカル IP アドレスを入力します。

```
Input the local IP: 172.18.192.256
```

注意 上記の IP アドレスは参考用です。IP アドレスの部分には、サーバのローカル IP アドレスを入力してください。

D-View8 アプリケーションを機能させるには、データベースサービス（MongoDB）が必要です。初めてインストールする場合は、新しいデータベースインスタンスを作成する必要があります。

4. プロンプトで「1」を入力し、MongoDB のインストールタイプとして「スタンドアロン」を選択します。

```
You intend to use: 1.standalone MongoDB; 2.MongoDB cluster [1/2]
```

■ **新規のデータベースインスタンスをインストールする場合：**

a. プロンプトの指示に従い、「y」を入力して新規のデータベース・インスタンスをインストールします。

```
If you need to install a new MongoDB. [y/n]
```

インストールが開始後、管理者アカウントの作成を行う必要があります。これにより、D-View8 インスタンスの組み込みデータの処理、初期化が続行されます。

b. プロンプトの指示に従い、管理者アカウントのユーザ名を入力します。

```
Username: [admin]
```

c. プロンプトの指示に従い、パスワードを入力します。「Confirm Password」欄にもう一度入力します。

```
Password: [admin]
Confirm Password: [admin]
```

インストールプロセスにより、Web、コア、プローブの各サービスがインストールされます。プロセスが完了すると、サービスがアクティブになります。

■ **既存のデータベースを使用する場合：**

a. プロンプトの指示に従い、「n」と入力して既存のデータベースインスタンスを検出します。

```
If you need to install a new MongoDB. [y/n]
```

b. プロンプトの指示に従い、「y」と入力して既存のインスタンスを構成します。

```
The system detects that you have MongoDB installed, do you want to use it? [y/n]
```

c. プロンプトの指示に従い、MongoDB インスタンスの IP アドレスとポートを入力します。

既存のインスタンスの IP アドレスを入力：

```
Input the existing mongodb IP: 172.18.192.201
```

既存のインスタンスのポートを入力：

```
Input the existing mongodb port: 27018
```

注意 上記の IP アドレスとポート番号は参照用です。データベースを紐づけるには、既存インスタンスの IP アドレスとポートを指定してください。

e. プロンプトの指示に従い、データベースの認証有無を選択します。アクセス認証が必要な場合は「y」を入力します。

```
Do MongoDB access require authentication? [y/n]
```

f. 必要に応じて、インスタンスへのアクセスが許可されるユーザ名とパスワードを入力します。

```
User Name: root
Password: root
```

5. インスタンスの作成または接続が完了した後、Web ブラウザを使用してアプリケーションを起動します。
6. Web ブラウザを開き、アドレスバーに D-View8 アプリケーションの IP アドレスを入力します。作成されたインスタンスの IP アドレスは、以下のように表示されます。

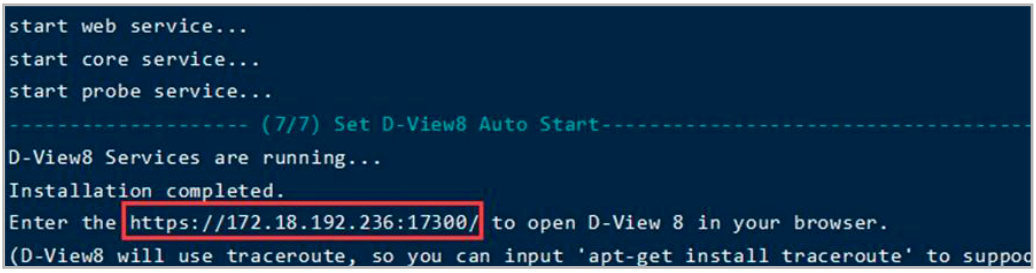


図 2-59　アプリケーション IP アドレスの表示

（参考）D-View8 サーバのインストール（Linux サーバ / クラスタ構成）※エンタープライズ版のみ

注意 Linux サーバへの D-View8 のインストールは未サポートです。

クラスタアーキテクチャ

D-View8 は、冗長性とロードバランシング機能をサポートしています。次の図は、クラスタアーキテクチャの説明図です。

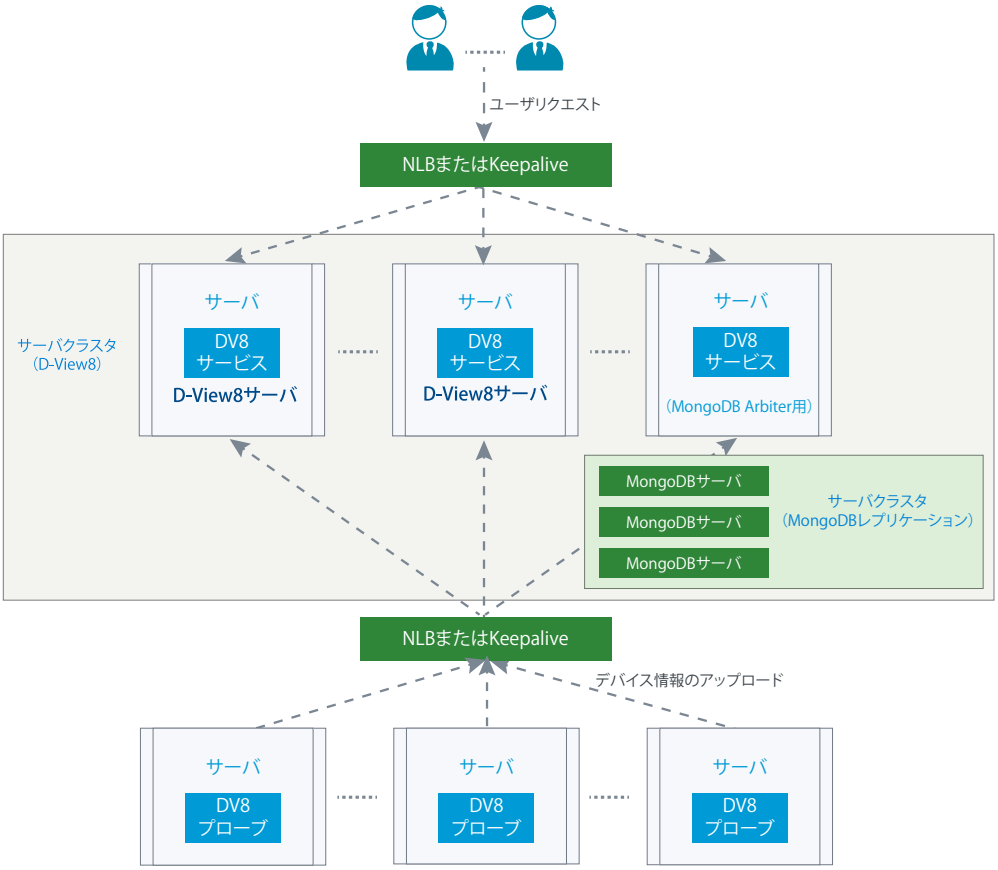


図 2-60　クラスタアーキテクチャ

次の図は、D-View8 と MongoDB のストラクチャ（構造）を示しています。ストラクチャには、プライマリ、セカンダリ、およびアービターが含まれます。基本的なアーキテクチャでは、D-View8 アプリケーションはプライマリとセカンダリデータベースの両方に接続します。セカンダリデータベースがプライマリに選出され、プライマリデータベースがセカンダリに降格する場合もあります。デフォルトでは、クライアントはプライマリから読み取りを行いますが、セカンダリデータベースからの読み取りを許可する設定にすることもできます。

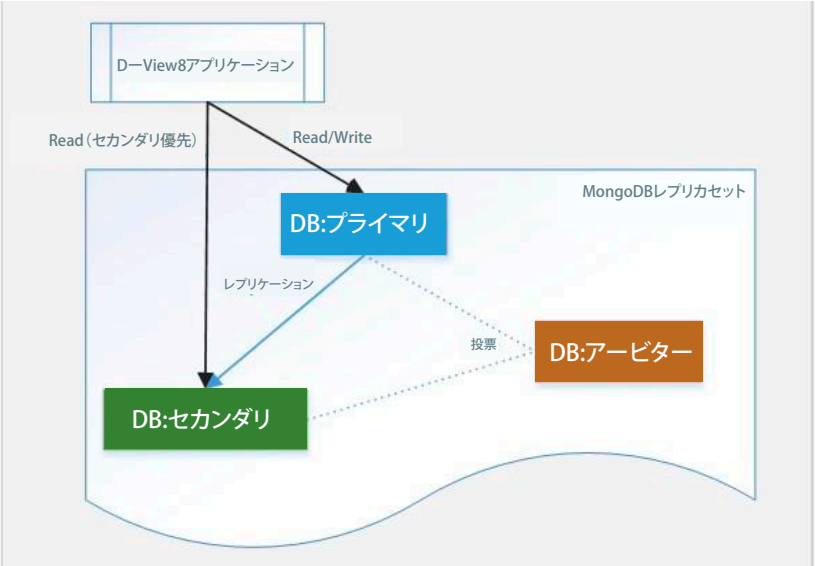


図 2-61　MongoDB ストラクチャ

クラスタの構築手順（概要）

クラスタ構築手順を以下の概略図で示します。

■ データ冗長性のサポート：

1. 3 台の Linux サーバを用意し、MongoDB をインストールします。

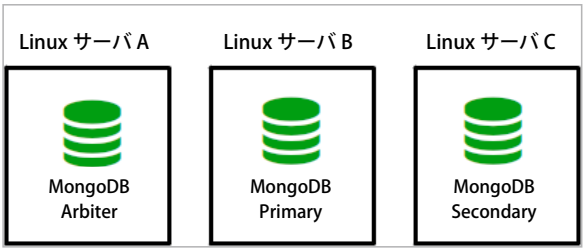


図 2-62　複数サーバの準備

2. 追加のサーバに D-View8 をインストールし、当該アプリケーションを MongoDB クラスタに接続します。

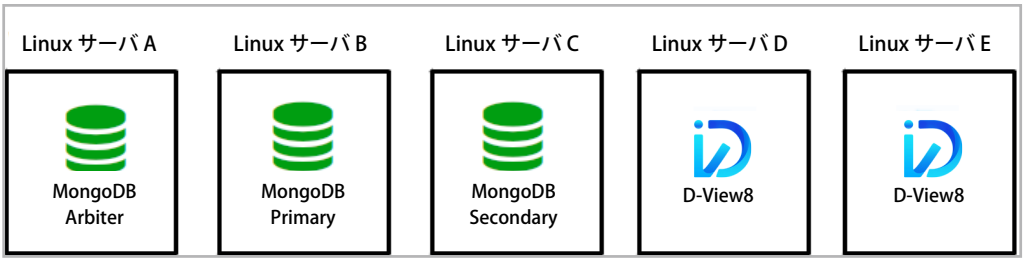


図 2-63　MongoDB クラスタへの接続

または、以下の図のように、追加のサーバの代わりにプライマリ / セカンダリデータベースサーバに D-View8 をインストールすることも可能です。

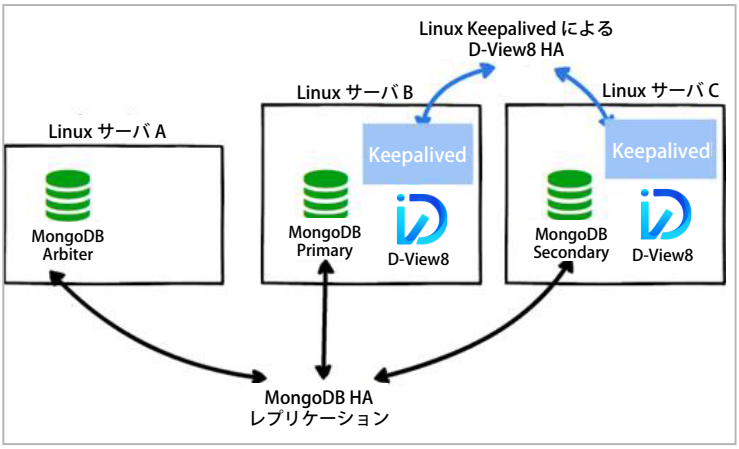


図 2-64　MongoDB クラスタへの接続

■ サーバ負荷分散のサポート：

3. Linux サーバに Keepalived をインストールします。

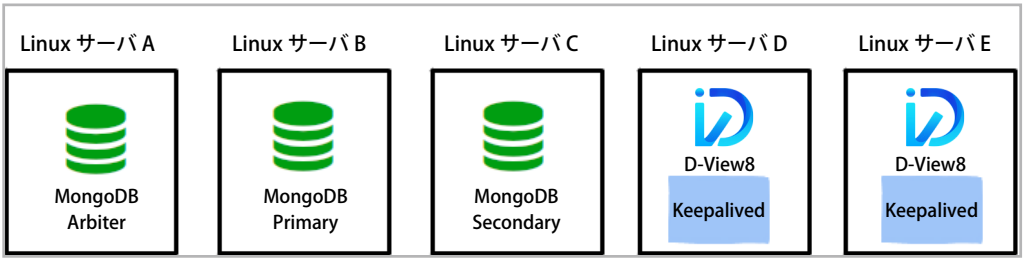


図 2-65　Keepalived のインストール

注意 HA（High Availability）と負荷分散をサポートするには、MongoDB サーバ、D-View8 サーバ、Keepalived を適切な順序でインストールする必要があります。インストール手順については、次のセクションで説明しています。2 台の D-View8 サーバで Keepalived を有効化し、サーバクラスタとして構成します。

4. 追加のデバイスを管理するには、追加の Linux サーバにプローブをインストールし、Keepalived により HA クラスタを構成する D-View サーバに接続します。

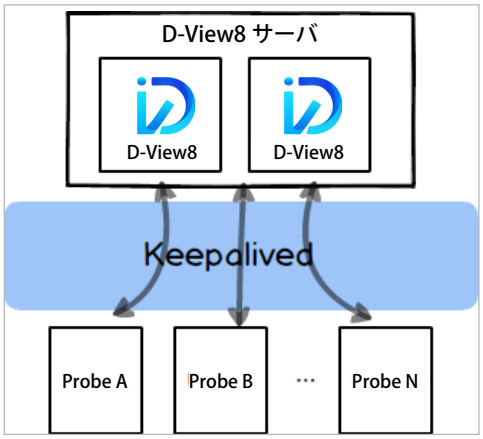


図 2-66　Keepalived アーキテクチャ

クラスタ構築手順

クラスタ構築手順について説明します。

- 「データ冗長性のサポート：MongoDB クラスタの構成」
- 「データ冗長性のサポート：複数サーバへの D-View8 インストール」
- 「サーバ負荷分散のサポート：Keepalived の構成」

メモ　本セクションでは、Linux サーバを 3 台使用したクラスタ構成の設定手順について説明しています。MongoDB レプリカセットのうち、2 台のサーバに D-View8 server サービスをインストールします。

Linux サーバ構成例

項目	サーバ A	サーバ B	サーバ C
IP アドレス	10.32.123.130	10.32.123.131	10.32.123.132
OS	Ubuntu 18.04 以上	Ubuntu 18.04 以上	Ubuntu 18.04 以上
MongoDB レプリカセット役割	Arbiter	Primary	Secondary
Keepalived 設定	—	仮想 IP：10.32.123.133	仮想 IP：10.32.123.133

D-View8 サーバには 3 つのコンポーネント（WebAPI、D-View8 Core、D-View8 Probe）が含まれています。このうち、D-View8 WebAPI と D-View8 Core は負荷分散機能をサポートしています。（以下のインストール手順の例では、WebAPI の負荷分散についてのみ記載します。）D-View8 サーバでは、Linux の Keepalived パッケージを使用した負荷分散とフェイルオーバ機能をサポートしています。

以下の例では、D-View8 サーバ B とサーバ C をロードバランサとして構成します。ネットワークトラフィックは仮想 IP を介してサーバ B とサーバ C にリダイレクトされます。ユーザは Web ブラウザから仮想 IP を使用して D-View8 サーバに接続することができます。

データ冗長性のサポート：MongoDB クラスタの構成

以下の手順に従い、サーバ A、サーバ B、サーバ C にそれぞれ MongoDB をインストールします。

メモ　MongoDB クラスタは、プライマリまたはセカンダリいずれかのデータベースが故障した場合でも動作しますが、アービターデータベースが故障すると、MongoDB PSA（primary-secondary-arbiter）は機能しません。

1. D-Link Japan のサイトから D-View8 MongoDB インストールパッケージをダウンロードします。
2. システムに root ユーザとしてログインします。
3. カレントディレクトリを D-View8 パッケージが保存されているディレクトリに変更します。（例：/home/dview8）
4. コマンドラインで次のように入力し、パッケージを解凍します。

```
tar -zxvf dview8-mongodb-linux-2.0.3.88.tgz
```

注意　上記はコマンドの実行例です。パッケージ名の部分には、ダウンロードしたファイル名を指定してください。

5. 解凍後のディレクトリに移動した後、init_mongo.sh シェルスクリプトを実行します。

```
./init_mongo.sh
```

6. 最初に組み込みデータをインポートする必要があります。[y] を入力して続行します。

```
Whether you first start MongoDB, first start will import D-View 8 built-in data. [y/n]
```

7. インスタンスをレプリケーションモードで起動して、MongoDB をクラスタで利用するように指定します。[y] と入力して続行します。

```
Are you going to use Cluster MongoDB and start MongoDB in replication mode. [y/n]
```

```
root@dview8:/home/dview8/mongodb-linux-x86_64-4.0.0# ./init_mongo.sh
.



---- check MongoDB port ----
MongoDB port : 27018 is free
Whether you first start MongoDB, first start will import D-View 8 built-in data.[y/n]
y
mongodb is not running!
stop mongodb......
about to fork child process, waiting until server is ready for connections.
forked process: 385940
child process started successfully, parent exiting
Creating built-in data for D-View8 database...
Creating built-in data system.js.
Creating built-in data DView8_ConfigurationCategory.
Creating built-in data DView8_ConfigurationTemplate.
Creating built-in data DView8_Credit.
Creating built-in data DView8_DeviceCategory.
...
...
Creating built-in data DView8_SyslogKeyWords.
D-View8 database built-in data created.
Are you going to use Cluster MongoDB and start MongoDB in replication mode.[y/n]
y
mongodb is running!
stop mongodb......
2022-08-20T06:04:11.324+0000 W CONTROL [main] enableMajorityReadConcern startup
parameter was supplied, but its value was ignored; majority read concern cannot
be disabled.
about to fork child process, waiting until server is ready for connections.
forked process: 386317
child process started successfully, parent exiting
------ all completed ------
root@dview8:/home/dview8/mongodb-linux-x86_64-4.0.0#
```

以上で、データベースサーバのインストールが完了します。TCP 27018 ポートを使用して通信が行われます。

データ冗長性のサポート：複数サーバへの D-View8 インストール

サーバ B、サーバ C にそれぞれ D-View8 アプリケーションをインストールし、それらを MongoDB クラスタに接続します。

メモ　MongoDB レプリカセットとは別に追加の Linux サーバを用意し、D-View8 サーバをインストールすることも可能です。

■ サーバ B への D-View8 インストール

以下の手順に従い、最初にサーバ B に D-View8 をインストールします。

1. D-Link Japan のサイトから D-View8 インストールパッケージをダウンロードします。
2. システムに root ユーザとしてログインします。
3. カレントディレクトリを D-View8 パッケージが保存されているディレクトリに変更します。（例：/home/dview8）
4. ルートメニューで次のコマンドを入力して、ダウンロードしたパッケージのインストールプロセスを開始します。

```
dpkg -i D-View_8_2.0.3.88_Installation.deb
```

注意　上記はコマンドの実行例です。パッケージ名の部分には、ダウンロードしたファイル名を指定してください。

5. プロンプトの指示に従い、ローカル IP アドレスを入力します。

```
Input the local IP: xxx.xxx.xxx.xxx
```

注意　本手順の構成例では、サーバ B の IP アドレス（例：10.32.123.131）を指定します。

D-View8 アプリケーションを機能させるには、データベースサービス（MongoDB）が必要です。

6. プロンプトで [2] を入力し、MongoDB のインストールタイプとして「クラスタ」を選択します。

```
You intend to use: 1.standalone MongoDB; 2.MongoDB cluster [1/2]
```

7. プロンプトで、プライマリ、セカンダリ、およびアービターデータベースの物理 IP アドレスとポートを入力します。

```
root@dview8:/home/dview8# dpkg -i D-View_8_2.0.3.88_Installation.deb
Selecting previously unselected package dview8.
(Reading database ... 108358 files and directories currently installed.)
Preparing to unpack D-View_8_2.0.3.88_Installation.deb ...
Before installation...
.
----
Unpacking dview8 (2.0.3.88) ...
Setting up dview8 (2.0.3.88) ...
Installing...
.
-----------------------------------------------------------------------------------------

--------------(1/7)check local file and directory environments----------------------------
-------------- (2/7) check local port environments----------------------------------------
---- check WebServer ----
WebServer_port is free
---- check CoreServer_port ----
CoreServer_port is free
---- check Probe_port ----
Probe_port is free
Now initial set the local IP for D-View 8 (input format similar to: 192.168.131.25),
Local IP address detected may be as follows, Select correct local IP First, Features such
as Config Backup/Restore,
Firmware Upgrade, Send Activation Email will work properly.
10.32.123.131
172.18.0.1
--------------------
please confirm that the input IP is valid:
Input the local IP：10.32.123.131 #Input the physical IP addresses for the D-VIEW 8 server
input: 10.32.123.131
-----------------(3/7)Chmod installation files-----------------------------------------
-----------------(4/7)Install D-View8 MongoDB Services-------------------------------------
D-View 8 requires a database service provided by MongoDB 4.0.3. So if you choose 'Install
a new MongoDB 4.0.3', the installation will try to install MongoDB 4.0.3. If you choose
'Use an existing MongoDB 4.0.3', you can let D-View 8 to connect a remote MongoDB service.
You intend to use: 1.standalone MongoDB; 2.MongoDB cluster[1/2]
2
-----------------------------------------------------------------------------------------
MongoDB cluster contains Primary node, Secondary node and Arbiter node.
The Primary: receives write and read operations.
The Secondary: become a primary if the current primary becomes unavailable.
The Arbiter: decide the secondary to upgrade as an primary after the primary is unavailable.
```

```
Input the existing the Primary IP：10.32.123.131
input: 10.32.123.131
Input the existing the Primary port：27018
input: 27018
Input the existing the Secondary IP：10.32.123.132
input: 10.32.123.132
Input the existing the Secondary port：27018
input: 27018
Input the existing the Arbiter IP：10.32.123.130
input: 10.32.123.130
Input the existing the Arbiter port：27018
input: 27018

Creating built-in data for D-View8 database...
Creating built-in data DView8_ConfigurationCategory.
Creating built-in data DView8_ConfigurationTemplate.
Creating built-in data DView8_Credit.
Creating built-in data DView8_DeviceCategory.
Creating built-in data DView8_DeviceTemplate.
Creating built-in data DView8_DeviceType.
Creating built-in data DView8_Email.
Creating built-in data DView8_MailServer.
Creating built-in data DView8_MonitorCategory.
Creating built-in data DView8_MonitorTemplate.
Creating built-in data DView8_NotificationSoundSetting.
Creating built-in data DView8_Organization.
Creating built-in data DView8_PanelTemplate.
Creating built-in data DView8_Role.
Creating built-in data DView8_TimeSetting.
Creating built-in data DView8_PortGlobalSetting.
Creating built-in data DView8_AlarmRuleDefine.
Creating built-in data DView8_User.
Creating built-in data DView8_VendorTemplate.
Creating built-in data sFlow_mapping_DSCP.
Creating built-in data template_config_view.
Creating built-in data DView8_TrapOID.
Creating built-in data snmp_mib_node.
Creating built-in data sFlow_NicVendorMapping.
Creating built-in data sFlow_mapping_application.
Creating built-in data DView8_SyslogKeyWords.
Creating built-in data DView8_MonitorBatchAlarmSetting.
Creating built-in data system.js.
D-View8 database built-in data created.
----------------- (5/7) Modify D-View8 Service files-------------------------------------
modify webserver files
modify coreserver files
modify probe files
------------------(6/7)Install D-View8 Local Services-----------------------------------
start web service...
start core service...
start probe service...

------------------(7/7)Set D-View8 Auto Start--------------------------------------------
D-View8 Services are running...
Installation completed.
Enter the https://10.32.123.131:17300/ to open D-View 8 in your browser.
(D-View8 will use traceroute, so you can input 'apt-get install traceroute' to support)
root@dview8:/home/dview8#
```

■ サーバ C への D-View8 インストール

8. 手順 1 ～ 7 を参照し、サーバ C に D-View8 をインストールします。

注意 手順 5 と手順 7 のローカル IP アドレス指定では、サーバ C の物理 IP アドレス（例：10.32.123.132）を指定します。

インストールが完了すると、割り当てた IP アドレスとポート番号を使用して、Web ブラウザからアプリケーションにアクセスすることができます。（例：https://10.32.123.131:17300/ および https://10.32.123.132:17300/）

サーバ負荷分散のサポート：Keepalived の構成

D-View8 サーバに Keepalived をインストールして、負荷分散を有効にします。Keepalived は LVS と VRRP を使用してロードバランサとして機能します。VRRP では MASTER と BACKUP の 2 つのステータスがあります。ここでは、サーバ B（10.32.123.131）を MASTER、サーバ C（10.32.123.132）を BACKUP として構成します。

1. SSH を使用して root アカウントでサーバ B にログインします。

2. Keepalived をインストールします。

```
root@dview8:~# apt install keepalived
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
keepalived
0 upgraded, 1 newly installed, 0 to remove and 71 not upgraded.
Need to get 361 kB of archives.
After this operation, 1,250 kB of additional disk space will be used.
Get:1 http://tw.archive.ubuntu.com/ubuntu focal-updates/main amd64
keepalived amd64 1:2.0.19-2ubuntu0.2 [361 kB]
Fetched 361 kB in 0s (1,129 kB/s)
Selecting previously unselected package keepalived.
(Reading database ... 108694 files and directories currently installed.)
Preparing to unpack .../keepalived_1%3a2.0.19-2ubuntu0.2_amd64.deb ...
Unpacking keepalived (1:2.0.19-2ubuntu0.2) ...
Setting up keepalived (1:2.0.19-2ubuntu0.2) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for dbus (1.12.16-2ubuntu2.2) ...
Processing triggers for systemd (245.4-4ubuntu3.15) ...

root@dview8:~#
```

3. /etc/keepalived ディレクトリが存在しない場合、ディレクトリを作成します。

```
root@dview8:~# mkdir /etc/keepalived
```

4. /usr/local/dview8/keepalived から /etc/keepalived に keepalived.conf と vip_service.sh をコピーします。

```
root@dview8:~# cp /usr/local/dview8/keepalived/* /etc/keepalived
```

5. コンフィグレーションファイル（keepalived.conf）を下記のように編集します。

注意 D-View8 サーバは D-View8 WebAPI と D-View8 Core にそれぞれポート 17300 と 17500 を使用します。このファイルでポート番号を設定します。

etc/keepalived/keepalived.conf

```
! Configuration File for keepalived

global_defs {  #Global Configuration
  router_id LVS_36      #The router_id is the load-balancing identifier, which should be unique.
}

vrrp_instance VI_1 {   # Identify a VRRP instance definition block
  state MASTER # Specify the instance state in standard use: MASTER or BACKUP, has to be
                 capitalized.
  interface eth0       # Specify the network interface for the instance to run on
  virtual_router_id 51 # Specify to which VRRP router id the instance belongs
  priority 50  # Specify the instance priority for VRRP MASTER router (lower means higher
                 priority), the main node has the  highest priority than other nodes.
  advert_int 1 # Specify the advertisement interval in seconds
  authentication {     # Identify a VRRP authentication definition block
            auth_type PASS    # specify the authentication method: PASS|AH
            auth_pass 1111    #Specify the password for authentication
  }
  virtual_ipaddress {  # identify a VRRP VIP definition block
            10.32.123.133
  }
}

virtual_server 10.32.123.133 17300 { #Assign service to use the Virtual IP, the D-View 8
WebAPI uses port 17300
  delay_loop 6 # Healthcheck time interval
  lb_algo rr
  lb_kind DR#Use the LVSDR mode
  persistence_timeout 5
  protocol TCP # specify the protocol kind: TCP|UDP

  real_server 10.32.123.131 17300 {
            weight 1   #Assign weight to service node
            TCP_CHECK {
            connect_timeout 3
            retry 1
            delay_before_retry 3
            connect_port 17300
            }
  }

  real_server 10.32.123.132 17300 {
  weight 1  #Assign weight to service node
            TCP_CHECK {
            connect_timeout 3
            retry 1
            delay_before_retry 3
            connect_port 17300
            }
  }
}
```

```
virtual_server 10.32.123.133 17500 { #Assign service to use the Virtual IP, the D-View 8
Core uses port 17500
  delay_loop 6 #Healthcheck time interval
  lb_algo rr
  lb_kind DR# Use the LVSDR mode
  persistence_timeout 5
  protocol TCP # specify the protocol kind: TCP|UDP

  real_server 10.32.123.131 17500 {
            weight 1   #Assign weight to service node
            TCP_CHECK {
            connect_timeout 3
            retry 1
            delay_before_retry 3
            connect_port 17500
            }
  }

  real_server 10.32.123.132 17500 {
            weight 1   #Assign weight to service node
            TCP_CHECK {
            connect_timeout 3
            retry 1
            delay_before_retry 3
            connect_port 17500
            }
  }
}
```

6. 以下のコマンドを実行して、Keepalived サービスを開始し、ステータスをチェックします。

```
root@dview8:~# service keepalived start
root@dview8:~# service keepalived status
```

「active (running)」のメッセージが表示されることを確認してください。

```
● keepalived.service - Keepalive Daemon (LVS and VRRP)
Loaded: loaded (/lib/systemd/system/keepalived.service; enabled; vendor preset: enabled)
Active: active (running) since Sat 2022-08-20 11:20:45 UTC; 51min ago
Main PID: 198630 (keepalived)
Tasks: 3 (limit: 9434)
Memory: 3.1M
CGroup: /system.slice/keepalived.service
            ├─198630 /usr/sbin/keepalived --dont-fork
            ├─198651 /usr/sbin/keepalived --dont-fork
            └─198652 /usr/sbin/keepalived --dont-fork
Aug 20 11:20:45 dview8 Keepalived_healthcheckers[198651]: Activating healthchecker for
service [10.32.123.131]:tcp:17500 for VS  [10>
Aug 20 11:20:45 dview8 Keepalived_healthcheckers[198651]: Activating healthchecker for
service [10.32.123.132]:tcp:17500 for VS  [10>
Aug 20 11:20:45 dview8 Keepalived_healthcheckers[198651]: Activating BFD healthchecker
Aug 20 11:20:47 dview8 Keepalived_healthcheckers[198651]: TCP connection to
[10.32.123.132]:tcp:17500 success. Aug 20 11:20:49 dview8 Keepalived_vrrp[198652]: (VI_1)
Entering MASTER STATE
```

```
Aug 20 11:20:49 dview8 Keepalived_healthcheckers[198651]: TCP connection to
[10.32.123.132]:tcp:17300 success. Aug 20 11:20:50 dview8 Keepalived_healthcheck
ers[198651]: TCP_CHECK on service [10.32.123.131]:tcp:17300 failed.
Aug 20 11:20:50 dview8 Keepalived_healthcheckers[198651]: Removing service
[10.32.123.131]:tcp:17300 to VS  [10.32.123.133]:tcp:17300
Aug 20 11:20:50 dview8 Keepalived_healthcheckers[198651]: TCP_CHECK on service
[10.32.123.131]:tcp:17500 failed.
Aug 20 11:20:50 dview8 Keepalived_healthcheckers[198651]: Removing service
[10.32.123.131]:tcp:17500 to VS  [10.32.123.133]:tcp:17500
lines 1-21/21 (END)
```

7. vip_service.sh の割り当て仮想 IP アドレスを編集します。

/etc/keepalived/vip_service.sh

```
#!/bin/bash
check_ptah=`which ifconfig |wc -l`
if [ $check_ptah -eq 0 ]
  then echo -e "\033[31mPlease run the 'apt install net-tools' command\033[0m"
 exit 1

fi
SNS_VIP=10.32.123.133 #Enter the Virtual IP address case "$1" in

start)
            ifconfig lo:0 $SNS_VIP netmask 255.255.255.255 broadcast $SNS_VIP
            /sbin/route add -host $SNS_VIP dev lo:0
            echo "1" >/proc/sys/net/ipv4/conf/lo/arp_ignore
            echo "2" >/proc/sys/net/ipv4/conf/lo/arp_announce
            echo "1" >/proc/sys/net/ipv4/conf/all/arp_ignore
            echo "2" >/proc/sys/net/ipv4/conf/all/arp_announce
            sysctl -p >/dev/null 2>&1
            echo "RealServer Start OK"
            ;; stop)

            ifconfig lo:0 down
            route del $SNS_VIP >/dev/null 2>&1
            echo "0" >/proc/sys/net/ipv4/conf/lo/arp_ignore
            echo "0" >/proc/sys/net/ipv4/conf/lo/arp_announce
            echo "0" >/proc/sys/net/ipv4/conf/all/arp_ignore
            echo "0" >/proc/sys/net/ipv4/conf/all/arp_announce
            echo "RealServer Stoped"
            ;;
*)
            echo "Usage: $0 {start|stop}"
            exit 1 esac
exit 0
```

8. 仮想 IP サービスが外部ループバックネットワークインタフェース「lo:0」に設定されていることを確認します。

```
root@dview8:/etc/keepalived# ./vip_service.sh start

RealServer Start OK

root@dview8:/etc/keepalived# ip a

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
  inet 127.0.0.1/8 scope host lo
           valid_lft forever preferred_lft forever
  inet 10.32.123.133/32 brd 10.32.123.133 scope global lo:0 # The loopback network interface
           valid_lft forever preferred_lft forever
  inet6 ::1/128 scope host
 valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
  link/ether ca:e1:88:d7:da:40 brd ff:ff:ff:ff:ff:ff
  inet 10.32.123.131/16 brd 10.32.255.255 scope global eth0
           valid_lft forever preferred_lft forever
  inet 10.32.123.133/32 scope global eth0
           valid_lft forever preferred_lft forever
  inet6 fe80::c8e1:88ff:fed7:da40/64 scope link
           valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
  link/ether 02:42:8e:b9:f3:bd brd ff:ff:ff:ff:ff:ff
  inet 172.18.0.1/16 brd 172.18.255.255 scope global docker0
           valid_lft forever preferred_lft forever
```

9. Keepalived の開始 / 停止時に合わせて /etc/keepalived/vip_service.sh の開始 / 停止を実行するために、/lib/systemd/system/keepalived.service を編集します。次の 2 行を追加します。

```
ExecStartPre=bash /etc/keepalived/vip_service.sh start
ExecStopPost=bash /etc/keepalived/vip_service.sh stop
```

/lib/systemd/system/keepalived.service

```
[Unit]
Description=Keepalive Daemon (LVS and VRRP)
After=network-online.target
Wants=network-online.target
# Only start if there is a configuration file
ConditionFileNotEmpty=/etc/keepalived/keepalived.conf

[Service]
Type=simple
# Read configuration variable file if it is present
EnvironmentFile=-/etc/default/keepalived
ExecStart=/usr/sbin/keepalived --dont-fork $DAEMON_ARGS

ExecStartPre=bash /etc/keepalived/vip_service.sh start # Add this line and the following line
ExecStopPost=bash /etc/keepalived/vip_service.sh stop
ExecReload=/bin/kill -HUP $MAINPID

[Install]
WantedBy=multi-user.target
```

10. 次のコマンドを実行して、Keepalived をリロードします。

```
root@dview8:/lib/systemd/system# systemctl daemon-reload
root@dview8:/lib/systemd/system# service keepalived restart
```

■ サーバ C への D-View8 インストール

上記「サーバ B への D-View8 インストール」の手順 1 ～ 10 を参照し、同様の手順で VRRP バックアップサーバ（サーバ C）に D-View8 をインストールします。

注意 バックアップサーバでは、/etc/keepalived/keepalived.conf を次の例のように編集する必要があります。

/etc/keepalived/keepalived.conf

```
! Configuration File for keepalived

global_defs {  #Global configuration
  router_id LVS_36     #router_id should be unique in the LAN
}

vrrp_instance VI_1 {   # identify a VRRP instance definition block
  state BACKUP #Here identify the VRRP backup server, has to be capitalized
  interface eth0       # Specify the network interface for the instance to run on
  virtual_router_id 51 # specify to which VRRP router id the instance belongs
  priority 100 # specify the instance priority for the VRRP BACKUP router
  advert_int 1 # Specify the advertisement interval in seconds (set to 1)
  authentication {     # Identify a VRRP authentication definition block
            auth_type PASS    #Authentication method
            auth_pass 1111    #Authentication password
  }

 virtual_ipaddress {   #Identify a VRRP VIP definition block; it can contain multiple ad-
            dresses without specifying subnetwork masks, but  it must align with the Vir-
            tual IP address in the LVS client setting.
            10.32.123.133
  }
}

virtual_server 10.32.123.133 17300 { #Assign the service to use the Virtual IP, the D-View 8
WebAPI uses port 17300
  delay_loop 6 #Healthcheck time interval
  lb_algo rr
  lb_kind DR# Use the LVSDR mode
  persistence_timeout 5
  protocol TCP #specify the protocol kind: TCP|UDP

  real_server 10.32.123.131 17300 { # Service Node 1
            weight 1   #Assign weight to the service node
            TCP_CHECK {
            connect_timeout 3
            retry 1
            delay_before_retry 3
            connect_port 17300
            }
  }
```

```
  real_server 10.32.123.132 17300 { #Service Node 2
  weight 1  #Assign weight to the service node
            TCP_CHECK {
            connect_timeout 3
            retry 1
            delay_before_retry 3
            connect_port 17300
            }
  }
}

virtual_server 10.32.123.133 17500 { # Assign the service to use the Virtual IP and port
#17500, the D-View 8 Core uses port 17500

  delay_loop 6 # Healthcheck time interval
  lb_algo rr
  lb_algo rr
  lb_kind DR# Use the LVSDR mode
  persistence_timeout 5
  protocol TCP # specify the protocol kind: TCP|UDP

  real_server 10.32.123.131 17500 {
            weight 1   # Assign weight to the service node
            TCP_CHECK {

            connect_timeout 3
            retry 1
            delay_before_retry 3
            connect_port 17500
            }
  }

  real_server 10.32.123.132 17500 {

            weight 1   # Assign weight to the service node
            TCP_CHECK {
            connect_timeout 3
            retry 1
            delay_before_retry 3
            connect_port 17500
            }
  }
}
```

/etc/keepalived/vip_service.sh を編集して VRRP バックアップサーバの仮想 IP アドレス（例：10.32.123.133）を指定する手順については、手順 7 を参照してください。
マスタサーバの仮想 IP アドレスが外部ループバックネットワークインタフェース「lo:0」に設定されていることを確認するには、手順 8 を実施します。
keepalived.service を編集し、keepalived の開始 / 停止に合わせて vip_service.sh を開始 / 停止するように設定するには、手順 9 を参照してください。

■ ステータスの確認

インストールパッケージに含まれるスクリプトでは、データベースサービスの開始 / 停止、およびステータスチェックが可能です。

```
root@dview8:/home/dview8/mongodb-linux-x86_64-4.0.0# ls -la *.sh
-rwxr-xr-x 1 root root 983 Aug 17 07:43 restart_mongo.sh
-rwxrwxrwx 1 root root 496 Aug 17 07:43 status_mongo.sh
-rwxrwxrwx 1 root root 686 Aug 17 07:43 stop_mongo.sh
```

D-View8 のバージョンを確認するには、以下のコマンドを実行します。

```
root@dview8:/home/dview8/mongodb-linux-x86_64-4.0.0# cat dv8-version
2.0.0.26
```

以上で、D-View8 の Web インタフェースに接続できるようになります。（接続 URL の例：https://10.32.123.133:17300）
クラスタ構成では、D-View8 サーバのクラスタノードのいずれかが接続不可になった場合でも、Web インタフェースの操作が可能です。

（参考）D-View8 プローブのインストール（Linux サーバ）

Linux サーバにプローブをインストールします。本セクションでは、Ubuntu 20.04.3 LTS を利用することを想定しています。

注意 Linux サーバへの D-View8 のインストールは未サポートです。

プローブには以下の 2 種類があります。

- 「Local Probe（ローカルプローブ）」：コアサーバと同じ IP アドレスを使用して D-View8 Core サービスに接続します。D-View8 サーバインストール時にデフォルトで同サーバ上にインストールされます。
- 「Remote Probe（リモートプローブ）」：D-View8 Core サーバとは異なる IP アドレスを持ちます。Probe インストールパッケージを使用してインストールします。

HA/ 冗長構成における動作

プローブは、Keepalived による HA（High Availability）機能および負荷分散機能で動作することも可能です。
HA 構成に組み込まれる場合、リモートプローブは仮想 IP およびポート 17500（D-View8 サーバのデフォルトポート）を使用してサーバクラスタに接続します。HA で動作しない場合、リモートプローブは物理 IP アドレスを使用して D-View8 サーバに直接接続します。

プローブのインストール手順

1. D-Link Japan のサイトから D-View8 プローブのインストールパッケージをダウンロードします。
2. システムに root ユーザとしてログインします。
3. カレントディレクトリを D-View8 パッケージが保存されているディレクトリに変更します。（例：/home/dview8）
4. パッケージのインストールを開始します。

```
root@dview8:/home/dview8# dpkg -i D-View_8_Probe_2.0.3.88_Installation.deb
(Reading database ... 109264 files and directories currently installed.)
Preparing to unpack D-View_8_Probe_2.0.3.88_Installation.deb ...

Before installation...
.
Unpacking dview8probe (2.0.3.88) ...
Setting up dview8probe (2.0.3.88) ...
post installer.....
```

5. ローカルサーバの物理 IP アドレスと、サーバクラスタの Core サーバの仮想 IP アドレスおよびポート番号を入力します。HA 構成に組み込まない場合、ローカルサーバの物理 IP アドレスと Core サーバの物理 IP アドレスおよびポート番号を入力します。

```
-----------------(1/7)check local file and directory environments--------------------------
-----------------(2/7)check local port environments-------------------------------------
---- check probe_port ----
probe_port is free
-----------------(3/7)input local ip / coreserver url------------------------------------
---------- local IP address detected may be as follows ----------
```

```
--------------------
172.18.0.1
10.32.123.134
172.17.134.220
--------------------
Now initial set the local IP for D-View 8 Probe, features such as Config Backup/Restore,
Firmware Upgrade will work properly. please confirm that the input IP is valid:(input format
similar to: 192.168.131.25)

input: 10.32.123.134
Now please enter D-View8 Core Server IP and Port. Probe connected Core Server successfully,
so Probe could work.


please confirm that the input IP is valid:(input format similar to: 192.168.131.25)
Input the CoreServer IP:10.32.123.133 #Input the Virtual IP and port number of the server
cluster for HA or a physical IP address of the server without HA
input: 10.32.123.133
Input the CoreServer Port:17500
input: 17500
-----------------
-----------------(4/7)Chmod installation files-----------------------------------------
-----------------(5/7)Modify D-View8 Probe Service files-----------------------------------
modify probe files
check file finished
-----------------(6/7)Install D-View8 Probe Local Services---------------------------------
start probe service
-----------------(7/7) Set D-View8 Probe Auto Start-------------------------------------
D-View8 Probe Service are running...
Installation completed.
```

6. Web ブラウザを開き、サーバクラスタの仮想 IP アドレス（または HA を利用しない場合、物理 IP アドレス）とポートを入力します。（例：https://10.32.123.133:17300）ログイン後、**System > Server Management** に移動し「Probe」タブを選択します。リモートプローブ一覧を確認することができます。

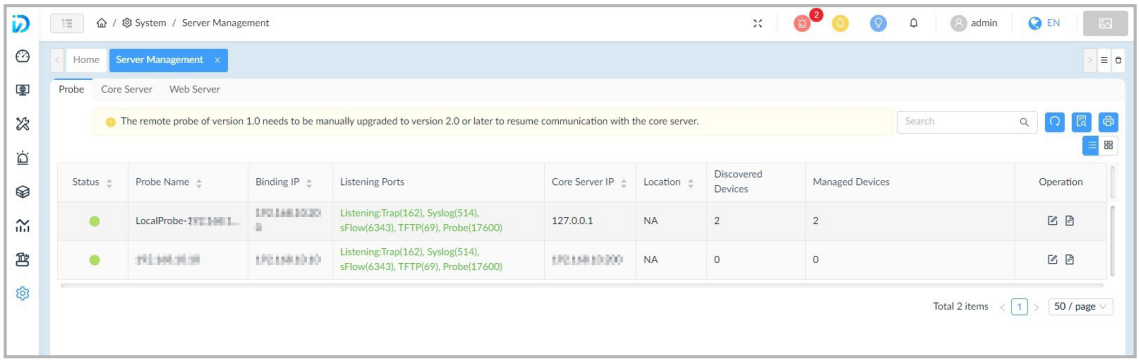


図 2-67　Probe 一覧

スクリプト

インストールパッケージに含まれるスクリプトでは、サービスの開始 / 停止およびステータスのチェックが可能です。また、config.sh スクリプトを使用して IP 設定の変更が可能です。

```
dview8@dview8:~$ cd /usr/local/dview8_probe/
dview8@dview8:/usr/local/dview8_probe$ ls -la
```

```
total 312
drwxr-xr-x  8 root root   4096 Aug 26 14:34 .
drwxr-xr-x 12 root root   4096 Aug 26 14:30 ..
-rwxr-xr-x  1 root root   3298 Jul 27 14:25 config.sh
-rwxr-xr-x  1 root root  11676 Aug 20 02:53 init.sh
drwxrwxrwx  4 root root   4096 Aug 26 14:30 jre
-rwxr--r--  1 root root 246605 Aug 26 14:33 libsigar-amd64-linux.so
drwxrwxrwx  2 root root   4096 Aug 26 14:30 LICENSE
drwxr-xr-x  2 root root   4096 Aug 26 14:34 logs
-rwxr-xr-x  1 root root    738 Jul 27 14:25 monitorProbe.sh
drwxrwxrwx  3 root root   4096 Aug 26 14:56 Probe
drwxrwxrwx  2 root root   4096 Aug 26 14:30 probeLibs
-rwxrwxrwx  1 root root   1553 Jul 27 14:25 restart.sh
-rwxrwxrwx  1 root root    550 Jul 27 14:25 status.sh
-rwxrwxrwx  1 root root    877 Jul 27 14:25 stop.sh
-rwxr-xr-x  1 root root    530 Jul 27 14:25 stop-upgradeprobe.sh
drwxr-xr-x  2 root root   4096 Aug 26 14:34 tftpfile
```

図 2-68　スクリプト

プローブのアンインストール

プローブを削除するには、以下のように dpkg コマンドを実行して dview8probe パッケージを削除します。

```
root@dview8:~# dpkg -P dview8probe
(Reading database ... 109422 files and directories currently installed.)
Removing dview8probe (2.0.3.88) ...
pre remove......
probe is running!
stop probe......
------ all completed ------
post remove......
Purging configuration files for dview8probe (2.0.3.88) ...
post remove......
dpkg: warning: while removing dview8probe, directory '/usr/local/dview8_probe/Probe' not
empty so not removed
```

D-View8 ソフトウェアのアップグレード

D-View8 の最新情報については、弊社ホームページの D-View8 製品ページを参照してください。

D-View8 ソフトウェアのアンインストール

アンインストール（Windows サーバ）

アプリケーションをアンインストールする前に、すべてのアプリケーションを閉じてください。

注意 Windows オペレーティングシステムの種類により、手順が異なる場合があります。

1. **スタート** > （**プログラム一覧**） > **D-Link** の順にクリックします。
2. D-View8 アプリケーションツールが表示されますので、「Uninstall」をクリックして、アンインストールプロセスを開始します。
3. アンインストールウィザードの指示に従ってアンインストールを実行します。

アンインストール（Linux サーバ）

アプリケーションをアンインストールする前に、すべてのアプリケーションを閉じてください。

注意 Linux サーバへの D-View8 のインストールは未サポートです。

1. su コマンドを使用してログオンし、root アクセス権を取得します。
2. 次のコマンドを入力し、アンインストールプロセスを開始します。

```
dpkg -P dview8
```

3. 以下のプロンプトで、[y] と入力して D-View8 サービスを停止し、処理を続行します。

```
Choose whether to stop D-View 8 Services? [y/n]
```

4. 設定ファイルがアプリケーションからパージされます。続けて、プロンプトで [y] と入力して MongoDB を削除します。

```
Do you want to delete mongodb? [y/n]
```

アプリケーションがアンインストールされます。

D-View7 から D-View8 へのソフトウェアの移行

D-View7 から D-View8 バージョンへ移行するには、D-View8 のインストール後に次の手順を実施する必要があります。

- D-View7 から D-View8 へのデータベースの移行
- D-View7 から D-View8 へのプローブのアップグレード

注意 D-View7 から D-View8 v2.0 以降への直接のアップグレードはサポートされません。最初に D-View8 v1.0.3.39 をインストールし、その後 v2.0.3.88 へアップグレードする必要があります。D-View8 v1.0.3.39 はサポートされませんので、v2.0.3.88 へアップグレードしてご利用ください。

これらの移行プロセスは、D-View8 Web インタフェース（**System > D-View 7 Upgrade**）から実行することができます。
手順を開始する前に、移行プロセス中にソフトウェアのアップグレードが妨げられないように、アンチウイルスソフトウェアが無効になっていることを確認してください。

メモ　D-View8 への移行には以下の処理が含まれます。

- 役割と権限が D-View8 の管理構造に変換されます。（「User Management」）
- プローブ設定が D-View8 の構成に変換されます。（「Sites and Networks」）
- センサ設定が D-View8 の構成に変換されます。（「Monitor & Alarm Settings」）

D-View7 および D-View8 のアーキテクチャ

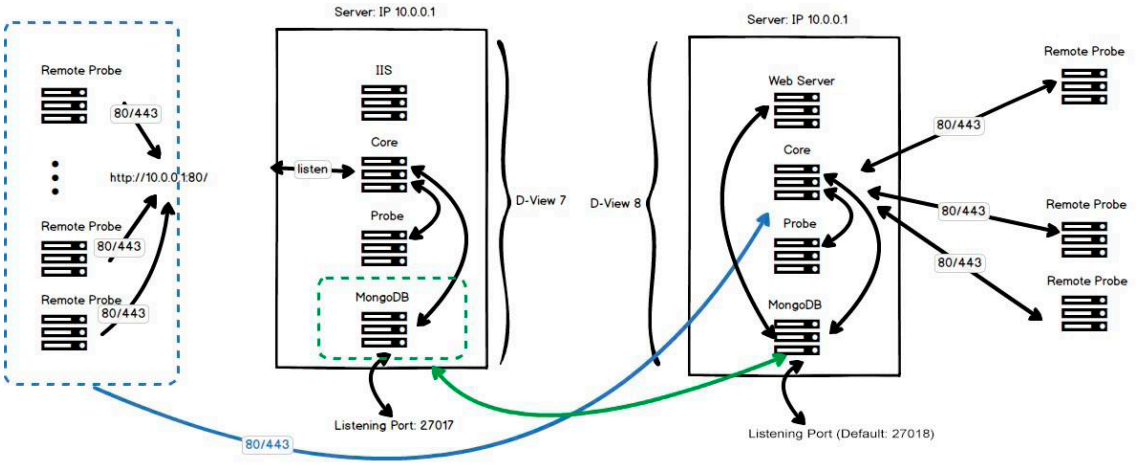


図 2-69　D-View アーキテクチャ

ソフトウェアの移行（D-View7 とは異なるサーバへ D-View8 をインストールする場合）

メモ　D-View8 と D-View7 は異なるサーバにインストール可能です。同じサーバにインストールする手順については、P.71 の「ソフトウェアの移行（D-View7 と同じサーバへ D-View8 をインストールする場合）」を参照してください。

■ D-View7 サービスの停止および IP アドレスの変更

注意　D-View7 から D-View8 への移行作業を行うには、D-View7 のバージョンが v1.5.2.x である必要があります。古いバージョンをご利用の場合、v1.5.2.x へアップグレードしてから本作業を行ってください。D-View7 の最新のアップグレードファイルは D-Link Japan のサイトからダウンロードいただけます。

1. D-View7 サーバで、D-View7 Service Management Tool を開きます。
2. 「Service Management」タブで、「Stop」をクリックして以下の D-View7 サービスを停止します。
   - Windows IIS
   - Core Server
   - License Agent Server
   - Probe Server
   - Probe File Server

   ※ MongoDB インスタンスは停止しないでください。

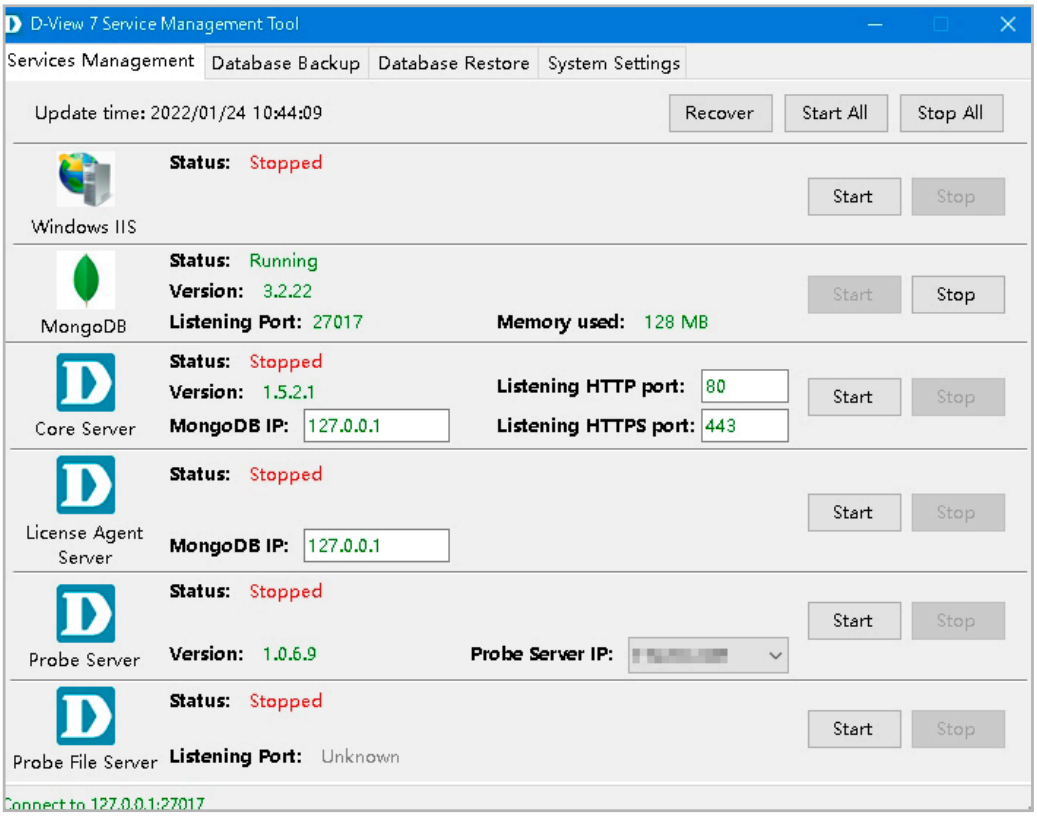


図 2-70　D-View7 サービスの停止

3. Windows のサービス管理画面から、以下の D-View7 関連サービスの「スタートアップの種類」を「手動」または「無効」に設定します。
   - World Wide Web 発行サービス（Windows IIS）
   - D-View7 CoreServer
   - D-View7 License Agent Server
   - D-View7 Probe Server
   - D-View7 Probe File Server

4. 現在のサーバ IP アドレスを D-View8 サーバで使用するために、D-View7 サーバの IP アドレスを変更します。
例えば IP アドレスが 10.0.0.1 の場合は、10.0.0.X に変更します。X は 1 以外の値です。
ここでは、Windows 上で IP アドレス「10.0.0.3」に変更する例を示します。

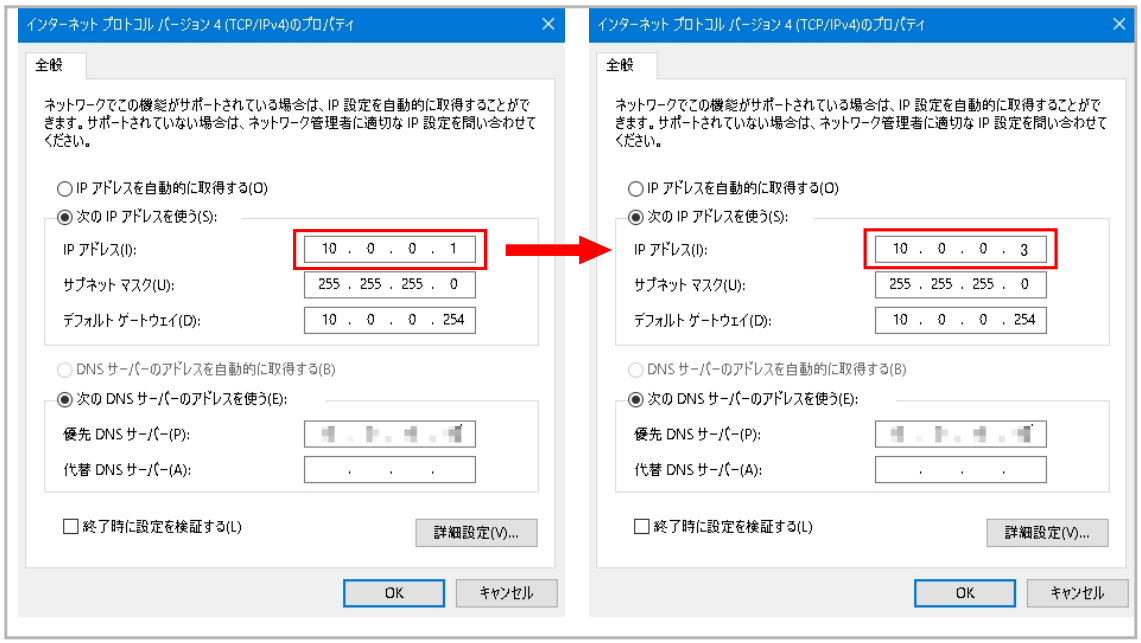


図 2-71　IP アドレスの変更

■ D-View8 のインストール

ダウンロードパッケージによるアップグレード手順は以下の通りです。

5. D-View8 をインストールするサーバ上で、D-Link Japan のサイトから D-View8 インストールパッケージをダウンロードします。

注意 D-View7 から D-View8 v2.0 以降への直接のアップグレードはサポートされません。ここでは、まず D-View8 v1.0.3.39 のインストールを実行する必要があります。

6. インストールパッケージをダブルクリックしてインストールを開始します。

7. 確認メッセージが表示されますので、「はい」をクリックして続行します。

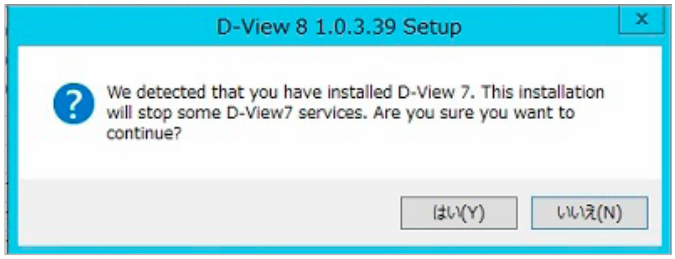


図 2-72　確認メッセージ

8. ウィザードに従い、インストールを実施します。
「Port Configuration」および「Database Service Environment Check」画面では、以下の設定を参照してください。その他インストール手順の詳細は、P.16 の「D-View8 サーバのインストール（Windows サーバ / スタンドアロン構成）」を参照してください。

(1) 「Port Configuration」画面で、以下のようにポートの構成を行います。
- 「Core Port」：D-View7 ポートを使用するように設定する必要があります。デフォルトでは、D-View7 リスニングポートは 80、D-View8 ポートは 17500 に設定されています。「Core Port」の値を 80 に変更します。
- 「Check」：構成設定を検証します。接続が確立できる場合は、「Check Pass!」が表示されます。それ以外の場合は、設定を見直してください。

(2) 「Next >」をクリックして D-View8 サーバのインストールプロセスを続行します。

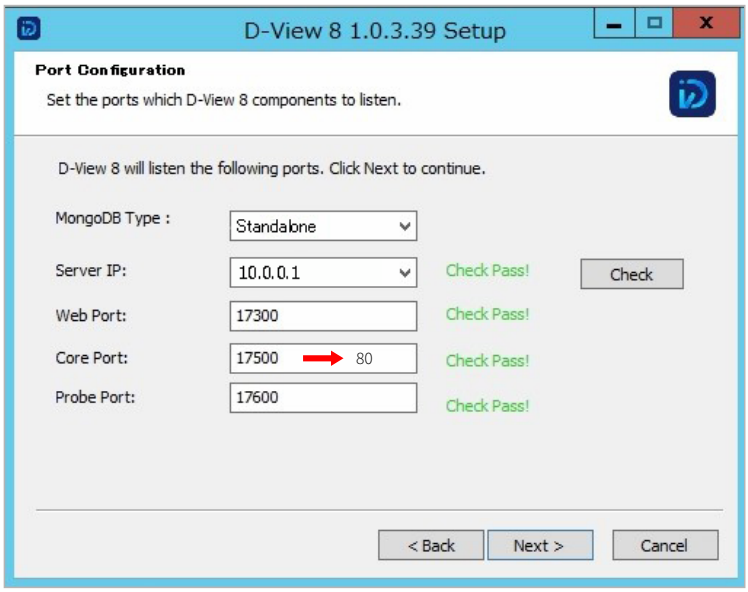


図 2-73　ポート設定

(3) 「Database Service Environment Check」画面では、「Install a new MongoDB」を選択して新規の MongoDB サービスをインストールします。

9. D-View8 サーバのインストール完了後、アプリケーションインタフェースにログインします。P.80 の「Web GUI の起動とログイン」を参照してください。

メモ　D-View8 の最初のログイン時に「ADD LICENSE」画面が表示されます。表示されるメッセージに従い、ライセンスのアクティベーションとパスワード変更を行います。

メモ　D-View8 ログイン時にサインインエラーが発生する場合、ブラウザのキャッシュを削除してから再度ログインしてください。

■ データベースの移行

10. ログイン後、D-View8 のウィザード画面が表示されます。

11. ウィザード画面で「D-View 7 Upgrade」を選択します。本機能により、D-View7 データベースとプローブを D-View8 サーバに移行することができます。

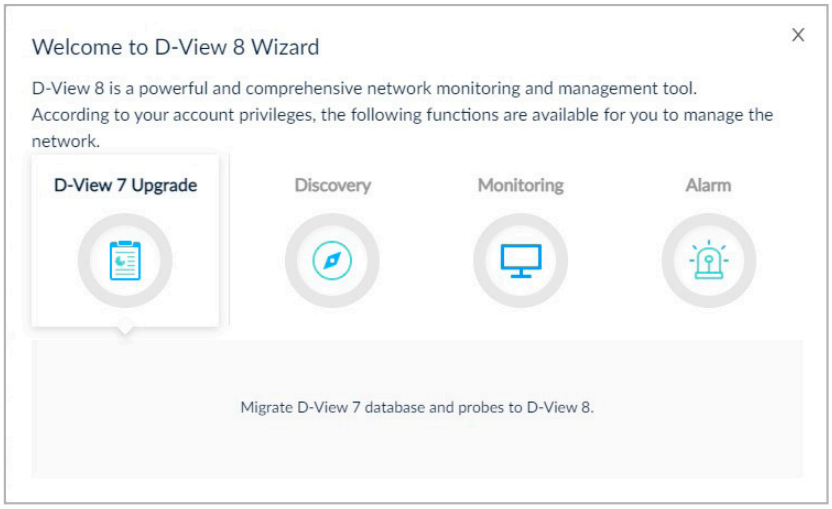


図 2-74　D-View7 アップグレード

メモ　D-View8 に最初にログインした後は、組織名、国、タイムゾーンの設定が必要となります。ウィザードに従って設定を進めてください。ネットワーク検出時に組織の設定が必要になります。

12. 「Database Migration」セクションが表示されます。各項目の設定後、ウィザードの「Next >>」をクリックして次の手順に進めます。
D-View7 MongoDB サーバへの接続を確立するには、次の設定を行う必要があります。

- 「MongoDB Address」：構成済みの新しい IP アドレスとポートを入力します。前の手順を参照してください。
  設定例）
  - IP アドレス : 10.0.0.3
  - ポート : 27017
- 「Authentication」：D-View7 MongoDB サーバが D-View7 インストールウィザードを使用してインストールされている場合、本項目で「SCRAM-SHA-1 (Mongo 3.x default)」を選択します。そうでない場合は「None」を選択します。
- 「Username 」：管理アクセス権を持つ登録済みプロファイル（admin）を入力します。
- 「Password」：管理者プロファイルに対応するパスワードを入力します。
- 「Authentication database」：「admin」と入力します。

メモ　接続の試行が失敗した場合は、認証で「None」を選択し、再度接続の確立を試みてください。

13. 「Connect」をクリックして、D-View7 の MongoDB サーバとの接続を開始します。

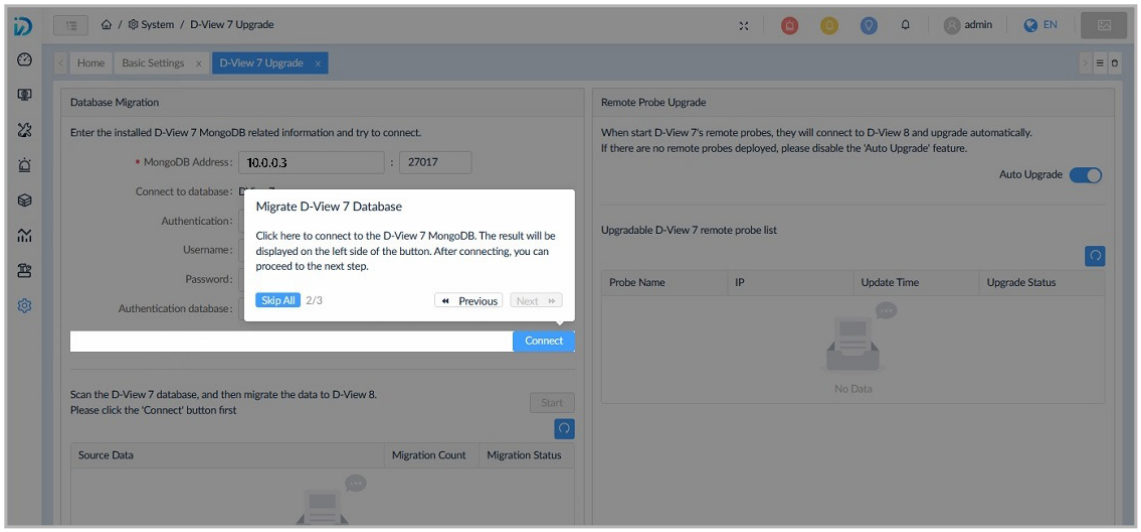


図 2-75　D-View7 MongoDB サーバへの接続

14. 接続に成功すると、「Connected successfully」のメッセージが表示されます。ウィザードの「Next >>」をクリックして手順を進めます。

15. 「Start」をクリックして移行を開始します。ウィザードの「Next >>」をクリックして手順を進めます。

16. 検出データが表示されます。ウィザードの「Next >>」をクリックして手順を進めます。

17. 前の手順に戻るには「<< Previous」をクリック、プロセスを自動化して完了するには「Skip All」をクリックします。

メモ　移行プロセスが中断された場合は、**System > D-View 7 Upgrade** をクリック、またはウィザードから「D-View7 Upgrade」を選択して、プロセスを再開します。

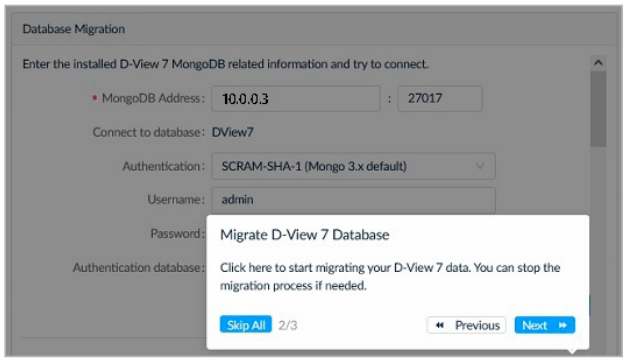


図 2-76　D-View7 の移行の続行

データベースの移行処理が完了すると、D-View8 ローカルプローブはコアサーバへのブリッジとして引き続き動作します。また、リモートプローブについても自動アップグレード機能（デフォルトで有効）により、自動的にアップグレードされます。

元の D-View7 MongoDB のデータは保持され、D-Viiew8 データベースにインポートされます。

■ D-View8 v2.0.3.88 へのアップグレード

18. D-View8 v2.0.3.88 のインストーラを実行し、D-View8 サーバおよびリモート Probe をアップグレードします。

注意　D-View8 v1.0.3.39 はサポートされません。v2.0.3.88 へアップグレードしてご利用ください。

メモ　アップグレード手順については、P.75 の「ソフトウェアのアップグレード」を参照してください。

ソフトウェアの移行（D-View7 と同じサーバへ D-View8 をインストールする場合）

■ D-View7 サービスの停止および IP アドレスの変更

注意　D-View7 から D-View8 への移行作業を行うには、D-View7 のバージョンが v1.5.2.x である必要があります。古いバージョンをご利用の場合、v1.5.2.x へアップグレードしてから本作業を行ってください。D-View7 の最新のアップグレードファイルは D-Link Japan のサイトからダウンロードいただけます。

1. D-View7 サーバで、D-View7 Service Management Tool を開きます。
2. 「Service Management」タブで、「Stop」をクリックして以下の D-View7 サービスを停止します。
   - Windows IIS
   - Core Server
   - License Agent Server
   - Probe Server
   - Probe File Server

   ※ MongoDB インスタンスは停止しないでください。

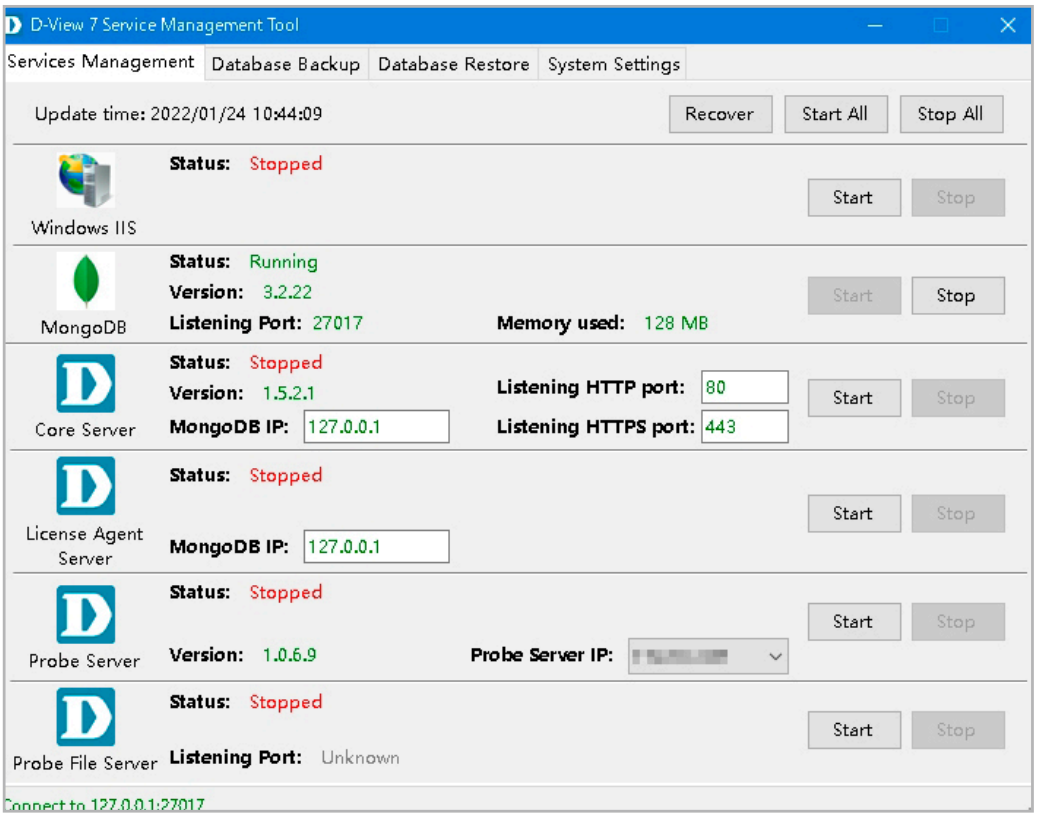


図 2-77　D-View7 サーバサービスの停止

3. Windows のサービス管理画面から、以下の D-View7 関連サービスの「スタートアップの種類」を「手動」または「無効」に設定します。
   - World Wide Web 発行サービス（Windows IIS）
   - D-View7 CoreServer
   - D-View7 License Agent Server
   - D-View7 Probe Server
   - D-View7 Probe File Server

■ D-View8 のインストール

4. D-Link Japan のサイトから D-View8 インストールパッケージをダウンロードします。

注意　D-View7 から D-View8 v2.0 以降への直接のアップグレードはサポートされません。ここでは、まず D-View8 v1.0.3.39 のインストールを実行する必要があります。

5. インストールパッケージをダブルクリックしてインストールを開始します。

6. 確認メッセージが表示されますので、「はい」をクリックして続行します。

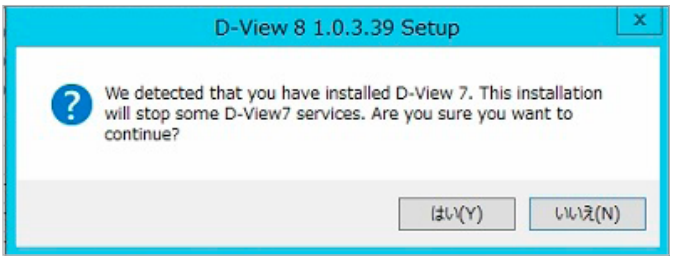


図 2-78　確認メッセージ

7. ウィザードに従い、インストールを実施します。
「Port Configuration」および「Database Service Environment Check」画面では、以下の設定を参照してください。その他インストール手順の詳細は、P.16 の「D-View8 サーバのインストール（Windows サーバ / スタンドアロン構成）」を参照してください。

(1) 「Port Configuration」画面で、以下のようにポートの構成を行います。
- 「Core Port」：D-View7 ポートを使用するように設定する必要があります。デフォルトでは、D-View7 リスニングポートは 80、D-View8 ポートは 17500 に設定されています。「Core Port」の値を 80 に変更します。
- 「Check」：構成設定を検証します。接続が確立できる場合は、「Check Pass!」が表示されます。それ以外の場合は、設定内容を見直してください。

(2) 「Next >」をクリックしてインストールプロセスを続行します。

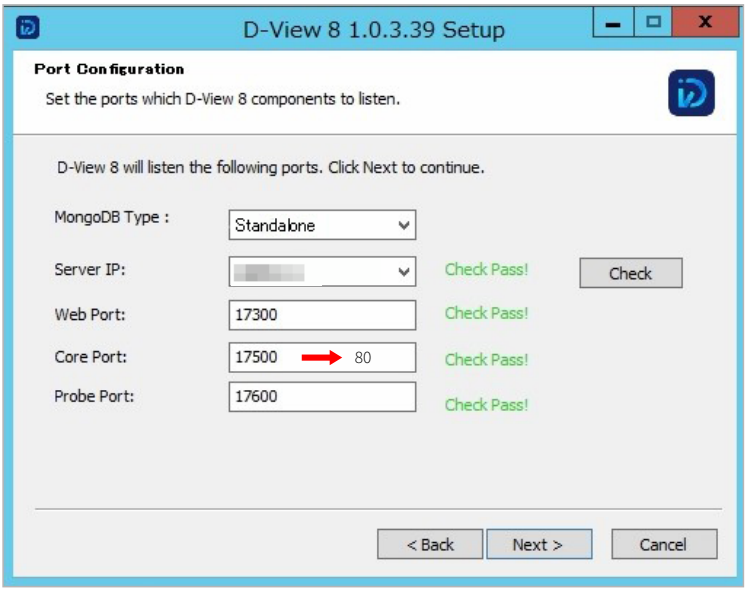


図 2-79　ポート構成

(1) 「Database Service Environment Check」画面では、「Install a new MongoDB」を選択して新規の MongoDB サービスをインストールします。

8. D-View8 サーバのインストールプロセス完了後、アプリケーションインタフェースにログインします。P.80 の「Web GUI の起動とログイン」を参照してください。

メモ　D-View8 の最初のログイン時に「ADD LICENSE」画面が表示されます。表示されるメッセージに従い、ライセンスのアクティベーションとパスワード変更を行います。

メモ　D-View8 ログイン時にサインインエラーが発生する場合、ブラウザのキャッシュを削除してから再度ログインしてください。

■ データベースの移行

9. ログイン後、D-View8 のウィザード画面が表示されます。

10. ウィザード画面で「D-View 7 Upgrade」を選択します。本機能により、D-View7 データベースとプローブを D-View8 サーバに移行することができます。

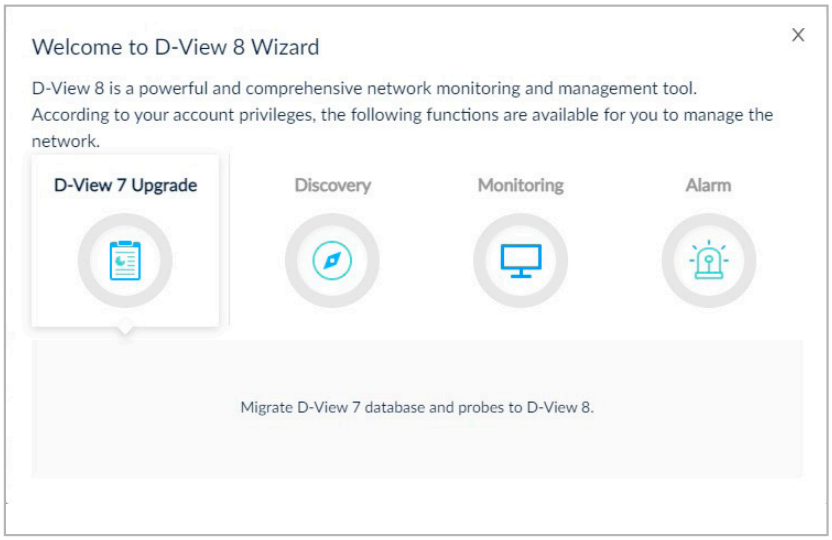


図 2-80　D-View7 アップグレード

メモ　D-View8 に最初にログインした後は、組織名、国、タイムゾーンの設定が必要となります。ウィザードに従って設定を進めてください。

11. 「Database Migration」セクションが表示されます。各項目の設定後、ウィザードの「Next >>」をクリックして次の手順に進めます。
D-View7 MongoDB サーバへの接続を確立するには、次の設定を行う必要があります。
- 「MongoDB Address」：MongoDB サーバ（localhost）の IP アドレスとポートを入力します。
  設定例）
  - IP アドレス : 127.0.0.1
  - ポート : 27017
- 「Authentication」:MongoDB インスタンスが D-View7 インストールウィザードを使用してインストールされている場合、本項目で「SCRAM-SHA-1 (Mongo 3.x default)」を選択します。そうでない場合は「None」を選択します。
- 「Username 」：管理アクセス権を持つ登録済みプロファイル（admin）を入力します。
- 「Password」：管理者プロファイルに対応するパスワードを入力します。
- 「Authentication database」：「admin」と入力します。

メモ　接続の試行が失敗した場合は、認証で「None」を選択し、再度接続の確立を試みてください。

12. 「Connect」をクリックして、D-View7 の MongoDB サーバとの接続を開始します。

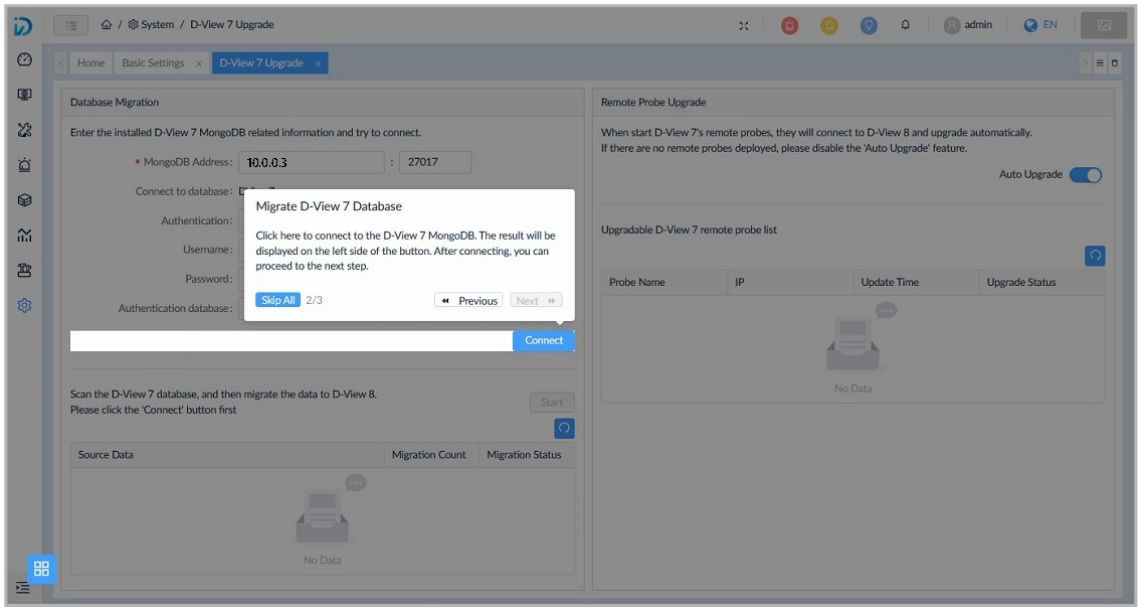


図 2-81　D-View7 MongoDB サーバへの接続

13. 接続に成功すると、「Connected successfully」のメッセージが表示されます。ウィザードの「Next >>」をクリックして手順を進めます。
14. 「Start」をクリックして移行を開始します。ウィザードの「Next >>」をクリックして手順を進めます。
15. 検出データが表示されます。ウィザードの「Next >>」をクリックして手順を進めます。
16. 前の手順に戻るには「<< Previous」をクリック、プロセスを自動化して完了するには「Skip All」をクリックします。

メモ　移行プロセスが中断された場合は、**System > D-View 7 Upgrade** をクリック、またはウィザードから「D-View7 Upgrade」を選択して、プロセスを再起動します。

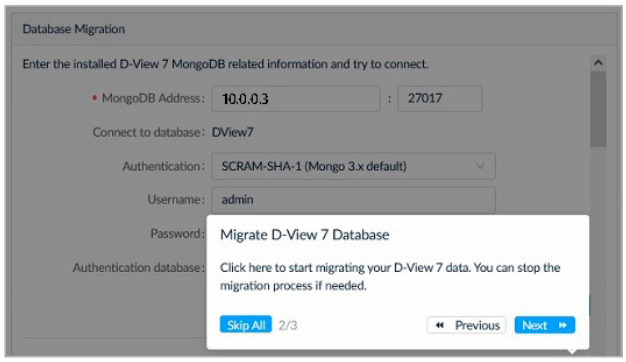


図 2-82　D-View7 の移行の続行

データベースの移行処理が完了すると、D-View8 ローカルプローブはコアサーバへのブリッジとして引き続き動作します。また、リモートプローブについても自動アップグレード機能（デフォルトで有効）により、自動的にアップグレードされます。

元の D-View7 MongoDB のデータは保持され、D-Viiew8 データベースにインポートされます。

■ D-View8 v2.0.3.88 へのアップグレード

17. D-View8 v2.0.3.88 のインストーラを実行し、D-View8 サーバおよびリモート Probe をアップグレードします。

注意　D-View8 v1.0.3.39 はサポートされません。v2.0.3.88 へアップグレードしてご利用ください。

メモ　アップグレード手順については、P.75 の「ソフトウェアのアップグレード」を参照してください。

ソフトウェアのアップグレード

D-View7 から D-View8 へ移行する場合、D-View8 v1.3.0.39 のアップグレード機能を利用します。v1.3.0.39 での利用はサポートされませんので、データベースの移行が完了した後、D-View8 v2.0.3.88 へのアップグレードを実行してください。

D-View8 v2.0.3.288 へのアップグレード（サーバアプリケーション）

1. D-View8 v2.0.3.88 のインストーラを実行し、D-View8 サーバをアップグレードします。
2. 以下の確認メッセージが表示されますので、「OK」「はい」をクリックします。

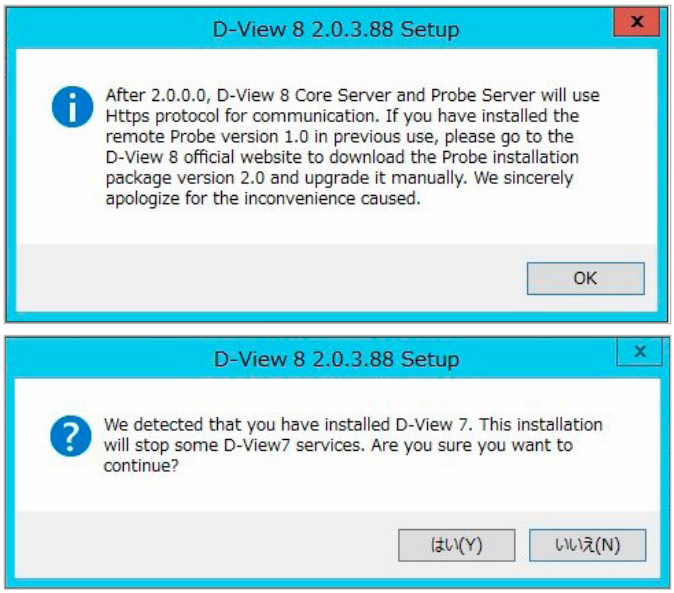


図 2-83　確認メッセージ

3. 「Welcome」画面で「Next >」をクリックします。

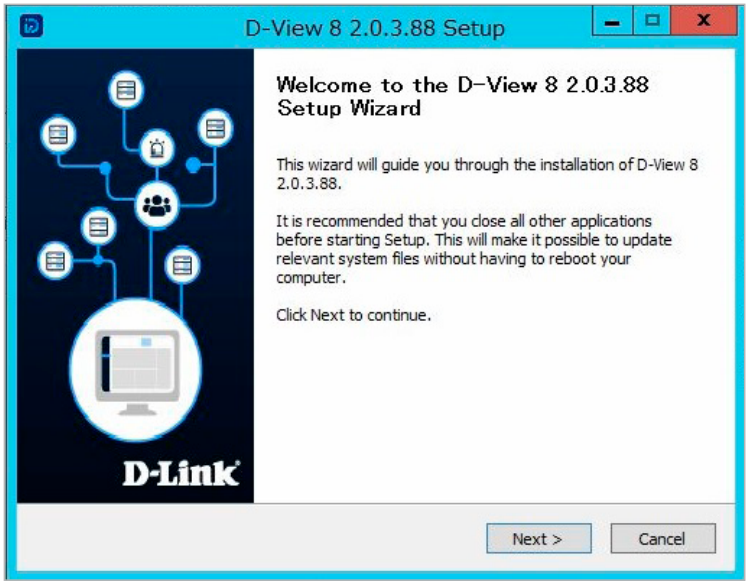


図 2-84　確認メッセージ

4. 古いバージョンのサーバがインストールされていることが自動的に検出されます。「Upgrade My D-View8」にチェックを入れたまま、「Next」をクリックします。

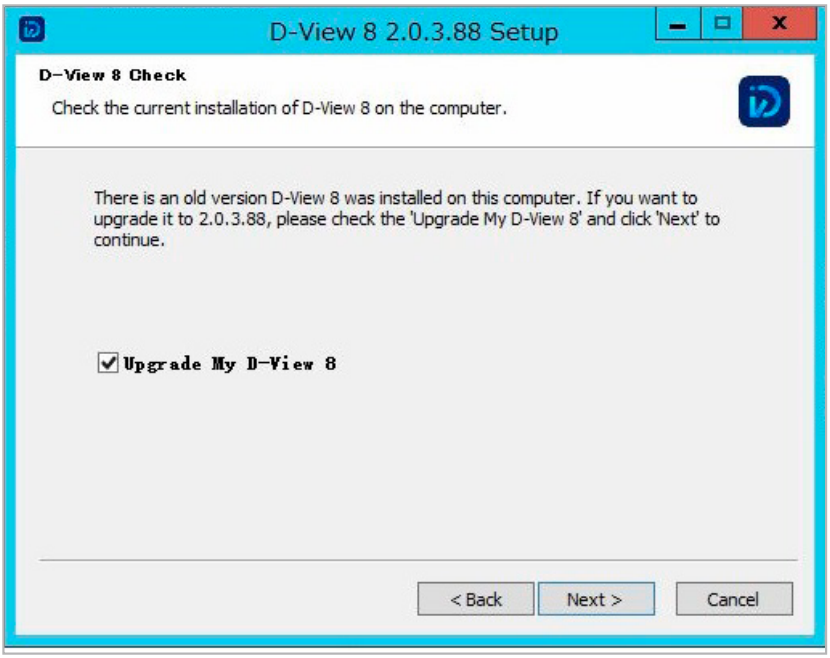


図 2-85　D-View8 v2.0.3.88 へのアップグレード

5. D-View8 のアップグレードが開始され、進捗状況が表示されます。インストール完了後、「Next >」をクリックします。

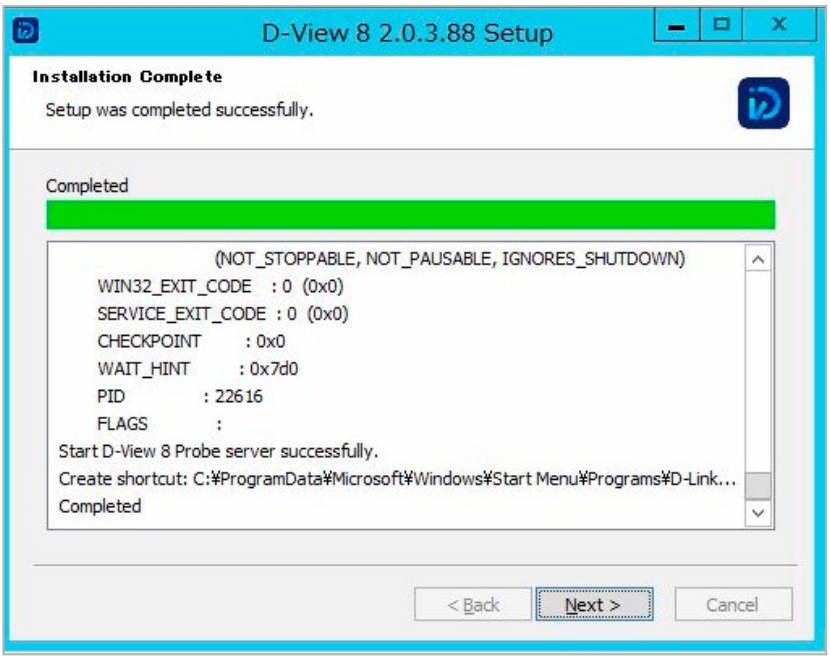


図 2-86　インストール完了

6. 「Finish」をクリックし、セットアップウィザードを終了します。

図 2-87　ウィザードの終了

メモ　D-View8 ログイン時にサインインエラーが発生する場合、ブラウザのキャッシュを削除してから再度ログインしてください。

D-View8 v2.0.3.88 へのアップグレード（リモート Probe）

D-View8 v2.0.3.88 の Probe インストーラを実行し、すべてのリモート Probe について、D-View8 リモート Probe をアップグレードします。

1. 接続ステータスとリモートプローブの IP アドレスを確認します。

   (1) D-View8 Web アプリケーションにログインします。

   (2) **System > Server Management** に移動し、「Probe」タブを選択します。

   (1) Probe の一覧で、コアサーバとリモートプローブの情報を確認できます。リモートプローブは、コアサーバと切断されていることを示す赤色で表示されます。

2. リモート Probe 上で、インストーラをダブルクリックします。

3. 以下の確認メッセージが表示されます。コアサーバが想定のバージョンにアップグレード済みであることを確認してください。

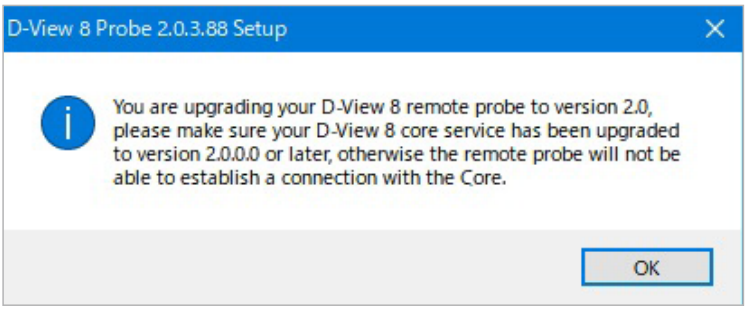


図 2-88　確認メッセージ

4. 「Welcome」画面で「Next >」をクリックします。

図 2-89　確認メッセージ

5. 古いバージョンのプローブがインストールされていることが自動的に検出されます。「Upgrade My D-View8 Probe」にチェックを入れたまま、「Next」をクリックします。

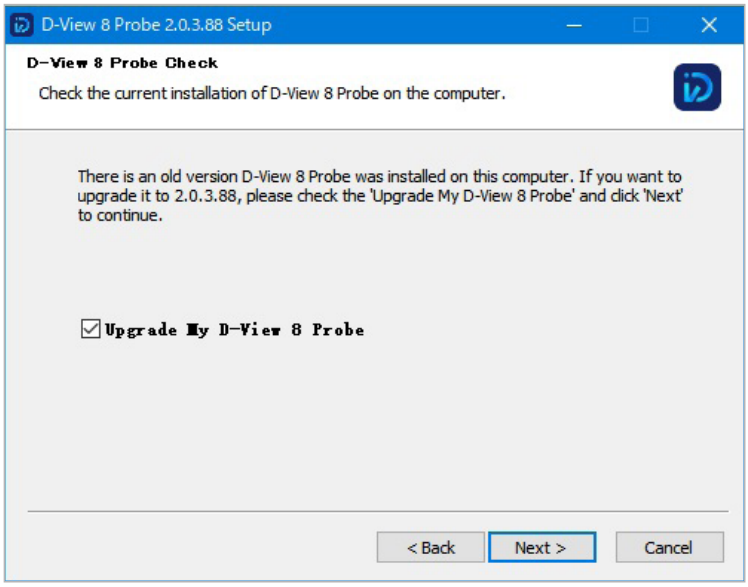


図 2-90　Probe チェック

6. D-View8 のインストールが開始され、進捗状況が表示されます。

7. インストール完了後、「Close」をクリックします。

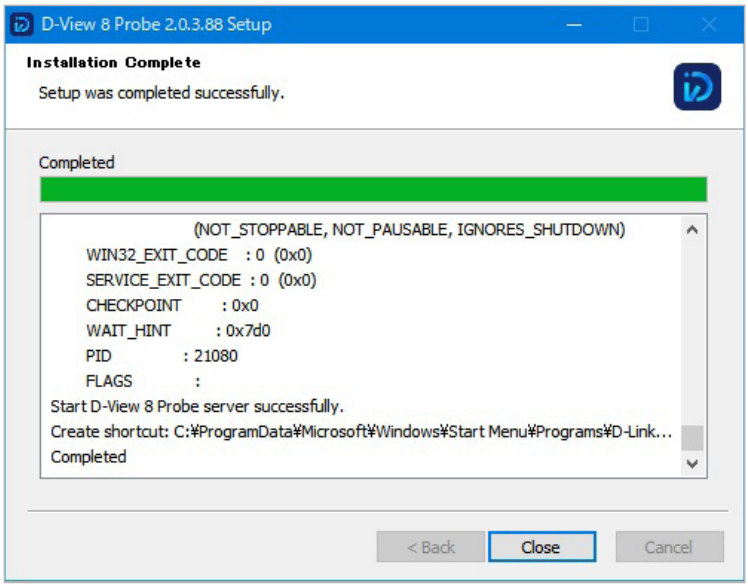


図 2-91　Probe インストール完了

8. D-View8 管理画面の Probe リストからリモート Probe の接続ステータスを確認できます（**System > Server Management Probe**）。

第 3 章　D-View8 の利用を開始する

D-View8 の利用を開始するには、D-Viiew8 ソフトウェアをインストールする必要があります。インストール手順については、P.16 の「第 2 章　製品のインストール」を参照してください。

注意 アプリケーションへのログイン後、パスワードを変更することを強くお勧めします。また、アカウント情報、アラート通知に使用する電子メール設定を構成することをお勧めします。

本章では、以下のトピックについて説明します。

- 「Web GUI の起動とログイン」
- 「Web ダッシュボードについて」
- 「ユーザパスワードの変更」
- 「通知用の電子メールサーバの設定」
- 「通知センターの設定」

Web GUI の起動とログイン

本アプリケーションは、Web ブラウザ経由でアクセスすることができます。アプリケーションにログインする前に、接続先サーバに D-View8 がインストールされていること、固定 IP アドレスが設定されていることをご確認ください。

注意 D-View8 は複数ユーザによる同時利用をサポートしています。複数のユーザが同じ設定に変更を加える可能性がありますので、D-View8 で作業を開始する前に、アクティビティの管理を調整することをお勧めします。

アプリケーションにログインするには :

1. ブラウザを開き、D-View8 サーバに割り当てられている IP アドレスを入力します。
   - アプリケーションがインストールされている D-View8 サーバ上から接続する場合は、ローカルホストの URL を入力します。
     - 例）https://localhost:17300（デフォルトポート「17300」を使用）
   - リモートコンピュータに接続する場合は、Web ブラウザのアドレスバーに D-View8 サーバの IP アドレスを入力します。D-Viiew8 サーバにアクセスする前に、ブラウザのキャッシュデータを削除します。

   以下のログイン画面が表示されます。

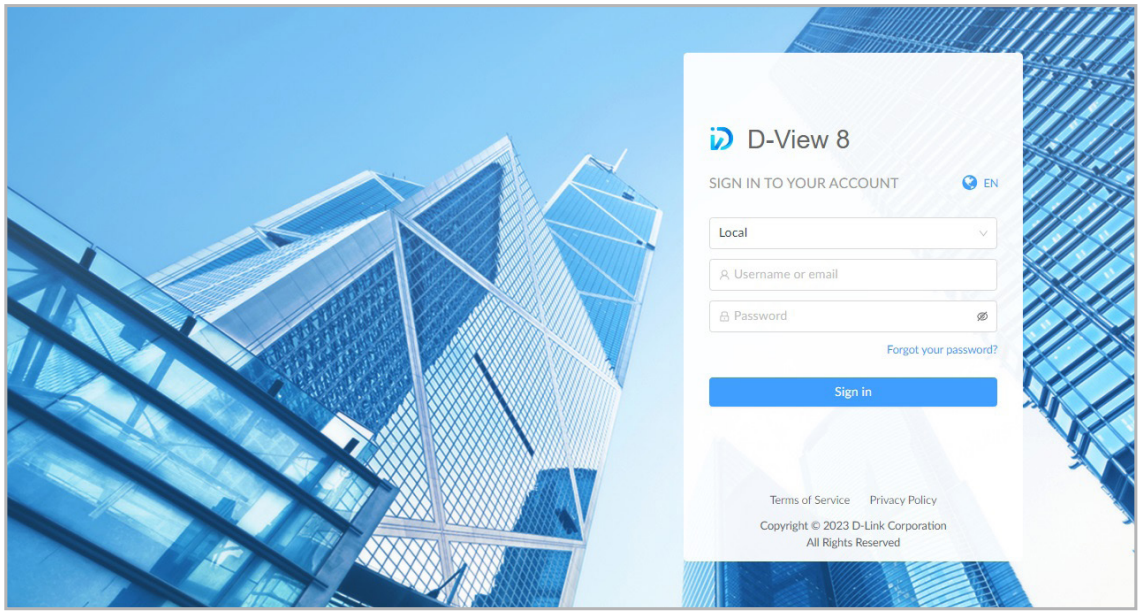


図 3-1　D-View8 ログイン画面

2. ドロップダウンメニューからユーザの定義済みアカウントタイプを選択します。
   - 「Local（ローカル）」: ローカルシステムで認証されるユーザアカウント。
   - 「RADIUS」: RADIUS（Remote Authentication Dial-In User Service）によって認証されるユーザアカウント。
   - 「Active Directory」: Microsoft Active Directory によって認証されるユーザアカウント。

図 3-2　アカウントへのサインイン

3. ユーザ名とパスワードを入力します。デフォルトでは、管理者ユーザ名 / パスワードは admin/admin です。

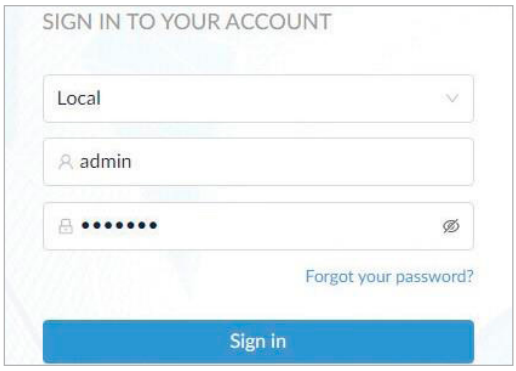


図 3-3　資格情報（ユーザ名とパスワード）の入力

4. 「Sign in」ボタンをクリックしてログインします。ダッシュボード画面が表示されます。

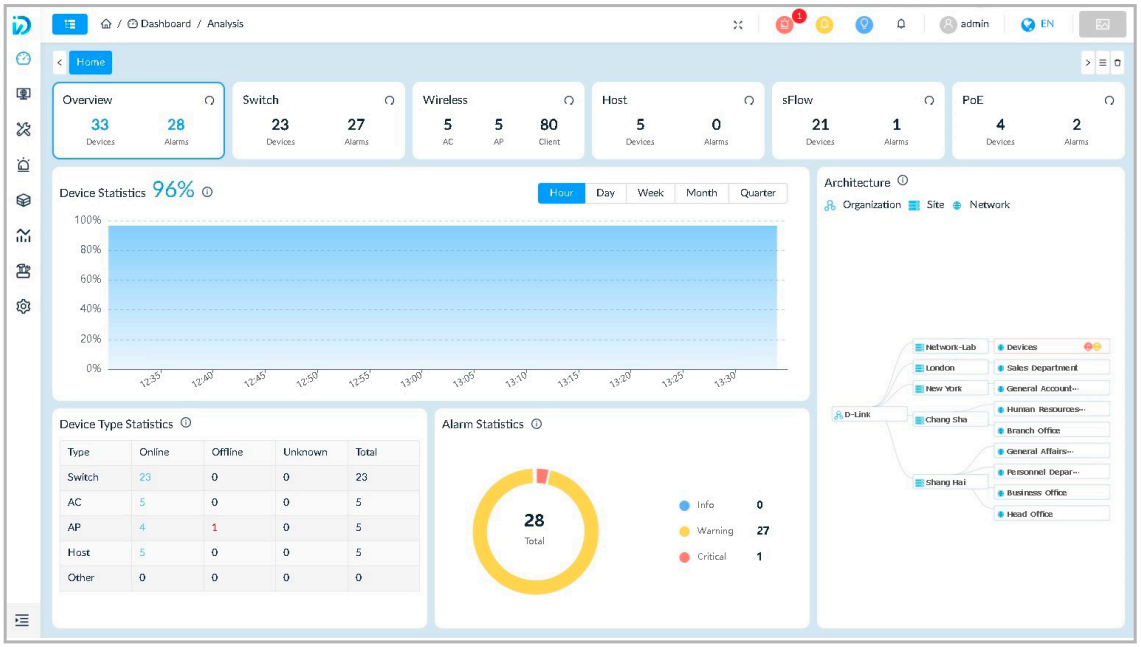


図 3-4　D-View8 ダッシュボードの表示

ダッシュボードの詳細は、P.83 の「Web ダッシュボードについて」を参照してください。

初回ログイン時のネットワーク設定

「Super Administrator」（デフォルトの admin アカウント）で最初にアプリケーションにログインすると、ウィザード画面が表示されます。「Discovery」タブを選択し、以下の手順を実施します。

（メモ）ネットワークプロファイルの構成やデバイスの検出は後から設定することもできます。ただし、ネットワーク設定を追加していない場合、ログイン時に再度ウィザードが表示されます。

1. 初回ログイン時は組織名などの必須の情報を設定する必要があります。ウィザードに従い設定を行います。
2. 「＋ Add Network」をクリックし、「Add Network」画面を開きます。
3. 以下の情報を入力し、ネットワークを作成します。
   - 「Network Name」：ネットワーク名を入力します。
   - 「Site Name」：サイト名を設定します。
4. Probe を選択します。ネットワークでデバイスを検出し、通信を行うには Primary プローブを設定する必要があります。
5. 「＋ Add Discovery Range」をクリックします。
6. 検出方法（IP、IP 範囲、サブネット、CSV インポート）を指定し、検出範囲を指定します。　詳細は、P.96 の「ネットワークの検出」を参照してください。
7. SNMP 項目で「Add SNMP Credential」を選択します。SNMP プロトコルにより、デバイス管理を行います。
8. 「Save」をクリックしてネットワーク検出設定を保存します。定義したネットワークに対しデバイスの検出が実行されます。

Web ダッシュボードについて

D-View8 ダッシュボードの機能には、Web インタフェースのメニューからアクセスできます。ユーザ権限により、表示されるツールが異なります。

Web ダッシュボードの見方

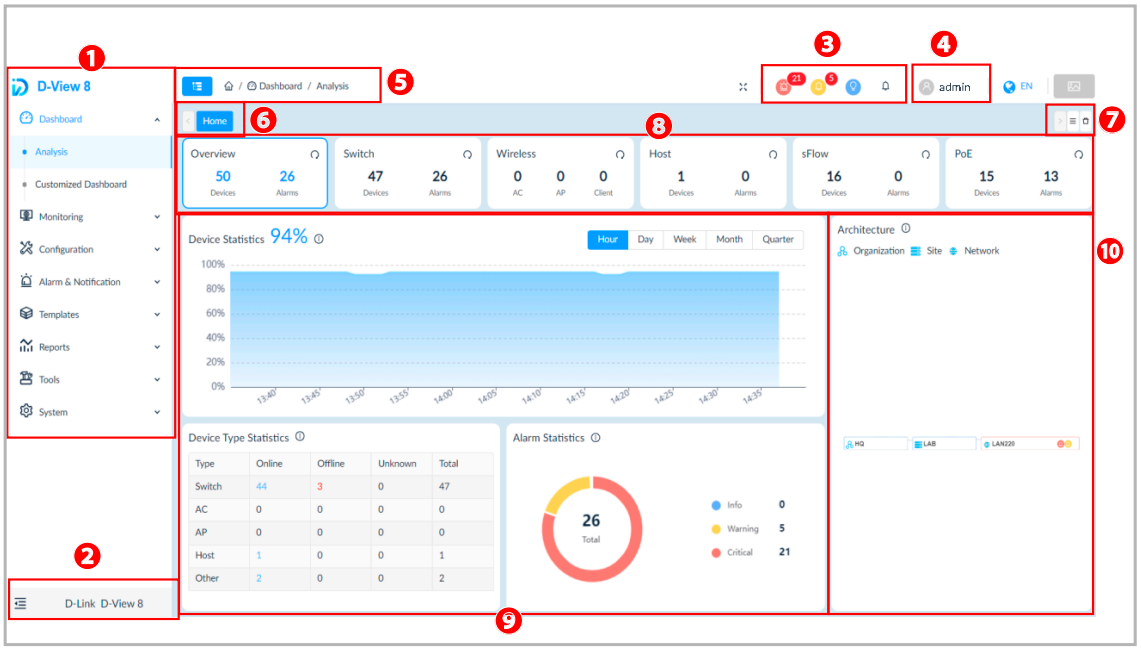


図 3-5　　ダッシュボード

Web ダッシュボードの見方

項番	項目	説明
1	メインメニュー	機能項目がツリー表示されます。本メニューから、各機能の画面にアクセスします。
2	メインメニュー（サイドバー）の折りたたみ / 展開	メインメニュー（サイドバー）の表示 / 非表示を切り替えます。
3	通知アイコン	システム状態の通知アイコンが表示されます。
4	ユーザプロファイル & ウィザード	ユーザプロファイルの構成やウィザードによる設定、ログアウト操作などを行います。
5	ナビゲーションメニュー	表示画面のナビゲーションメニューが表示されます。
6	メニュータブ	開いた画面の履歴がタブとして表示されます。タブをクリックして画面を表示することができます。
7	メニューセレクタ	開いた画面の履歴一覧から表示画面を選択したり、履歴を削除することができます。
8	ウィジェットメニュー	デバイス種類別に、管理デバイスとアラーム統計が表示されます。このメニューをクリックすると、下部に統計情報が表示されます。
9	ウィジェット（統計情報）	システムで定義されたウィジェットが表示されます。
10	アーキテクチャ図	ネットワークアーキテクチャが表示されます。

また、D-View8 のダッシュボードでは以下の共通機能が利用できます。

- テーブルに表示されているデータは、列名をクリックしてソートしたり、キーワード検索やフィルタを実行することができます。
- ⓘ にマウスオーバーすると、機能の Help 情報が表示されます。
- メイン画面では、上部ツールバーから共通のツール機能または関連画面にすばやくアクセスできます。

図 3-6　　検索フィールド / ツール機能

- 統計データ内の項目がハイパーリンクになっている場合、リンクをクリックして関連する詳細データを確認できます。

機能一覧

D-View8 ダッシュボードで使用できるメニューおよびそれらの機能について説明します。

注意　利用可能なメニューや設定は、ログインユーザやライセンス、デバイスの種類などによって異なります。

カテゴリ	項目	説明
Dashboard（ダッシュボード）		
Analysis		Analysis 画面上部には、デバイスの種類毎に以下の 6 つのタブが表示されます。 ・「Overview」 ・「Switch」 ・「Wireless」 ・「Host」 ・「sFlow」 ・「PoE」 選択したデバイスカテゴリについて、アラーム統計、Online/Offline ステータス、CPU/ メモリ使用率などのデバイス情報の概要を提供します。デバイスの種類などにより、表示される情報が異なります。
Customized Dashboard		ダッシュボードをカスタマイズして、指定した情報を表示するように設定できます。
Monitoring（モニタリング）		
Network Discovery		次のネットワーク検出パラメータを設定できます。 ・「Basic Information（基本情報）」：検出するネットワークとサイトの名前。 ・「Probe Mode（プローブモード）」：プライマリ / セカンダリプローブを選択します。 ・「Discovery Range（検出範囲）」:検出範囲として、単一の IPv4/IPv6 アドレス、IPv4/IPv6 アドレス範囲、IPv4/IPv6 サブネット、またはファイルからの範囲のインポートを指定することができます。 ・「Schedule Information（スケジュール情報）」：1 回のみの検出、または繰り返しの検出スケジュールを定義します。 検出ルールの実行ステータスと関連する詳細情報を表示します。 注意　IPv6 デバイスの管理はサポートされません。
Device View		デバイスの管理は以下の 5 つのカテゴリに分類されます。 ・「All（すべて）」 ・「Managed（管理）」 ・「Unmanaged（非管理）」 ・「Ignored（無視）」 ・「Conflicted（競合）」 デバイスタイプ（スイッチ、無線、ホスト、その他）ごとに、各デバイスの概要を表示します。 システム名のリンクをクリックすると、各デバイスの詳細情報を確認できます。 IP アドレスにマウスオーバーし、接続プロトコルを選択すると、デバイスの管理インタフェースに接続することができます。
Interface View		デバイスの接続インタフェースに関する情報を表示します。以下の項目が含まれます。 ・システム / モデル名 ・デバイスの IP アドレス ・インタフェース情報（インデックス / インタフェース名 /MAC アドレス） ・接続先情報（MAC アドレス / インタフェース名） ・VLAN 情報（VLAN ID/VLAN 名 /VLAN タイプ /VLAN ポートステータス） ・更新時間 これら値を元に、デバイスを検索することができます。
Topology Map		・組織 / サイト / ネットワークにおけるデバイス間の接続情報について表示します。 ・デバイスの Online/Offline ステータス、リンク情報などを確認することができます。 ・トポロジの背景として PNG または JPG 形式の画像ファイルをアップロードすることができます。 ・サポートされるトポロジレイアウトの種類：スター / ツリー / 円形 / グリッド ・トポロジマップのズームイン / ズームアウトが可能です。 ・カスタマイズトポロジを設定できます。

カテゴリ	項目	説明
Connection View		インタフェースのリンク情報を表示します。 • リンクステータス • アラーム • リンク名 • 接続デバイスの情報（IP アドレス / 接続インタフェース） • トラフィック統計（TX/RX） • リンク使用率 • リンクの種類（LACP または General） • 最終更新時間 • 検知ソース（LLDP や FDB など） リンク名をクリックすると、以下のような詳細情報が表示されます。 • 選択したリンクの概要情報 • 選択したリンクの監視情報 • 選択したリンクのアラーム情報
Rack View		デバイスラックを視覚的に表示、管理します。
sFlow Analyzer		デバイスから sFlow データを収集し、関連する統計レポートを生成します。 以下の種類の統計レポートを確認することができます。 • パケットの送信元または宛先に基づくレポート • QoS ルールに基づくレポート • レイヤ 4 アプリケーションに基づくレポート • プロトコルに基づくレポート • 2 つのエンドポイントのカンバセーションに基づくレポート
Device Group		デバイスグループを作成します。これにより、管理タスクを簡素化することができます。
Configuration（設定）		
Batch Configuration		複数のデバイスに対して一括で設定を行うことができます。 2 つのサブ機能： • 「Quick Configuration（クイック設定）」：各機能のテンプレートを利用して設定を行います。 • 「Advanced Configuration（詳細設定）」：特定のタイプのデバイスに対して複数の機能のパラメータを含むプロファイルを作成できます。同じタイプ / モデルに属する複数のデバイスに同一のプロファイルを適用できます。
Task Management		作成したタスクを表示して、実行結果を確認します。 • 「Current Task」：現在のタスクを表示します。 • 「Historical Task」：過去のタスクを表示します。 タスクが失敗した場合、その原因を確認することができます。
Firmware Management		デバイスのファームウェアを集中管理します。 • スケジュールを指定してデバイスをアップグレードできます。
Configuration Management		デバイスのコンフィグレーションファイルのバックアップ / リストアを行います。 • 複数デバイスのコンフィグレーションファイルを同時にバックアップ / リストアすることができます。 • スケジュールを指定してファイルをバックアップ / リストアできます。
File Management		コンフィグレーションファイル、ファームウェアファイルの管理を行います。 • ファイル比較により、2 つのコンフィグレーションファイルの差分を確認します。 • D-View8 にコンフィグレーションファイル / ファームウェアファイルをアップロードします。 • コンフィグレーションファイルをベースラインファイルとして指定することで、ファイルのバージョン管理に役立てることができます。
Alarm & Notification（アラームと通知）		
Alarms	ネットワークデバイスから収集されたすべてのアラーム情報を表示します。	
	Active Alarms	未確認のすべてのネットワークアラームを表示します。
	Historical Alarms	確認済みのすべてのネットワークアラームを表示します。

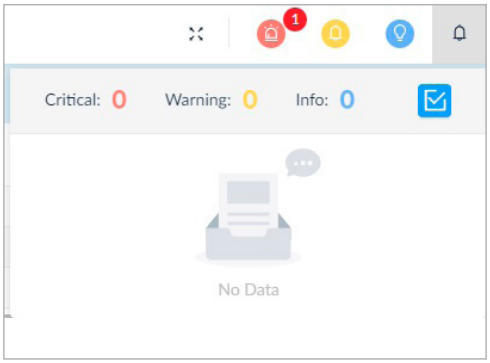
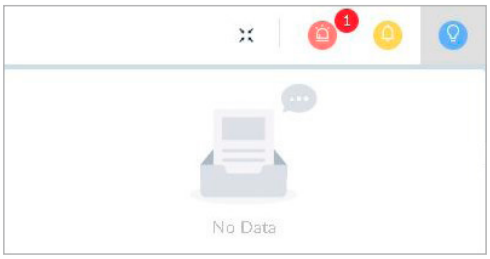
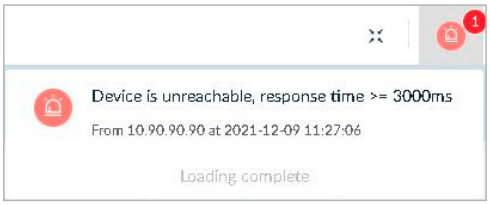
カテゴリ	項目	説明
Trap & Syslog	デバイスから受信したトラップおよびシステムログを表示します。	
	Trap	トラップログには以下の情報が含まれます。 • 受信時刻 • デバイスシステム名 • デバイスの IP アドレス • SNMP バージョン • 標準トラップタイプ • トラップの説明 • トラップの元のメッセージ
	Syslog	Syslog には以下の情報が含まれます。 • 受信時刻 • Syslog を生成するデバイスのシステム名 • デバイスの IP アドレス • Syslog 重大度 • Syslog メッセージ
Trap & Syslog Editor	トラップ OID の説明、Syslog のキーワードとその説明を編集します。	
Monitor & Alarm Settings	Monitor Settings	監視の ON/OFF ステータスや、データを収集する間隔を設定します。
	Alarm Settings	アラームルールとして、アラーム生成のトリガとなるデータしきい値を設定します。 アラームがトリガされたときにデバイスや D-View サーバが実行する CLI コマンドを設定します。
Notification Center	アラームがトリガされたときの通知方法を設定できます。通知方法として、Web スクロールメッセージ、電子メール、実行スクリプトを指定可能です。	
Templates（テンプレート）		
Device Template	D-View8 で管理するデバイスがデフォルトの管理対象リストにない場合に、そのデバイスを追加するためのツールです。本機能は、特にサードパーティ製デバイスの管理に役立ちます。 以下の項目を定義することができます。 • モデル名 • デバイスタイプ • ベンダ名 • デバイスのシステム OID（SOID） • ハードウェアバージョン • パネルテンプレート	
Device Support	サードパーティベンダやデバイスを管理するための情報を定義することができます。	
	Vendor	以下の項目によりベンダを定義します。 • ベンダ名 • ベンダ OID
	Device Category	以下の項目によりデバイスカテゴリを定義します。 • カテゴリ名 • カテゴリの画像
	Device Type	以下の項目によりデバイスタイプを定義します。 • デバイスタイプ名 • デバイスカテゴリ • 説明
Panel Template	D-Link デバイスの定義済みパネルテンプレートに加え、カスタマイズしたパネルを作成できます。 以下の項目を定義することができます。 • パネルの詳細： 　- テンプレート名 　- 説明 • パネル図： 　- パネルロゴ（PNG または JPG 形式、2MB 未満） 　- パネルの高さと幅 　- ポート番号規則 　- ポートレイアウト設計	

カテゴリ	項目	説明
Monitor Template	デバイス情報を収集するための様々な監視テンプレートを提供します。 監視テンプレートはデバイステンプレートに紐づけることができます。	
	Monitor Category	監視のデータソースを識別するためのカテゴリを定義します。 • カテゴリ名 • ユニット（-、℃、%、bits、bps、ms、pps、rpm） • プロトコル（SNMP、HTTP(S)、WMI） • 折れ線グラフ（Not Supported（デフォルト）、Support） • 説明
	Monitor Template	定義済みデータソースを監視および収集するための監視テンプレートを定義します。 • テンプレート名 • 監視カテゴリ • ベンダ名 • 監視間隔 • 説明
Configuration Template	デバイスを設定するための設定テンプレートを提供します。 設定テンプレートはデバイステンプレートに紐づけることができます。	
	Configuration Category	設定の種類を分類するカテゴリテンプレートを定義します。 • カテゴリ名 • 設定の種類（Quick Configuration/Advanced Configuration） • テンプレートの説明 • テンプレート情報
	Configuration Template	特定のデバイスを設定する設定テンプレートを定義します。 • テンプレート名 • ベンダ名 • テンプレートの説明 • 設定カテゴリの選択 • 設定方法（SSH/Telnet または SNMP） • CLI コマンドリスト（SSH/Telnet が選択されている場合） • ドラッグ & ドロップによる GUI オブジェクトの配置・構成
Reports（レポート）		
General Reports	D-View8 で用意されているテンプレートレポートに対し、各レポートに応じた設定パラメータ（データソースやデータ収集間隔など）を設定することができます。生成されたレポートはエクスポートしたり、マイレポートに保存したり、スケジュール化することができます。以下のレポートが利用可能です。 • デバイスレポート - デバイスの正常性 - トラップ - Syslog - デバイス Top N • 有線インタフェースレポート - 有線トラフィック - 有線スループット Top N • 無線レポート - 無線クライアント数 - 無線トラフィック • アドバンストレポート - インベントリ	
Scheduled Report	レポートは、1 回のみまたは繰り返しのスケジュールレポートに設定することができます。	
My Reports	「My Reports」カテゴリには、「General Reports」の中で「My Reports」として分類された保存済みレポートリストが表示されます。最大 500 件のレポートエントリを保存できます。	
Tools（ツール）		
MIB Browser	MIB データを読み取り可能な形式で取得して表示します。 MIB 情報をグラフィカルインタフェースで確認することができます。	
MIB Compiler	デバイスの MIB ファイルを D-View8 にコンパイルします。適切な形式の標準または拡張 MIB のコンパイルが可能です。コンパイルされた MIB は MIB ブラウザで管理することができます。	
ICMP Ping	デバイスの動作状態とネットワークのパフォーマンスを確認します。	
SNMP Test	SNMPv1/v2c/v3 を使用してデバイスの SNMP 機能をチェックします。	
Trace Route	ネットワーク経路をチェックし、ネットワークを通過するパケットの伝送遅延を測定します。	
CLI	ターミナルインタフェースを利用してデバイスに接続します。	

カテゴリ	項目	説明
File Comparison	2 つのコンフィグレーションファイルを比較し、差分を確認します。 差分箇所はハイライト表示されます。	
System（システム構成）		
Basic Settings	Organization	組織の名前、ロゴ、国、タイムゾーンを設定します。
	Mail Server Settings	メールサーバを設定します。
	Forward Trap	トラップメッセージの送信先トラップレシーバを設定します。
	Forward Syslog	Syslog メッセージの送信先システムログレシーバを設定します。
	REST API	他のアプリケーションが D-View8 からトークンを取得するための API キーを生成します。 サードパーティ製アプリケーションはトークンを使用して D-View8 から必要な情報を取得できます。
	Credentials	SNMP プロトコルバージョン、コミュニティ名、その他関連パラメータを設定します。 また、Windows WMI（Windows Management Instrumentation）および SSH/Telnet の資格情報を定義することもできます。
	sFlow Settings	各種トラフィックインジケータに対し、sFlow パラメータマッピングを設定します。
	System Preferences	D-View8 Web インタフェースのテーブル表示パラメータとテーマを設定します。
User Management	Users	ユーザの電子メールアドレス、ユーザ名、ログイン時間、認証タイプなどを表示します。 ユーザの追加、編集、削除を行います。
	Role Privileges	ユーザ役割（組織 / サイト / ネットワーク）における機能毎のアクセス権限を一覧表示します。
	AD Server	Windows Active Directory Server の情報を設定します。
	RADIUS Server	RADIUS サーバの情報を設定します。 プライマリ / セカンダリ RADIUS サーバ設定をサポートしています。
Scheduling	Recurrent Schedule List	繰り返しのスケジュールを定義できます。頻度や期間を設定します。
	Time Range Schedule List	勤務時間など、指定曜日の特定の範囲の時間を定義できます。
Server Management	Probe Core Server Web Server	D-View Core Server、Web Server、Probe のステータスを監視します。 CPU/ メモリ / ハードドライブ / ネットワークトラフィックの使用量など、サーバステータスのレポートをチェックします。
D-View 8 Log	User Operation Log	Web インタフェースにおけるユーザ操作アクティビティのログが保存されます。
	System Log	サーバとプローブについて、D-View8 のオンライン / オフラインステータスのログが保存されます。
	Device Maintenance Log	デバイスに対する設定操作のログが保存されます。
D-View 7 Upgrade	D-View7 から D-View8 へアップグレードするための機能を提供します。 メモ　本機能は現在のバージョンでは利用できません。D-View7 からアップグレードを行う場合に、D-View8 v1.0.3.39 を一旦インストールし、本機能を使用してデータベースの移行を行います。	
	Database Migration	データベースの移行を行います。
	Remote Probe Upgrade	リモートプローブのアップグレードを行います。
About	About 画面には、以下の情報が表示されます。 • D-View8 のエディション（Standard/Enterprise） • 購入版の簡単な説明 • ソフトウェアバージョン • 最終更新日時 • メンテナンスライセンス • 使用中 / サポートされるノードの数 • システム稼働時間	

通知アイコン

Web 画面の右上に配置された通知アイコンにより、システムのステータスが通知されます。
以下の種類のシステム情報を確認することができます。

項目	説明	アイコン表示
Notifications （通知） 	アラームの通知が有効になっている場合に、全ての重要度の通知情報が表示されます。	
Info Alarm （情報アラーム） 	適切なシステム運用を維持するため、または意図しない結果を避けるために注意が必要な、システム機能に関する情報アラームが表示されます。	
Warning Alarm （警告アラーム） 	システムの動作に影響を与える可能性のある、システムエラーまたは障害に関する警告アラームが表示されます。	
Critical Alarm （重大なアラーム） 	システムエラーまたは障害に関する重大なアラームが表示されます。 アラーム内容について早急に確認し、必要に応じて対処・修復を行う必要があります。	

ユーザメニュー

ワークスペース右上のユーザ名をクリックすると、以下のメニューが利用できます。

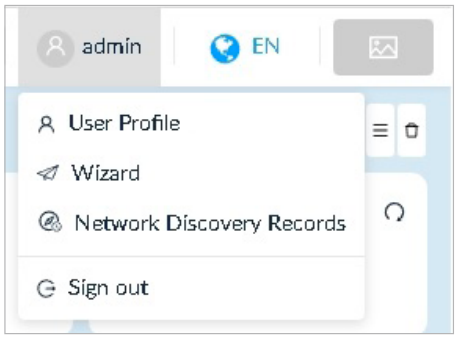


図 3-7　ユーザメニュー

項目	説明	
User Profile		現在のユーザ情報を確認、編集します。
Wizard	D-View 7 Upgrade	ウィザードに従って、D-View7 データベースとプローブを D-View8 に移行します。「Super Administrator」以外は利用できません。 メモ　本機能は現在のバージョンでは利用できません。D-View7 からアップグレードを行う場合に、D-View8 v1.0.3.39 を一旦インストールし、本機能を使用してデータベースの移行を行います。
	Discovery	ウィザードに従って、ネットワークの追加とデバイスの検出を行います。
	Monitoring	ウィザードに従って、カスタマイズトポロジの作成、ラックの定義、またはカスタマイズダッシュボードの作成を行います。
	Alarm	ウィザードに従って、アラームと通知のカスタマイズを行います。
Network Discovery Records		検出されたネットワークの履歴を表示します。
Sign out		インタフェースからログアウトします。

ユーザパスワードの変更

セキュリティのため、D-View8 の利用を開始する際にパスワードを安全なパスワードに変更することを強くお勧めします。組織管理者は、管理するドメイン内でユーザを作成することができます。(例:「Super Admin」は「Organization」「Site」「Network」の役割のユーザを作成可能です。「Organization Admin」は、「Site」「Network」の役割のユーザを作成することが可能です。)

1. ワークスペース右上のログインユーザ名をクリックし、ユーザメニューを表示します。

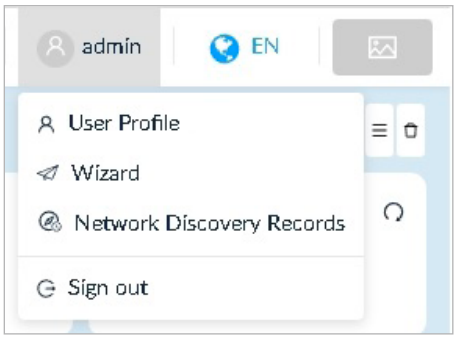


図 3-8　ユーザメニュー

2. 「User Profile」を選択し、ユーザのプロファイル画面を表示します。

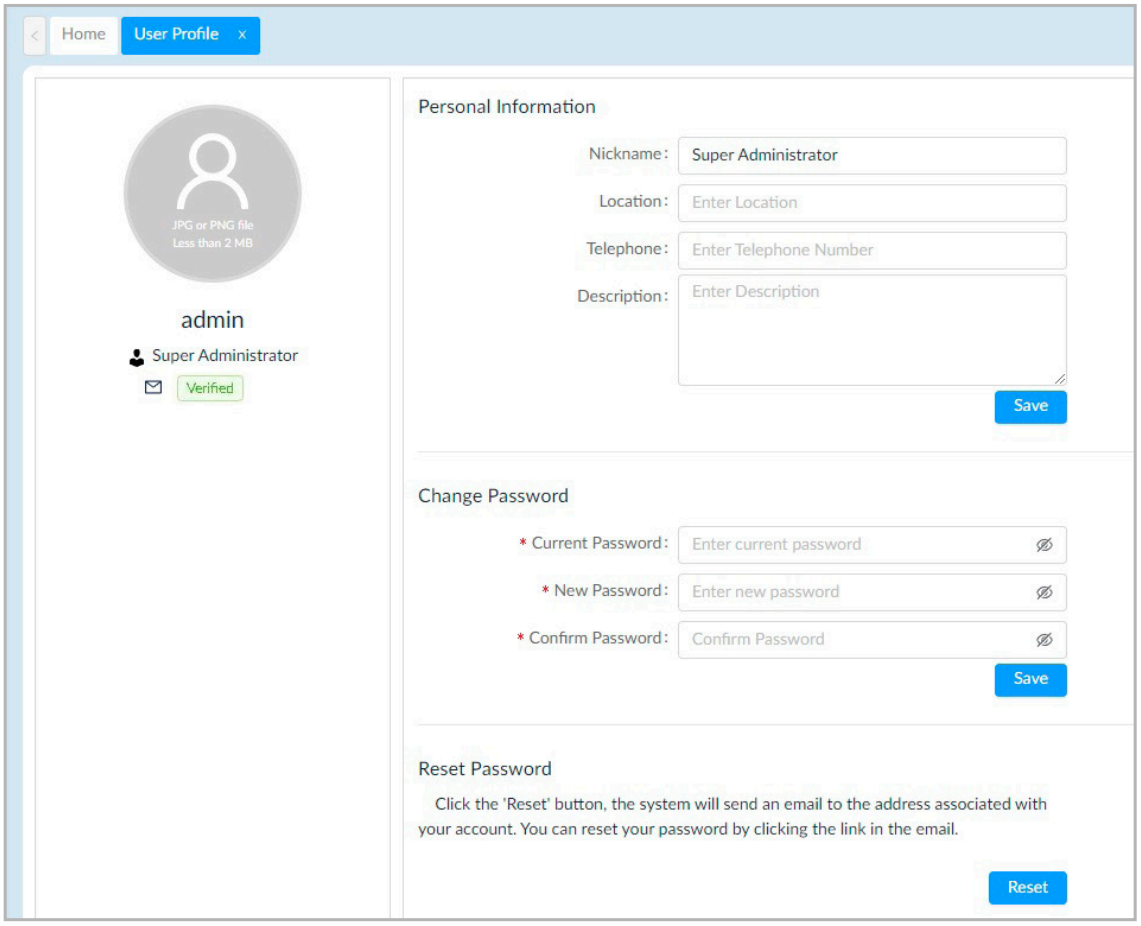


図 3-9　ユーザプロファイル

3. 「Change Password」セクションで、以下の項目を入力します。
   - 「Current Password」:現在のパスワードを入力します。
   - 「New Password」:新しいパスワードを入力します。
   - 「Confirm Password」:確認のため、新しいパスワードを再度入力します。
4. 「Save」をクリックして、新しい設定を保存します。

本画面では、パスワード変更のほか、アカウント名や E メールアドレス、自動サインアウトの設定を行うこともできます。

通知用の電子メールサーバの設定

通知の送信用に、電子メールサーバを設定する必要があります。電子メールサーバ設定は、「Super Administrator」または「Organization Administrator」のみ変更可能です。

メモ　通知の送信先電子メールアドレスの設定を含むアラーム通知プロファイルの追加については、P.93 の「通知センターの設定」を参照してください。

1. **System > Basic Settings** をクリックします。
2. 「Mail Server Settings」タブを選択します。

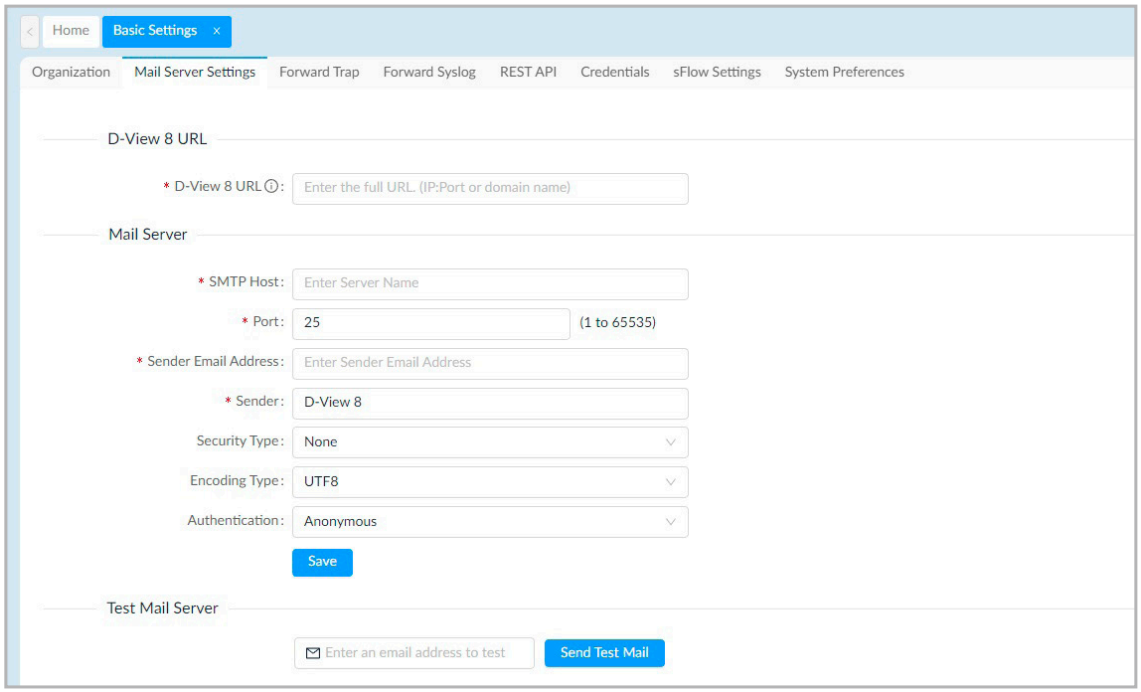


図 3-10　メールサーバ設定

3. 「D-View 8 URL」項目で、URL およびポート（例：https://63.216.155.109:59800）を入力します。
   ユーザアカウントの E メール検証およびパスワードリセット時の E メールで使用されます。
4. 「Mail Server」セクションで、次の情報を入力します。

項目	説明
Mail Server	
SMTP Host	SMTP サーバのアドレスを入力します。
Port	送信メールサーバの SMTP ポートを入力します。
Sender Email Address	送信メールアドレスを入力します。
Sender	送信メールアドレスの送信者名を入力します。
Security Type	送信メールサーバで使用する暗号化方式を選択します。（オプション） • 選択肢：「None（なし）」「SSL」
Encoding Type	文字エンコーディングの種類を選択します。（オプション） • 選択肢：「UTF8」「ASCII」
Authentication	サーバで使用する認証方法を選択します。 • 選択肢：「Anonymous（匿名）」「SMTP Authentication（SMTP 認証）」 SMTP 認証を選択した場合は、次の項目を入力します。 • 「Username」：サーバにアクセスする権限を持つユーザ名を入力します。 • 「Password」：指定したユーザ名のパスワードを入力します。

注意　D-View8 の SMTP サーバとして Gmail を使用する場合、Google アカウントで 2 段階認証プロセスを有効化して、アプリパスワードを設定する必要があります。

5. 「Save」をクリックして、メールサーバの設定を保存します。
6. 「Test Mail Server」セクションで、設定したメールサーバ構成を検証するためのテストメールを送信します。
   有効なメールアドレスを入力し、「Send Test Mail」をクリックします。

通知センターの設定

D-View8 がアラーム通知を配信するには、通知ルールを設定する必要があります。
通知ルールが定義されると、D-View8 システムにより、通知メッセージが E メール経由で送信、または Web アプリケーションに表示されます。通知メッセージはダッシュボードの右上からすぐに確認することができます。通知ルールには、アラームレベルなどのトリガ条件が含まれます。

メモ　管理デバイスに対し、本設定を行うことができます。ネットワークおよびデバイスの検出については、P.96 の「ネットワークの検出」を参照してください。

1. **Alarm & Notification > Notification Center** をクリックします。
2. 「+ Add Notification Rule」をクリックします。

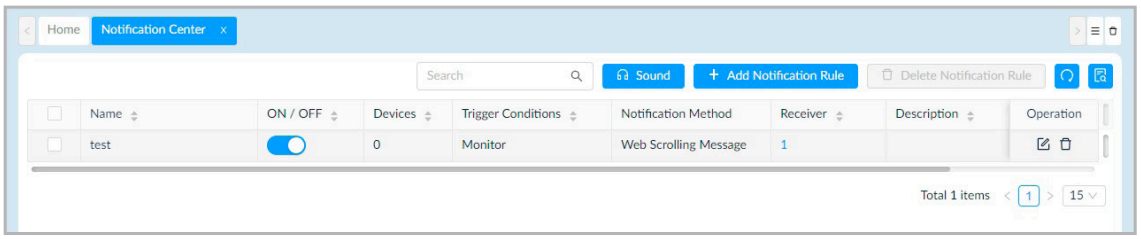


図 3-11　通知センター

3. 「Notification Management Details」画面が表示されます。

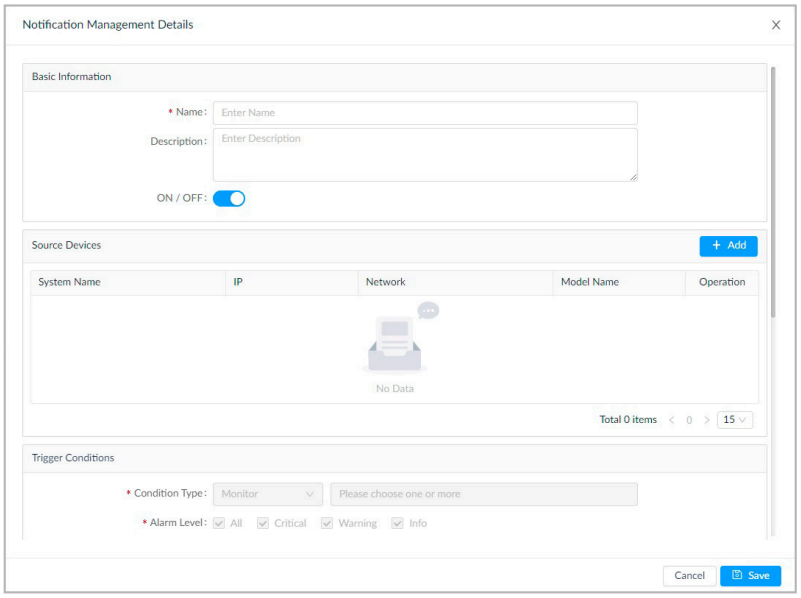


図 3-12　通知の管理詳細

4. 「Basic Information」セクションで、基本情報を入力します。
5. 「ON/OFF」スライドボタンをクリックして、ルールを有効または無効にします。
6. 「Source Devices」セクションで「+ Add」をクリックして、デバイス選択画面を表示します。

7. 「Device List」から、通知ルールに含めるデバイスを選択します。

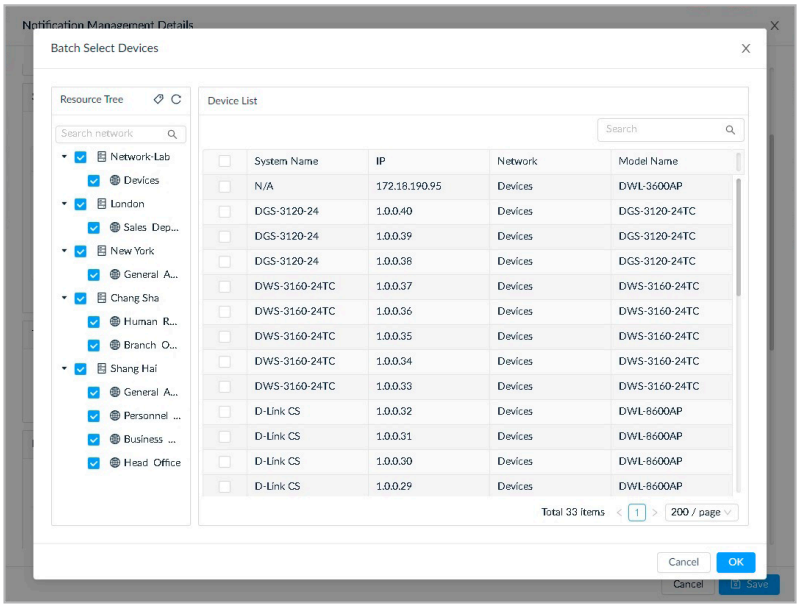


図 3-13　デバイス選択

8. 「OK」をクリックしてデバイスの選択を決定し、デバイス選択画面を閉じます。

9. 「Notification Management Details」画面の「Trigger Conditions」セクションで、通知を生成する条件を設定します。

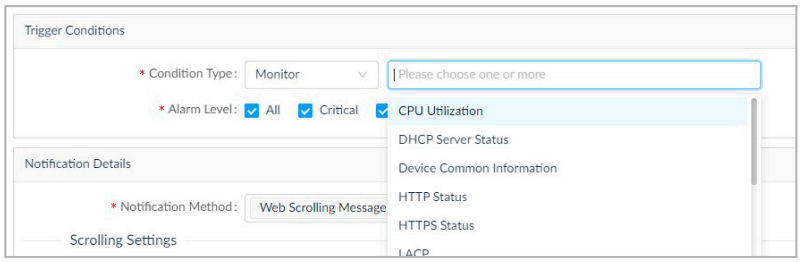


図 3-14　トリガ条件指定

項目	説明
Trigger Conditions（トリガ条件）	
Condition Type	トリガ条件の種類を指定します。 • 「Monitor」:「Monitor」のアラームルールによって生成されたアラームがトリガとなり、指定された通知が送信されます。 • 「Trap」:「Trap」のアラームルールによって生成されたアラームがトリガとなり、指定された通知が送信されます。 • 「Syslog」:「Syslog」のアラームルールによって生成されたアラームがトリガとなり、指定された通知が送信されます。 • 「Wired Traffic」:「Wired Traffic」のアラームルールによって生成されたアラームがトリガとなり、指定された通知が送信されます。 「Monitor」を指定した場合、デバイスの種類に応じて利用可能な監視項目が表示されます。 以下のような項目が表示されます。 - 「CPU Utilization」 - 「DHCP Server Status」 - 「Device Common Information」 - 「Fan」 - 「HTTP Status」 - 「LACP」 - 「LLDP」 - 「Memory Utilization」 - 「Private Port」 - 「RMON Status」 - 「Response Time」 - 「SNTP Status」 - 「SSH Status」 - 「STP Status」 - 「Safeguard Status」 - 「Syslog Status」

項目	説明
	- 「Telnet Status」 - 「Trap Status」 - 「Wireless Access Points」 - 「Wireless Error Packets」 - 「Authenticated Clients」 - 「Wireless Traffic（bit）」 - 「Wireless Traffic（packet）」 など トリガとなるアラームルールを設定するには、**Alarm & Notification > Monitor & Alarm Settings > Alarm Settings** に移動し、該当ツリー / 項目を選択します。
Alarm Level	通知をアクティブ化するアラームの種類を選択します。 • 「All」：すべてのアラームレベルが通知対象となります。 • 「Critical」：障害や異常を示す重大なエラー情報が通知対象となります。 • 「Warning」：問題を引き起こす可能性がある警告イベントの情報が通知対象となります。 • 「Info」：インフォメーションレベルの情報が通知対象となります。 指定する重大度レベルで定義されたアラームルールが存在する場合、通知が有効になります。
Model	トリガ条件の種類で「Wired Traffic」を選択した場合、選択したデバイスのモデル名が表示されます。「All（すべて）」または特定のポートを選択し、トリガ条件として割り当てます。

注意　利用可能なトリガ条件の項目は製品によって異なります。

10. 「Notification Details」セクションで、通知を配信する方法を選択します。

項目	説明
Notification Details（通知詳細）	
Notification Method	通知方法を指定します。 • 「Web Scrolling Message」：Web スクロールメッセージによる通知を行います。 • 「Email」：E メール通知を行います。 • 「Execute Script」：スクリプトを実行します。
Scrolling Settings	
Sound	通知の方法として「Web Scrolling Message」を選択した場合、アラートの音設定を選択します。 • 選択肢：「Mute（ミュート / 音を消す）」「Enable Voice（音声を有効にする）」
Script Settings	
Command Line	通知の方法として「Execute Script」を選択した場合、実行するスクリプトを入力します。 通知が生成された際に、タスクを自動化またはデバイスのプロパティやステータスを変更するスクリプトを指定します。
Apply Command to	通知の方法として「Execute Script」を選択した場合、スクリプトを適用する対象のデバイスを選択します。 • 「Itself」：指定した対象デバイスにスクリプトを適用します。 • 「Other Devices」：他のデバイスを指定します。「Device Attribute」セクションでデバイスを追加することができます。 リモートのデバイスでスクリプトを実行するには、デバイスにログインするためのアカウント情報を指定する必要があります。デバイス毎にアカウント情報やプロトコルを指定することが可能です。
Alarm Handling	「Acknowledge Alarm after script execution」のチェックボックスにチェックを入れて、繰り返しのスクリプト処理を終了させるためのオプションを指定します。アラームは、スクリプトの実行毎に自動的に「Acknowledge（承認）」ステータスになります。 • 「Number of Repetitions」：繰り返しの最大回数 (1-100）を指定します。 • 「Cycle Time」：サイクル時間（5-1440 分）を指定します。 指定したサイクル時間内で繰り返しの最大回数に達すると、自動スクリプトが停止します。

11. 「Notification Receiving Administrator」セクションで、通知を受信するユーザを設定します。
「Current Administrator」にチェックを入れると、現在の admin ユーザが自動的に受信ユーザとして設定されます。「+ Add」をクリックして、対象ユーザを追加することができます。

12. 「Notification Suspension Period」セクションで、通知の配信が停止される期間を設定します。
定義済みのスケジュールを選択するか、「Add Schedule」をクリックして新規のスケジュールを作成します。

13. 「Save」クリックして、通知ルールを保存します。 設定をキャンセルするには、「Cancel」をクリックします。

メモ　アラーム通知の詳細は、P.168 の「通知イベントの表示と管理」を参照してください。

第 4 章　ネットワークとデバイスの検出・管理

ネットワークの管理を行うには、ネットワーク上のデバイスを検出する必要があります。

本章では、以下のトピックについて説明します。

- 「ネットワークの検出」
- 「ネットワークデバイスの管理」
- 「デバイスグループの管理」
- 「SNMP 設定」
- 「バッチ構成による複数ネットワークの管理」

ネットワークの検出

D-View8 は、プローブを介してネットワークデバイスの管理を行います。プローブサーバはバックグラウンドプロセスとして動作し、管理デバイスが NAT 環境やファイアウォールを経由する他のネットワークに存在する場合、新規デバイスの検出やデバイスの統計情報収集、D-View サーバへのデータ転送を行います。

D-View8 のプローブは、D-Link 製品のほかにも SNMP プロトコルに準拠したネットワークデバイスに対応しています。

各ネットワークセグメントにプローブを配置することにより、プローブサーバでデータが収集された後、D-View8 サーバへ転送されコンパイル / 分析が行われるため、帯域幅の使用を軽減できます。これにより、オープンな接続の数が減り、すべてのデバイスがサーバと直接通信する必要がなくなるため、ネットワークのオーバーヘッドが削減されます。また、ネットワークデバイスをグループに分けることで、管理をシンプルかつ効率的に行うことができます。

プローブに接続されているデバイスに対しては、管理者によるコマンド（再起動、イベントログの管理、デバイス設定の変更など）を実行する役割も担っています。

ネットワーク検出機能では、標準の SNMP MIB をサポートする D-Link またはサードパーティ製の有線 / 無線デバイス（アクセスポイント、スイッチなどデバイスなど）を検出できます。

ネットワーク検出機能により、D-View8 サーバで設定されているアクティブなネットワークを監視・管理できます。ネットワーク情報は、ダッシュボードの「Architecture」セクションに表示されます。また、検出されたすべてのデバイスおよび統計情報なども確認することができます。

ネットワーク検出プロファイルの作成

（メモ）「Super Administrator」（デフォルトの admin ユーザ）が最初に D-View8 にログインすると、ウィザードが表示されます。「Discovery」を選択して、ガイドに従いネットワーク検出手順を実行します。最初に組織の設定が必要になります。

ネットワークプロファイルの作成

1. **Monitoring > Network Discovery** をクリックします。
2. 「+ Add Network」をクリックします。

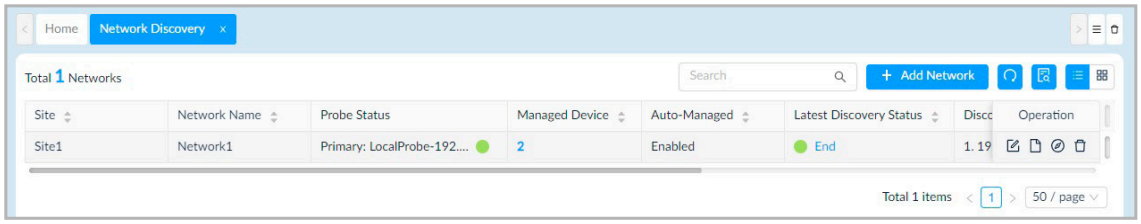


図 4-1　　ネットワーク検出プロファイル一覧

3. ネットワーク検出プロファイルを設定します。

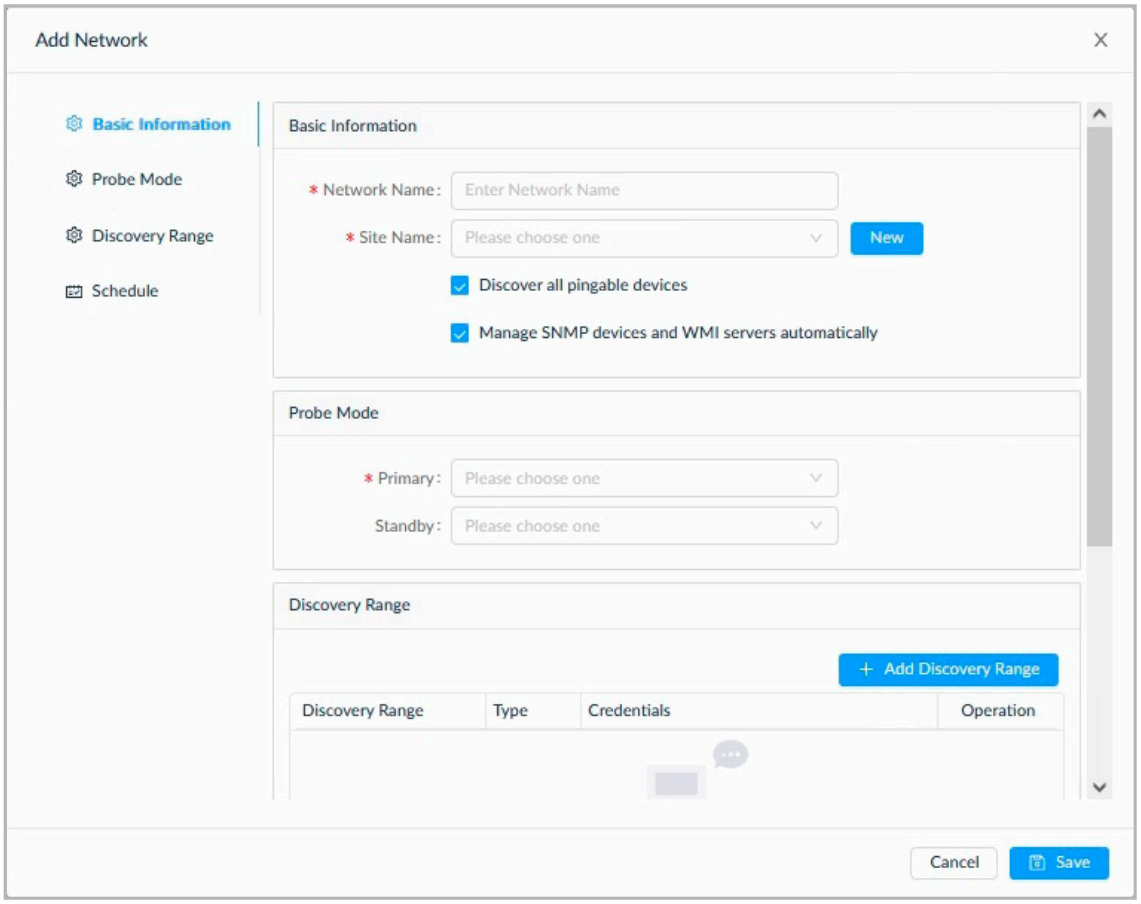


図 4-2　ネットワークプロファイルの追加

設定項目：

項目	説明
Basic Information（基本情報）	
Network Name	ネットワーク名を入力します。
Site Name	ドロップダウンメニューをクリックして既存のサイトを選択するか、「New」をクリックしてサイト名を入力します。
Discover all pingable devices	Ping コマンドに応答するすべてのデバイスを自動的に検出する機能を有効または無効に設定します。 ・ 初期値：有効
Manage SNMP devices and WMI servers automatically	すべての SNMP および WMI デバイスの自動管理を有効または無効に設定します。 ・ 初期値：有効 本項目にチェックを入れると、検出されたすべての SNMP デバイス /WMI デバイスが D-View8 の管理デバイスとなります。無効にした場合、検出されたデバイスは「Unmanaged」カテゴリに配置されます。これらの非管理デバイスは、「Device View」画面から管理デバイスに手動で設定することができます。
Probe Mode（Probe モード）	
Primary	ドロップダウンメニューから Probe を選択し、Probe モードをプライマリとして設定します。 メモ　プローブモードがプライマリとして識別された場合、スタンバイプローブとして指定することはできません。
Standby	ドロップダウンメニューから Probe を選択し、Probe モードをスタンバイとして設定します。スタンバイ Probe はプライマリ Probe が失敗した場合のバックアップ Probe となります。
Discovery Range（検出範囲）	
Add Discovery Range	「+ Add Discovery Range」をクリックして、ネットワーク検索の範囲を定義します。 詳細は、P.98 の「検出範囲の追加・編集」を参照してください。
Discovery Range	定義したネットワーク検出範囲が表示されます。
Type	検出範囲の指定方式が表示されます。
Credentials	本項目の入力欄をクリックし、検出に使用する認証情報を指定します。 SNMP の場合、SMNP v1/v2c/v3 のプロトコルバージョンを指定することができます。 **System > Basic Settings** の「Credentials」タブで定義された SNMP/WMI 資格情報を利用、または本画面の「Add SNMP Credential」「Add WMI Credential」から新規の資格情報を定義することもできます。詳細は、P.225 の「接続プロトコルの認証情報の設定」を参照してください。

項目	説明
Edit	（Edit）アイコンを選択して、検出範囲を変更します。
Delete	（Delete）アイコンをクリックして、検出範囲を削除します。
Schedule（スケジュール）	
Schedule Type	ネットワーク検出機能の実行スケジュールの種類を指定します。 ・ 選択肢：「One Time（1 回のみ）」「Recurrent（繰り返し）」
Execution Time	スケジュールの種類で「One Time」を指定した場合、検出ジョブを実行するタイミングを選択します。 ・ 選択肢：「Immediately（今すぐ実行）」「Specify a Date（時刻を指定）」 「Specify a Date」を選択した場合、検出ジョブを実行する日時を指定します。
Schedule	スケジュールの種類で「Recurrent」を指定した場合、検出ジョブを実行するスケジュールを選択します。 スケジュール設定については、P.236 の「スケジュール機能」を参照してください。

4. 「Save」をクリックして、ネットワーク検出プロファイルを保存します。
   設定をキャンセルするには、「Cancel」をクリックします。

検出範囲の追加・編集

1. **Monitoring > Network Discovery** をクリックします。

2. 「+ Add Network」をクリック、または既存のネットワーク検出プロファイルの （Edit）アイコンをクリックします。

3. 「Discovery Range」セクションで「+ Add Discovery Range」または （Edit）をクリックします。

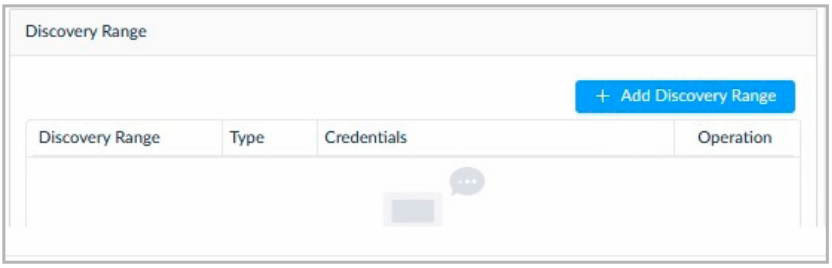


図 4-3　ネットワークの追加 / 編集

4. 検出範囲を設定します。

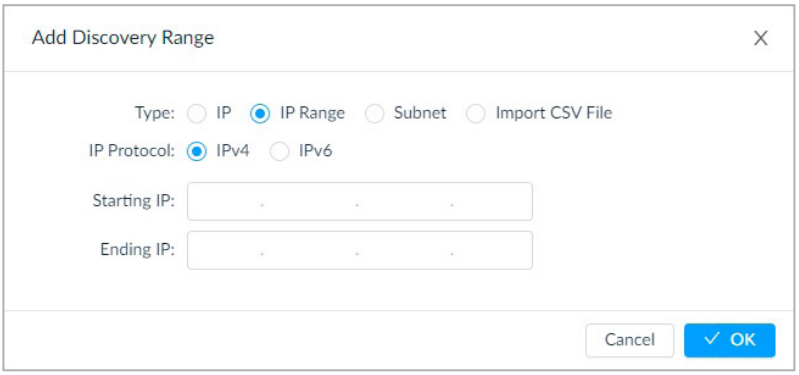


図 4-4　検出範囲の追加

設定項目：

項目	説明
Type	検出範囲の指定方法を選択します。 ・ 選択肢：「IP」「IP Range」「Subnet」「Import CSV File」
IP	「IP」を選択した場合、検出範囲として単一の IP アドレスを入力します。 ・「IP Protocol」：IP プロトコル（IPv4/IPv6）を選択します。 ・「IP」：IP アドレスを入力します。 注意　IPv6 デバイスの管理はサポートされません。

項目	説明
Starting/Ending IP	「IP Range」を選択した場合、IP アドレス範囲を定義します。 • 「IP Protocol」：IP プロトコル（IPv4/IPv6）を選択します。 • 「Starting IP」：検出範囲の開始 IP アドレスを指定します。 • 「Ending IP」：検出範囲の終了 IP アドレスを指定します。
Subnet	「Subnet」を選択した場合、CIDR 表記でサブネットアドレスを入力して、検出範囲を定義します。（例：172.17.2.0/24（IPv4 アドレス）、2001:db8:abcd:0012::0/64（IPv6 アドレス） • 「IP Protocol」：IP プロトコル（IPv4/IPv6）を選択します。 • 「Subnet」：サブネットアドレスを入力します。
File	「Import CSV File」を選択した場合、「Select File」をクリックして、定義済みのファイルをアップロードします。 **ファイルのアップロード条件 :** • インポートファイルの拡張子は「.csv」にする必要があります。 • 検出ルールは、1 行につき 1 つのみ記述できます。 • パラメータを区切るには、カンマ "," を使用します。 • SNMP v2 パラメータの順序は、①検出 IP、② SNMP バージョン、③ RO コミュニティ、④ RW コミュニティです。 • SNMP v3 パラメータの順序は、①検出 IP、② SNMP バージョン、③ユーザ名、④モード、⑤認証アルゴリズム、⑥認証パスワード、⑦暗号化アルゴリズム、⑧暗号化パスワードです。 • パラメータは以下の値に設定できます : - モード：「authNoPriv」「noAuthNoPriv」「Auth」 - 認証アルゴリズム：「MD5」「SHA」 - プライベートアルゴリズム：「AES」「DES」 • 検出 IP には、単一の IP、IP 範囲、またはサブネットを指定できます。 • IP 範囲は、「Start IP-End IP」の形式で指定します。開始 IP は終了 IP より大きくすることはできません。 • サブネットは、「IP/subnet mask」の形式で指定します。 • CSV ファイルのインポートでは、SNMPv1/v2c/v3 デバイスの検出のみサポートされます。 • 使用可能な SNMP バージョンの値は「V1」「v1」「V2」「v2」「V3」「v3」です。（大文字または小文字を使用可能） • CSV ファイルに定義可能な IP アドレスの数は、最大 5,000 です。 • ファイルサイズは最大 1MB です。 **サンプルルール :** 192.168.1.10,v2,public,private 192.168.1.15-192.168.1.17,v2,public,private 192.168.2.0/24,v2,public,private 192.168.1.1,V3,user,noAuthNoPriv 192.168.1.1-192.168.1.17,V3,user,AuthNoPriv,SHA,password 192.168.1.0/24,v3,user,authPriv,MD5,password,AES,password

5. 必要に応じて認証プロトコルの設定を行います。

6. 「Save」をクリックして、検出範囲を保存します。
   設定をキャンセルするには、「Cancel」をクリックします。

ネットワーク検出ジョブの実行

ネットワーク検出機能では、1 回限りの検出ジョブが用意されており、すぐに実行できます。

1. **Monitoring** > **Network Discovery** をクリックします。

2. 既存のネットワークプロファイルの （Discover）アイコンをクリックして、ネットワーク内のデバイスの検出を開始します。

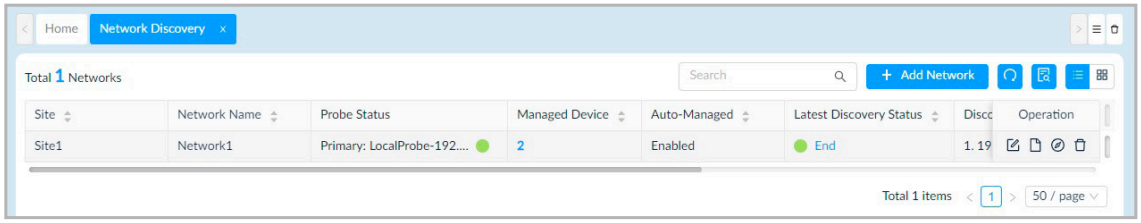


図 4-5　　ネットワーク検出プロファイル一覧

「Latest Discovery Status（最新の検出ステータス）」欄に、検出の実行ステータスが表示されます。
例えば、ジョブが処理中の場合は「Running（実行中）」と表示されます。

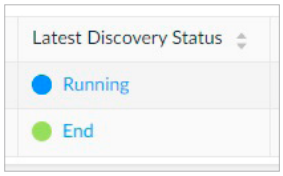


図 4-6　　最新の検出ステータス - 実行中

検出されたデバイスの一覧が表示されます。

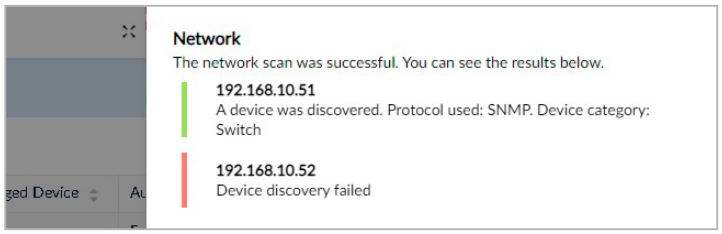


図 4-7　　検出結果の表示

ネットワーク検出プロファイルの編集・削除

1. **Monitoring > Network Discovery** をクリックします。

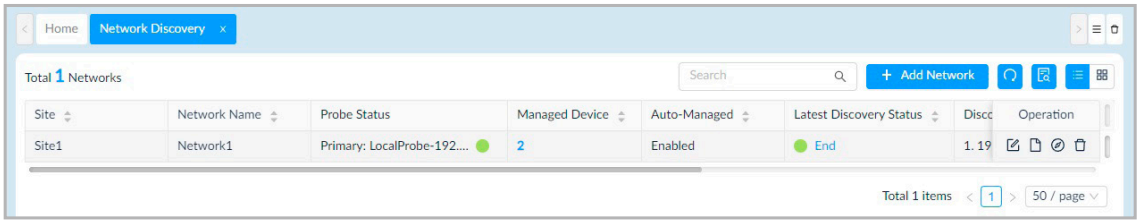


図 4-8　　ネットワーク検出プロファイル一覧

2. 既存プロファイルの操作アイコンをクリックして、プロファイルを編集または削除します。

プロファイルの編集：

(1) 既存のネットワークプロファイルの （Edit）アイコンをクリックします。

(2) プロファイルの内容を編集し、「Save」をクリックして保存します。キャンセルする場合は「Cancel」をクリックします。
設定項目の詳細は、P.96 の「ネットワーク検出プロファイルの作成」を参照してください。

プロファイルの削除：

(1) 既存のネットワークプロファイルの （Delete）アイコンをクリックします。

(2) 確認メッセージが表示されます。プロファイルを削除する場合は「OK」、キャンセルする場合は「Cancel」をクリックします。

（Network Information ）をクリックして、ネットワーク検出プロファイルの詳細を確認することもできます。Probe の情報も含まれます。

ネットワークデバイスの管理

D-View8 では、デバイスの集中管理に役立つ機能を提供します。

このセクションでは、次の項目について説明します。
- デバイス情報の表示
- デバイス管理
- デバイス情報の変更
- デバイスへの Ping/ 設定保存 / 再起動
- インタフェースリストの表示とエクスポート
- 接続リストの表示とエクスポート

デバイス情報の表示

「Device View（デバイスビュー）」画面には、デバイスの管理カテゴリ毎にデバイスの一覧が表示され、ステータスや基本情報を確認することができます。既定のビューは「All（すべて）」です。システム名をクリックすると、デバイス情報画面が表示されます。

メモ　ライセンスの期限が切れると、管理ノード数の制限（D-View8 フル機能は利用可能）についてのアラートと、追加ライセンスの適用を促すメッセージが「Device View」画面に表示されます。ライセンスに関する詳細は、P.238 の「ライセンス管理」を参照してください。

1. **Monitoring > Device View** をクリックします。

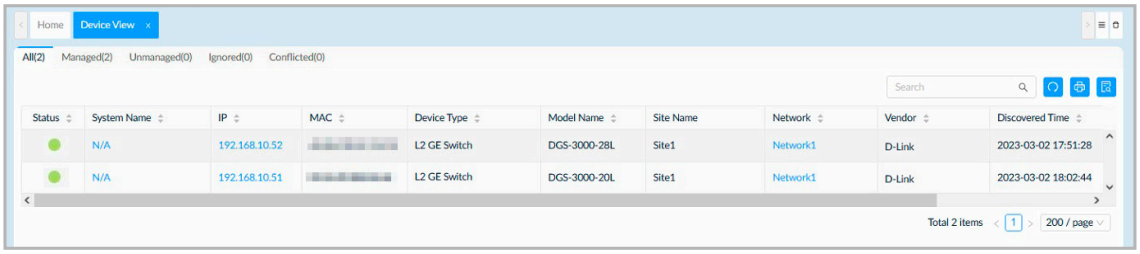


図 4-9　　デバイスビュー

表示項目：

項目	説明
デバイスの管理カテゴリ（タブ）	デバイスは以下の種類に分類されます。タブを選択して、各デバイスリストを表示します。 • 「All（すべて）」：検出されたすべてのデバイスが表示されます。 • 「Managed（管理対象）」：D-View8 で管理されるすべてのデバイスが表示されます。 • 「Unmanaged（管理対象外）」：すべての非管理デバイスが表示されます。以下のような理由で非管理に分類されます。 - SNMP または WMI を使用して通信ができない - SOID などの必須のシステムパラメータが取得できない - サポートされる管理ノード数を超えている • 「Ignored（無視）」：検出から除外されるデバイスが表示されます。 • 「Conflicted（競合）」：競合する IP アドレスを持つデバイスが表示されます。
「All」タブ選択時の表示項目	
Status	ステータスを表示します。 • ステータス表示：オンライン（緑）/ オフライン（赤）/ 不明（グレー）
System Name	デバイスを識別するシステム名を表示します。
IP	IP アドレスを表示します。
MAC	MAC アドレスを表示します。
Device Type	デバイスタイプを表示します。（例：L2/L3 Switch、Access Point、Workstation）
Model Name	デバイスのモデル名を表示します。
Site Name	デバイスが属するネットワークサイトを表示します。
Network	デバイスが属するネットワークを表示します。
Vendor	デバイスのベンダ名を表示します。
Discovered Time	デバイスの直近の検出時間を表示します。
Management Type	デバイスが管理対象か非管理対象かを表示します。

列名をクリックして、各項目でソートすることができます。（アルファベットなどの昇順または降順）

「Managed」タブでは、（Columns Selector）アイコンをクリックして列項目を追加したり削除したりすることもできます。

デバイス管理

1. **Monitoring > Device View** をクリックします。
2. 上部のタブを選択して、特定カテゴリのデバイスを表示することができます。
以下の画面例では、「Managed（管理）」デバイスカテゴリで、「Switch-All」が選択されています。ドロップダウンメニューからデバイスの種類を選択して、特定のカテゴリのデバイスを一覧表示することができます。

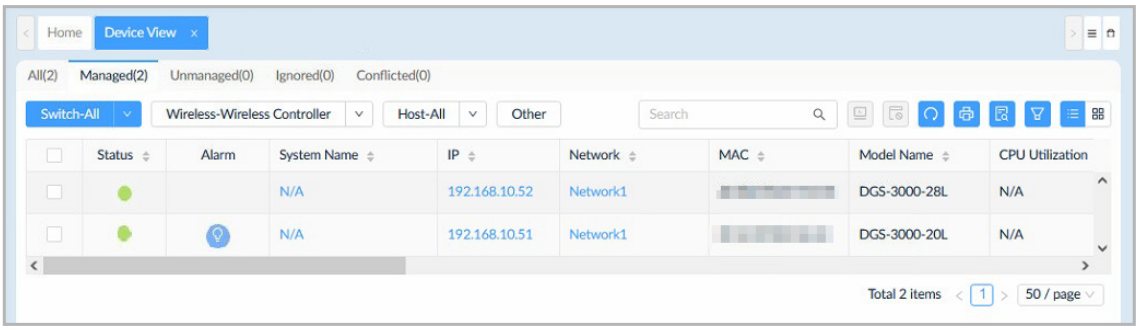


図 4-10　デバイスビュー（管理タブ）

表示 / ツール項目：

項目	説明
表示項目	
Managed タブ	D-View8 の管理対象デバイスを表示します。 • 「Switch（スイッチ）」：スイッチを表示します。以下の種類を指定することができます。 - 「All」「sFlow」「PoE」 • 「Wireless（無線）」：無線デバイスを表示します。以下の種類を指定することができます。 - 「Access Point」「SSID」「Wireless Client」「Wireless Controller」 • 「Host（ホスト）」：ホストデバイスを表示します。以下の種類を指定することができます。 - 「All」「Process」「Software」 • 「Other（その他）」：上記のデバイスカテゴリに属していないその他のデバイスを表示します。
ツールバー	
Search	キーワードを入力し、表示される対象項目を選択してデバイスを検索・表示します。
Unmanage	（Unmanage）アイコンをクリックして、選択した管理デバイスを非管理対象として設定します。 非管理デバイスに設定されると、監視設定などは削除されます。
Manage	（Manage）アイコンをクリックして、選択した非管理デバイスを管理対象に設定します。
Ignore	（Ignore）アイコンをクリックして、選択した管理 / 非管理デバイスを無視するように設定します。 「Ignore」配下のデバイスは、ネットワーク検出時に除外されます。再度検出するには、デバイスを削除する必要があります。
Refresh	（Refresh）アイコンをクリックして、デバイスの一覧を更新します。
Export	（Export）アイコンをクリックして、検出されたデバイス情報を CSV ファイルにエクスポートします。 1 回のエクスポートで最大 5,000 件のエントリをダウンロードできます。
Advanced Query	（Advanced Query）アイコンをクリックして、高度な検索を実行します。 検索するデバイスに関連する情報を入力・指定します。
Columns Selector	（Columns Selector）アイコンをクリックして、テーブルに表示する列項目をカスタマイズします。 表示するデバイスの種類によって、表示可能な列の項目は異なります。以下はスイッチ項目の例です。 • 「Default（デフォルト表示項目）」：「Status」「Alarm」「System Name」「Network」「IP」「MAC」「Uptime」「Vendor」「CPU Utilization」「Memory Utilization」「Firmware Version」「Hardware Version」「Model Name」「Temperature」「Device Type」「Serial Number」「Discovered Time」

項目	説明
	• 「Other（その他項目）」：「Device Category」「Site Name」「PoE Status」「sFlow Status」「Stack Info」「Current Activated License」「Activated / Total Licenses」「Port Count」「Latest Discovered Time」「Trap Status」「DHCP Status」「Total Flash」「Syslog Status」「Attached on Probe」「SNTP /NTP Status」「SSH Status」「Spanning Tree」「LLDP Status」「LACP Status」「RMON Status」「Safeguard Engine Status」 「All」をクリックして、すべてのカテゴリを選択または選択解除します。 「Apply」をクリックして、選択内容を適用します。
View List	（スライドバー）をクリックして、「Device View」テーブルをリスト表示 / グラフィック表示に切り替えます。

注意　デバイスの種類により利用可能なオプションが異なります。

3. デバイスの詳細情報を確認するには、システム名のリンクをクリックします。

デバイス情報の変更

管理デバイスのデバイス情報を変更します。システム名、システムの場所、システムの連絡先、また、デバイスの種類に応じてその他の情報を変更できます。

1. **Monitoring > Device View** をクリックします。
2. カテゴリメニューから「Managed」タブを選択し、管理デバイスの一覧を表示します。
   必要に応じて、ドロップダウンメニューよりデバイスの種類を選択します。
3. 対象デバイスのシステム名をクリックし、デバイス情報画面を表示します。

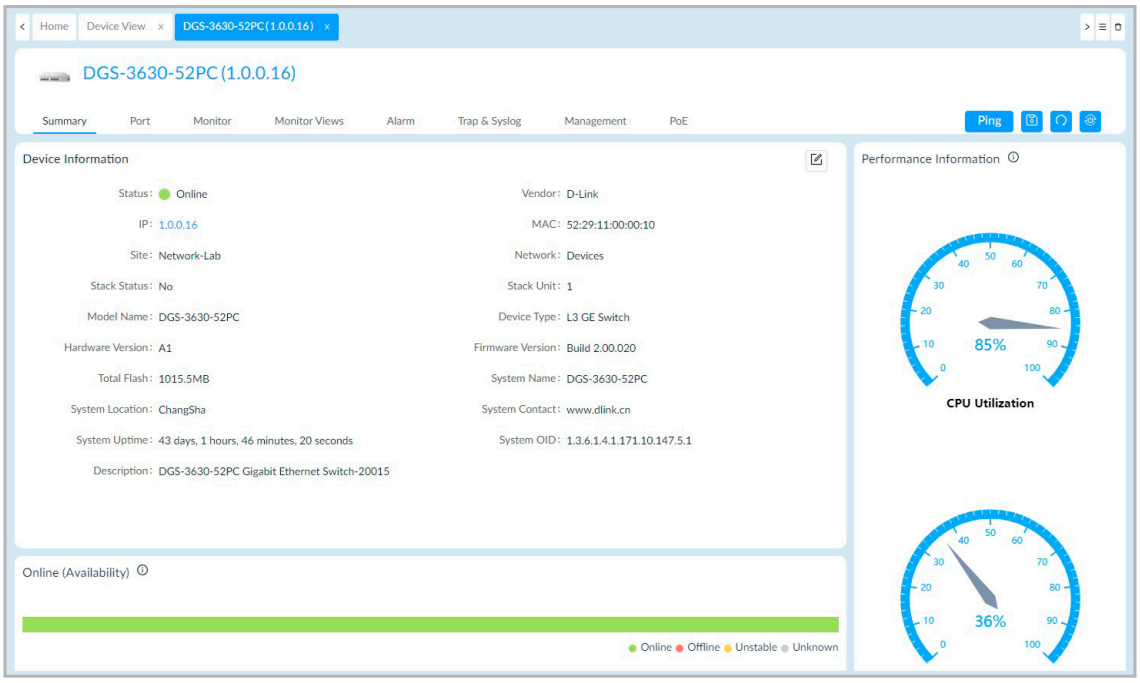


図 4-11　デバイス詳細画面

4. 「Summary」タブ配下の「Device Information（デバイス情報）」セクションで、（Edit Device Information）アイコンをクリックします。
5. デバイス情報を変更します。
6. 「Save」をクリックして、変更したデバイス情報を保存します。

メモ　デバイス情報画面では、「Summary」タブ以外でその他の情報（アラームやリソース監視設定など）も確認することができます。利用可能な情報はデバイスの種類により異なります。無線 AP の場合、「Wireless」タブで SSID、チャネル、認証情報などが表示されます。

「Device Information（デバイス情報）」画面では、以下の情報を確認することができます。表示される項目はデバイスの種類により異なります。

表示 / 設定項目：

項目	説明
Summary	
Device Information	デバイス情報の概要が表示されます。 「Device Information」：（Edit Device Information）アイコンをクリックして、以下の項目を変更します。 • 「System Name（システム名）」 • 「System Location（システムの場所）」 • 「System Contact（システムの連絡先）」 スイッチが物理スタックをサポート しており有効化されている場合、かつプライマリマスタ として設定されている場合は、「Stack Status」の「View」ボタンにマウスオーバーすることで物理スタックされたユニット（スイッチ）の情報を確認することができます。物理スタックされているユニットの情報には、ユニット ID、モデル名、物理 スタックの優先度、MAC アドレス、およびファームウェアバージョンの情報 が含まれます。（なお、物理スタックにおいてスレーブ、または バックアップマスタとしての役割を担うスイッチのステータス表示は、オフラインとなります。）「Port」タブおよび「Monitor」タブには、物理スタックされている全てのユニットの情報が表示されます。（詳細は 、以下の「Port」タブと「Monitor」タブのステータス説明を参照してください。） 「Save」をクリックして更新内容を保存するか、「Cancel」をクリックして設定をキャンセルします。 注意　DAP-X2810 では「System Contact」の設定は未サポートです。 注意　DGS-1100-05PDV2/05V2/08V2/08PV2 では、「Hardware Version」「Firmware Version」「Total Flash」の表示はサポートされません。 注意　DXS-1210/B1 シリーズでは「Total Flash」の表示はサポートされません。
Online (Availability)	過去 24 時間のデバイスのオンライン / オフライン状態を表示します。
Performance Information	CPU 使用率とメモリ使用率をグラフィカルに表示します。
SNMP Credentials	デバイスの SNMP 設定を構成します。設定内容については、P.225 の「接続プロトコルの認証情報の設定」を参照してください。 更新内容をすべて破棄するには、「Reset」をクリックします。 設定を検証するには、「Test」をクリックします。 設定を保存するには、「Save」をクリックします。
SSH/Telnet Credentials	SSH または Telnet 接続のセキュリティ設定を行います。設定内容については、P.225 の「接続プロトコルの認証情報の設定」を参照してください。
Additional Information	（Edit Additional Information）アイコンをクリックして、デバイスの詳細情報を追加します。 「Purchase Date」「Keeper」「Warranty Expiration」「Service Vendor」「Service Contact」「Description」といった項目を追加することができます。
LACP Working Status	LACP が有効な場合、LACP（Link Aggregation Control Protocol）のステータスを表示します。
Hardware Health	デバイスのファン、電源、温度に関する稼働ステータスを表示します。
Port	
「Port」タブを選択すると、ポートの概要と一覧が表示されます。 • 表示カテゴリ：「Monitor」「Comparison」「Alarm Settings」 メモ　デバイスの接続情報は、識別可能な一意の SOID を持ち、D-View8 サーバに SNMP データを送信可能な管理デバイスのみで利用可能です。 注意　スイッチでスタックを使用している場合、そのポートのステータスは「Unknown」と表示されます。 注意　DGS-1210 シリーズにおいて、「In/Out Ucast (packets)」の値は 0 と表示されます。 注意　DXS-3400 シリーズ、DGS-3630 シリーズの SFP+ コンボスロットを利用している場合、同番の Copper ポート側がリンクアップ表示されます。 注意　DGS-1100-05PDV2/05V2/08V2/08PV2 では、ポートエラー状態の場合にステータスが正しく表示されません。	

項目	説明
Monitor	■ **「Monitor」を選択した場合** 「Port List」にポート一覧が表示されます。ON/OFF スイッチを使用してポート毎の設定を行います。チェックボックスで選択したポートを一括設定することもできます。 ・「Monitoring Status」:「Wired Traffic」の監視設定を有効 / 無効に設定します。 ・「Alarm Switch」:「Wired Traffic」のアラームが定義されている場合、ON ステータスとなります。アラームの ON/OFF を設定します。 ・「Admin Status」:インタフェースのステータスを有効 / 無効に設定します。 「Wired Traffic」の監視設定は、**Alarm & Notification > Monitor & Alarm Settings** の「Monitor Settings」から設定することも可能です。左側ツリーから「 Wired Traffic 」を選択し、監視対象のポートを指定して設定します。
	（View Port Detail）/ （View Ports Overview）アイコンをクリックして、ポート毎のトラフィック統計グラフとポート一覧の概要情報の表示を切り替えることができます。トラフィック統計グラフを表示するポートは、パネルビューから選択します。
Comparison	■ **「Comparison」を選択した場合** 特定のポートのトラフィック統計情報をグラフで表示します。 パネルビューでポートをクリックして、ポートを選択 / 解除します。2 つまでのポートを選択し、比較することができます。 2 台のデバイスから 2 つのポートを選択することもできます。「Compare port with another device」から別のデバイスを選択し、そのデバイスのポートと比較します。パネル端の「>」「<」をクリックして表示するデバイスを切り替えます。 メモ　比較の基準（例えば、RX/TX バイト、合計転送バイト、および RX/TX エラー）を「Interface Monitoring Results」セクション下の「Select Monitor Charts」より選択することもできます。 メモ　スイッチが物理スタック をサポートしており有効化されている場合、かつプライマリマスタとして設定されている場合は、物理スタックされたユニットのポートが表示されます。 メモ　パネル上のポートにマウスオーバーすることで、選択したポートの（Rx/Tx レート、ポートの種別、帯域幅、PoE の情報を含む）情報を表示させることができます。
Alarm Settings	■ **「Alarm Settings」を選択した場合** パネルビューで選択したポートのアラーム設定を確認できます。 ポート毎のアラーム設定は、**Alarm & Notification > Monitor & Alarm Settings** の「Alarm Settings」タブから設定します。左側ツリーから「 Wired Traffic」を選択し、Rx/Tx トラフィックレート、エラーレート、破棄レート、帯域使用率に基づくアラームルールを設定します。
Wireless	
無線デバイスの場合、「Wireless」タブが表示されます。 注意　「Authentication time」「Connection Time」「RX(pps)/TX(pps)」の値は「N/A」または「0」と表示されます。（DAP シリーズ） 注意　DAP-X2810 では、「Wireless」タブは未サポートです。	
Monitor	
System Monitor	「Monitor」タブを選択すると、CPU、メモリ、応答時間などのデータがグラフィカルに表示されます。「Hour（時間）」「Day（日）」「Week（週）「Month（月）」「Quarter（四半期）」別の統計を表示できます。 「Monitor Settings」をクリックし、各メトリックの監視ステータスを ON/OFF に設定します。 ・利用可能なカテゴリ（例）:「802.1Q VLAN」「BaseInfo」「CPU Utilization」「Device Common Information」「DHCP Server Status」「HTTP Status」「LACP」「LLDP」「Memory Utilization」「Power Status」「Private Port」「RMON Status」「Response Time」「SNTP Status」「SSH Status」「STP Status」「Temperature」「Syslog Status」「Telnet Status」「Trap Status」「Safeguard Status」「Syslog Status」「sFlow Profile」 利用可能な監視カテゴリはデバイスにより異なります。監視ステータスの管理は **Alarm & Notification > Monitor & Alarm Settings**、利用可能な監視カテゴリとテンプレートの管理は **Templates > Monitor Template** から行います。 デバイスに対しカスタムの監視機能を定義することができます。詳細は、P.198 の「デバイステンプレートの生成」を参照してください。
Customized Monitor	デバイスにカスタム定義の監視設定を追加すると、「System Monitor 」タブの右に「Customized Monitor」タブが表示されるようになります。

項目	説明
Monitor Views	
Rack View / System Topology	「Monitor Views」タブを選択すると、ラックビュー、トポロジマップの概要が表示されます。 ラック名のリンクをクリック、または **Monitoring > Rack View** に移動して、ラックビュー画面を表示します。詳細は、P.180 の「第 9 章　ラックグループの管理」を参照してください。 トポロジ名のリンクをクリック、または **Monitoring > Topology Map** に移動して、トポロジマップ画面を表示します。詳細は、P.173 の「ネットワークトポロジの表示と管理」を参照してください。
Alarm	
Active Alarms / Historical Alarms	「Alarm」タブを選択すると、アクティブまたは承認済み（履歴）のアラームイベントが表示されます。承認済みイベントは、自動スクリプトにより承認となったエントリまたは管理者の「Acknowledge」設定により手動で承認となったエントリです。 「Alarm Settings」をクリックして、監視 / トラップ /Syslog のアラームルールを ON/OFF に設定します。（**Alarm & Notification > Monitor & Alarm Settings** の「Alarm Settings」タブで設定済みのアラームルールについて、有効 / 無効ステータスを設定することができます。）
Trap & Syslog	
Trap / Syslog	「Trap & Syslog」タブを選択すると、トラップと Syslog のエントリが表示されます。 すべてのトラップイベントと Syslog を確認するには、**Alarm & Notification > Trap & Syslog** 画面に移動します。詳細は、P.162 の「トラップログと Syslog の表示」を参照してください。
Management	
Management	「Management」タブを選択し、デバイス設定やタスクの表示と設定、ファームウェアおよびコンフィグレーションファイルの管理を行います。 利用可能な設定カテゴリは、デバイスによって異なります。デバイスに紐づく Quick configuration と Advanced Configuration の一覧は、「More Settings」から確認できます。 全体で利用可能な Quick configuration と Advanced Configuration の設定は、**Configuration > Batch Configuration > Quick Configuration** または **Advanced Configuration** に移動します。 また、設定テンプレートを使用してデバイスのカスタマイズ設定を作成できます。**Templates > Configuration Template** に移動します。詳細な手順については、P.201 の「設定テンプレートの生成」と P.198 の「デバイステンプレートの生成」を参照してください。 本画面で主要項目の ON/OFF ステータスを設定したり、「More Settings」から項目を選択してクイック設定タスクを実行することもできます。 **注意** D-View8 によるファームウェア / コンフィグ管理について、以下の制限があります。 • D-View8 によるファームウェアアップグレード機能は、物理スタック構成のスイッチ、DIS-200G シリーズ、DAP-X2850 ではサポートされません。 • D-View8 によるバックアップ / リストアは DGS-1100-05PDV2/05V2/08V2/08PV2、DAP-X2810 ではサポートされません。
PoE	
PoE 対応デバイスの場合、「PoE」タブが表示されます。 **注意** DGS-1100-05PDV2/05V2/08V2/08PV2 では、「PoE」タブは未サポートです。	
ツールバー	
Ping	画面右上の「Ping」をクリックして、「ICMP Ping」画面を表示します。
Save to Device	画面右上の（Save to Device）をクリックして、更新された設定をデバイスに保存します。
Refresh from Device	画面右上の（Refresh from Device）アイコンをクリックして、デバイスとパネルの情報を同期します。
Reboot	画面右上の（Reboot）アイコンをクリックしてデバイスを再起動します。 **注意** D-View8 によるデバイスの再起動は、DIS-200G シリーズ、DGS-1100-05PDV2/05V2/08V2/08PV2 ではサポートされません。

注意 D-View8 で利用可能な監視 / 設定項目は製品によって異なります。

※ D-View8 において管理デバイスでサポートされている Monitor 及び Configuration 機能は、「Device Template」画面で確認することができます。（**Templates > Device Template** に移動し、特定のモデルを検索して、このモデルに設定されているすべての監視および設定テンプレートを表示します。）ただし、管理対象デバイスでシステムデフォルトとして採用されているシステムビルトテンプレートの一部は、まだ検証プロセス中であり、正常に動作しない可能性があります。サポートされる製品については、P.13 の「サポートされる製品」を参

照してください。

※デバイス側で CLI/SNMP に対応している場合、ユーザ定義の監視 / 設定テンプレートを作成して管理に役立てることもできます。対応可否は製品や機能により異なります。

※設定機能の制限事項に関しては、弊社ホームページの製品ページから対象製品のユーザマニュアルをご確認ください。

デバイスへの Ping/ 設定保存 / 再起動

ネットワークデバイスに対し、Ping の送信、設定の保存、再起動を実行します。これらのタスクを実行するには、デバイスがオンラインである必要があります。

1. **Monitoring > Device View** をクリックします。
2. カテゴリメニューから、「Managed」タブを選択します。デフォルトでは「Switch-All」カテゴリメニューが表示されます。
   ドロップダウンメニューからデバイスの種類を選択して、特定のカテゴリのデバイスを一覧表示することができます。
3. 対象デバイスのシステム名をクリックし、デバイス情報画面を表示します。

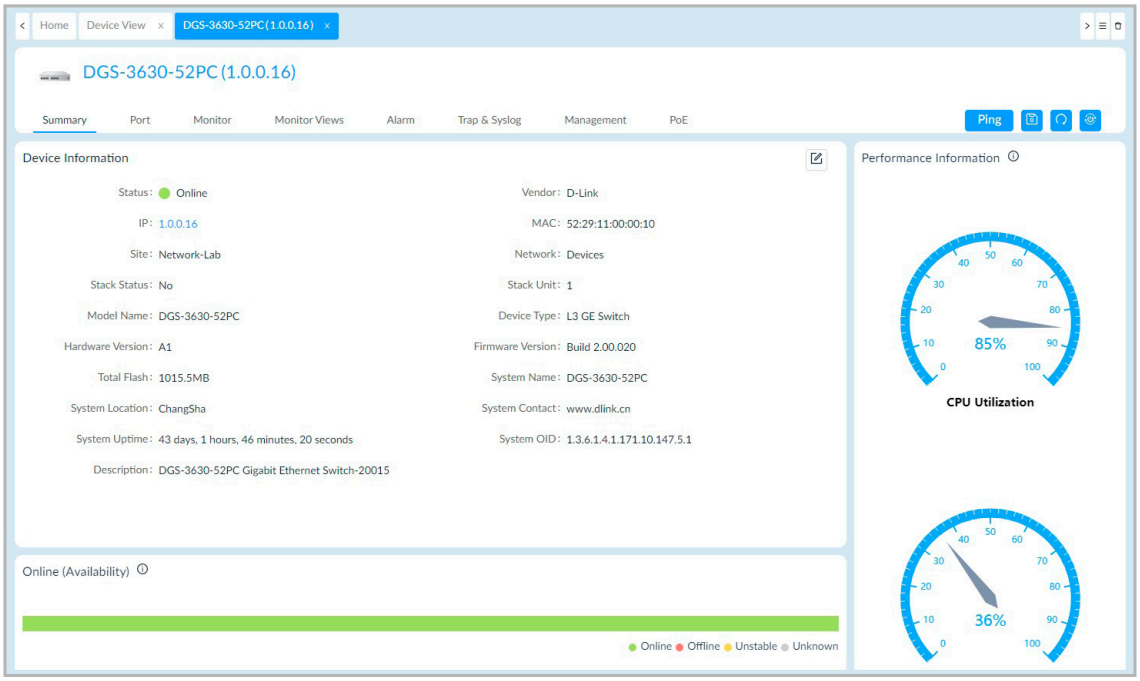


図 4-12　デバイス詳細画面

4. 右上のツールバーから、次のアクションを実行することができます。

項目	説明
Ping	Ping をクリックして、「ICMP Ping」画面を表示し、デバイスに対し Ping を実行します。Ping を実行する際、Ping の回数や Ping リクエストパケットのサイズなどを設定することができます。
Save to Device	（Save to Device）アイコンをクリックして、更新した設定をデバイスに保存します。
Refresh from Device	（Refresh from Device）アイコンをクリックして、デバイスの情報と同期します。
Reboot	（Reboot）アイコンをクリックして、デバイスを再起動します。

注意　D-View8 によるデバイスの再起動は、DIS-200G シリーズ、DGS-1100-05PDV2/05V2/08V2/08PV2 ではサポートされません。

インタフェースリストの表示とエクスポート

管理デバイスのインタフェース（ポート）を表示し、一覧を表形式（.csv）ファイルにエクスポートできます。このリストには管理デバイスの情報のみが含まれます。

1. **Monitoring > Interface View** をクリックし、インタフェース一覧を表示します。

表示項目：

項目	説明
System Name	システム名のリンクをクリックすると、デバイス情報画面に遷移します。
Model Name	デバイスモデル名が表示されます。
IP	デバイスの IP アドレスが表示されます。
Network	デバイスのネットワークが表示されます。
Interface Index	デバイスのポート番号が表示されます。
Interface Name	デバイスのポートの名前が表示されます。
Interface MAC	ポートの MAC アドレスが表示されます。
Connected MAC	接続先デバイスの接続ポートの MAC アドレスが表示されます。
Connected Interface Name	接続先デバイスの接続ポートのインタフェース名が表示されます。
VLAN ID	ポートが所属する VLAN ID が表示されます。
VLAN Name	ポートが所属する VLAN 名が表示されます。
VLAN Type	ポートに設定されている VLAN タイプが表示されます。
VLAN Port Status	VLAN ポートのステータス（タグ付きまたはタグなし）が表示されます。
Update Time	情報が最後にデバイスと同期された時刻が表示されます。

2. ツールバーメニューから、（Export）アイコンをクリックすると、エクスポートが開始されます。

   エクスポートされたファイルはブラウザの既定のフォルダに保存されます。

接続リストの表示とエクスポート

接続されたデバイスについて、インタフェースレベルでの詳細データを含む接続に関する情報を表示します。一覧を表形式（.csv）ファイルにエクスポートすることもできます。このリストには管理デバイスの情報のみが含まれます。

1. **Monitoring > Connection View** をクリックし、接続の一覧を表示します。

表示項目：

項目	説明
Status	リンクの接続状態が表示されます。
Alarm	リンクの接続されたいずれかのデバイスのアラームが表示されます。
Link Name	リンクの両端のデバイスの IP アドレスが表示されます。リンク名をクリックすると、デバイスのパフォーマンス情報やポートのオンラインステータスなど、リンクの詳細情報を確認できます。
Device A	リンクの一方のデバイスの IP アドレスが表示されます。
Interface A	デバイス A の接続ポートが表示されます。
Device B	リンクのもう一方のデバイスの IP アドレスが表示されます。
Interface B	デバイス B の接続ポートが表示されます。
RX/TX	送受信データが表示されます。
Utilization	帯域幅使用率（%）が表示されます。
Type	接続タイプが表示されます。
Last Updated	最後に情報がデバイスと同期された時刻が表示されます。
Detection Source	検出元またはプロトコルが表示されます。

2. ツールバーメニューから、（Export）アイコンをクリックすると、エクスポートが開始されます。

   エクスポートされたファイルはブラウザの既定のフォルダに保存されます。

デバイスグループの管理

デバイスグループを定義することにより、ネットワークデバイスの管理を簡素化することができます。
- グループには、ネットワーク検出により検出されたデバイスを追加することができます。
- グループは、組織、サイト、またはネットワーク範囲に対し作成することができます。
- 作成したグループは、バッチ設定やファームウェア管理でターゲットデバイスを適用する際に使用できます。

デバイスグループの追加

1. **Monitoring > Device Group** をクリックします。
2. 「Device Group」セクションで、「+ Add Device Group」をクリックします。

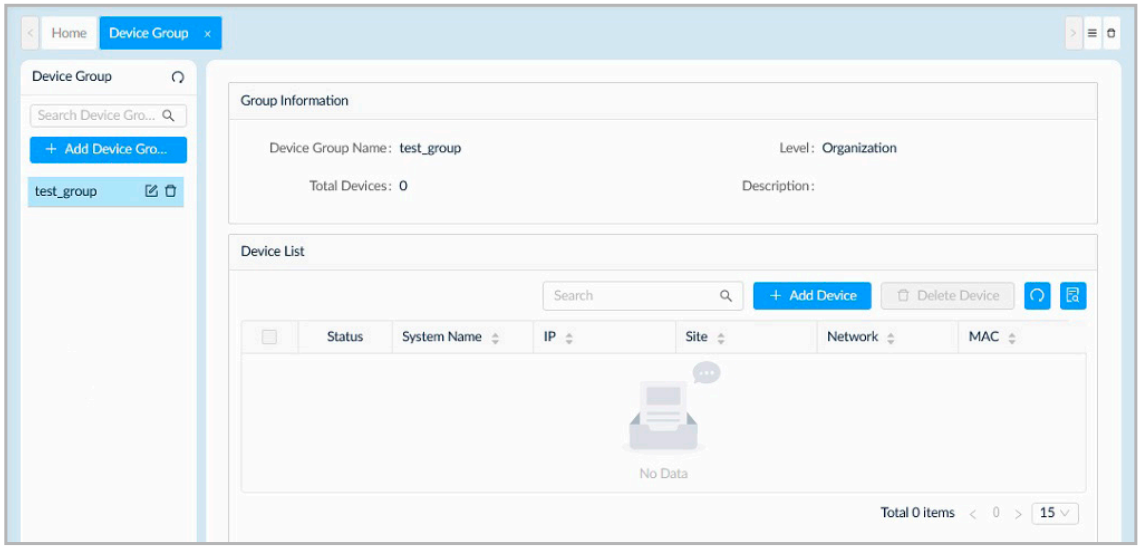


図 4-13　デバイスグループ

3. グループ情報を入力します。

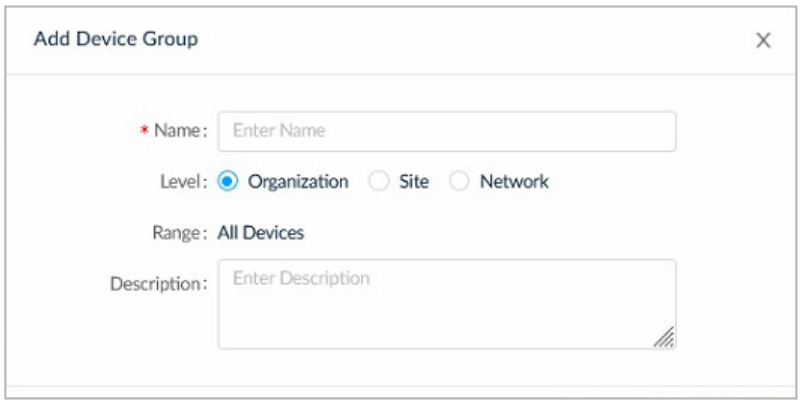


図 4-14　デバイスグループの追加

設定項目：

項目	説明
Name	グループの名前を入力します。
Level	グループレベルを選択します。 • 「Organization」：組織内で検出されたすべてのデバイスを追加対象とします。（初期値） • 「Site」：指定したサイト内のデバイスを追加対象とします。 • 「Network」：指定したネットワーク内のデバイスを追加対象とします。
Description	グループの識別に役立つ短い説明を入力します。

4. 「Save」クリックして、デバイスグループを保存します。 設定をキャンセルするには、「Cancel」をクリックします。
5. グループ情報画面が右側に表示されます。

グループへのデバイスの追加

1. **Monitoring > Device Group** をクリックします。
2. 「Device Group」の一覧からデバイスグループを選択します。グループが存在しない場合は、「+ Add Device Group」をクリックして新規グループを追加します。

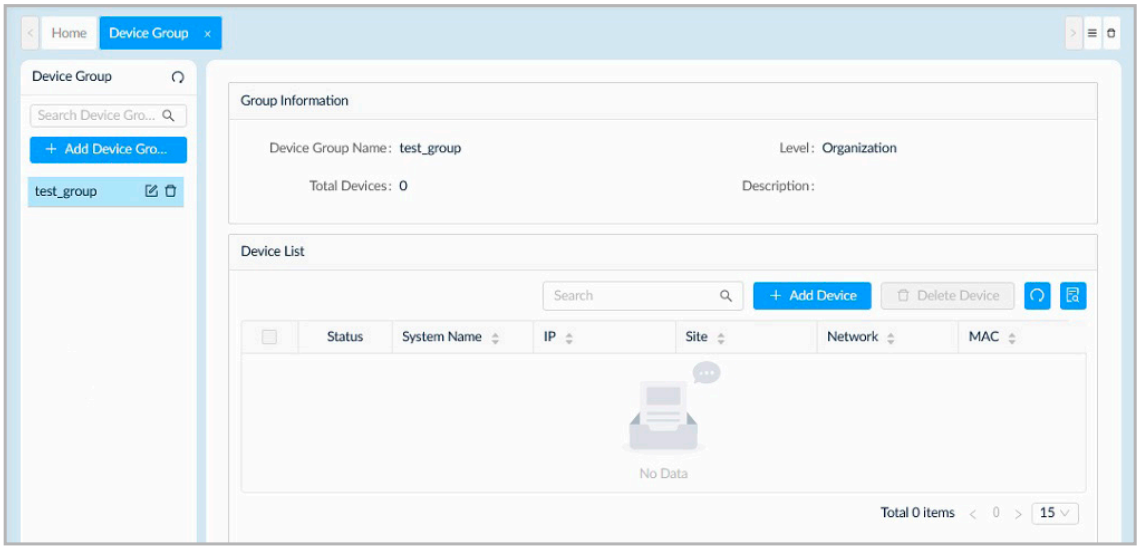


図 4-15　デバイスグループ

3. 「+ Add Device」をクリックします。
「Add Device」画面には、特定のレベル（組織、サイト、ネットワーク）配下の検出デバイスが表示されます。

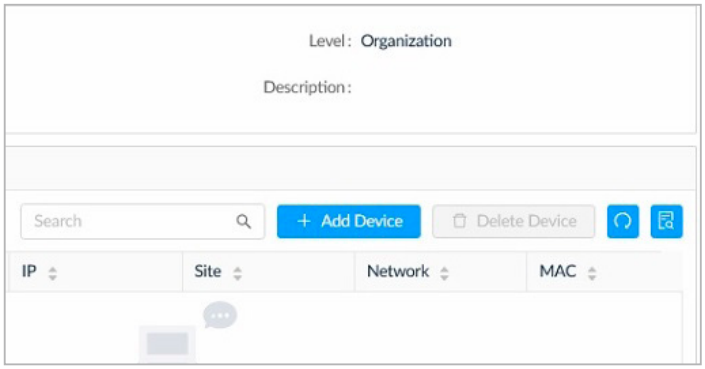


図 4-16　デバイスの追加

4. 「Resource Tree」から、追加対象のデバイスが含まれるサイト / ネットワークを選択します。

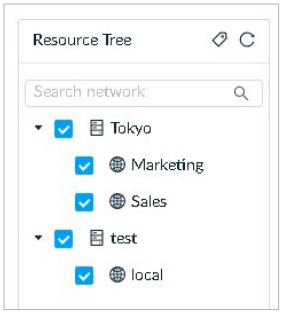


図 4-17　リソースツリー

5. 「Device List」のエントリから、グループに追加するデバイスを選択します。
検索フィールドをクリックして、IP アドレスまたはモデル名を入力し、検索結果をフィルタリングすることもできます。検索結果から、リストに含めるデバイスを選択します。

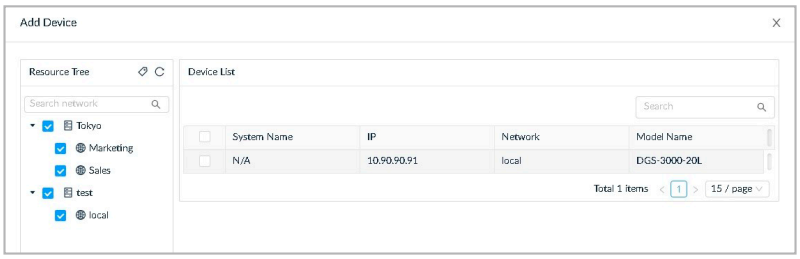


図 4-18　デバイスエントリの選択

6. 「Save」をクリックして、選択したデバイスをグループに追加します。

デバイスグループの編集または削除

1. **Monitoring > Device Group** をクリックし、以下の画面を表示します。

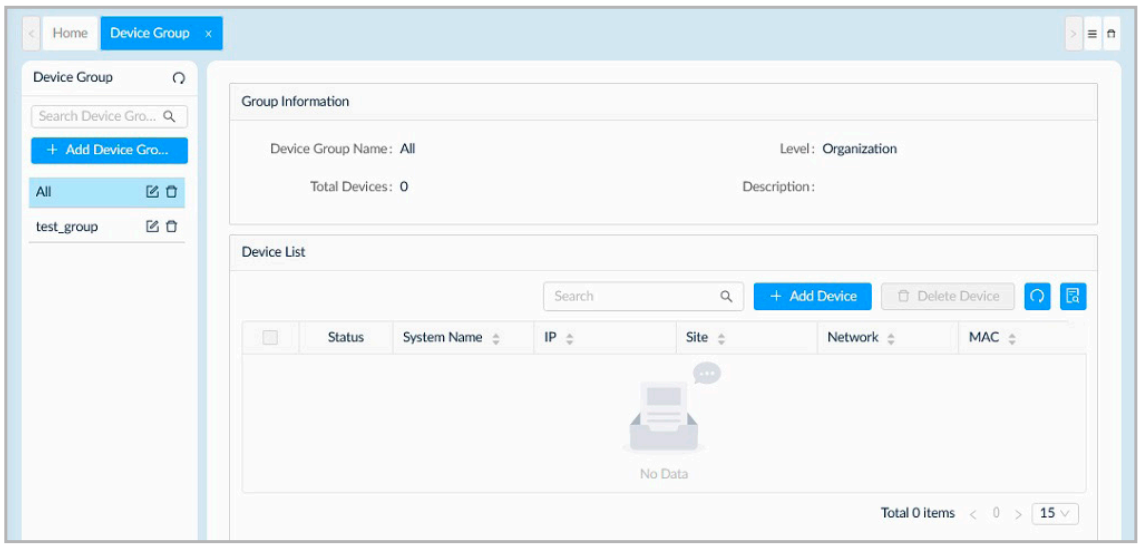


図 4-19　デバイスグループ

2. 既存のデバイスグループに対し、以下のアクションを実行します。
   - 編集：（Edit）アイコンをクリックして、デバイスグループ情報を編集します。
   - 削除：（Delete）アイコンをクリックして、デバイスグループを削除します。

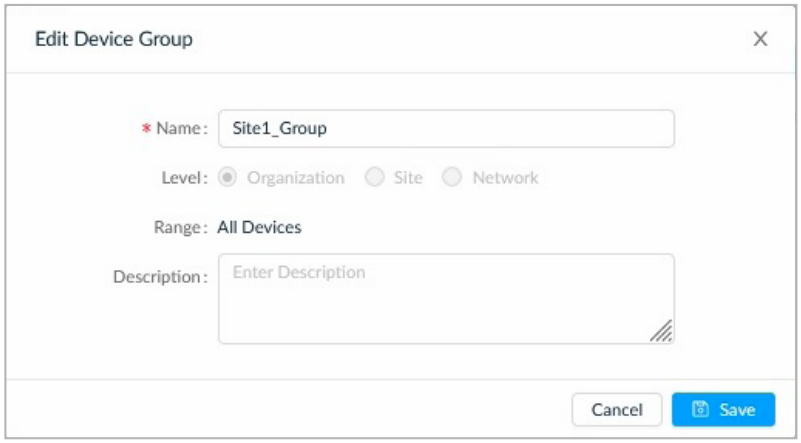


図 4-20　デバイスグループの編集

グループからのデバイスの削除

1. **Monitoring > Device Group** をクリックし、以下の画面を表示します。
2. 「Device Group」の一覧からデバイスグループを選択します。
3. デバイスを選択し、「Delete Device」をクリックして削除します。

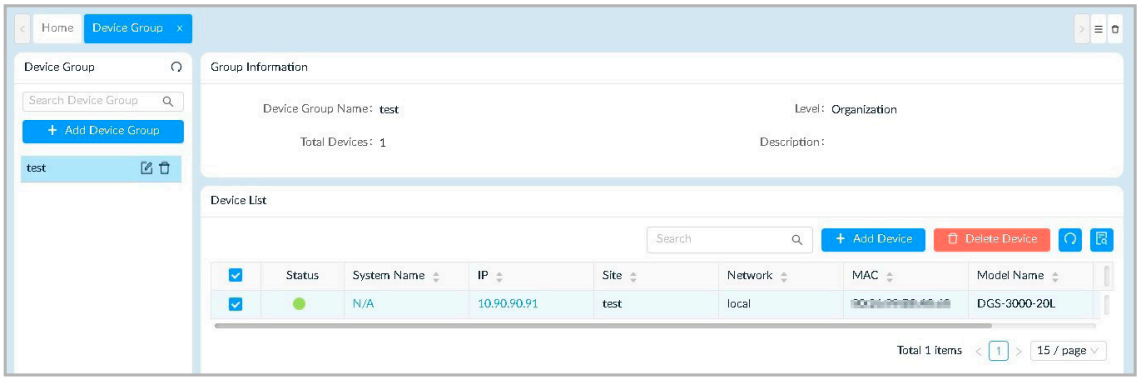


図 4-21　グループからのデバイスの削除

4. 確認メッセージが表示されるので、「Yes」をクリックしてグループからの削除処理を実行します。
   アクションをキャンセルするには、「No」をクリックします。

SNMP 設定

ネットワークの検出とデバイス情報の取得は、SNMP（Simple Network Management Protocol）を使用します。SNMP を使用することで、D-View8 アプリケーションはデバイスの特定のパラメータを監視できるようになります。また、特定のタイプのトラップがデバイスから送信される際に、アラームをトリガします。

SNMP 認証情報の設定

ネットワーク検出と監視のために、デバイスを個別にポーリングできます。SNMP 資格情報リストで必要な SNMP 設定を行います。

1. **System > Basic Settings** をクリックします。
2. 「Credentials」タブを選択して、以下の画面を表示します。デフォルトで「SNMP Credentials」タブが表示されます。

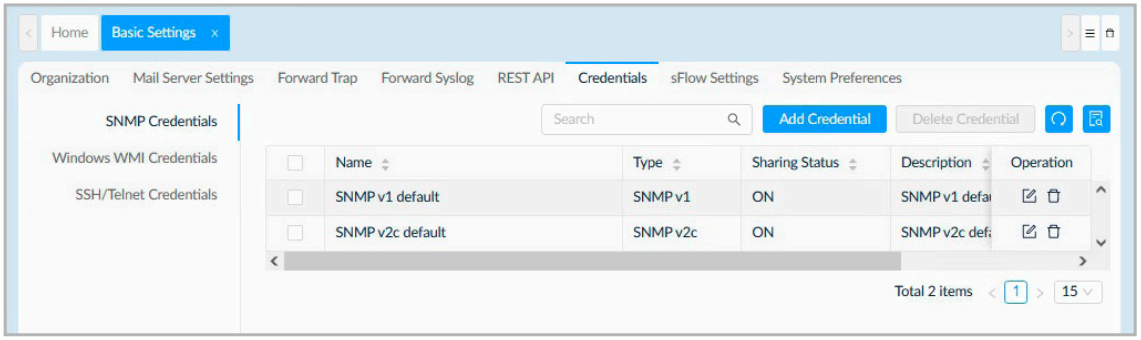


図 4-22　SNMP 認証情報

3. 「Add Credential」をクリックし、以下の画面を表示します。

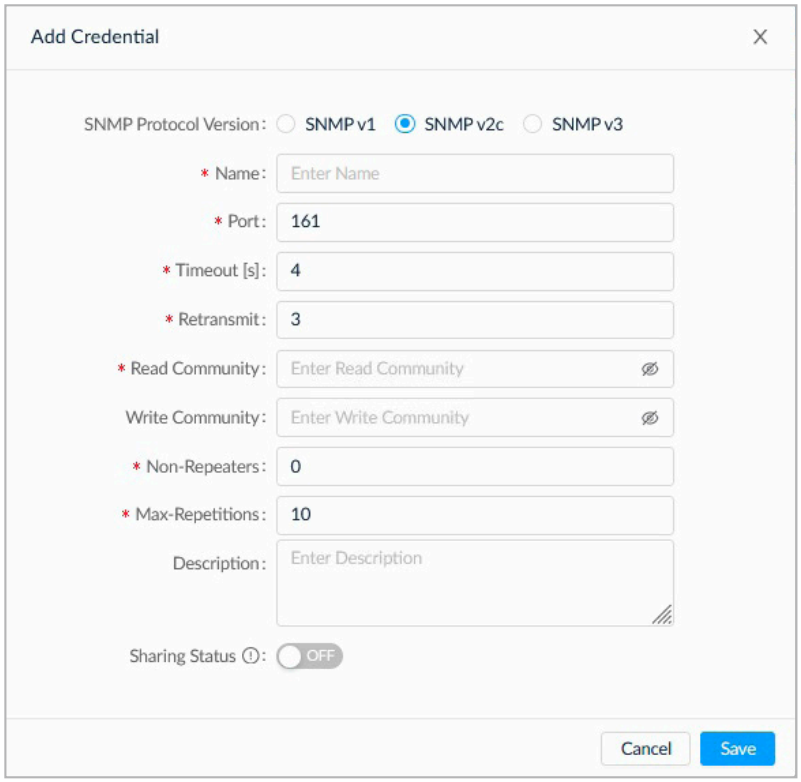


図 4-23　SNMP プロファイルの追加

詳細は、P.225 の「接続プロトコルの認証情報の設定」を参照してください。

SNMP テスト

SNMP 機能は、互換性のあるツールを使用して各種プラットフォームでテストすることができます。D-View8 では、SNMP エージェントへの SNMP アクセスをテストする便利な SNMP ツールを利用可能です。

1. **Tool > SNMP Test** をクリックします。
2. 左側ペインでパラメータを設定し、エージェントデバイスにアクセスします。
3. 右側にテスト結果が表示されます。

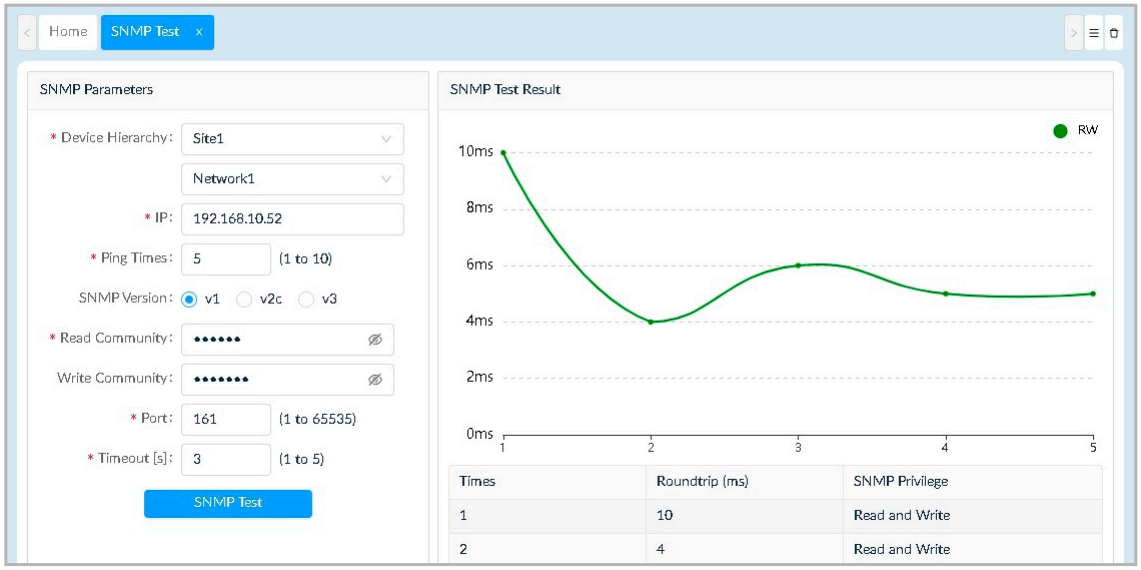


図 4-24　SNMP テスト

詳細は、P.249 の「SNMP テストの実行」を参照してください。
検証された SNMP パラメータは、**System > Basic Settings > Credentials** の「SNMP Credential」リストに保存して、ネットワーク検出などに利用することができます。

MIB の表示

管理情報ベース（MIB）は、ネットワークデバイスの設定とクエリを容易にする体系化されたデータです。D-View8 の MIB ブラウザを使用し、SNMP 経由でポーリングされたデータの抽出に役立てることができます。本機能では、SNMP の 3 つのバージョンすべてをサポートします。

注意　本機能はエンタープライズ版のみサポートされます。

1. **Tools > MIB Browser** をクリックします。
2. ネットワークを選択、接続先 SNMP エージェントの IP アドレスを入力し、「Contact」をクリックしてエージェントに接続します。
3. 左ペインから MIB オブジェクトを指定し、「Operation」のいずれかの処理を実行して情報を取得します。

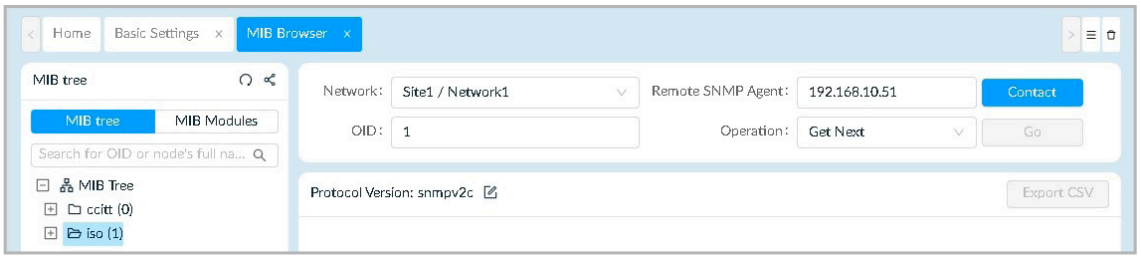


図 4-25　MIB ブラウザ

詳細は、P.244 の「MIB ブラウザ」を参照してください。

SNMP によるデバイスの監視

SNMP を使用して、パケット伝送および関連するエラーのデータを収集、レポートに表示することにより、デバイスとネットワークを監視します。監視するデータは、テンプレートを作成してカスタム定義することもできます。

1. **Templates > Monitor Template** をクリックします。
2. 「Monitor Category」タブで、監視カテゴリを作成します。ソースデータの種類を定義します。
3. 「Monitor Template」タブで、監視テンプレートを作成します。カテゴリで定義されたデータ型に従い、OID を指定します。

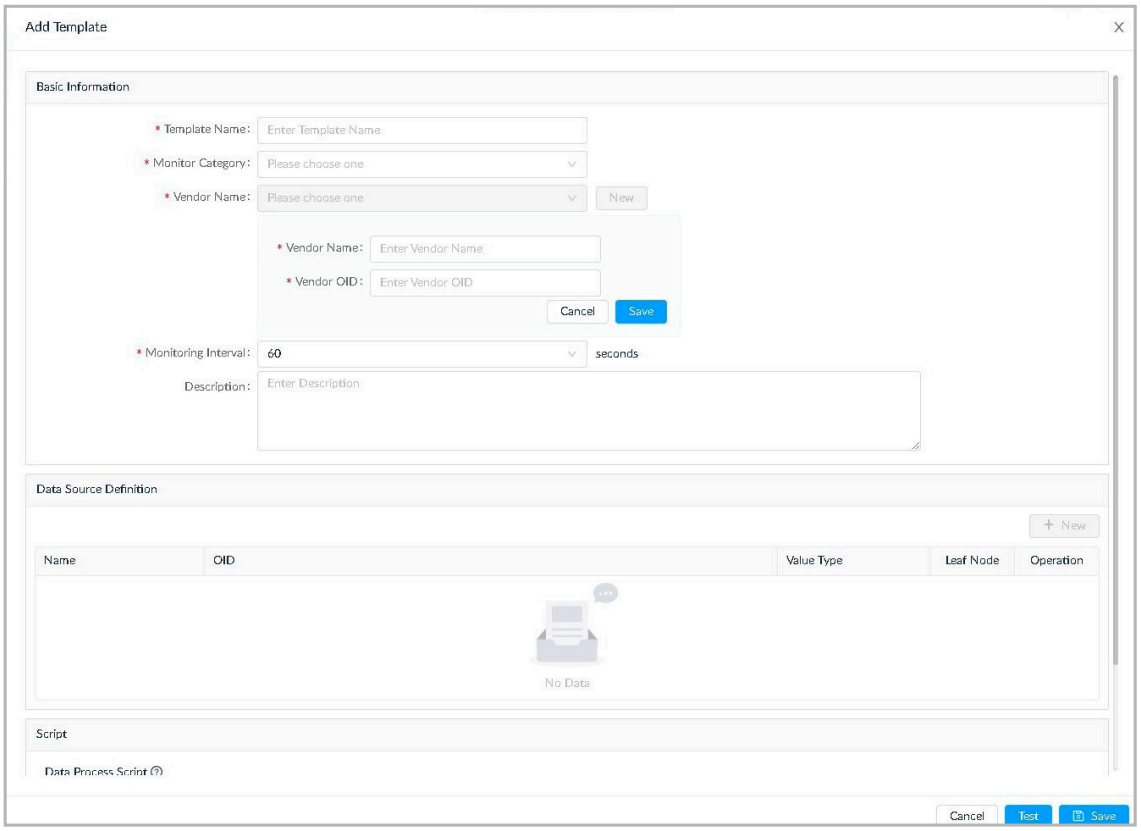


図 4-26　テンプレートの追加

4. **Templates > Device Template** をクリックし、デバイスモデルを先ほど定義した監視テンプレートに関連付けます。

詳細は、P.198 の「デバイステンプレートの生成」および P.200 の「監視テンプレートの生成」を参照してください。

トラップの表示とアラームの生成

D-View8 では、トラップの表示や指定ホストへ転送設定を行うことができます。また、特定のトラップが送信されたときにアラートをトリガすることもできます。

注意 D-View8 で利用可能な監視項目は製品によって異なります。

トラップの有効化

1. **Monitoring > Device View** をクリックします。
2. デバイスのシステム名をクリックして、デバイス情報画面を開きます。
3. 「Management」タブをクリックし、「Trap Status」を有効にして、D-View8 をトラップサーバとして設定します。
4. デバイスに対しトラップサーバが有効になると、デバイス情報画面の「Trap & Syslog」タブ、または **Alarm & Notification ＞ Trap & Syslog** に移動してトラップ情報を確認することができます。

トラップの管理

1. **Alarm & Notification ＞ Trap & Syslog** に移動して、すべてのトラップイベントを表示します。
2. **Alarm & Notification ＞ Trap & Syslog Editor** では、OID の説明を追加して、トラップ OID を定義することもできます。

詳細は、P.162 の「トラップログと Syslog の表示」、P.163 の「トラップエディタ機能」を参照してください。

トラップにアラームを設定

1. **Alarm & Notification > Monitor & Alarm Settings** に移動し、「Alarm Settings」タブをクリックします。
2. 左側のメニューの「Trap」カテゴリから、アラームのトリガに使用する項目を選択します。
3. 「+ Add」をクリックしてアラームルールを追加し、指定したトラップ OID または変数のバインディング値を持つトリガ条件を定義します。

詳細は、P.165 の「アラームおよび監視の管理」を参照してください。

トラップの転送

1. **System > Basic Settings** に移動し、「Forward Trap」タブをクリックします。
2. 「Add Destination Host」をクリックし、トラップを送信する宛先ホストを追加します。

バッチ構成による複数ネットワークの管理

D-View8 では、定義済みのスケジュールを使用して、ネットワーク全体でデバイスを一括設定できます。

設定テンプレートの作成

バッチ構成を行うには、設定テンプレートを準備する必要があります。システムで定義済みのテンプレートが用意されているほか、カスタマイズテンプレートを作成することができます。また、2 種類の設定タイプ（単一の設定カテゴリのクイック設定と、バッチ設定に使用する複数の設定カテゴリから構成される詳細設定）のオプションが利用可能です。

設定テンプレートの追加

1. **Templates > Configuration Template** に移動します。
2. 「Configuration Template」タブを開き、左側メニューから作成したカテゴリを選択します。
3. 右上の「+ Add Template」をクリックします。
4. 以下の情報を入力、選択します。

メモ　以下の項目は、名前の 頭に v2 が付く設定カテゴリ以外に適用されます。名前の頭に v2 が付く設定テンプレートを作成する場合は、P.198 の「デバイステンプレートの生成」を参照してください。

項目	説明
Template Settings	
Name	テンプレートの名前を入力します。
Configuration Category	選択したカテゴリが表示されます。
Vendor	ドロップダウンメニューからベンダ OID を持つベンダを選択します。
Protocol	設定に使用するプロトコルを選択します。 • 選択肢：「SSH/Telnet」「SNMP」
Description	テンプレートの簡単な説明を入力します。

CLI Command	SSH/Telnet を使用する場合は、デバイスを設定する CLI コマンドを入力します。
	
	スクリプトの記述ルール：
	• '#' で始まる行は、コマンドではなくコメントと見なされます。
	• 各行には、CLI コマンドを 1 つだけ記載します。
	• 文字列の前後に '%' を使用して、変数としてラベル付けします。例）%IP% は、IP を変数としてラベル付けします。
	• 変数の値は、コンポーネント設定の「Name」項目で指定することができます。（「Name」の値と変数名が一致するように指定します）
	• デッドロック操作を防止するには、処理が停止しない CLI コマンドの使用を避けてください。例）ping10.0.0.1
	• デッドロック操作を防止するには、終了するために特別な入力エントリを必要とする CLI コマンドの使用を避けてください。例）show port
	
	サンプルスクリプト：
	`config ssh authmode password enable`
	`config ssh server contimeout 120`
	`enable SSH`
	
	変数を含むサンプルスクリプト：
	`config fdb aging_time %TimeoutSeconds%`
	
	サンプルコメント：
	`# this is a comment`

Engineering View	
画面下部のテンプレートデザインセクションでは、コンポーネント設定（構成レイアウトと項目）を設定できます。SNMP 項目の場合は、OID と値タイプを入力する必要があります。また、デザインにコントロール / 入力フォーム（例：テキスト入力フォーム、ラジオボタン）を追加することもできます。	

5. デザインにコントロール / 入力要素を追加したり、プリセット構成項目のコンポーネント設定を構成します。SNMP オブジェクトに適切な OID と値タイプを設定します。

メモ　SNMP オブジェクトについては、事前に MIB ブラウザや SNMP ツールを使用して、有効性をテストおよび検証する必要があります。

6. テンプレートでコンポーネントを追加することが可能な場合は、「Layout Component Size」から 1 列、2 列、3 列、または 4 列のオプションを使用して、最初にレイアウトを選択します。次に、表示する入力コントロールとテキストフィールドを選択して構成します。
7. 「Save」をクリックしてテンプレートを保存します。

作成したテンプレートを編集、プレビュー、削除することもできます。また、JSON（JavaScript Object Notation）ファイルとしてダウンロードすることもできます。

注意 設定機能の制限事項に関しては、弊社ホームページの製品ページから対象製品のユーザマニュアルをご確認ください。

設定テンプレートのデバイスへの紐づけ

定義したテンプレートをデバイスに紐づけることで、関連デバイスではその設定をベースとして利用することができるようになります。

1. **Templates > Device Template** に移動します。
2. 左側の「Device Type」からデバイスモデルを選択します。
3. 「Template Information」セクションの下部にある「Configuration」タブを選択します。
4. 「Associate Configuration Template」をクリックして、関連付ける設定テンプレートを選択します。

詳細は、「デバイステンプレートの生成」および「設定テンプレートの生成」を参照してください。

バッチ設定

設定テンプレートをデバイスに関連付けた後、バッチ設定を使用して、選択したデバイスに単一の設定または複数の一括設定を適用できます。

1. **Configuration > Batch Configuration** に移動します。
2. 設定テンプレートのタイプに応じて、「Quick Configuration」または「Advanced Configuration」タブを選択します。
3. 「Advanced Configuration」タブの場合、「Add Profile」をクリックして以下の設定を行います。
   (1) プロファイルの名前と説明を入力します。
   (2) 「Device Hierarchy」でデバイスモデルを選択します。
   (3) 「Configuration Feature List」で設定カテゴリを選択します。プロファイルには、複数のカテゴリを含めることができます。
   (4) 「Next」をクリックして、選択したカテゴリの構成項目を設定します。
   (5) 「Save」をクリックして、設定プロファイルを保存します。
4. 「Quick Configuration」タブの場合は、以下の設定を行います。
   (1) 左側のカテゴリ一覧から設定カテゴリを選択します。
   (2) 設定変更を適用するタスクを作成します。タスクの作成手順については、次のセクションの「バッチ設定のタスクの作成」を参照してください。

バッチ設定の詳細は、P.137 の「タスクとプロファイルの作成」を参照してください。

バッチ設定のタスクの作成

■ クイック設定

1. 「Quick Configuration」タブを開き、左側のカテゴリ一覧から設定カテゴリを選択します。
2. 選択カテゴリの設定画面が表示されるので、以下の情報を入力します。

設定項目：

項目	説明
Task Information	
Task Name	タスクの名前を入力します。
Task Description	タスクを識別するための簡単な説明を入力します。
Configuration Information	
Status/Input	タスクの設定内容を指定します。設定項目は、設定カテゴリのテンプレートにより異なります。
Target Devices	
Add Devices	「Add Devices」をクリックして、設定対象のデバイスを追加します。選択した機能に対応しているデバイスのみ選択できます。ユーザ定義の設定カテゴリの場合、最初に設定テンプレートをデバイステンプレートに関連付ける必要があります（**Templates > Device Template**）。

項目	説明
Schedule Information	
Schedule Type	• 「One Time」：1 回のみのタスク適用を実行します。 -「Immediately（即時）」：すぐにタスクを開始します。 -「Specify a Date（日付の指定）」：「Date」をクリックして、タスクを実行する日時を指定します。 • 「Recurrent」：タスクを実行する頻度と有効期間を指定します。スケジュール設定の詳細は、P.236 の「スケジュール機能」を参照してください。

3.　右上の「Add Task」をクリックし、タスクを作成します。

タスクの管理画面を開くには、にマウスオーバーして、「Task Management」を選択します。

■ 詳細設定

1.　「Advanced Configuration」タブを開き、一覧からプロファイルを選択します。

2.　「Operation」の ＋ （Create Task）アイコンをクリックし、以下の情報を入力します。

設定項目：

項目	説明
Task Information	
Task Name	タスクの名前を入力します。
Task Description	タスクを識別するための簡単な説明を入力します。
Target Devices	
Add Devices	「Add Devices」をクリックして、設定対象のデバイスを追加します。
Schedule Information	
Schedule Type	• 「One Time」：1 回のみのタスク適用を実行します。 -「Immediately（即時）」：すぐにタスクを開始します。 -「Specify a Date（日付の指定）」：「Date」をクリックして、タスクを実行する日時を指定します。 • 「Recurrent」：タスクを実行する頻度と有効期間を指定します。スケジュール設定の詳細は、P.236 の「スケジュール機能」を参照してください。

3.　「Save」をクリックして新しいタスクを作成します。

タスクの管理画面を開くには、「Task Management」をクリックします。タスクの管理についての詳細は、P.142 の「現在のタスク」を参照してください。

詳細な手順については、P.139 の「設定プロファイルの追加」、P.141 の「デバイスへのプロファイルの適用（タスクの作成）」を参照してください。

第 5 章　ネットワークの監視

ダッシュボードやその他の様々な機能を使用して、ネットワークを監視できます。ダッシュボードに表示される情報は、「Customized Dashboard」画面でカスタマイズ可能です。

本章では、以下のトピックについて説明します。

- 「デフォルトダッシュボードの表示」
- 「ダッシュボードのカスタマイズ」
- 「レポートの表示とエクスポート」
- 「レポート設定の管理」
- 「ファームウェアバージョンの表示」
- 「D-View8 通知の表示」
- 「複数のネットワークの監視」

デフォルトダッシュボードの表示

デフォルトのダッシュボードでは、本アプリケーションに接続されているリソースの構成・管理情報を提供します。これらの情報をネットワークの評価、活用、集中管理に利用することができます。

メモ　ライセンスの期限が切れると、管理ノード数の制限（D-View8 フル機能は利用可能）についてのアラートと、追加ライセンスの適用を促すメッセージがダッシュボード画面に表示されます。ライセンスの更新手順については、P.238 の「ライセンス管理」を参照してください。

1. ダッシュボードにログインします。

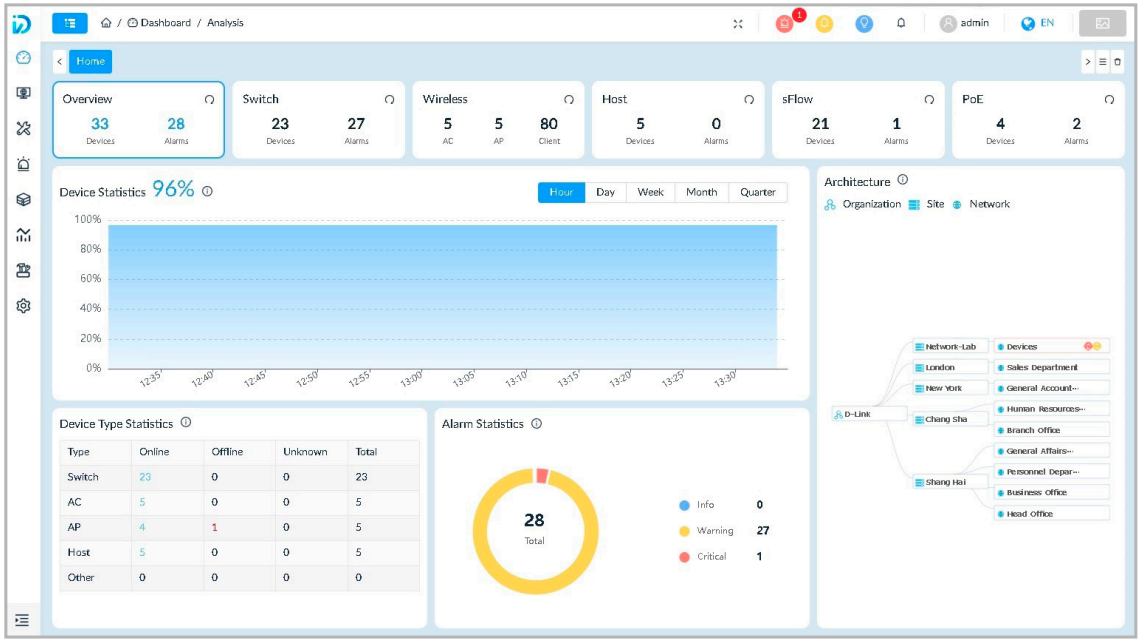


図 5-1　　デフォルトダッシュボード（Analysis）

デフォルトでは、「Overview（概要）」パネル選択時には次のウィジェットが表示されます。統計情報を更新するには、上部パネルの をクリックします。

項目	説明
Device Statistics	管理対象デバイスのオンライン状態の統計データを表示します。
Architecture	D-View8 ネットワークアーキテクチャ図を表示します。
Device Type Statistics	管理対象デバイスの接続テータス（オンライン / オフライン）について、デバイス種類毎に統計情報を表示します。
Alarm Statistics	管理対象デバイスのアラームについて、各重要度の割合を円グラフ統計で表示します。

チャートやグラフ上のデータをクリックして、関連画面に移動することができます。

「Switch」ダッシュボードの項目

ダッシュボードで「Switch」パネルをクリックすると、次のウィジェットが表示されます。統計情報を更新するには、 をクリックします。

項目	説明
Alarm Statistics	スイッチデバイスのアラームについて、各重要度の割合を円グラフ統計で表示します。
Running Status	スイッチデバイスの接続テータス（オンライン / オフライン）の統計データを表示します。
Temperature Statistics	スイッチデバイスの指定温度範囲に基づく統計情報を表示します。 • 温度範囲：40、60、80、90℃
Top 10 Wired Throughput (Rx / Tx)	現在または指定期間で最も多くのトラフィックを送受信している上位 10 件のスイッチを表示します。
Top 10 Memory Utilization	現在または指定期間でメモリ使用率が最も高い上位 10 件のスイッチを表示します。
Top 10 CPU Utilization	現在または指定期間で CPU 使用率が最も高い上位 10 件のスイッチを表示します。
Top 10 Response Times	現在または指定期間で応答時間が最も長い上位 10 件のスイッチを表示します。

メモ　期間の指定は、現在 / 過去 1 時間 /24 時間 /7 日間 /30 日間 /90 日間から選択することができます。

「Wireless」ダッシュボードの項目

ダッシュボードで「Wireless」パネルをクリックすると、次のウィジェットが表示されます。統計情報を更新するには、 をクリックします。

項目	説明
Alarm Statistics	無線デバイスのアラームについて、各重要度の割合を円グラフ統計で表示します。
Running Status	無線デバイス（コントローラ /AP）の接続テータス（オンライン / オフライン）の統計データを表示します。
AP Summary	AP デバイス種類の統計（割合）を表示します。
Top 10 Wireless Throughput	現在または指定期間で最もトラフィックを送受信している上位 10 件の無線デバイスを表示します。
Top 10 Wireless Error Packets	現在または指定期間でエラーパケットが最も多い上位 10 件の無線デバイスを表示します。
Clients by 802.11 Protocol	クライアントが使用する 802.11 プロトコルタイプの統計（割合）を表示します。
Clients by Authentication Type	クライアント認証タイプの統計（割合）を表示します。
Top 10 Devices by Critical Alarms	重大なアラームを生成した上位 10 件の無線デバイスを表示します。
Top 10 SSIDs by Current Client	現在接続しているクライアントが最も多い上位 10 件の SSID を表示します。
Top 10 Response Times	現在または指定期間で応答時間が最も長い上位 10 件の無線デバイスを表示します。
Top 10 APs by Current Client	現在接続しているクライアントが最も多い上位 10 件の AP を表示します。

メモ　期間の指定は、現在 / 過去 1 時間 /24 時間 /7 日間 /30 日間 /90 日間から選択することができます。

注意　DAP-X2810 の無線クライアント情報の監視はサポートされません。

「Host」ダッシュボードの項目

ダッシュボードで「Host」パネルをクリックすると、次のウィジェットが表示されます。統計情報を更新するには、 をクリックします。

項目	説明
Alarm Statistics	ホストデバイスのアラームについて、各重要度の割合を円グラフ統計で表示します。
Running Status	ホストデバイスの接続テータス（オンライン / オフライン）の統計データを表示します。
Top 10 CPU Utilization	現在または指定期間で CPU 使用率が最も高い上位 10 件のホストを表示します。
Top 10 Memory Utilization	現在または指定期間でメモリ使用率が最も高い上位 10 件のホストを表示します。
Top 10 Most Installed Applications	ネットワーク内のホストに最もインストールされている上位 10 件のアプリケーションを表示します。
Top 10 Volumes with Most Disk Usage	ネットワークでディスク使用量が最も多い上位 10 件のボリュームを表示します。
Top 10 Response Times	現在または指定期間で応答時間が最も長い上位 10 件のホストを表示します。
Top 10 Volumes with Least Disk Usage	ネットワーク内でディスク使用量が最も少ない上位 10 件のボリュームを表示します。

メモ　期間の指定は、現在 / 過去 1 時間 /24 時間 /7 日間 /30 日間 /90 日間から選択することができます。

sFlow ダッシュボードの項目

ダッシュボードで「sFlow」パネルをクリックすると、次のウィジェットが表示されます。統計情報を更新するには、 をクリックします。

項目	説明
Top 10 Endpoints	最も使用された上位 10 件のエンドポイントを表示します。
Alarms Statistics	管理対象ネットワーク内の sFlow アラームの各重要度の割合を円グラフで表示します。
Top 10 Applications	指定期間でトラフィックが最も多い上位 10 件のアプリケーションを表示します。
Top 10 Protocol	指定期間でトラフィックが最も多い上位 10 件のプロトコルを表示します。
Top 10 QoS	指定期間でトラフィックが最も多い上位 10 件の QoS を表示します。
Top 10 Conversations	指定期間でトラフィックが最も多い上位 10 件のカンバセーションを表示します。

メモ　sFlow ダッシュボードはエンタープライズライセンスでのみサポートされます。

メモ　期間の指定は、過去 1 時間 /24 時間 /7 日間 /30 日間 /90 日間から選択することができます。

PoE ダッシュボードの項目

ダッシュボードで「PoE」パネルをクリックすると、次のウィジェットが表示されます。統計情報を更新するには、 をクリックします。

項目	説明
Alarm Statistics	PoE デバイスのアラームについて、各重要度の割合を円グラフ統計で表示します。
Running Status	管理対象 PSE デバイスの接続テータス（オンライン / オフライン）の統計データを表示します。
Top 10 PSEs by Current PD Count	電源供給デバイス数が多い上位 10 件の PSE デバイスを表示します。
Top 10 Ports by Current Flow	電流量が多い上位 10 件の PoE デバイスポートを表示します。
Top 10 Ports by Power Output	電力を最も消費している上位 10 件の PoE ポートを表示します。
Top 10 PSEs by Power Output	電力を最も消費している上位 10 件の PoE デバイスを表示します。
Top 10 Response Times	現在または指定期間で応答時間が最も長い上位 10 件の PoE デバイスを表示します。

メモ　期間の指定は、現在 / 過去 1 時間 /24 時間 /7 日間 /30 日間 /90 日間から選択することができます。

ダッシュボードのカスタマイズ

デフォルトのダッシュボードでは、各カテゴリの基本的な統計情報が表示されます。ダッシュボードビューのカスタマイズを行うことで、任意のウィジェットを表示することができます。

カスタマイズダッシュボードの作成

1. **Dashboard** > **Customized Dashboard** をクリックし、以下の画面を表示します。
2. 「+ Add Dashboard」をクリックします。

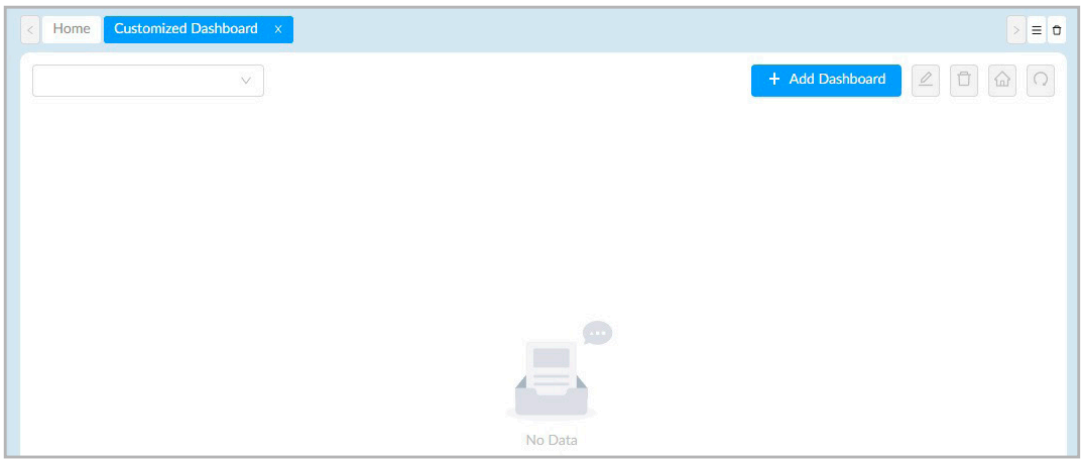


図 5-2　　カスタマイズダッシュボード

3. 「Add Customized Dashboard」画面で、次の情報を設定します。

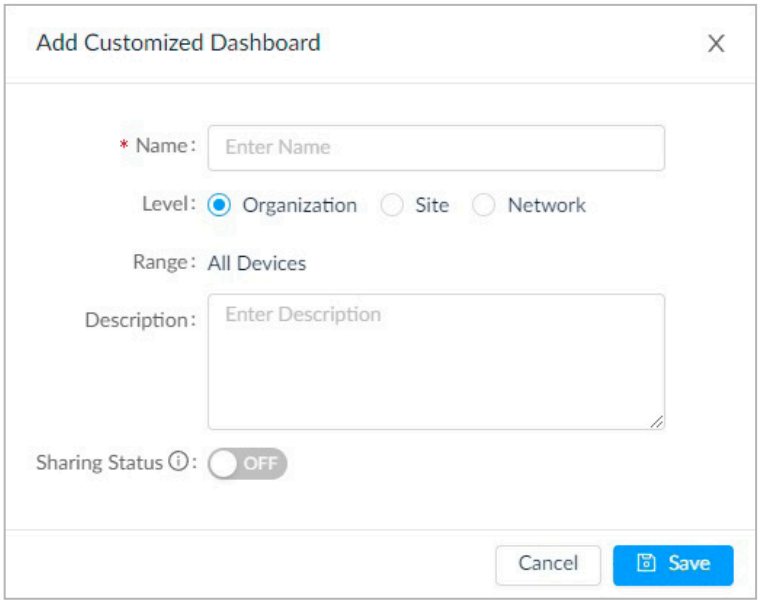


図 5-3　　カスタマイズダッシュボードの追加

設定項目：

項目	説明
Name	ダッシュボードの名前を入力します。
Level	対象の階層レベルを選択します。 • 「Organization」：組織内で検出されたすべてのデバイスを追加対象とします。（初期値） • 「Site」：指定したサイト内のデバイスを追加対象とします。 • 「Network」：指定したネットワーク内のデバイスを追加対象とします。
Description	ダッシュボードの識別に役立つ短い説明を入力します。
Sharing Status	スライドバーを ON/OFF にして、ダッシュボードの共有を有効または無効にします。 共有ステータスを有効にすると、権限を持つ他の管理者がこのダッシュボードを表示、編集、削除できるようになります。 • 初期値：OFF（無効）

4. 「Save」をクリックして、ダッシュボードを作成します。デフォルトでは、空のダッシュボードが表示されます。

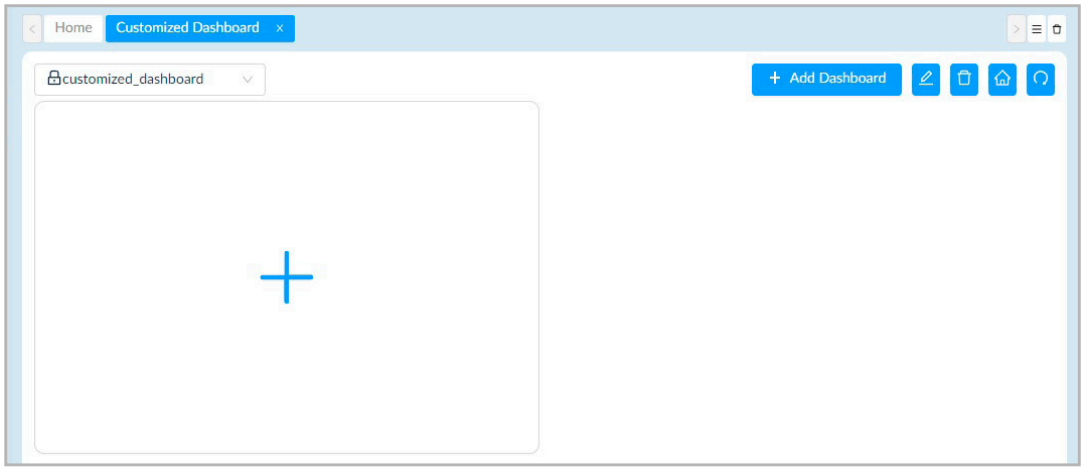


図 5-4　　カスタマイズダッシュボード

5. ダッシュボード上の＋（追加）アイコンをクリックして、「Add Graphics」画面を表示します。

6. ダッシュボードにグラフを追加します。
最初に、「Select device」セクションで、ソースデータとするデバイスを選択します。以下の項目で検索を行うこともできます。
- システム名
- IP
- モデル名
- デバイスカテゴリ
- ネットワーク名

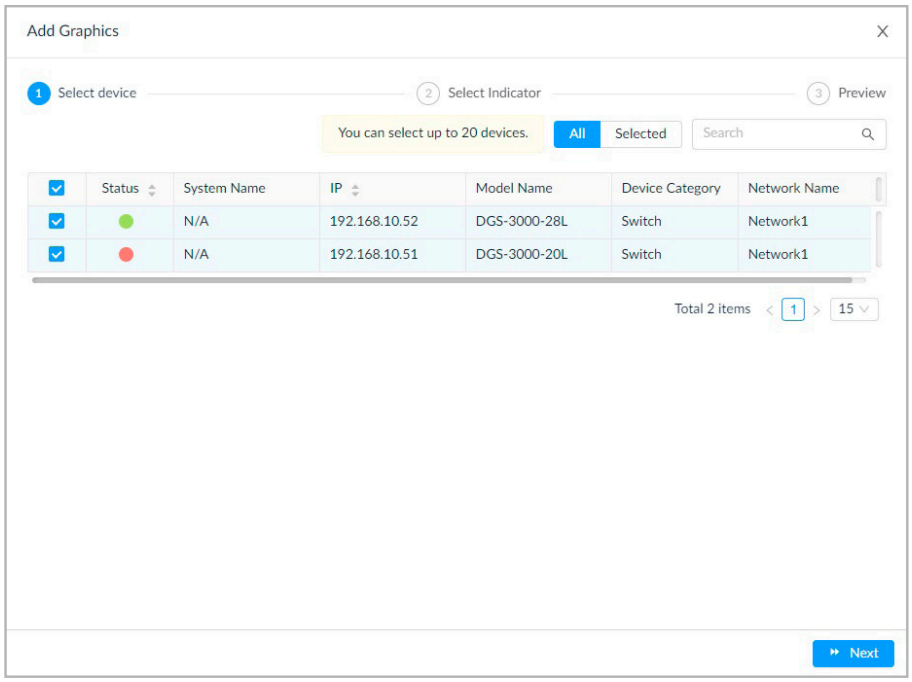


図 5-5　　グラフの追加（①デバイスの選択）

7. 「>> Next」をクリックして次の手順へ進みます。

8. インジケータを選択し、表示する監視情報を指定します。

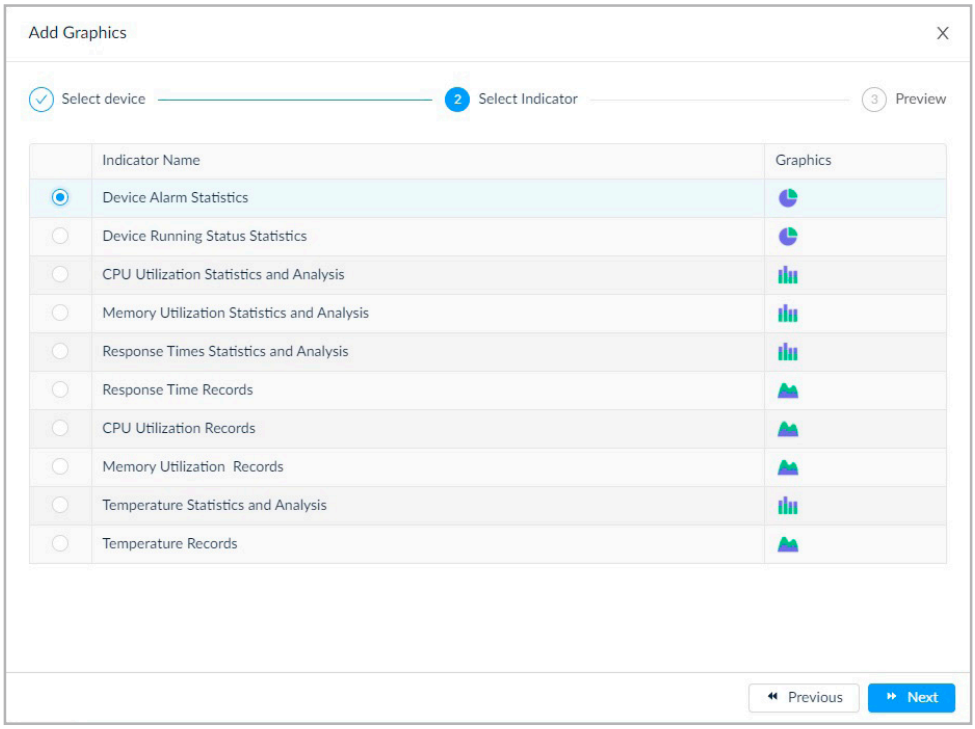


図 5-6　グラフの追加（②インジケータの選択）

システムやネットワークパフォーマンスの統計項目として、以下のようなインジケータを選択することができます。
使用可能なカテゴリは、デバイスのサポート機能によって異なります。

• 「Device Alarm Statistics」 • 「Device Running Status Statistics」 • 「CPU Utilization Statistics and Analysis」 • 「Memory Utilization Statistics and Analysis」 • 「Top 10 Response Time」 • 「Response Time Records」 • 「CPU Utilization Records」 • 「Memory Utilization Records」 • 「Wireless Throughput (Bytes)」 • 「Total Bytes Transmitted」 • 「Total Packets Transmitted」 • 「Current Traffic」 • 「Packets Per Second」	• 「Interface Utilization」 • 「Total Errors and Discards」 • 「Discard Rate」 • 「Error Rate」 • 「Wireless Throughput (Packets)」 • 「Wireless Error Packets」 • 「Wireless Clients by Protocol」 • 「Wireless Clients by Authentication Type」 • 「Wireless Clients by SSID」 • 「Wireless Clients by AP」 • 「SIM Traffic」 • 「Temperature Statistics and Analysis」 • 「Temperature Records」

一部の統計のレポートタイミングは、各監視機能のポーリング間隔に依存します。
監視の ON/OFF ステータスや間隔は以下の画面から設定することができます。
- **Alarm & Notification > Monitor & Alarm Settings > Monitor Settings**
- または、**Monitoring > Device View** 画面のシステム名のリンクをクリック、デバイス情報画面で「Monitor」タブをクリック

注意 DAP-X2810 の無線クライアント情報の監視はサポートされません。

9. 「>> Next」をクリックして次の手順へ進みます。

10. プレビュー画面が表示されます。「OK」をクリックして新しいグラフを作成します。

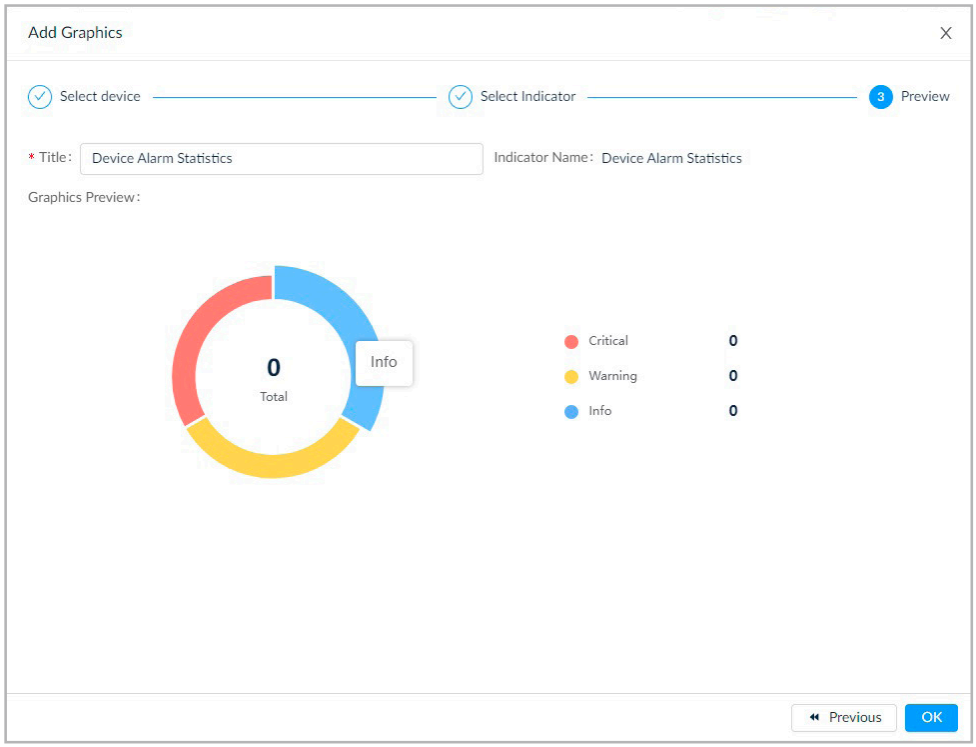


図 5-7　　グラフの追加（③プレビュー）

カスタマイズダッシュボードの変更

1.　**Dashboard** > **Customized Dashboard** をクリックし、「Customized Dashboard」画面を表示します。

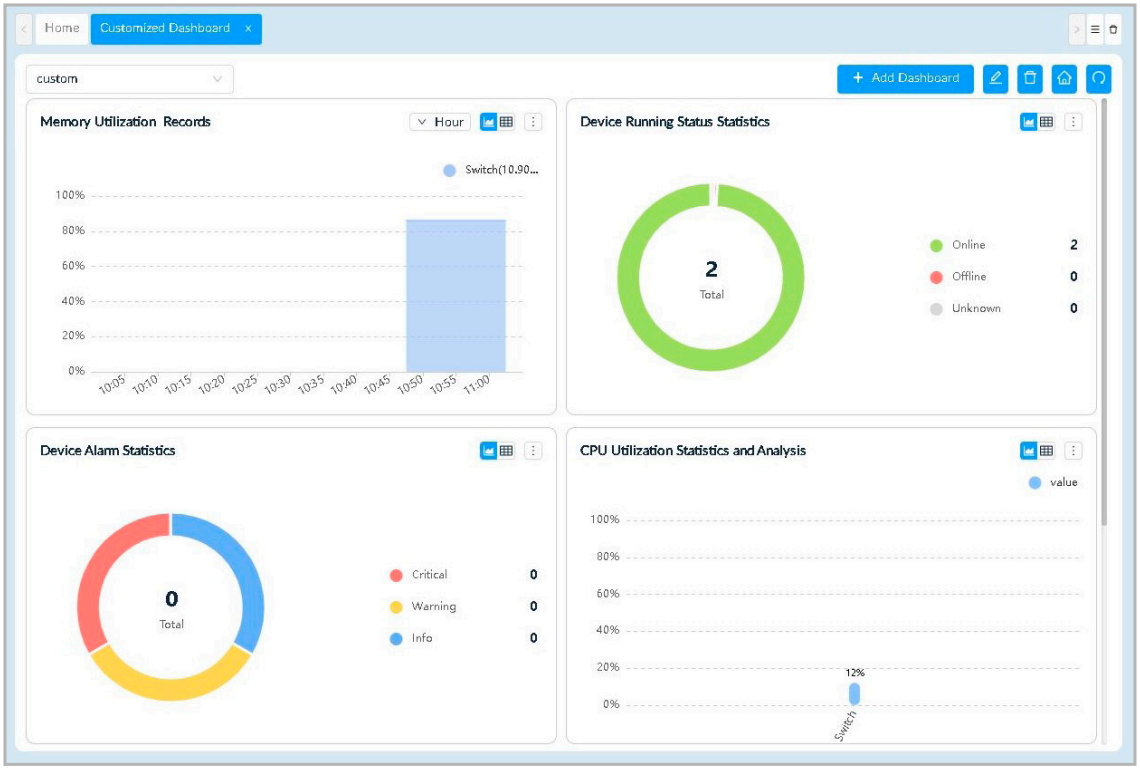


図 5-8　　カスタマイズダッシュボード

ダッシュボードのウィジェットを変更

ここでは「Memory Utilization Records」ウィジェットを使用して説明します。

2. ウィジェット右上の ⋮ （Settings）ボタンをクリックします。

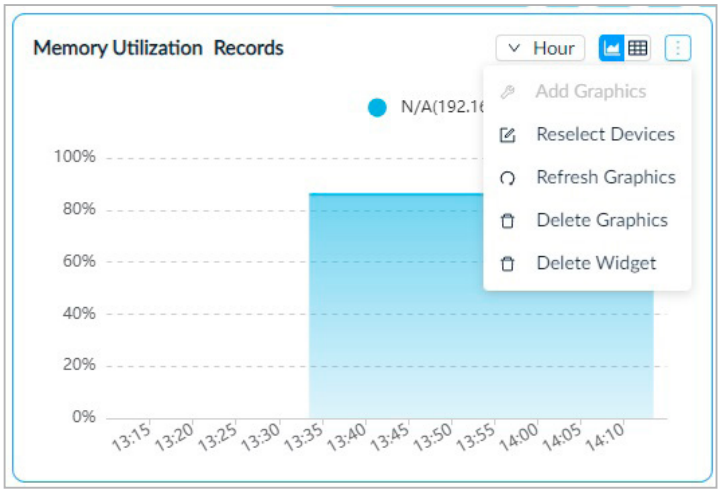


図 5-9　設定オプション

3. 以下のオプションをクリックして、アクションを実行します。
   - 「Add Graphics」：グラフィックが削除されている場合、新しいグラフィックを追加します。
   - 「Reselect Devices」：デバイスを指定し直します。
   - 「Refresh Graphics」：情報を再同期します。
   - 「Delete Graphics」：ウィジェットフレームからグラフィックを削除します。
   - 「Delete Widget」：ウィジェットをダッシュボードから削除します。

メモ　利用可能なオプションは、ウィジェット機能によって異なります。

ダッシュボードの編集または削除

ダッシュボードを編集または削除する場合は、以下の操作を実行します。

ダッシュボードの編集：画面右上の （Edit）をクリックしてダッシュボードの名前や説明を編集します。

ダッシュボードの削除：画面右上の （Delete）をクリックしてダッシュボードを削除します。

ダッシュボードをホームページに設定

新しいダッシュボードをホームページに適用してデフォルトのシステムダッシュボードを置き換えることもできます。

ダッシュボード右上の （Apply to homepage）クリックして、ホームページに適用します。

メモ　ホームページをデフォルトのダッシュボードに戻すには、**Dashboard > Analysis** に移動し、画面右上の「Restore」をクリックします。

レポートの表示とエクスポート

ネットワークで検出されたデバイスの各種監視項目に関するレポートを表示します。以下のレポートを使用できます。

- 「General Reports」
- 「Scheduled Reports」
- 「My Reports」

指定期間に基づき、統計データが生成されます。

メモ　レポート機能の詳細は、P.204 の「第 12 章　レポート機能」を参照してください。

■ レポートの表示手順

1. **Reports > General Reports** をクリックします。

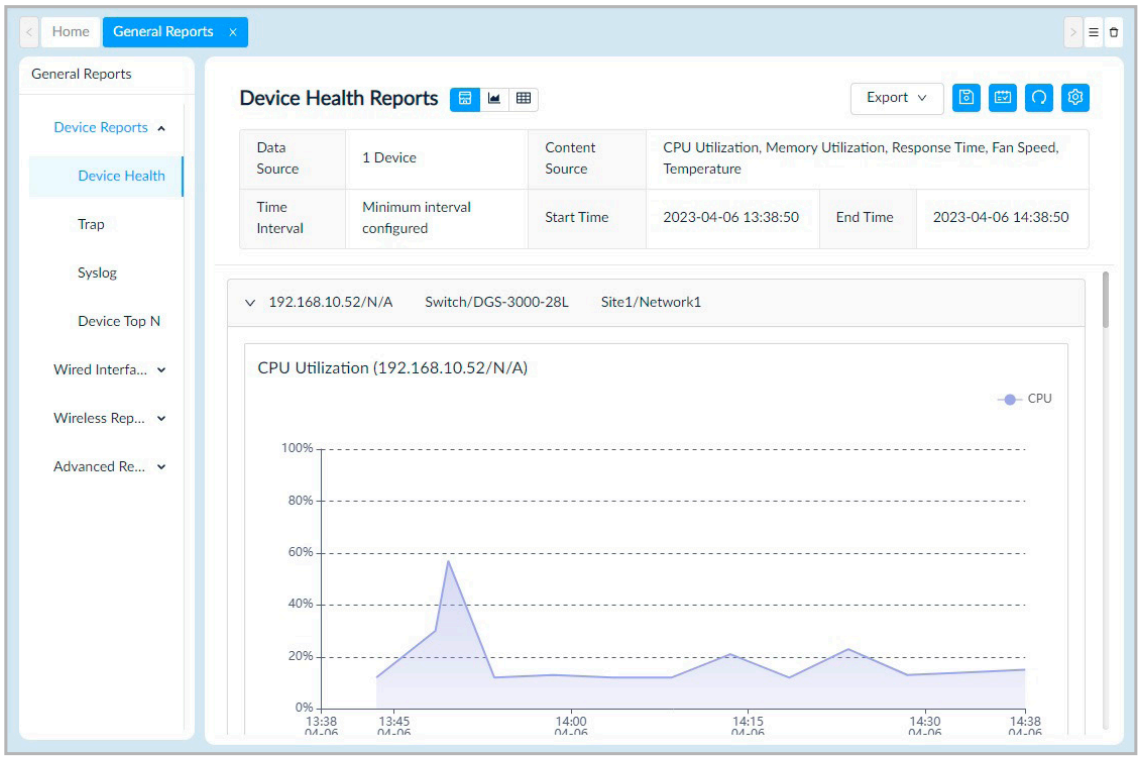


図 5-10　General Reports（デバイスの正常性レポート）

2. 「General Reports」の一覧からレポートを選択します。
   レポートには以下の種類があります。デフォルトでは「Device Health Reports」画面が表示されます。

レポート種別	カテゴリ	項目
General Reports	Device Reports	Device Health
		Trap
		Syslog
		Device Top N
	Wired Interface Reports	Wired Traffic
		Wired Throughput Top N
	Wireless Reports	Wireless Client Count
		Wireless Traffic
	Advanced Reports	Inventory
Scheduled Reports	One Time	—
	Recurrent	—
My Reports	My Reports	—

メモ　デフォルトの状態では、レポートは生成されていません。「The report parameters are required, click HERE to configure.」のリンクをクリックして、レポートパラメータを設定することができます。

エクスポート手順

3. 「Export」ドロップダウンメニューからファイル形式（PDF、Excel、CSV）をクリックして、レポートファイルをダウンロードします。
ファイルはブラウザの既定ダウンロードフォルダに保存されます。

注意 DAP-X2810 の無線クライアント情報の監視はサポートされません。

レポート設定の管理

1. **Reports > General Reports** をクリックします。
デフォルトでは、「Device Health Reports（デバイスの正常性レポート）」画面が表示されます。

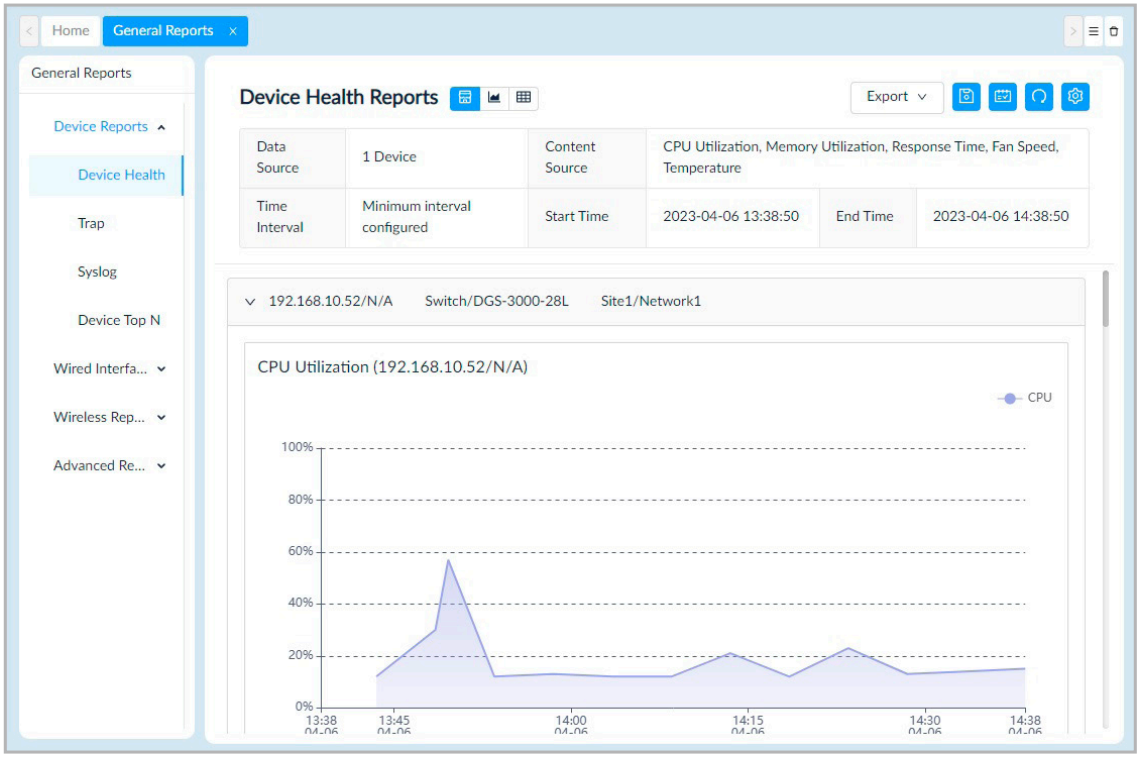


図 5-11　デバイスの正常性レポート

レポート上部のツールバーには、以下の機能が表示されます。

アイコン	項目名	説明
	Show All/ Show Chart only/ Show Table only	レポートの表示形式を選択します。 • 「Show All」：利用可能な情報をすべての形式で表示します。 • 「Show Chart only」：利用可能な情報をグラフ形式で表示します。 • 「Show Table only」：使用可能な情報を表形式で表示します。
Export	Export	レポート情報をファイルに保存します。
	Save to My Reports	現在のレポートを「My Report」として保存します。
	Upgrade to Scheduled Reports	現在のレポートを 1 回または繰り返しのスケジュールレポートとして設定します。
	Refresh	レポート情報を再同期します。
	Report Settings	現在のレポートの設定を変更します。

2. （Report Settings）アイコンをクリックし、レポート設定を行います。

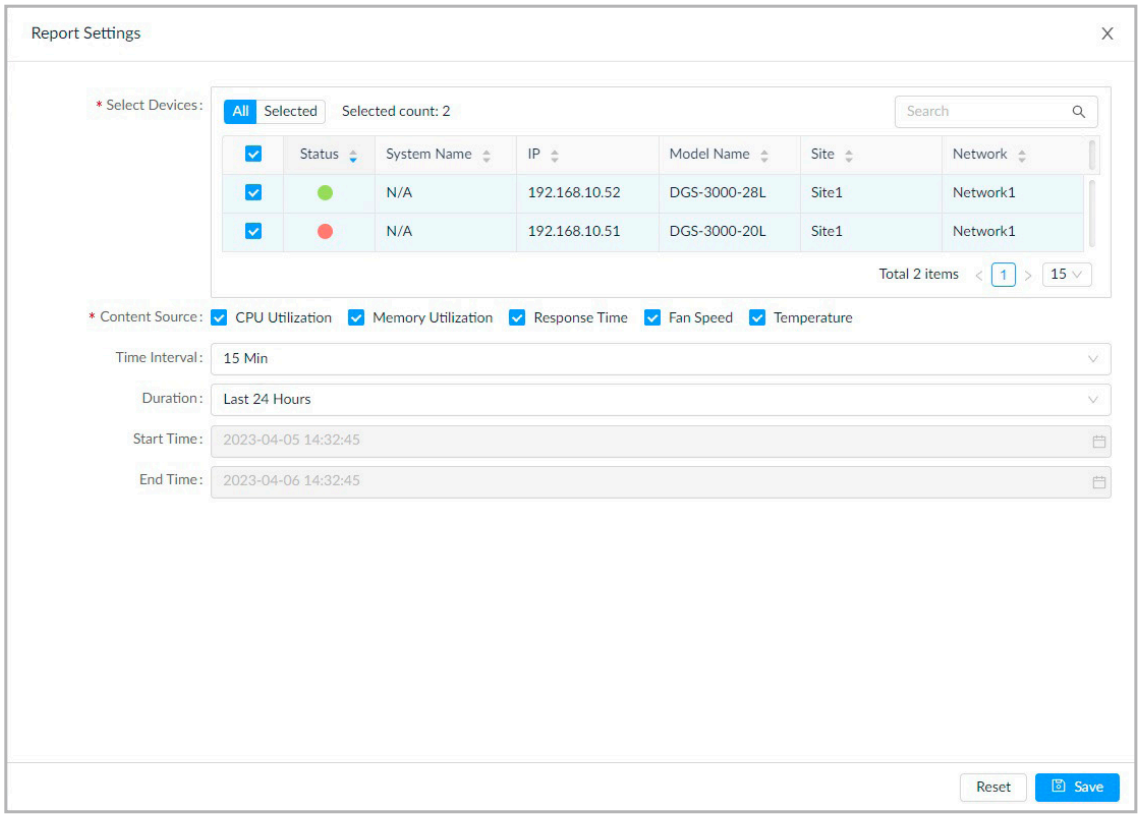


図 5-12　レポート設定

設定項目：

項目	説明
Select Devices	チェックボックスにチェックを入れ、レポートに含めるデバイスを選択します。 スライドバーをクリックすると、表示するデバイスを切り替えることができます。 ・「All（すべて）」「Selected（選択したデバイス）」
Search	キーワードを入力し、表示される対象項目を選択してデバイスを検索・表示します。 ・ 検索項目：「System Name」「IP」「Model Name」「Site」「Network」
Content Source	レポート設定に含める項目にチェックを入れます。 ・ 選択肢：「CPU Utilization」「Memory Utilization」「Response Time」「Fan Speed」「Temperature」
Time Interval	レポート間隔を指定します。 ・ 選択肢：「Minimum interval configured」「15 Min」「2 Hour」「8 Hour」「1 Day」
Duration	レポートの取得期間を選択します。 ・ 選択肢：「Last 24 Hours」「Today」「Yesterday」「Customized（「Start Time」/「End Time」選択）」

メモ　利用可能な設定項目およびそのパラメータは、レポートカテゴリや選択内容によって異なります。ここでは、「Device Health Reports」の一例を説明しています。

3.　「Save」をクリックしてレポート設定を保存します。「Reset」をクリックすると、保存済みの設定内容がデフォルトの状態にリセットされます。

ファームウェアバージョンの表示

検出された D-Link デバイスのファームウェアバージョンを表示します。

1. **Configuration > Firmware Management** をクリックします。

図 5-13　ファームウェア管理

管理デバイスのファームウェアバージョンを確認できます。

メモ　ファームウェアのアップグレード手順については、P.144 の「デバイスのファームウェアアップグレード」を参照してください。

D-View8 通知の表示

D-View8 は、Web アプリケーションと電子メールによる通知機能を提供しています。即時の対応が必要なイベントに対し、通知ルールを設定できます。詳細は、P.93 の「通知センターの設定」を参照してください。

1. ダッシュボードにログインすると、以下の画面が表示されます。

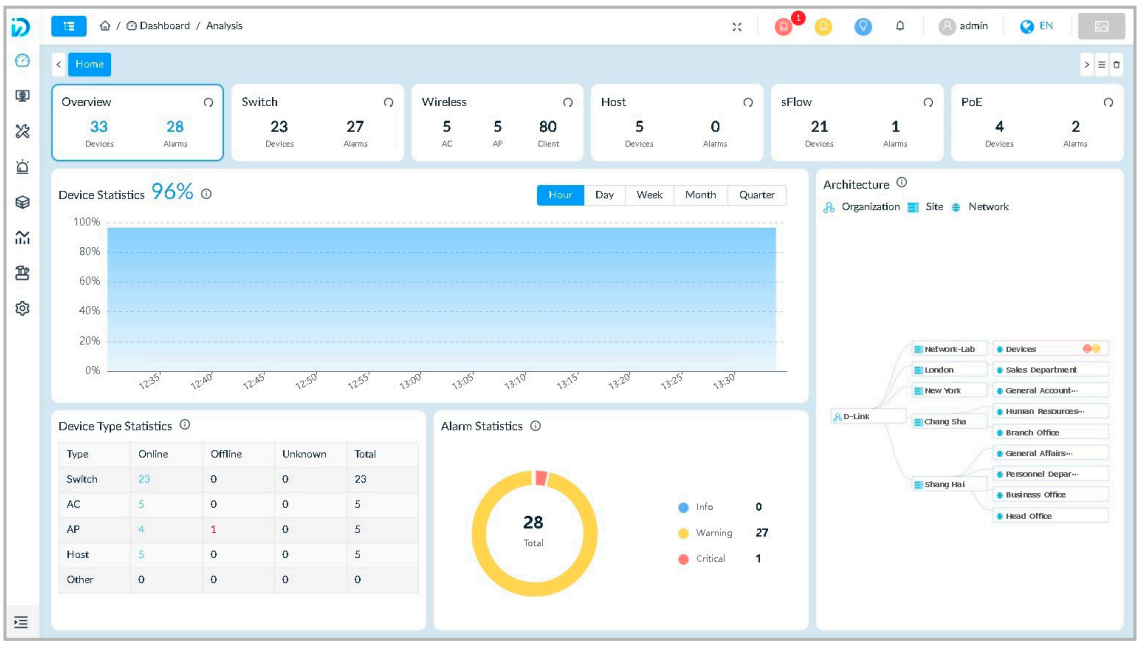


図 5-14　ダッシュボード

2. アナンシエータ右端の通知ボタン（ 🔔 ）をクリックします。通知のポップアップが表示されます。

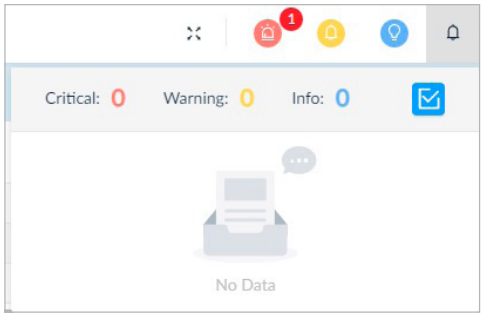


図 5-15　ツールバー通知

通知の一覧をクリアするには、（Acknowledge All）をクリックします。（本画面には履歴は保存されません）。

この通知に関する詳細を確認するには、通知エントリをクリックしてアラームの詳細画面を開きます。
通知ルールについては、通知センターから表示できます（**Alarm & Notification > Notification Center**）。

複数のネットワークの監視

D-View8 の監視機能により、ネットワーク全体のデバイスを効率的に監視できます。
監視機能を利用するには、監視カテゴリとテンプレートが定義されている必要があります。システム / ユーザ定義の監視テンプレートを利用することも可能です。使用する通信プロトコルは SNMP、WMI、HTTP から選択できます。

監視テンプレートの構成

監視カテゴリの追加

最初に監視カテゴリを作成して、監視テンプレートの通信プロトコル、測定単位、およびデータソースを定義する必要があります。

1. **Templates > Monitor Template** に移動し、「Monitor Category」タブを開きます。
2. 監視カテゴリが表示されます。

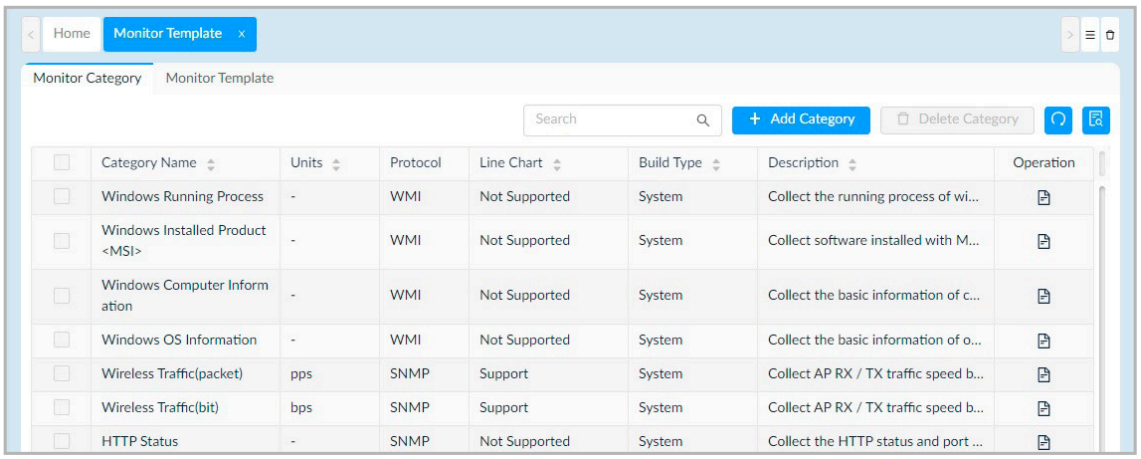


図 5-16　監視カテゴリ

監視カテゴリ一覧には、2 種類のビルドタイプ（System/User）の設定カテゴリが表示されます。
- 「User」：ユーザによって作成された設定カテゴリを示します。
- 「System」：システムによって作成された設定カテゴリを示します。「System」タイプの設定カテゴリは変更することはできません。

3. 右上の「+ Add Category」をクリックします。
4. 以下の情報を入力します。

設定項目：

項目	説明
Category Name	監視カテゴリの名前を入力します。
Units	使用する測定単位を選択します。
Protocol	使用するプロトコルを選択します。 • 選択肢：「SNMP」「HTTP(S)」「WMI」
Line Chart	監視結果を視覚的に表示する折れ線グラフ機能の有効 / 無効を設定します。 追加した監視設定の結果は、デバイステンプレートに監視テンプレートを関連付けた後、以下の画面から確認することができます。 (1) **Monitoring > Device View** に移動してシステム名のリンクをクリック (2) **Monitor > Customized Monitor** タブを選択
Description	カテゴリの簡単な説明を入力します。
Data Source Definition	「+ Add」をクリックして、各データタイプの名前と値タイプを定義します。

3. 「Save」クリックして、監視カテゴリを作成します。

監視テンプレートの追加

1. **Templates > Monitor Template** に移動し、「Monitor Template」タブを開きます。
2. 左側の監視カテゴリ一覧から目的のカテゴリを選択します。
3. 右上の「+ Add Monitor Template」をクリックし、以下の情報を入力します。

設定項目：

項目	説明
Template Name	テンプレートの名前を入力します。
Monitor Category	設定するカテゴリを選択します。
Vendor Name	ドロップダウンメニューから、ベンダ OID を持つベンダを選択します。 新規にベンダを追加するには、「New」をクリックして新規作成します。ベンダの情報については、**Templates > Device Support** を参照してください。
Monitoring Interval	監視するポーリング間隔を指定します。 • 選択肢：「60」「300」「600」「1800」「7200」（秒） • 初期値：60（秒）
Description	このテンプレートの簡単な説明を入力します。
Data Source Definition	監視対象デバイスから取得する特定のデータオブジェクトを定義します。オプションは、デバイス監視に使用される通信プロトコルによって異なります。
Script	追加したデータソースの値を Groovy で処理するスクリプトを入力します。

4. 「Save」クリックして、監視テンプレートを作成します。

テンプレートの紐づけ

作成したテンプレートは、デバイスモデルに関連付けたり、デフォルトでモニタリングするように設定できます。
デバイステンプレートへの紐づけは、**Templates > Device Template** から行うことができます。

監視設定の構成

監視の ON/OFF ステータスやポーリング間隔などの設定を行います。

1. **Alarm & Notification > Monitor & Alarm Settings** に移動し、「Monitor Settings」タブを開きます。

2. 左側の監視カテゴリ一覧から、監視カテゴリを選択します。このカテゴリの監視テンプレートに関連付けられているデバイスが表示されます。

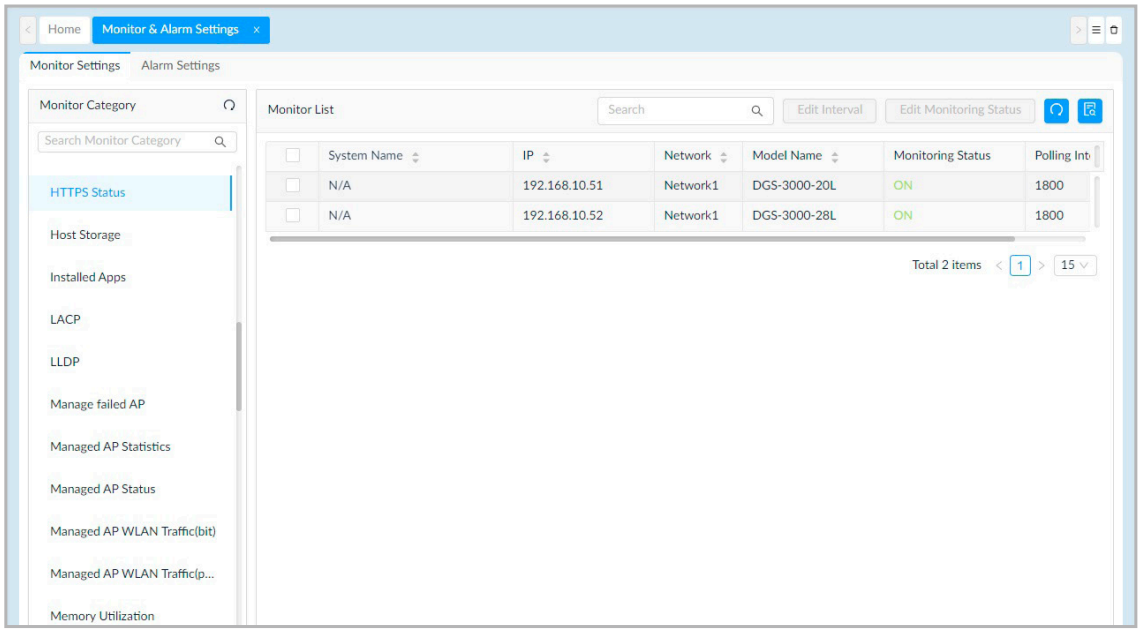


図 5-17　監視設定

3. 設定するデバイスのチェックボックスにチェックを入れて、「Edit Interval」および「Edit Monitoring Status」ボタンから設定を行います。

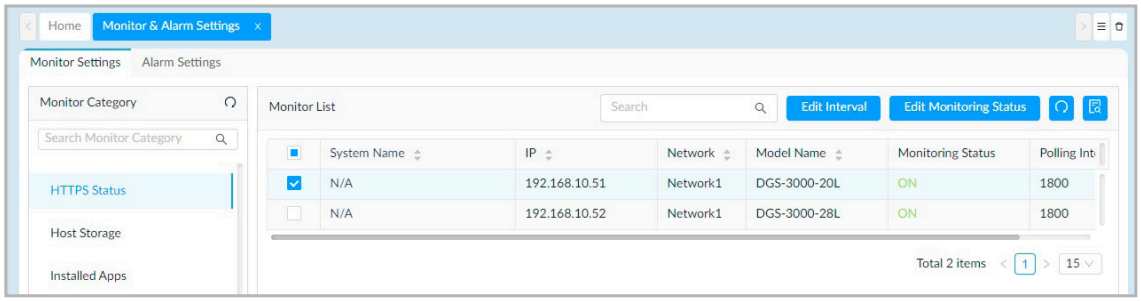


図 5-18　監視設定

各デバイスのデバイス情報画面から、監視機能を有効または無効にすることもできます。

(1) **Monitoring > Device View** に移動します。

(2) 対象デバイスのシステム名のリンクをクリックして、デバイス情報画面を表示します。

(3) 「Monitor」タブを選択して「Monitoring Settings」をクリックし、各項目を設定します。（P.104 の「デバイス情報の変更」参照）。

アラームルールの作成

アラームルールを設定すると、定義したアラームの生成条件に応じてアラームを生成し、通知アイコンとして表示することができます。通知アイコンについては、P.89 の「通知アイコン」を参照してください。

1. **Alarm & Notification > Monitor & Alarm Settings** に移動し、「Alarm Settings」タブを開きます。
2. 左側の一覧から、監視条件を選択します。

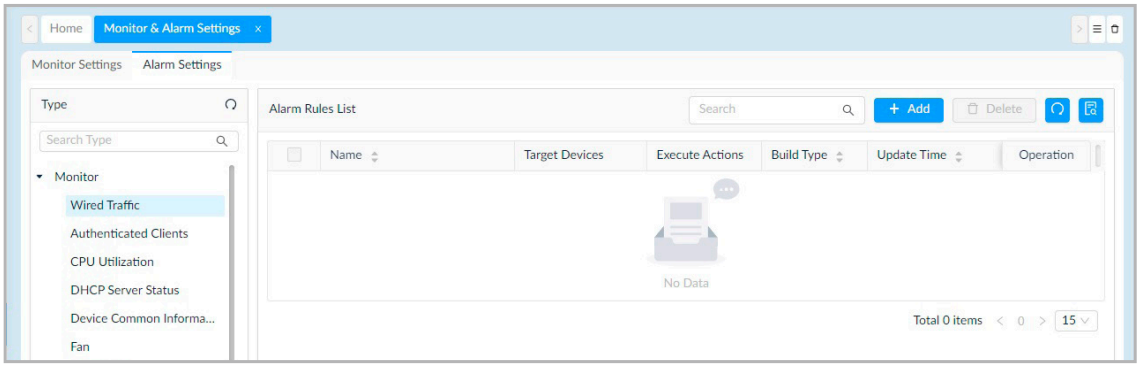


図 5-19　アラーム設定

3. 「+ Add」をクリックして、ルールを設定します。
   ルールによって、必要な設定は異なります。ただし、次の共通設定はすべてのアラームルールタイプで表示されます。

設定項目：

項目	説明
Set Profile Information	
Basic Information	アラームルールの名前と説明を入力します。
Rule Information	• 「Generation Conditions」:アラームの各重大度（「Info」「Warning」「Critical」）に対し、しきい値を設定します。 • 「Release Conditions」：アラーム解除のしきい値を設定します。
Inhibition Schedule Settings	指定されたスケジュールの期間、アラームの配信が停止します。 定義済みのスケジュールを選択するか、「Add Schedule」をクリックして新しいスケジュールを追加します。
Set Target Devices (Optional)	
Select Target Devices	「+ Add」をクリックして、設定するデバイスを追加します。
Set Actions (Optional)	
Set Actions	「+ Add Action」をクリックし、選択したデバイスに対して実行するスクリプトを設定します。 このスクリプトは、アラーム送信元のほか、指定デバイスまたは D-View8 サーバで実行できます。「Device Command」または「Server Command」タブをクリックし、対象のデバイスで実行するスクリプトを設定します。 デバイスでコマンドを実行するために、デバイスにログインするための資格情報とプロトコルを設定します。

4. 「>> Next」または「OK」をクリックして、次の画面に進みます。
5. 「Save」をクリックしてルールを作成します。

第 6 章　デバイス構成とファームウェア / コンフィグレーションの管理

D-View8 では、デバイス構成の保存と復元が簡単に行えます。また、スケジュールによるファームウェアのアップグレードや設定の変更も可能です。

本章では、以下のトピックについて説明します。

- 「タスクとプロファイルの作成」
- 「タスクの管理」
- 「デバイスのファームウェアアップグレード」
- 「コンフィグレーションファイルのバックアップとリストア」
- 「ネットワークファイル管理」

注意 D-View8 で利用可能な監視 / 設定項目は製品によって異なります。

※デバイス側で CLI/SNMP に対応している場合、ユーザ定義の監視 / 設定テンプレートを作成して管理に役立てることもできます。対応可否は製品や機能により異なります。

※設定機能の制限事項に関しては、弊社ホームページの製品ページから対象製品のユーザマニュアルをご確認ください。

注意 D-View8 によるファームウェア / コンフィグ管理について、以下の制限があります。

- D-View8 によるファームウェアアップグレード機能は、物理スタック構成のスイッチ、DIS-200G シリーズ、DGS-1100-05PDV2/05V2/08V2/08PV2、DAP-X2850 ではサポートされません。
- D-View8 によるコンフィグバックアップ / リストアは、DGS-1100-05PDV2/05V2/08V2/08PV2、DAP-X2810 ではサポートされません。

タスクとプロファイルの作成

ネットワーク上の検出デバイスに対し、特定の設定ジョブ（タスク）を作成できます。また、プロファイルに機能設定を追加し、定義済みプロファイルを作成した後、タスクとして実行することも可能です。

これらのバッチ設定では、「Quick Configuration（クイック設定）」タスク、または「Advanced Configuration（詳細設定）」タスクを利用できます。

- 「Quick Configuration（クイック設定）」：各機能の GUI テンプレートを利用してタスクを作成します。
- 「Advanced Configuration（詳細設定）」：特定のタイプのデバイスに対して複数の機能のパラメータを含むプロファイルを作成できます。同じタイプ / モデルに属する複数のデバイスに同一のプロファイルを適用できます。

メモ　ライセンスの期限が切れると、管理ノード数の制限（D-View8 フル機能は利用可能）についてのアラートと、追加ライセンスの適用を促すメッセージが「Batch Configuration」画面に表示されます。ライセンスの更新手順については、P.238 の「ライセンス管理」を参照してください。

設定タスク（実行ジョブ）の追加

1. **Configuration > Batch Configuration** をクリックし、「Batch Configuration」画面を表示します。

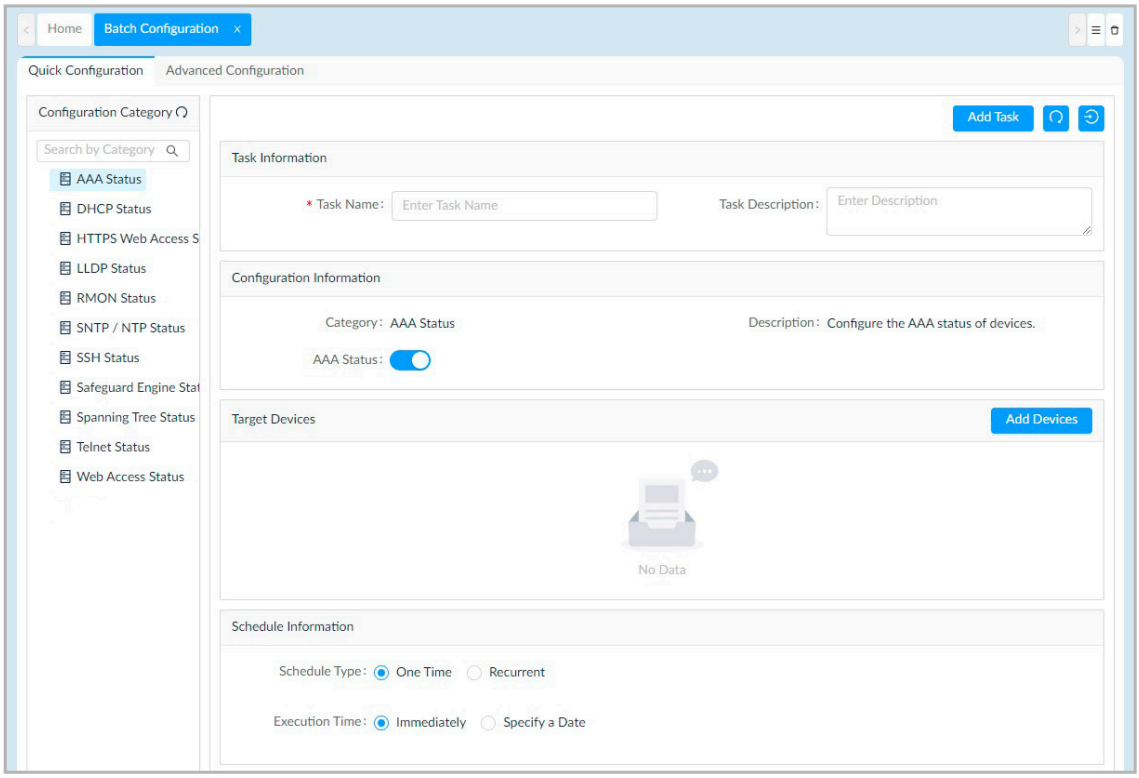


図 6-1　　バッチ設定（クイック設定タブ）

2. 「Configuration Category」の設定カテゴリ一覧からカテゴリを選択します。検索フィールドに特定のキーワードを入力して検索することもできます。

3. タスクの設定を行います。

項目	説明
Task Information（タスク情報）	
Task Name	タスクの名前を入力します。
Task Description	タスクの識別に役立つ説明を入力します。
Configuration Information（設定情報）	
Category	設定するタスクカテゴリ名が表示されます。
Status/Input	タスクの設定内容を指定します。 ユーザ定義カテゴリの場合、オプションはテンプレートのデザインと選択したプロトコルによって異なります。
Target Devices（対象デバイス）	
Add Devices	設定対象のデバイスを追加します。 この機能に対応しているデバイスのみ選択できます。 メモ　異なるネットワークに属する複数のデバイスを選択できます。セキュリティのために設定を同じネットワーク下のデバイスのみに制限するには、次のセクションで説明する設定プロファイルを使用します。

項目	説明
Schedule Information（スケジュール情報）	
Schedule Type	タスクの頻度を指定します。 • 選択肢：「One Time（1 回のみ）」「Recurrent（繰り返し）」
Execution Time	「One Time」を選択した場合、タスクの実行時間を指定します。 • 選択肢：「Immediately（今すぐ実行）」「Specify a Date（日時指定）」
Schedule	「Recurrent」を選択した場合、定義済みのスケジュールを選択するか、「Add Schedule」をクリックして新しくスケジュールを作成します。スケジュール設定の詳細は、P.236 の「スケジュール機能」を参照してください。

メモ　「Configuration Information」の設定項目は、設定の種類により利用可能なオプションが異なります。

4.　タスクの定義が完了したら、「Add Task」をクリックしてタスクを作成します。

（Refresh）アイコンをクリックして、タスクの入力フォームを再同期します。

アイコンから「Task Management」を選択すると、「Task Management」画面が開きます。

アイコンから「Configuration Template」を選択すると、「Configuration Template」画面が開きます。

タスク管理画面については、P.142 の「現在のタスク」を参照してください。

注意　D-View8 で利用可能な設定項目は製品によって異なります。

※デバイス側で CLI/SNMP に対応している場合、ユーザ定義の設定テンプレートを作成して管理に役立てることもできます。対応可否は製品や機能により異なります。

※設定機能の制限事項に関しては、弊社ホームページの製品ページから対象製品のユーザマニュアルをご確認ください。

設定プロファイルの追加

複数の設定カテゴリを含むプロファイルを設定および管理し、迅速なネットワーク展開に役立てることができます。

- クイック設定とは異なり、「Advanced Configuration」タイプのカテゴリに対応できます。
- 複数の機能カテゴリのパラメータを含めることができます。
- 定義したプロファイルはネットワーク内の複数のデバイスに対し、タスクとして適用できます。

1. **Configuration > Batch Configuration** をクリックします。
2. 「Advanced Configuration（詳細設定）」タブを選択し、「Advanced Configuration」画面を表示します。
3. 「Add Profile」をクリックします。

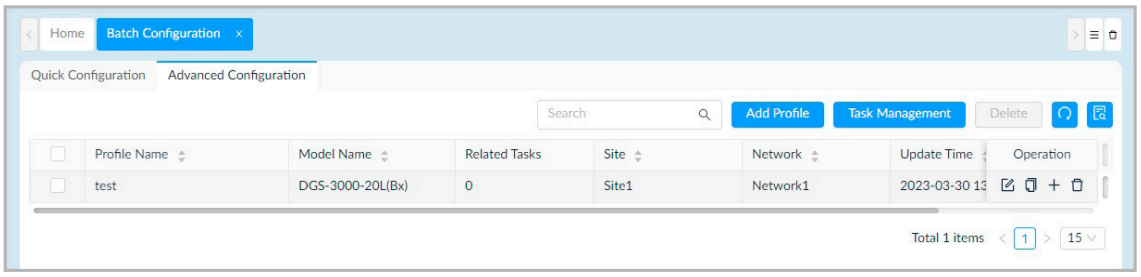


図 6-2　　バッチ設定（詳細設定タブ）

4. プロファイルを定義するための情報を入力します。

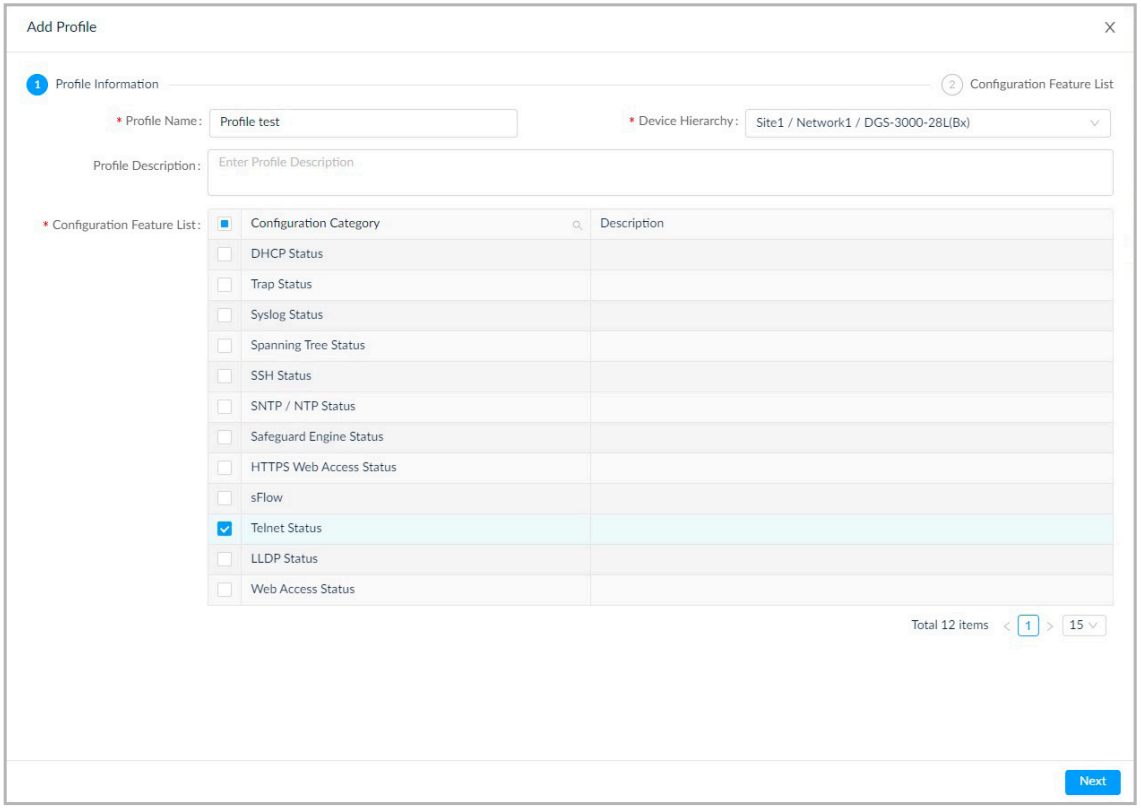


図 6-3　　プロファイルの追加

設定項目：

項目	説明
Profile Name	プロファイル名を入力します。
Device Hierarchy	ドロップダウンメニューをクリックして、設定を適用するモデル名を指定します。プロファイル作成後、プロファイルからタスクを作成する際に対象モデルのデバイスを指定することができます。詳細は、P.141 の「デバイスへのプロファイルの適用（タスクの作成）」を参照してください。
Profile Description	プロファイルを識別するための説明を入力します。

項目	説明
	カテゴリを選択します。 • 「AAA Status」 • 「DHCP Status」 • 「HTTPS Web Access Status」 • 「LLDP Status」 • 「RMON Status」 • 「SNTP / NTP Status」 • 「SSH Status」 • 「Trap Status」 • 「Syslog Status」 • 「Safeguard Engine Status」 • 「Spanning Tree Status」 • 「Telnet Status」 • 「Web Access Status」 メモ　設定カテゴリのリストは、デバイスの種類により異なります。ここでは「Quick Configuration」タイプのほか、「Advanced Configuration」タイプのカテゴリを選択することができます。ユーザ定義の設定テンプレートを利用する場合、事前に設定テンプレートをデバイステンプレートに関連付ける必要があります（**Templates > Device Template**）。

5. 「Next」をクリックして続行し、選択したカテゴリ機能のパラメータを設定します。
6. 各カテゴリの設定が完了したら、「Save」をクリックして保存します。前の画面に戻るには、「Previous」をクリックします。

注意　D-View8 で利用可能な設定項目は製品によって異なります。

※デバイス側で CLI/SNMP に対応している場合、ユーザ定義の設定テンプレートを作成して管理に役立てることもできます。対応可否は製品や機能により異なります。

※設定機能の制限事項に関しては、弊社ホームページの製品ページから対象製品のユーザマニュアルをご確認ください。

設定プロファイルの変更と削除

1. **Configuration > Batch Configuration** をクリックします。
2. 「Advanced Configuration」タブを選択します。定義済みの設定プロファイルが表示されます。

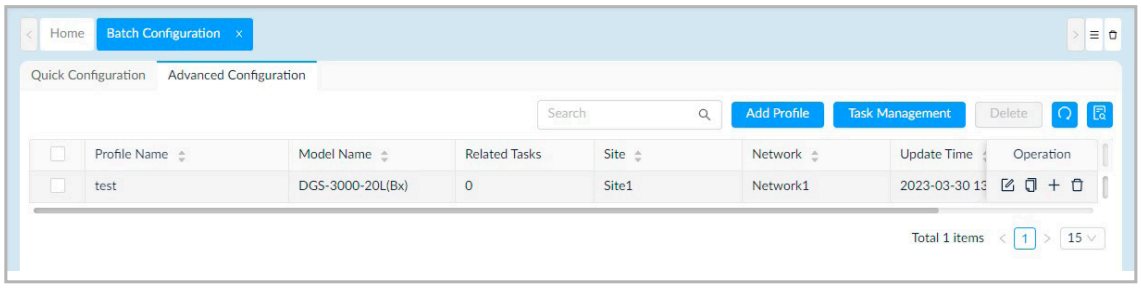


図 6-4　　バッチ設定（詳細設定タブ）

3. 「Operation（操作）」列のアイコンをクリックして、次のアクションを実行します。

項目	説明
Edit	（Edit）アイコンをクリックして、設定プロファイルの内容を変更します。
Share	（Share）アイコンをクリックして、プロファイルをコピーし、他のネットワーク上の同種のデバイスを設定します。
Create Task	＋（Create Task）アイコンをクリックして、プロファイルのタスクを作成し、スケジュールに従って指定デバイスに設定を実行します。詳細な手順については、次のセクションを参照してください。
Delete	（Delete）アイコンをクリックして、プロファイルを削除します。

デバイスへのプロファイルの適用（タスクの作成）

1. **Configuration > Batch Configuration** をクリックします。
2. 「Advanced Configuration」タブを選択します。
3. 「Operation」列の ＋ （Create Task）アイコンをクリックして、タスクを作成します。

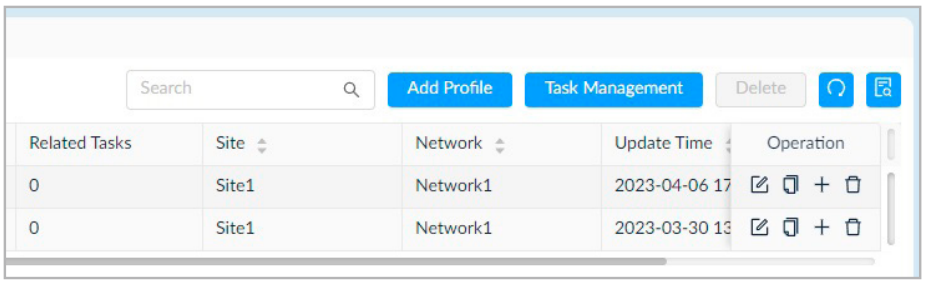


図 6-5　　バッチ設定（詳細設定タブ）

4. 「Task Settings」画面で、タスクの設定を行います。

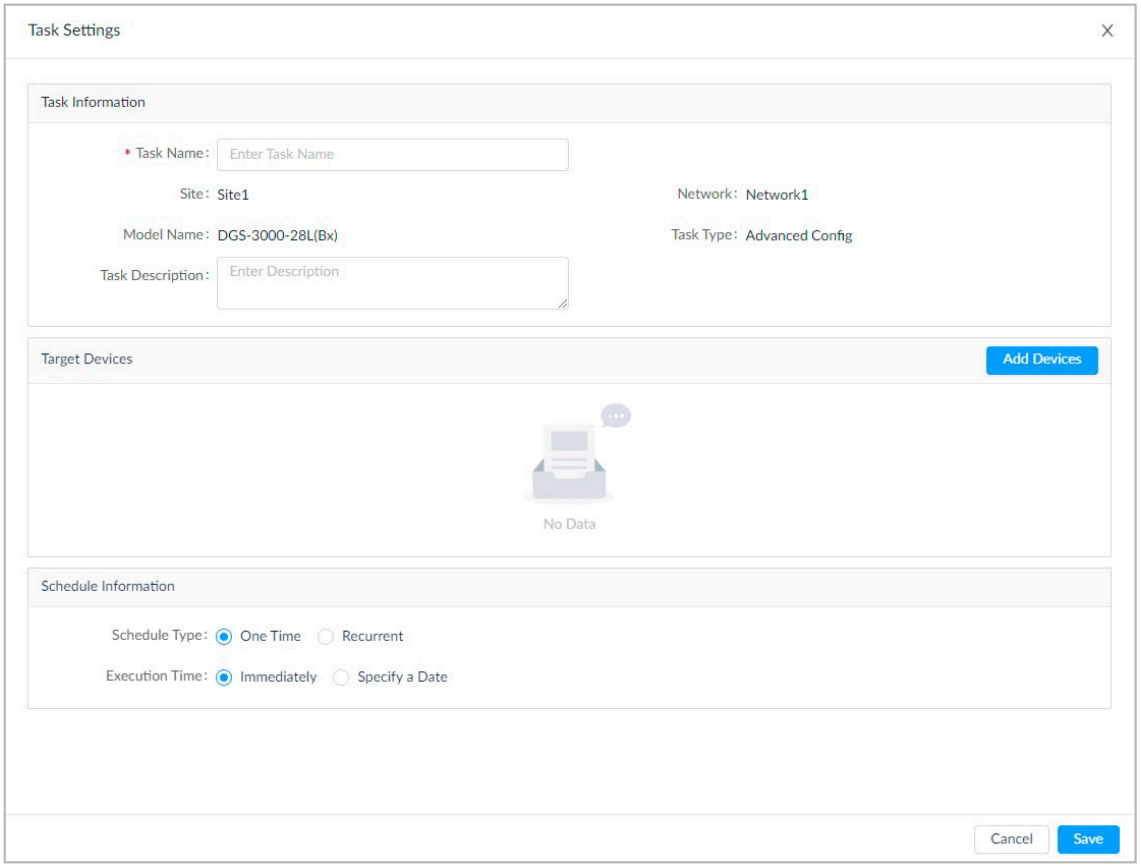


図 6-6　　タスクプロファイルの作成

設定項目：

項目	説明
Task Information（タスク情報）	
Task Name	タスクの名前を入力します。
Task Description	タスクの識別に役立つ説明を入力します。
Target Devices（対象デバイス）	
Add Devices	設定対象のデバイスを追加します。対象のデバイスを選択するか、検索機能を使用してデバイスを検索します。 メモ　指定ネットワーク配下の同じモデルのデバイスのみ選択できます。他のネットワークに設定プロファイルを適用するには、「Operation」列の「Share」機能を使用します。 メモ　あらかじめ複数のネットワークにまたがるデバイスグループをデバイスグループ化し、「Device Group」タブから目的のグループを選択することもできます。（P.110 の「デバイスグループの管理」参照）

項目	説明
Schedule Information（スケジュール情報）	
Schedule Type	タスクの頻度を指定します。 • 選択肢：「One Time（1 回のみ）」「Recurrent（繰り返し）」
Execution Time	「One Time」を選択した場合、タスクの実行時間を指定します。 • 選択肢：「Immediately（今すぐ実行）」「Specify a Date（日時指定）」
Schedule	「Recurrent」を選択した場合、定義済みのスケジュールを選択するか、「Add Schedule」をクリックして新しくスケジュールを作成します。スケジュール設定の詳細は、P.236 の「スケジュール機能」を参照してください。

5. 「Save」をクリックして、新しいタスクを作成します。

タスク管理画面を開くには、「Task Management」をクリックします。詳細は P.142 の「現在のタスク」を参照してください。

タスクの管理

Task Management（タスク管理）機能では、現在および実行済みのタスクを管理できます。本アプリケーションで開始されたタスクは、編集、削除、再実行、および実行履歴の表示が可能です。

現在のタスク

1. **Configuration > Task Management** をクリックします。
2. デフォルトでは、「Current Task（現在のタスク）」タブが表示されます。

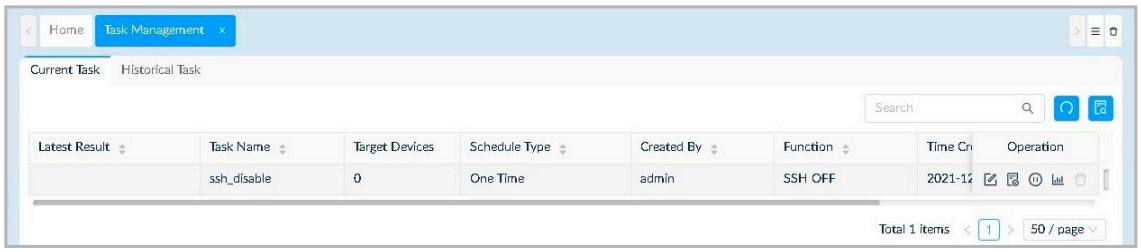


図 6-7　　タスク一覧（現在のタスク）

以下の項目を表示、また、タスクに対し操作を実行することができます。

項目	説明
Latest Result	タスクの実行ステータスを表示します。
Task Name	タスクの名前を表示します。
Target Devices	タスクが割り当てられているデバイスの数を表示します。
Scheduled Type	スケジュールの種類を表示します。（「One Time」または「Recurrent」）
Created By	タスク作成者の名前を表示します。
Function	タスクで実行する機能を表示します。
Time Created	タスクの作成日時を表示します。
Next Execution Time	タスクが次に実行される開始時間を表示します。
Operation（操作）	
Edit Configuration	（Edit Configuration）アイコンをクリックして、タスクの設定パラメータを編集します。設定プロファイルの場合、プロファイルの内容を編集します。
Edit Task	（Edit Task）アイコンをクリックして、タスク情報、対象デバイス、スケジュールを変更します。
Pause Task	（Pause Task）アイコンをクリックして、タスクを非アクティブ化（一時停止）します。
Restart Task	（Restart Task）アイコンをクリックして、一時停止したタスクを再度アクティブ化します。
Show Task Record	（Show Task Record）クリックすると、タスクの操作 / 実行などのイベントが時系列で表示されます。
Delete Task	（Delete Task）アイコンをクリックして、タスクを削除します。タスクを削除するには、タスクを停止する必要があります。

実行済みタスク

1. **Configuration > Task Management** をクリックします。デフォルトでは、「Current Task（現在のタスク）」タブが表示されます。
2. 「Historical Task（実行済みタスク）」タブをクリックして、実行済みタスクの一覧を表示します。

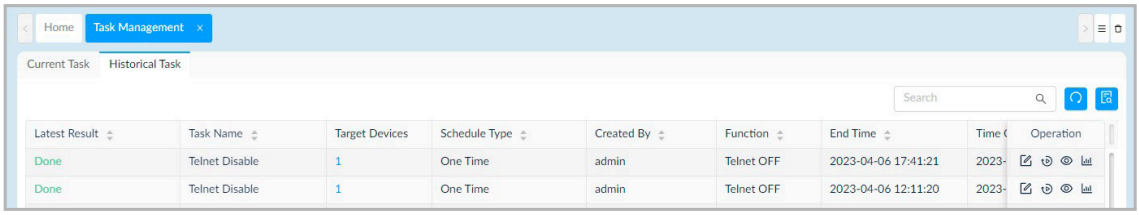


図 6-8　　タスク一覧（実行済みタスク）

以下の項目を表示、また、タスクに対し操作を実行することができます。

項目	説明
Latest Result	タスクの実行ステータスを表示します。結果の詳細画面を開くには、リンクをクリックします。
Task Name	タスクの名前を表示します。
Target Devices	タスクが割り当てられているデバイスの数を表示します。
Scheduled Type	スケジュールの種類を表示します。（「One Time」または「Recurrent」）
Created By	タスク作成者の名前を表示します。
Function	タスクで実行する機能または設定プロファイルを表示します。
End Time	タスクの終了日時を表示します。
Time Created	タスクの作成日時を表示します。
Operation（操作）	
Edit Configuration	（Edit Configuration）アイコンクリックして、タスクの設定パラメータを編集します。設定プロファイルの場合、プロファイルの内容を編集します。
Re-execute Task	（Re-execute Task）アイコンをクリックして、再実行するタスクの内容を設定します。再スケジュールされたタスクは「Current Task」に表示されます。
Review Task	（Review Task）をクリックして、タスク名や種類、ターゲットデバイス、スケジュールなどのタスクの詳細を表示します。
Show Task Record	（Show Task Record）クリックすると、タスクの操作 / 実行などのイベントが時系列で表示されます。

デバイスのファームウェアアップグレード

ファームウェアアップグレードタスクを使用し、ファームウェアのアップグレードを実行、またはアップグレードのスケジュールを設定します。ファームウェアファイルは、ファイル管理機能で事前にアップロードしておくことも可能です（**Configuration > File Management**）。

メモ　ライセンスの期限が切れると、管理ノード数の制限（D-View8 フル機能は利用可能）についてのアラートと、追加ライセンスの適用を促すメッセージが「Firmware Management」画面に表示されます。ライセンスの更新手順については、P.238 の「ライセンス管理」を参照してください。

注意　D-View8 によるファームウェアアップグレード機能は、物理スタック構成のスイッチ、DIS-200G シリーズ、DGS-1100-05PDV2/05V2/08V2/08PV2、DAP-X2850 ではサポートされません。

ファームウェアアップグレードタスクの実行またはスケジュール

1. **Configuration > Firmware Management** をクリックし、「Firmware Management」画面を表示します。

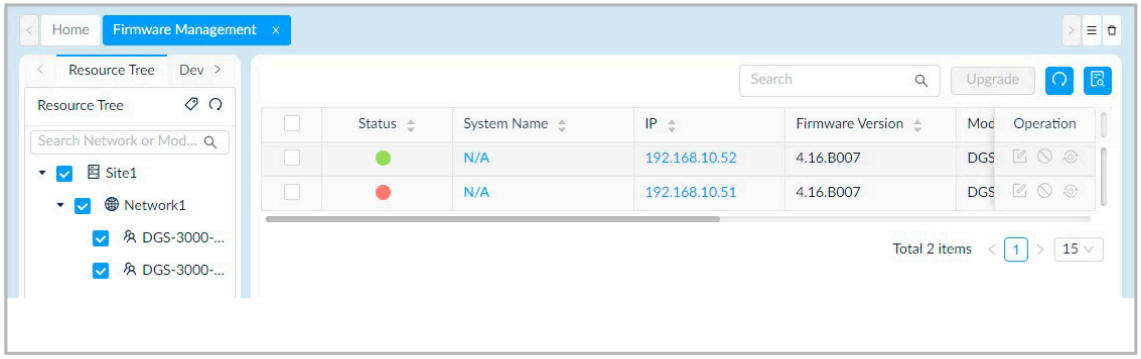


図 6-9　ファームウェア管理

以下の項目を表示、また、デバイスに対し操作を実行することができます。

項目	説明
Status	デバイスのオンライン / オフライン状態を表示します。
System Name	デバイスのシステム名を表示します。
IP	デバイスの IP アドレスを表示します。
Firmware Version	デバイスのファームウェアバージョンを表示します。
Model Name	デバイスのモデル名を表示します。
Upgrade Result	ファームウェアアップグレードの実行結果、またはスケジュールされたファームウェアアップグレードのステータスを表示します。
Site/Network	デバイスが属するサイトとネットワークを表示します。
Operation（操作）	
Edit	（Edit）アイコンクリックして、ファームウェアのアップグレードタスクを変更します。スケジュールされたタスクを編集することができます。
Stop	（Stop）アイコンをクリックして、アップグレードタスクを停止します。
Reboot Device	（Reboot Device）アイコンをクリックして、ファームウェアアップグレード後にデバイスを再起動します。

2. 「Resource Tree」の一覧から、アップグレードタスクを適用するサイト / ネットワーク配下のデバイスを選択します。検索フィールドにキーワードを入力して、デバイスを検索することも可能です。または、「Device Group」の一覧から対象のグループを選択します。
3. 対象のデバイスにチェックを入れ、「Upgrade」をクリックします。

4. 「Firmware Upgrade」画面が表示されます。

「Firmware File」セクションで（Select Firmware File）アイコンをクリックして、利用可能なファームウェア一覧を表示します。

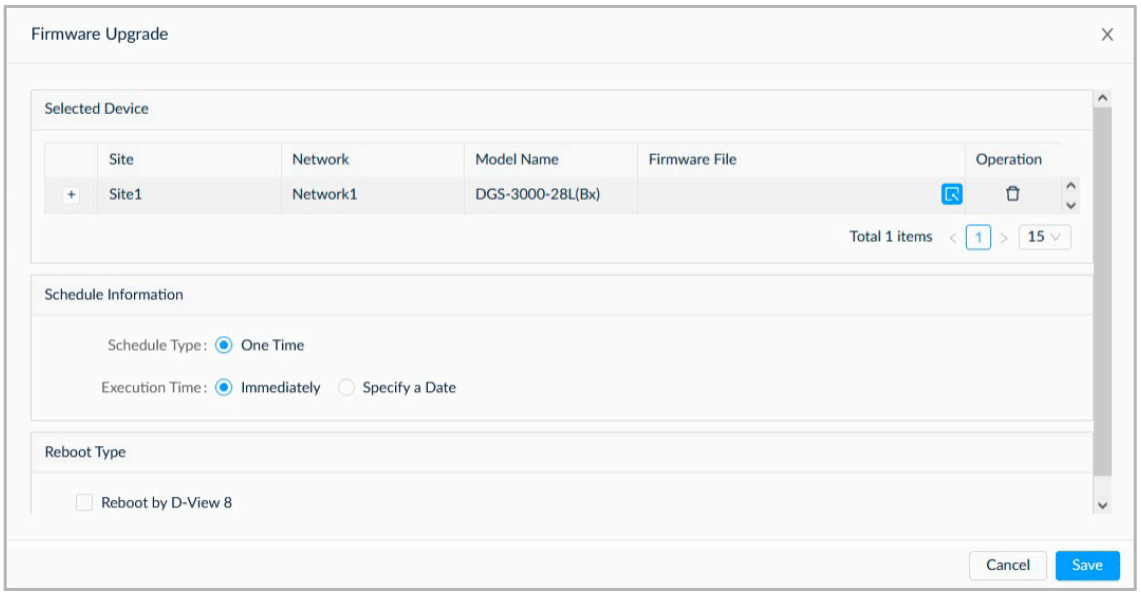


図 6-10　ファームウェアアップグレード

5. 対象のファイルを選択し、「OK」をクリックして続行します。

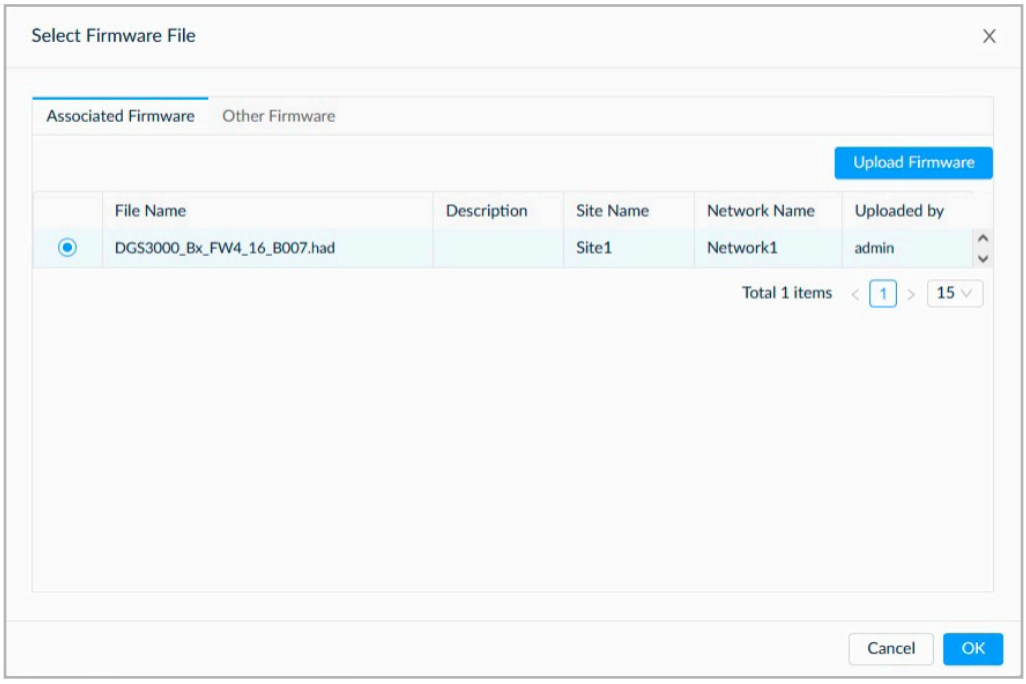


図 6-11　ファームウェアファイルの選択

メモ　ファームウェアファイルの選択画面には、以下のファイル情報が表示されます。

- 「Associated Firmware」タブ：D-View8 システムにアップロードされた、デバイスに紐づくファームウェアファイル一覧が表示されます。
- 「Other Firmware」タブ：D-View8 システムにアップロードされた、デバイスに紐づかないファームウェアファイル一覧が表示されます。

メモ　D-View8 サーバにアップロードされたファームウェアファイルについては、**Configuration > File Management** を確認してください。

6. 以下の設定を行います。

設定項目：

項目	説明
Selected Device（選択されたデバイス）	
Selected Device	選択されたデバイスを表示します。（Delete）アイコンをクリックして、選択したデバイスを削除できます。
Schedule Information（スケジュール情報）	
Schedule Type	ファームウェアアップグレードは、1 回のみのタスクとして指定します。 • 選択肢：「One Time（1 回のみ）」
Execution Time	タスクの実行時間を指定します。 • 選択肢：「Immediately（今すぐ実行）」「Specify a Date（日時指定）」
Reboot Type（再起動タイプ）	
Reboot by D-View 8	本オプションを有効にすると、ファームウェアのアップグレード後にデバイスの再起動を実行します。通常、新しいファームウェアを有効にするには再起動が必要です。 • 初期値：無効

7. 「Save」をクリックして、アップグレードタスクを作成します。設定をキャンセルするには、「Cancel」をクリックします。

注意 ファームウェアのアップグレードを実行する際は、リリースノートに記載されている注意事項などをよく読み、対象のスイッチのモデルやファームウェアバージョン / ハードウェアバージョンが、適用予定のファームウェアをサポートしていることを確認してください。ファームウェアを間違えると、デバイスが損傷する可能性があります。

注意 デバイスの再起動に関して、以下の点にご注意ください。

- 再起動オプションを有効化せずにアップグレードタスクを実行した場合、タスクが「Upgrading: Waiting for reboot manually」ステータスになった後、5 分程度待機してから再起動を実施する必要があります。（ファームウェアファイルのフラッシュへの書き込みに数分程度要します。）
- DXS-1210/B1 シリーズでは、ファームウェアアップグレードの結果が一時的に「Time Out」と表示され、その後「Upgrading: Waiting to reboot manually」に移行します。
- 手動で再起動を実施する場合、本ファームウェア管理画面の「Operation」欄の「Reboot Device」をクリックしてデバイスを再起動してください。

「Upgrade Result」列にファームウェアアップグレードタスクの結果が表示されます。

コンフィグレーションファイルのバックアップとリストア

D-View8 では、デバイスの設定ファイルのメンテナンスなどを目的としてバックアップ機能を使用することができます。

コンフィグレーションファイルのバックアップ

定期的なシステムバックアップは、バックアッププロファイルを使用して自動的に実行できます。

メモ　ライセンスの期限が切れると、管理ノード数の制限（D-View8 フル機能は利用可能）についてのアラートと、追加ライセンスの適用を促すメッセージが「Configuration Management」画面に表示されます。ライセンスの更新手順については、P.224 の「REST API キーの生成」を参照してください。

注意　D-View8 によるバックアップ / リストア機能は、DGS-1100-05PDV2/05V2/08V2/08PV2、DAP-X2810 ではサポートされません。

バックアップタスクの作成

1. **Configuration > Configuration Management** をクリックします。デフォルトでは、「Backup（バックアップ）」タブが表示されます。

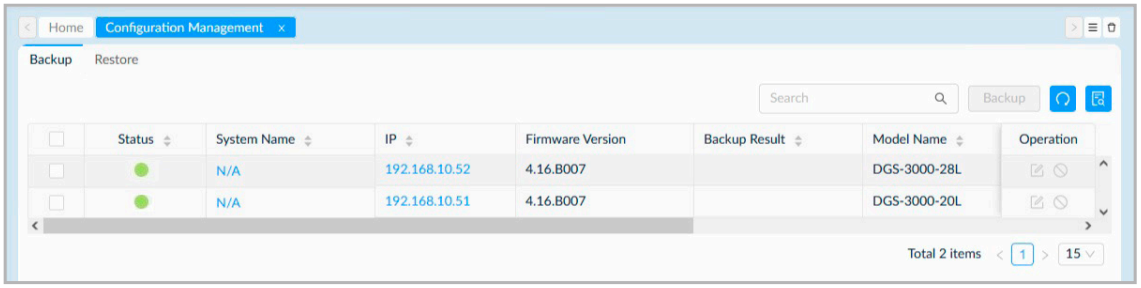


図 6-12　バックアップタスク

以下の項目を表示、また、デバイスに対し操作を実行することができます。

項目	説明
Status	デバイスのオンライン / オフライン状態を表示します。
System Name	デバイスのシステム名を表示します。
IP	デバイスの IP アドレスを表示します。
Firmware Version	デバイスのファームウェアバージョンを表示します。
Backup Result	バックアップの実行結果、またはスケジュールされたバックアップのステータスを表示します。
Model Name	デバイスのモデル名を表示します。
Site/Network	デバイスが属するサイトとネットワークを表示します。
Device Category	デバイスカテゴリを表示します。
Operation（操作）	
Edit	（Edit）アイコンクリックして、バックアップタスクを変更します。スケジュールされたタスクを編集することができます。
Stop	（Stop）アイコンをクリックして、バックアップタスクを停止します。

2. 設定をバックアップするデバイスを選択し、「Backup」をクリックしてタスクを設定します。

3. 「Backup」画面が表示されます。

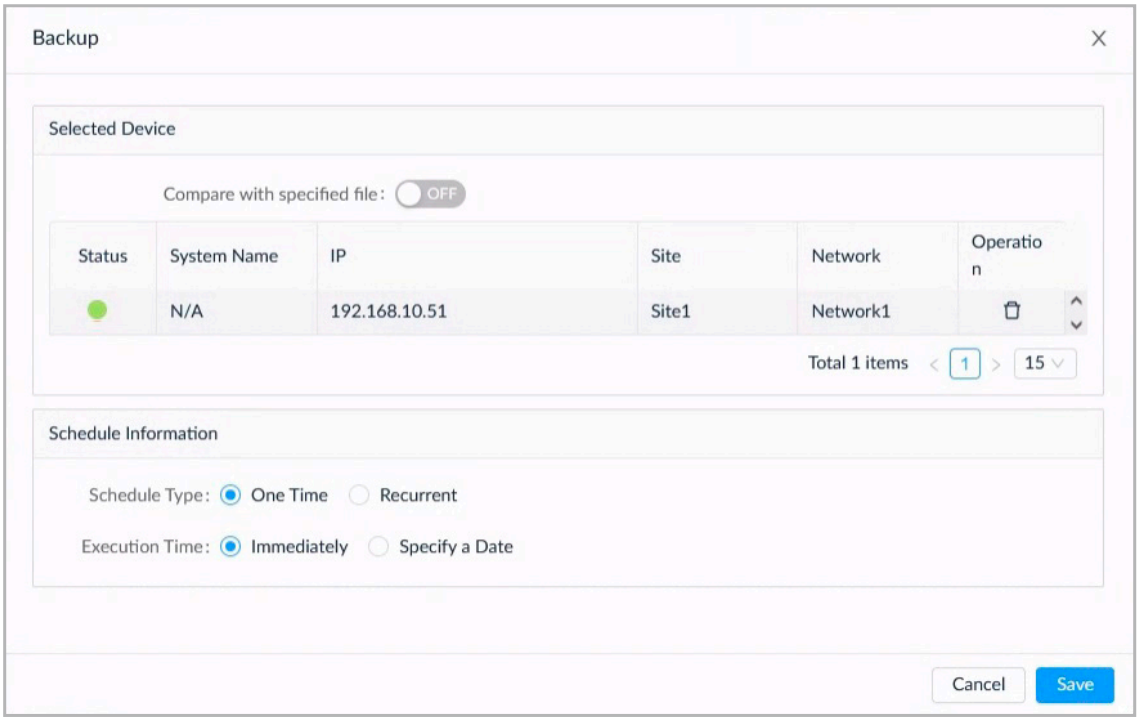


図 6-13　バックアップ設定

既存のコンフィグレーションファイル、または新しいコンフィグレーションファイルをアップロードしてデバイスの設定を比較し、ベースライン（基準の設定ファイル）と既存の設定が異なる場合にアラームが生成されるように設定することもできます。

構成設定の比較とアラーム設定：

(1) 「Compare with specified file」を ON にして、比較機能を有効にします。

(2) 「Actions when different」の「Generate Alarm」項目で、アラームのしきい値（「Critical（重大）」、「Warning（警告）」、または「Info（情報）」）を選択します。

(3) 「Restore Configuration」を「ON」にすると、デバイスの現在のコンフィグレーションファイルと基準の設定ファイルとの間に差異がある場合、基準の設定ファイルの構成にリストアします。比較およびリストア用に、基準の設定ファイルを選択する必要があります。

(4) 対象デバイスの「File」欄でドロップダウンメニューをクリックし、「Upload File」をクリックして、比較用の設定ファイルをアップロードします。

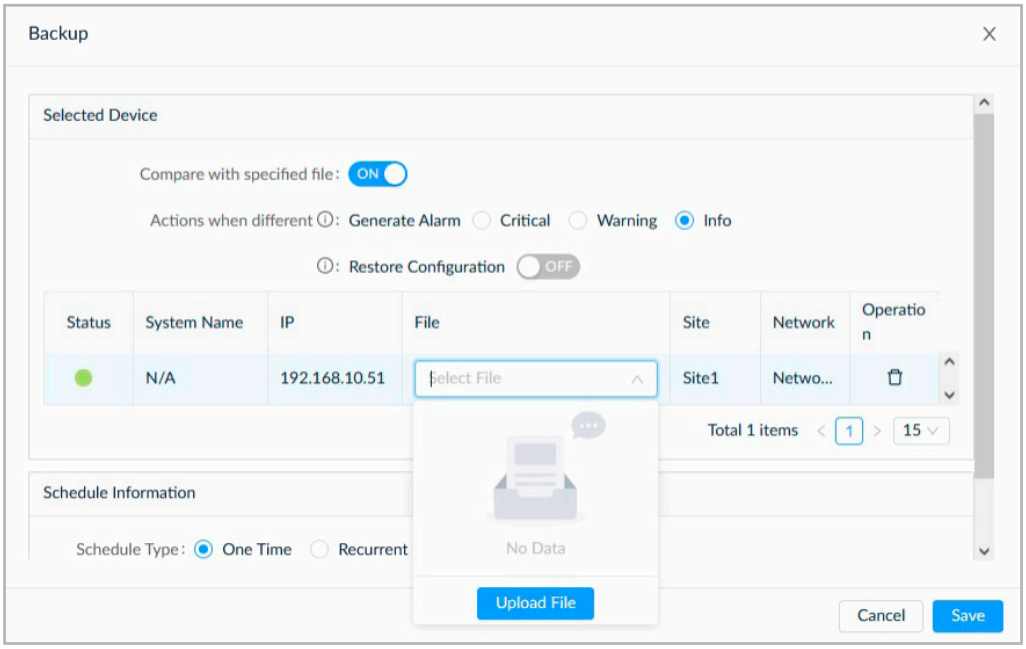


図 6-14　設定ファイルのアップロード

(5) 「Upload File」画面が表示されます。

(6) 「Select File」をクリックして、比較用のコンフィグレーションファイルを指定します。

(7) 「Set as Baseline」にチェックを入れて、この設定ファイルをベースライン（基準の設定ファイル）として定義します。ベースライン設定は、他のファイルとの識別性や追跡のために利用することできます。

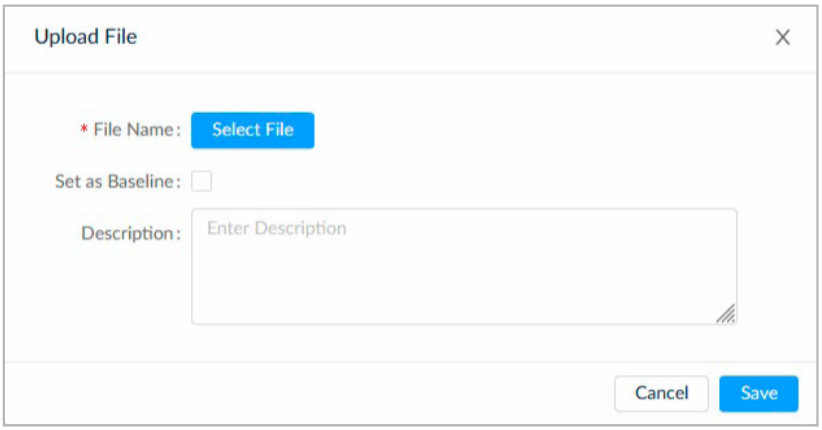


図 6-15　ファイルのアップロード

(8) 「Save」をクリックして、設定を保存します。設定をキャンセルするには、「Cancel」をクリックします。

メモ　アップロードされたコンフィグレーションファイルは「File Management」画面で確認したり、設定の復元に利用したりすることができます。

注意　DGS-1210/Fx をご利用の場合、設定内容の更新を反映するには、デバイス詳細画面で「Save to Device」ボタンをクリックして既定のコンフィグに設定を保存してから、バックアップ / リストアを実行する必要があります。

4. 「Schedule」セクションで、スケジュールを設定します。
   - 「Schedule Type」:「One Time（1 回）」または「Recurrent（繰り返し）」
     - 「Execution Time」:「One Time」を指定した場合は、「Immediately（即時）」または「Specify a Date（日付の指定）」を指定します。
     - 「Schedule」:「Recurrent」を指定した場合はスケジュールを指定します。定義済みのスケジュールを選択するか、「Add Schedule」をクリックして新しいスケジュールを追加します。スケジュール設定の詳細は、P.236 の「スケジュール機能」を参照してください。

5. 「Save」をクリックして、バックアップタスクを保存します。設定をキャンセルするには、「Cancel」をクリックします。
   タスクが作成され、「Backup Result」列にバックアップタスクの実行状況が表示されます。

タスクの編集または停止

1. **Configuration > Configuration Management** をクリックします。

2. デフォルトでは、「Backup（バックアップ）」タブが表示されます。

3. 「Operation 」列の （Edit/ 編集）または （Stop/ 停止）アイコンをクリックします。

図 6-16　バックアップタスク

コンフィグレーションファイルのリストア

デバイス設定は、基準の設定ファイルが割り当てられた定義済みのバックアップタスクにより復元できます。

注意 D-View8 によるバックアップ / リストア機能は、DGS-1100-05PDV2/05V2/08V2/08PV2、DAP-X2810 ではサポートされません。

注意 DGS-1210/Fx をご利用の場合、設定内容の更新を反映するには、デバイス詳細画面で「Save to Device」ボタンをクリックして既定のコンフィグに設定を保存してから、バックアップ / リストアを実行する必要があります。

リストアタスクの作成

1. **Configuration > Configuration Management** をクリックします。
2. デフォルトでは、「Backup（バックアップ）」タブが表示されます。「Restore」タブをクリックします。

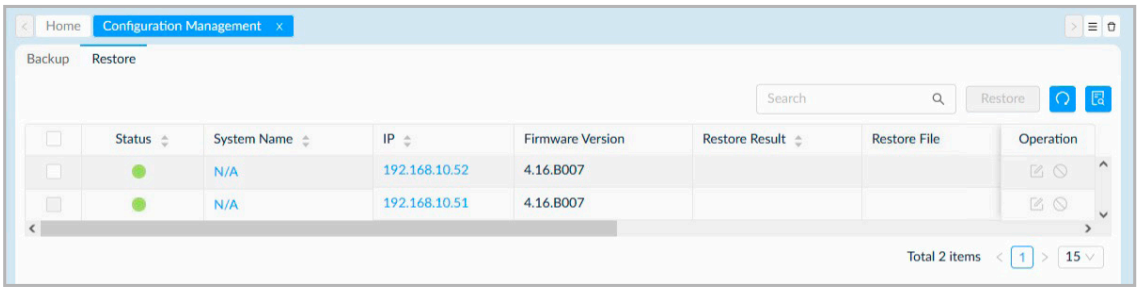


図 6-17　デバイス構成のリストア

メモ リストアファイルを変更するには、「Restore File」列の（Select）アイコンをクリックし、設定ファイルを選択します。

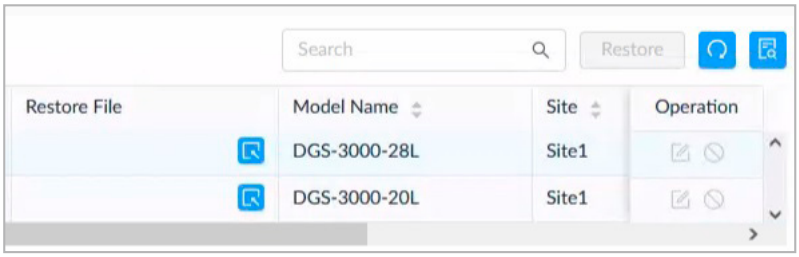


図 6-18　リストアファイル

「Select Restoration File」画面では、ベースラインファイルを簡単に管理することができます。また、次のアクションを実行できます。

- ファイルのアップロード
- ダウンロード
- ベースラインとして設定 / ベースラインから解除
- ファイル内容の表示

3. 定義済みのベースラインファイルまたはバックアップファイルを持つデバイスを選択し、「Restore」をクリックしてタスクを設定します。
4. 「Restore」画面の「Schedule」セクションで、スケジュールを設定します。
   - 「Schedule Type」:「One Time（1 回）」または「Recurrent（繰り返し）」
     - 「Execution Time」:「One Time」を指定した場合は、「Immediately（即時）」または「Specify a Date（日付の指定）」を指定します。
     - 「Schedule」:「Recurrent」を指定した場合はスケジュールを指定します。定義済みのスケジュールを選択するか、「Add Schedule」をクリックして新しいスケジュールを追加します。スケジュール設定の詳細は、P.236 の「スケジュール機能」を参照してください。
5. 「Save」をクリックしてリストアタスクを保存します。設定をキャンセルするには、「Cancel」をクリックします。

タスク作成後、「Restore Result」列に実行ステータスが表示されます。

注意 D-View8 を使用して DAP シリーズ、DGS-1210 シリーズ、DXS-1210/B1 シリーズのコンフィグレーションをリストアする場合、リストアタスクが「Done」ステータスになった後、ユーザが手動でデバイスを再起動する必要があります。

タスクの編集または停止

1. **Configuration > Configuration Management** をクリックします。
2. 「Restore」タブをクリックします。
3. 「Operation 」列の （Edit/ 編集）または （Stop/ 停止）アイコンをクリックします。

図 6-19　リストアタスク

ネットワークファイル管理

ファイル管理機能を使用して、様々なデバイスのファームウェアとコンフィグレーションファイルを管理できます。この機能により、ファイルのアップロード、削除、ファイル比較、ファイルの整理、検索が可能になります。ファームウェアやコンフィグレーションのベースライン機能を使用することで、メンテンナンスの能率化や、ネットワーク間の一貫性の維持に役立てることができます。

ファイル管理のメニュー項目

ファイルの表示と管理メニュー

1. **Configuration > File Management** をクリックし、「File Management」画面を表示します。

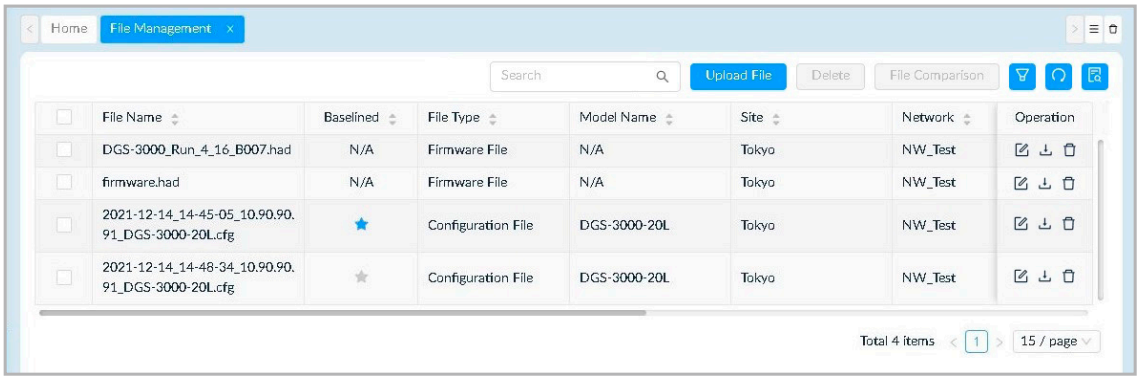


図 6-20　ファイル管理

ファイル管理画面では、以下の機能を使用することができます。

項目	説明
ツールバー	
Search	キーワード（ファイル名 / サイト / ネットワーク）を入力して、ファイルを検索します。
Upload File	ファイルをアップロードします。
Delete	ファイルエントリを選択し、「Delete」をクリックして削除します。
File Comparison	比較する 2 つの設定ファイルを選択し、「File Comparison」をクリックします。どちらのファイルもテキストベースである必要があります。ファイル比較画面は、**Tools > File Comparison** から開くこともできます。

項目	説明
Column Selector	（Column Selector）アイコンをクリックして、本画面に列を追加または削除します。 • 「Default（デフォルト表示項目）：「File Name」「Baselined」「File Type」「Model Name」「Site」「Network」「File Size」「Related Devices」「Status」「Upload Time」「Description」 • 「Other（その他表示項目）：「Uploaded by」「MD5」 すべての列オプションを有効にするには、「All」を選択します。 「Apply」をクリックして、選択した項目を適用します。
Refresh	（Refresh）アイコンをクリックして、一覧を再同期します。
Advanced Query	（Advanced Query）アイコンをクリックして、高度な検索を開始します。
Operation（操作）	
Edit	（Edit）アイコンをクリックして、ファイルの情報を編集します。
Download	（Download）アイコンクリックして、ファイルをローカルシステムにエクスポートします。
Delete File	（Delete File）アイコンをクリックしてファイルを削除します。

ファイルのアップロード

1. **Configuration > File Management** をクリックし、「File Management」画面を表示します。
2. 「Upload File」をクリックして、「Upload File」画面を表示します。

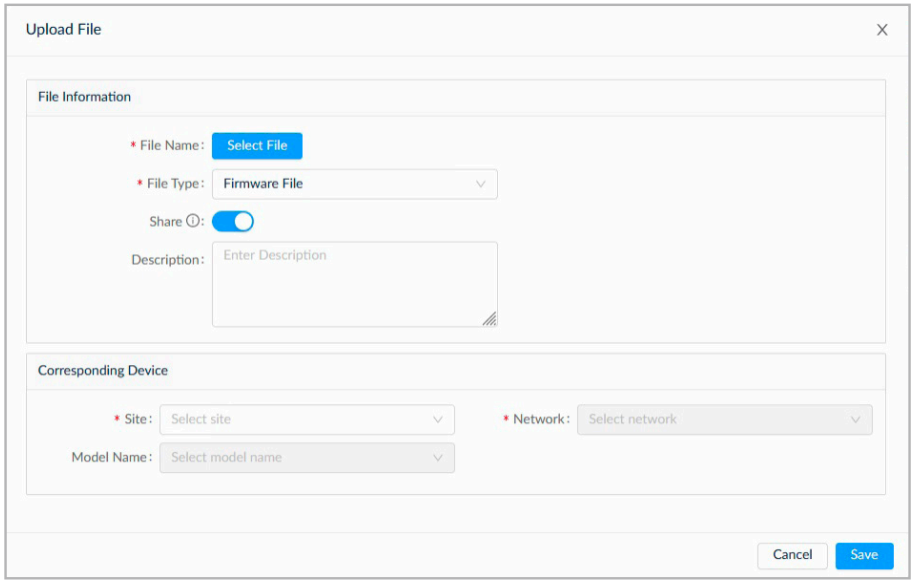


図 6-21　ファイルのアップロード

3. 以下の項目を設定し、ファイルをアップロードします。

設定項目：

項目	説明
File Information（ファイル情報）	
File Name	「Select File」をクリックして、ファイルを指定します。
File Type	ファイルの種類を選択します。 • 選択肢：「Firmware File」「Configuration File」
Share	他のネットワークへの共有を有効または無効に設定します。 ファイルの種類で「Firmware File」が選択されている場合のみ使用可能です。
Set as Baseline	ファイルをベースラインテンプレートとして指定します。 ファイルの種類で「Configuration File」が選択されている場合のみ使用可能です。
Description	ファイルタイプの識別に役立つ短い説明を入力します。

項目	説明
Corresponding Device（対応デバイス）	
Site	サイトを選択します。
Network	サイトに紐づくネットワークを指定します。
Model Name	ファイルに対応するデバイスのモデル名を選択します。
Device	選択したモデル名に対応するデバイスを選択します。（ファイルの種類が「Configuration File」の場合）

4. 「Save」をクリックして、設定を保存します。設定をキャンセルするには、「Cancel」をクリックします。

ファームウェアファイルの管理

デバイスに最新のファームウェアバージョンを適用することにより、全体的なセキュリティと機能を向上したり、不具合を修正したりすることができます。最新のファームウェア情報は、D-Link Japan の製品サイトを確認してください。

注意　ファームウェアを更新する際は、適用予定のファームウェアファイルがそのデバイスでサポートされていることを確認してください。間違ったファームウェアを使用すると、デバイスが損傷する可能性があります。

このセクションでは、次の手順について説明します。

- ファームウェアファイルのインポート
- ファームウェアファイルの変更
- ファームウェアファイルのエクスポート
- ファームウェアファイルの削除

メモ　ファームウェアのアップグレード手順については、P.144 の「デバイスのファームウェアアップグレード」を参照してください。

注意　D-View8 によるファームウェアアップグレード機能は、物理スタック構成のスイッチ、DIS-200G シリーズ、DGS-1100-05PDV2/05V2/08V2/08PV2、DAP-X2850 ではサポートされません。

ファームウェアファイルのインポート

1. **Configuration > File Management** をクリックし、「File Management」画面を表示します。
2. 「Upload File」をクリックします。

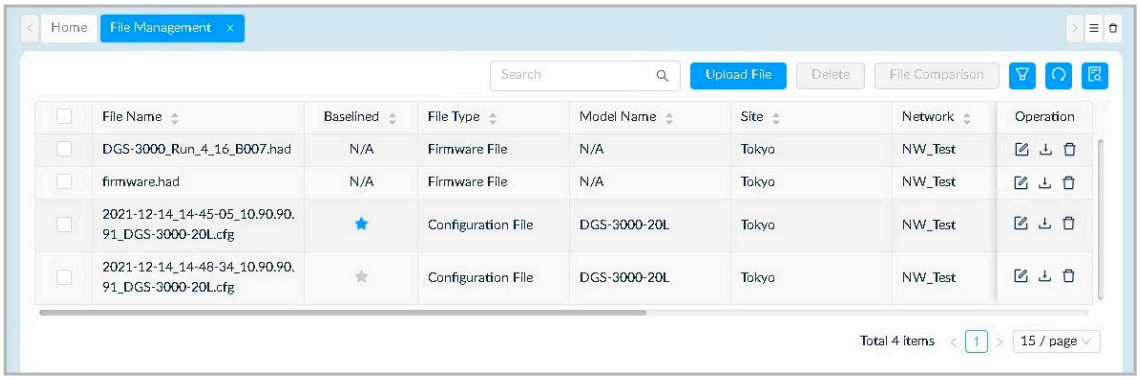


図 6-22　ファイル管理

3. 「Upload File」画面で、以下の項目を設定します。

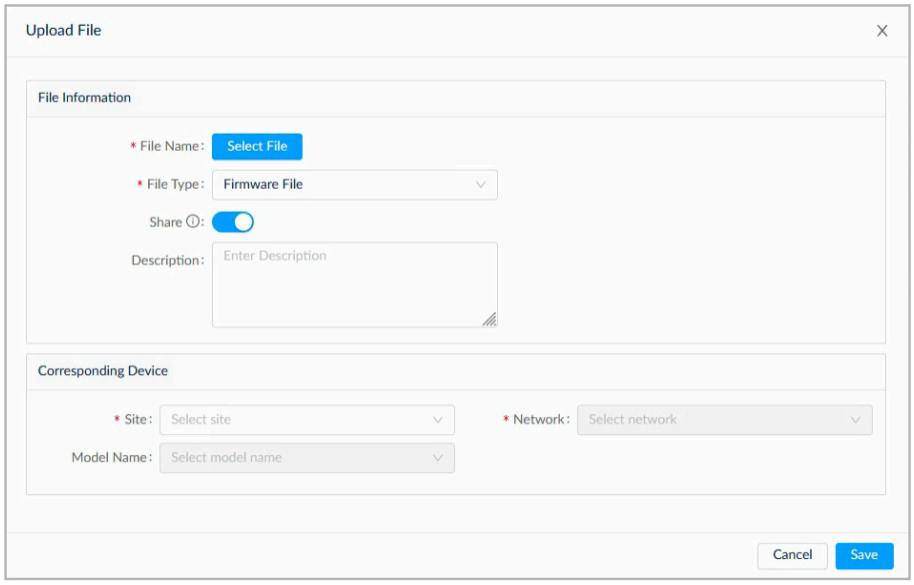


図 6-23　ファイルのアップロード（ファームウェアファイル）

設定項目：

項目	説明
File Name	「Select File」をクリックして、ファームウェアファイルを選択します。
File Type	ファイルの種類として「Firmware File」を指定します。
Share	本オプションをクリックし、ファイルの他のネットワークへの共有を有効または無効に設定します。
Description	ファイルの簡単な説明を入力します。
Site	ドロップダウンメニューをクリックして、デバイスモデルが属するサイトを選択します。
Network	ドロップダウンメニューを選択して、サイトに紐づくネットワークを選択します。
Model Name	ドロップダウンメニューをクリックして、ファームウェアに対応するモデル名を指定します。

4. 「Save」をクリックして、ファームウェアファイルのエントリを保存します。設定をキャンセルするには、「Cancel」をクリックします。

ファームウェアファイルの変更

1. **Configuration > File Management** をクリックし、「File Management」画面を表示します。

2. 既存エントリの （Edit）アイコンをクリックします。

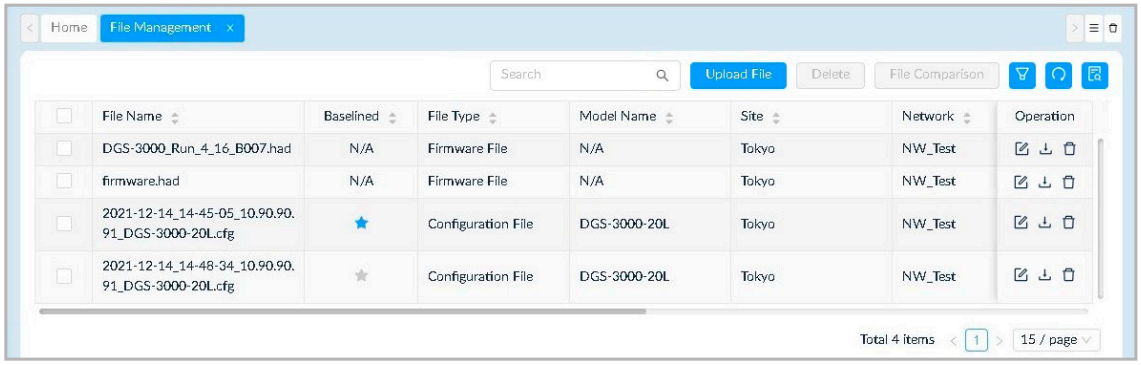


図 6-24　ファイル管理

3. 以下の画面で、ファイルの情報を変更します。

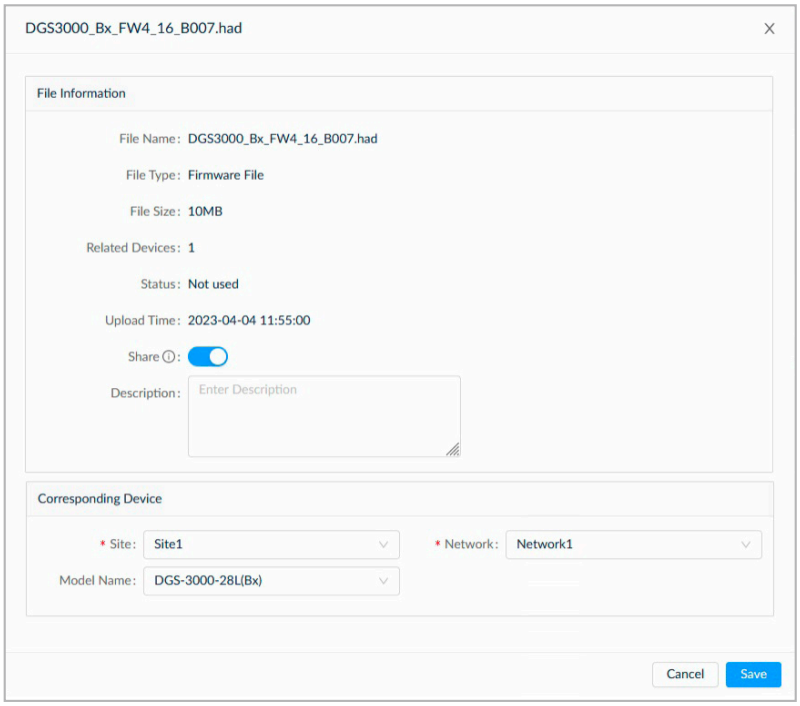


図 6-25　ファイル情報の設定（ファームウェアファイル）

4. 他のネットワークへの共有を有効または無効に設定するには、「Share」オプションをクリックします。
5. 「Description」に、エントリを識別しやすくするための説明を入力します。
6. 必要に応じて対応するデバイス情報を変更します。
   - 「Site」
   - 「Network」
   - 「Model Name」
7. 「Save」をクリックしてファームウェアファイル情報の変更を保存します。設定をキャンセルするには、「Cancel」をクリックします。

ファームウェアファイルのエクスポート

1. **Configuration > File Management** をクリックし、「File Management」画面を表示します。
2. 既存エントリの （Download）アイコンをクリックします。

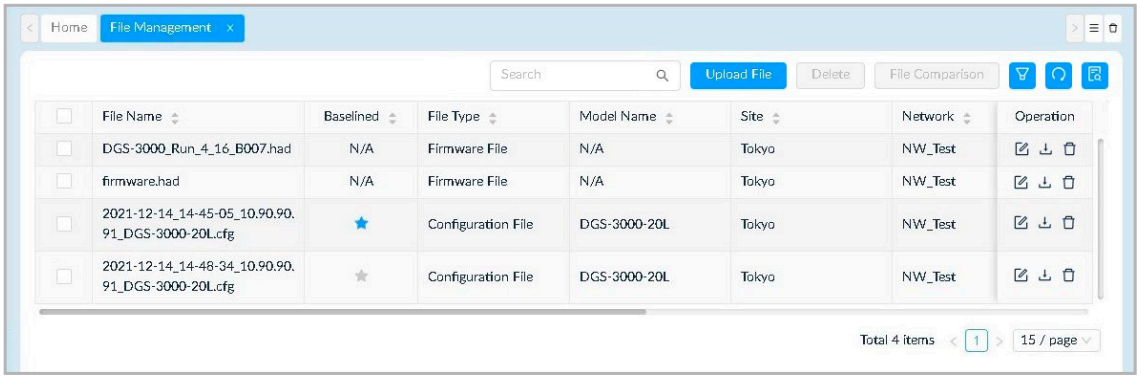


図 6-26　ファイル管理

ファイルは、ブラウザの既定ダウンロードフォルダに保存されます。

ファームウェアファイルの削除

1. **Configuration > File Management** をクリックし、「File Management」画面を表示します。

2. 既存エントリの （Delete File）アイコンをクリックします。または、デバイスを選択して「Delete」をクリックします。

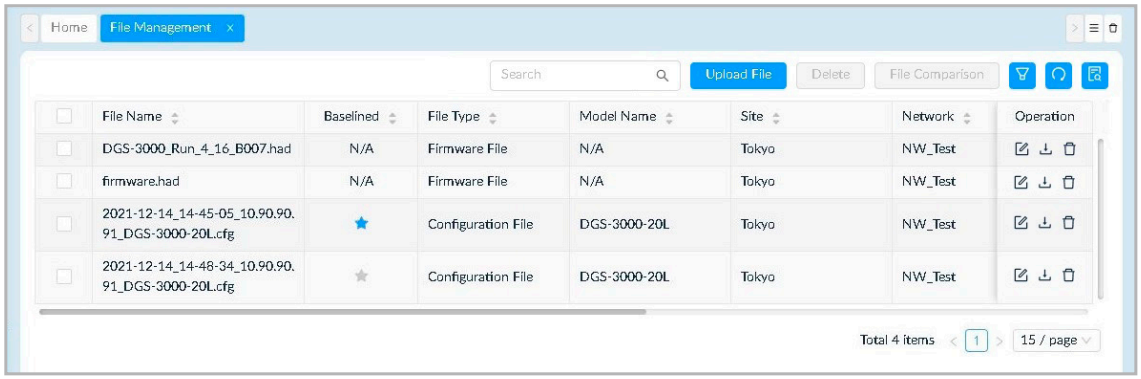


図 6-27　ファイル管理

3. ファイルの削除を確認するメッセージが表示されます。「Yes」をクリックして削除処理を実行します。
操作をキャンセルするには、「No」をクリックします。

コンフィグレーションファイルの管理

コンフィグレーション管理により、デバイス構成のバックアップやリストアに使用するファイルを管理します。

このセクションでは、次の手順について説明します。
- コンフィグレーションファイルのインポート
- コンフィグレーションファイルの変更
- コンフィグレーションファイルのエクスポート
- コンフィグレーションファイルの削除

注意 D-View8 によるバックアップ / リストア機能は、DGS-1100-05PDV2/05V2/08V2/08PV2、DAP-X2810 ではサポートされません。

コンフィグレーションファイルのインポート

インポートしたコンフィグレーションファイルは、ネットワーク上の D-Link デバイスの設定リストアに利用できます。また、リストアタスクのスケジュールを設定して、バッチ処理で繰り返し実行するように設定することもできます。

1. **Configuration > File Management** をクリックし、「File Management」画面を表示します。

2. 「Upload File」をクリックします。

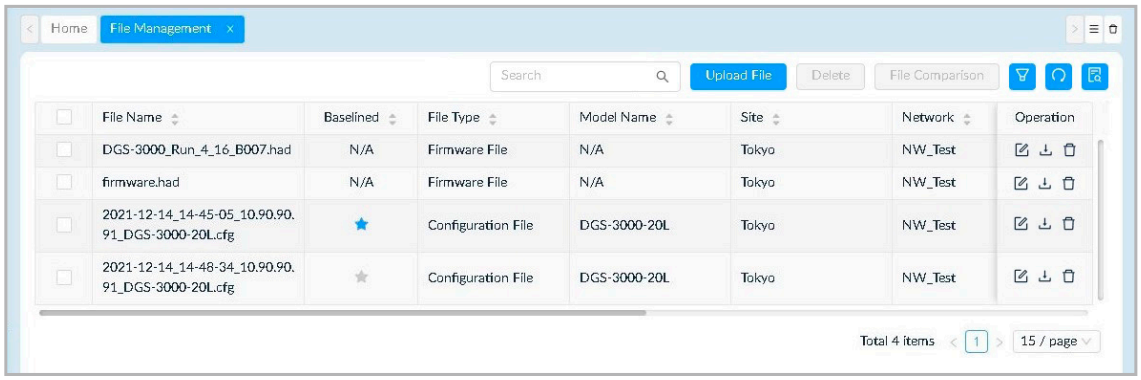


図 6-28　ファイル管理

3. 「Upload File」画面で、以下の項目を設定します。

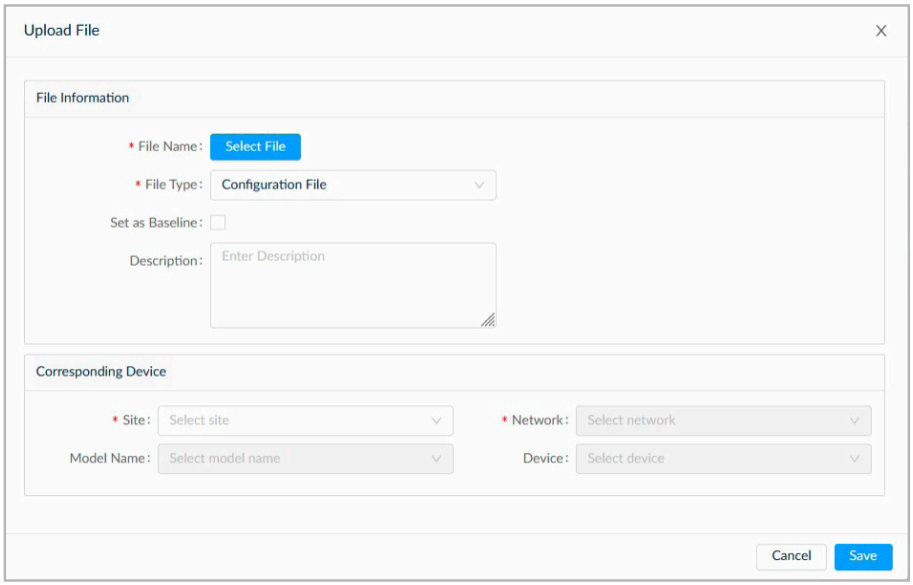


図 6-29　ファイルのアップロード（コンフィグレーションファイル）

設定項目：

項目	説明
File Name	「Select File」をクリックして、コンフィグレーションファイルを選択します。
File Type	ファイルの種類として「Configuration File」を指定します。
Set as Baseline	本オプションにチェックを入れると、ベースラインとして指定されます。ベースラインファイルは、ファイル比較やデフォルトのリストアファイル用に利用することができます。
Description	ファイルの簡単な説明を入力します。
Site	ドロップダウンメニューをクリックして、デバイスモデルが属するサイトを選択します。
Network	ドロップダウンメニューを選択して、サイトに紐づくネットワークを選択します。
Model Name	ドロップダウンメニューをクリックして、コンフィグレーションに対応するモデル名を指定します。
Device	ドロップダウンメニューをクリックして、コンフィグレーションに対応するデバイスを選択します。

4. 「Save」をクリックして、ファイルのエントリを保存します。設定をキャンセルするには、「Cancel」をクリックします。

コンフィグレーションファイルの変更

デバイスの設定ファイルは、ネットワーク上の他のデバイスを設定するためのテンプレートとして使用できます。最初に、ターゲットデバイスに適用する設定ファイルを割り当てる必要があります。

1. **Configuration > File Management** をクリックし、「File Management」画面を表示します。

2. 既存エントリの （Edit）アイコンをクリックします。

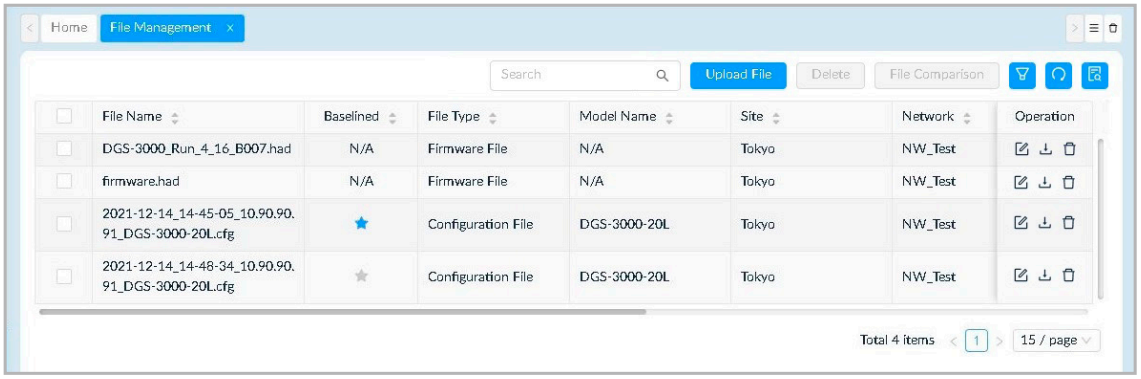


図 6-30　ファイル管理

3. 以下の画面で、ファイルの情報を変更します。

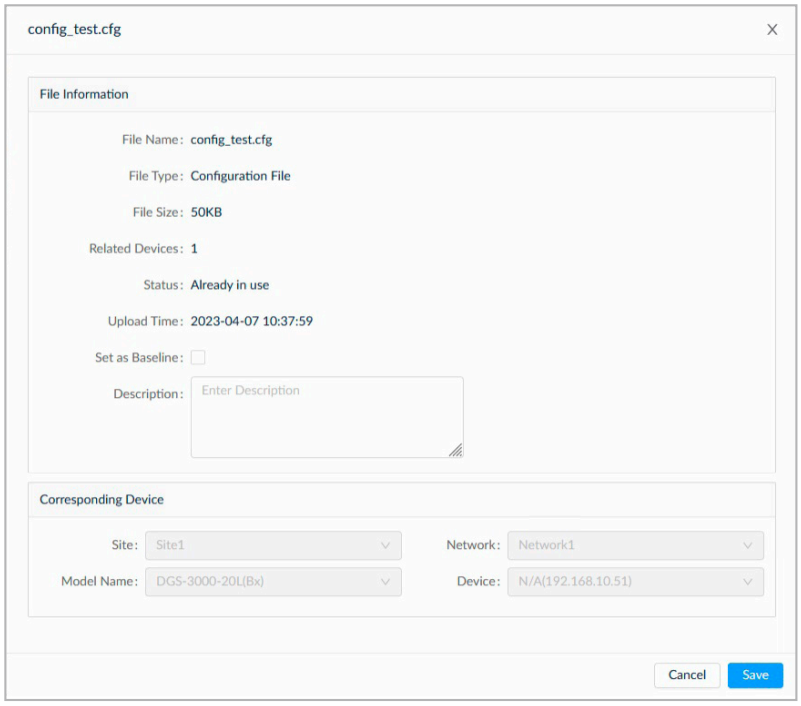


図 6-31　ファイル情報の設定（コンフィグレーションファイル）

4. リストアのデフォルト設定となるベースラインとして指定するには、「Set as Baseline」にチェックを入れます。
5. 「Description」に、エントリを識別しやすくするための説明を入力します。
6. 必要に応じて対応するデバイス情報を変更します。
   - 「Site」
   - 「Network」
   - 「Model Name」
   - 「Device」
7. 「Save」をクリックしてコンフィグレーションファイル情報の変更を保存します。設定をキャンセルするには、「Cancel」をクリックします。

コンフィグレーションファイルのエクスポート

1. **Configuration > File Management** をクリックし、「File Management」画面を表示します。
2. 既存エントリの （Download）アイコンをクリックします。

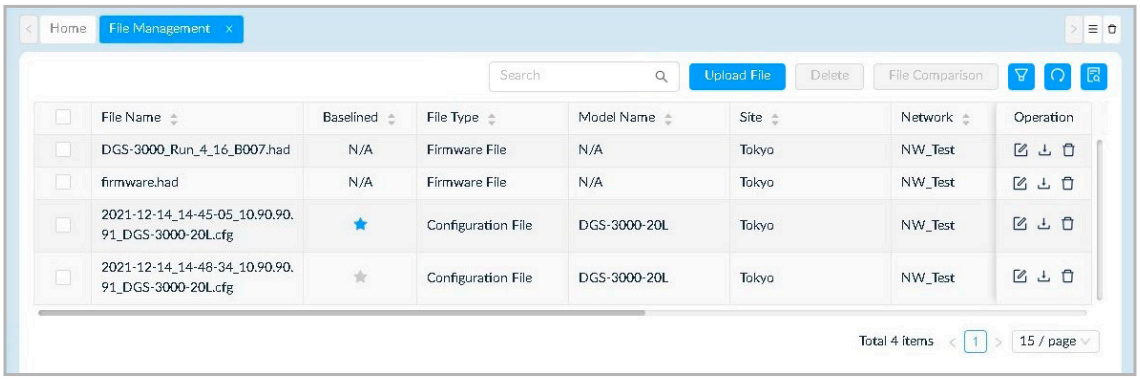


図 6-32　ファイル管理

ファイルは、ブラウザの既定ダウンロードフォルダに保存されます。

コンフィグレーションファイルの削除

1. **Configuration > File Management** をクリックし、「File Management」画面を表示します。

2. 既存エントリの （Delete File）アイコンをクリックします。または、デバイスを選択して「Delete」をクリックします。

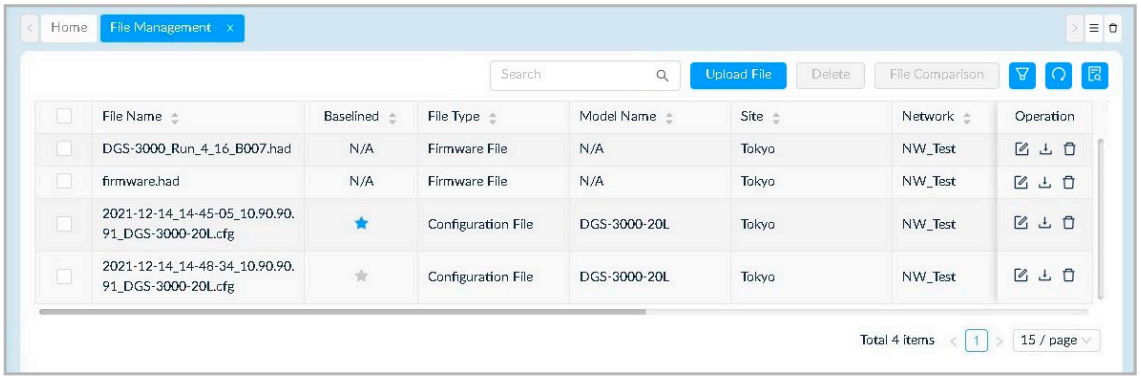


図 6-33　ファイル管理

3. ファイルの削除を確認するメッセージが表示されます。「Yes」をクリックして削除処理を実行します。
操作をキャンセルするには、「No」をクリックします。

第 7 章　アラームと通知

アラーム設定では、指定したデータのしきい値を超えるとアラームが生成されます。アラームの通知方法として、電子メール、Web 通知、または指定デバイスに対するスクリプトの実行を設定できます。

本章では、以下のトピックについて説明します。

- 「アラームの表示と管理」
- 「トラップログと Syslog の表示」
- 「トラップエディタ機能」
- 「Syslog エディタ機能」
- 「アラームおよび監視の管理」
- 「通知の管理」

注意　D-View8 で利用可能な監視項目は製品によって異なります。

※デバイス側で CLI/SNMP に対応している場合、ユーザ定義の監視テンプレートを作成して管理に役立てることもできます。対応可否は製品や機能により異なります。

※設定機能の制限事項に関しては、弊社ホームページの製品ページから対象製品のユーザマニュアルをご確認ください。

注意　DAP-X2810 の無線クライアント情報の監視はサポートされません。

アラームの表示と管理

■ アラームの表示と管理メニュー

1. **Alarm & Notification > Alarm** をクリックします。
   - 「Active Alarms」タブ：アクティブなアラームの一覧が表示されます。
   - 「Historical Alarms」タブ：アラーム履歴の一覧が表示されます。

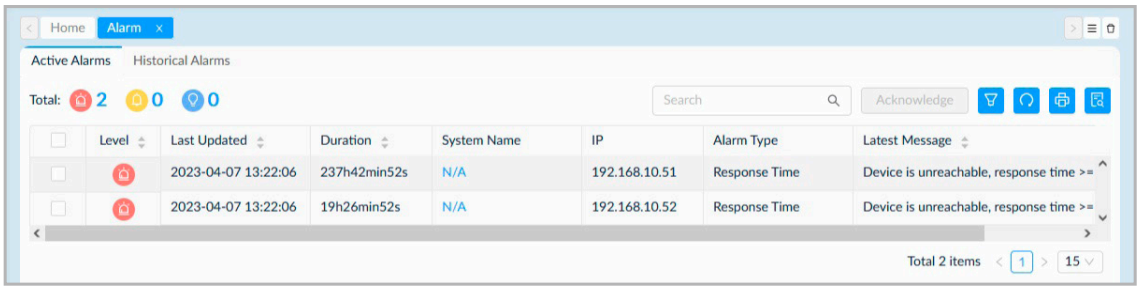


図 7-1　アラーム一覧

表示項目：

項目	説明
Active Alarms	このタブでは、現在アクティブなアラームイベントの一覧を表示します。
Historical Alarms	このタブでは、承認済み（Acknowledge）として指定されたアラームイベント、または停止済みのアラームイベントの一覧を表示します。
Level	アイコン毎に、以下のアラームの重要度を示します。 ・「Critical（赤色）」：「重大レベル（最も深刻）」を示します。 ・「Warning（黄色）」：「警告レベル」を示します。 ・「Critical（青色）」：「情報レベル」を示します。

■ アラームの停止

2. アラームイベントのチェックボックスにチェックを入れます。
3. 「Acknowledge」をクリックして、アラームを停止します。
   アラームイベントは承認済みのイベントとして、「Historical Alarms」タブ配下の一覧に移動されます。アラーム設定を無効化するわけではありません。

■ エントリの検索・表示

エントリを検索するには、「Search」フィールドにキーワードを入力、または（Advanced Query）から高度な検索が可能です。

本画面に列を追加または削除するには、（Column Selector）アイコンをクリックします。

すべての列オプションを有効にするには、「All」を選択します。「Apply」をクリックして、選択した項目を適用します。
- 「Default（デフォルト表示項目）」：「Level」「Last Updated」「Duration」「System Name」「IP」「Alarm Type」「Latest Message」
- 「Other（その他項目）」：「Site」「Network」「Device Category」「Time Generated」「Support PoE」

テーブルの情報を再同期するには、（Refresh）アイコンをクリックしします。

■ ファイル出力

イベント一覧を CSV ファイルとしてエクスポートするには、（Export）アイコンをクリックします。1 回のエクスポートで最大 10,000 件のエントリをダウンロードできます。

トラップログと Syslog の表示

Trap & Syslog リストには、デバイスのトラップイベントと Syslog メッセージが表示されます。

- トラップイベント：SNMP バージョン、元のトラップメッセージ、および変換されたメッセージが記録されます。
- Syslog：メッセージには重大度のラベルが割り当てられます。

また、トラップとログをリモートログサーバに送信することもできます（トラップサーバの設定は **System > Basic Settings > Forward Trap** 、Syslog サーバの設定は、**System > Basic Settings > Forward Syslog** から行います）。
トラップおよび Syslog 画面では、一覧の更新や CSV ファイルへのエクスポートが可能です。

メモ　システム上でログとトラップを収集するために、管理対象デバイスに対し D-View8 をトラップサーバおよび Syslog サーバとして設定する必要があります。D-View8 上で利用可能なトラップ /Syslog 設定は、デバイスによって異なります。

(1) **Monitoring > Device View** に移動し、デバイスのシステム名のリンクをクリックしてデバイス情報画面を開きます。
(2) 「Management」タブをクリックして、「Trap Status」、「Syslog Status」から D-View8 をトラップサーバ、Syslog サーバとして設定します。「Device Information」画面では、「Trap & Syslog」タブをクリックして、当該デバイスのトラップイベントと Syslog メッセージを表示することもできます。

1. **Alarm & Notification > Trap & Syslog** をクリックします。
   - 「Trap」タブ：デバイスのトラップイベントが表示されます。
   - 「Syslog」タブ：デバイスの Syslog イベントが表示されます。

図 7-2　トラップログ

ツール項目：

項目	説明
Search	トラップまたは Syslog 一覧をフィルタリングするためのキーワードを入力します。
Column Selector	（Column Selector）アイコンをクリックして、本画面に列を追加または削除します。
Refresh	（Refresh）アイコンをクリックして、一覧を更新します。
Export	（Export）アイコンをクリックして、一覧を CSV ファイルにエクスポートします。
Advanced Query	（Advanced Query）アイコンをクリックして、高度な検索を開始します。
Edit	トラップの場合は、（Edit）アイコンをクリックして、OID およびバインディング変数値の説明を変更できます。

元のトラップイベントからのメッセージに基づき、変換されたメッセージが表示されます。
トラップ OID やバインディング変数値の説明については、（Edit）アイコンをクリックして編集することができます。この変更は、「Trap Editor」画面にも保存されます（**Alarm & Notification > Trap & Syslog Editor > Trap Editor**）。

特定のトラップ OID またはバインディング値を持つトラップイベントに基づいて、アラームルールを設定することもできます。詳細は、P.165 の「アラームおよび監視の管理」を参照してください。

「Syslog」タブでは、Syslog ログ一覧が表示されます。

図 7-3　システムログ

Syslog に含まれる重大度レベル（Severity）は、以下の状態を示します。

項目	説明
Emergency	デバイスが正常に動作していないことを示します。
Alert	すぐに調査が必要であることを示します。
Critical	デバイスが重大な状態であることを示します。
Error	デバイスでエラーが検出されたことを示します。
Warning	デバイスの動作の警告状態を示します。
Notice	正常な状態ですが、オペレータの注意を必要とする重要な状態を示します。
Informational	エラーではありませんが、参照またはトラブルシューティングの目的で記録する必要がある特定の状態を示します。
Debug	デバッグ目的のメッセージを示します。

Syslog メッセージの特定キーワードに説明を定義することで、Syslog レポート内で特定のログメッセージを簡単に見つけることができます。詳細は、P.204 の「第 12 章　レポート機能」および P.164 の「Syslog エディタ機能」を参照してください。

トラップエディタ機能

トラップにより管理対象デバイスの潜在的なエラーに関するアラートを取得し、Syslog によりデバイス操作の問題を記録することができます。トラップのオブジェクト識別子（OID）を定義すると、問題の特定に役立ちます。すべての管理対象デバイスのトラップメッセージを表示するには、**Alarm & Notification >Trap & Syslog > Trap** に移動します。

1. **Alarm & Notification > Trap & Syslog Editor** をクリックし、「Trap Editor」画面を表示します。

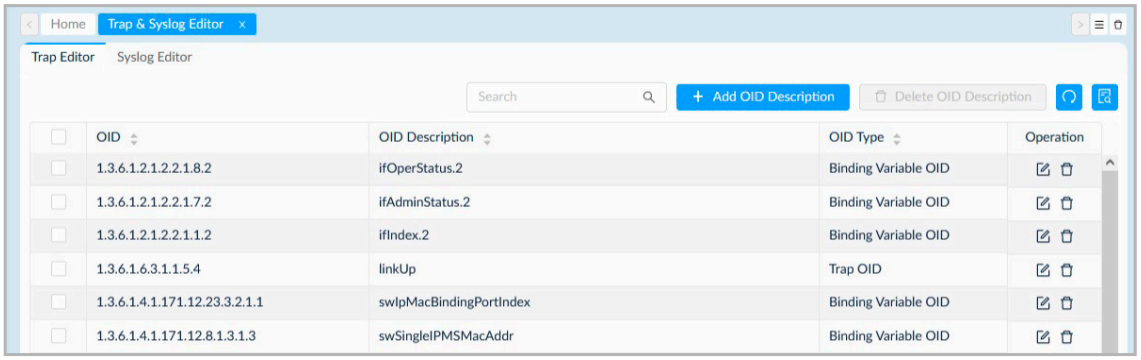


図 7-4　トラップエディタ

2. 「+ Add OID Description」をクリックして、以下の項目を設定します。

項目	説明
OID Type	Trap の種類を選択します。 • 選択肢：「Trap OID」「Binding Variable OID」
OID	一意のオブジェクト識別子の値（OID）を追加します。
OID Description	OID の識別に役立つ単語や説明を入力します。Trap ログや Trap レポートに表示されます。
Binding Variable Value/ Value Description	「Binding Variable OID」を選択した場合、バインディング変数 OID に対し、変数値と説明を入力します。

■ エントリの編集

エントリを編集するには、（Edit）アイコンをクリックします。

■ エントリの削除

エントリを削除するには、エントリを選択後、「Delete Syslog Description」をクリックします。または、対象エントリの（Delete）アイコンをクリックして、エントリを削除します。

■ トラップレポートの生成

レポートテンプレートを使用して、トラップレポートを生成できます。定義された OID の説明は、トラップイベントを示す強調表示されたテキストとして表示されます。詳細は、P.205 の「レポートの生成」を参照してください。

Syslog エディタ機能

Syslog 機能は、デバイスデータのログを記録することで、問題の分析やトラブルシューティングに役立てることができます。
さらに、Syslog エディタ機能では、特定のログメッセージを視覚化するのに役立つ Syslog の説明を追加できます。Syslog エディタで定義された説明を使用した Syslog レポートを生成するには、**Reports > General Reports** と選択し、「Device Reports」の「Syslog」カテゴリを選択します。（詳細は、P.204 の「レポートテンプレート」を参照してください。）すべての管理対象デバイスのログを表示するには、**Alarm & Notification >Trap & Syslog > Syslog** に移動します。

1. **Alarm & Notification > Trap & Syslog Editor** をクリックし、「Syslog Editor」画面を表示します。

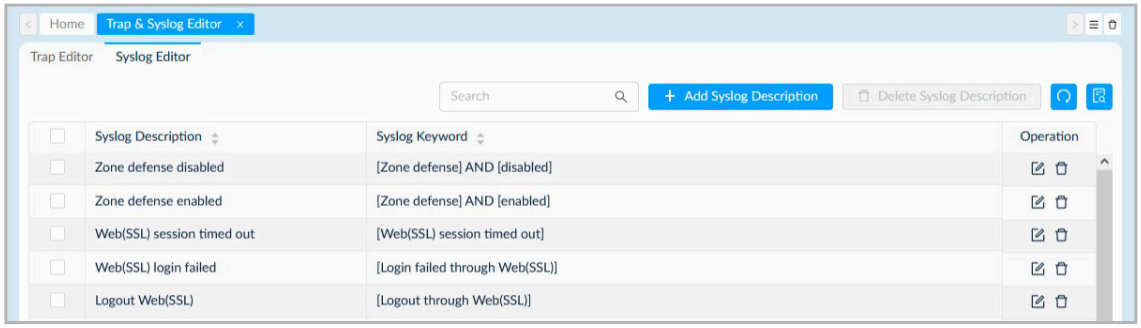


図 7-5　Syslog エディタ

2. 「+ Add Syslog Description」をクリックして、以下の項目を設定します。

項目	説明
Syslog Description	ログメッセージ内の指定キーワードを示す、Syslog の説明を入力します。Syslog レポートのワードクラウドでハイライトテキストとして表示されます。詳細は、P.205 の「レポートの生成」を参照してください。
Syslog Keyword	Syslog に含まれるキーワードを指定します。

■ エントリの検索・表示

エントリを検索するには、「Search」フィールドにキーワード（Syslog 説明 /Syslog キーワード）を入力、または（Advanced Query）から高度な検索が可能です。

テーブルの情報を更新するには、（Refresh）アイコンをクリックしします。

■ エントリの編集・削除

エントリを編集するには、（Edit）アイコンをクリックします。

エントリを削除するには、エントリを選択後、「Delete Syslog Description」をクリックします。または、対象エントリの（Delete）アイコンをクリックして、Syslog キーワードを削除します。

Syslog に関連して、Syslog の重大度に基づいてアラームルールを設定したり、特定の種類のログメッセージが出力された場合に警告するように設定したりすることもできます。詳細は、P.165 の「アラームおよび監視の管理」を参照してください。

アラームおよび監視の管理

監視とアラームの設定を管理します。

アラームルールの設定

アラームルールでは、アラームをトリガする条件を設定します。CPU やメモリの使用率、その他様々なシステム監視項目によってトリガすることができます。

アラームルールの表示

1. **Alarm & Notification > Monitor & Alarm Settings** をクリックします。
「Alarm Settings」タブを開きます。

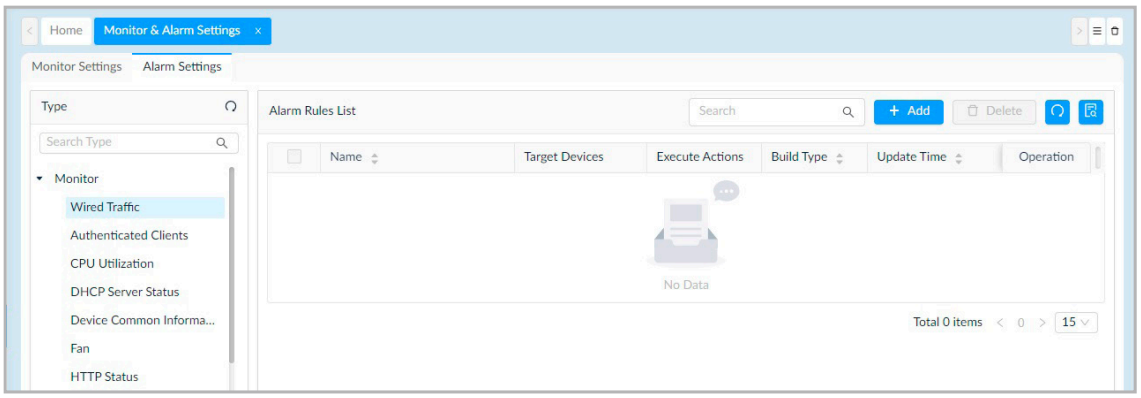


図 7-6　アラーム設定

2. 以下のシステム定義カテゴリのデバイスステータス項目について、アラームルールを設定できます。

カテゴリ	項目	説明
Monitor	Wired Traffic	Rx/Tx トラフィック、エラーレート、廃棄レート、帯域幅使用率に基づくアラート。
	Authenticated Clients	認証済みクライアントの Rx/Tx 速度とクライアント数に基づくアラート。
	CPU Utilization	CPU 使用率に基づくアラート。
	DHCP Server Status	DHCP ステータスに基づくアラート。
	Device Common Information	ファームウェアバージョン、ハードウェアバージョン、MAC アドレス、シリアル番号、合計フラッシュ容量に基づくアラート。
	Fan	ファンのステータスまたは速度に基づくアラート。
	HTTP Status	HTTP ステータスまたはポート番号に基づくアラート。
	HTTPS Status	HTTPS ステータスに基づくアラート。
	Installed Apps	インストール済みアプリの数に基づくアラート。
	LACP	LACP ステータスに基づくアラート。
	LLDP	LLDP ステータスに基づくアラート
	Managed AP WLAN Traffic(packet)	WLAN の Rx または Tx トラフィックに基づくアラート。
	Memory Utilization	メモリ使用率に基づくアラート。
	Power Status	電源ステータスに基づくアラート。
	Private Port	プライベート MIB を使用する D-Link スイッチのポート詳細に基づくアラート。
	RMON Status	RMON ステータスに基づくアラート。
	Response Time	応答時間に基づくアラート（システムのデフォルトのアラーム）。
	Running Software	ホストで実行されているソフトウェアに基づくアラート。
	SIM Traffic	SIM カード上のアップロードおよびダウンロードトラフィックに基づくアラート。
	SNTP Status	SNTP ステータスに基づくアラート。
	SSH Status	SSH バージョン、ステータス、最大認証失敗試行回数、セッションキー再生成回数、最大セッション数、接続タイムアウト、ポート番号に基づくアラート。
	STP Status	STP ステータスに基づくアラート。
	Safeguard Status	セーフガードステータスに基づくアラート。
	Syslog Status	Syslog ステータスに基づくアラート。
	Telnet Status	Telnet ステータスとポートに基づくアラート。
	Temperature	温度インジケータと測定値に基づくアラート。
	Trap Status	トラップステータスに基づくアラート。

カテゴリ	項目	説明
	Wireless Access Points	スタンドアロン AP、管理対象 AP、合計 AP、不正 AP の数に基づくアラート。
	Wireless Error Packets	無線で送信された Rx/Tx エラーパケットの数に基づくアラート。
	Wireless Traffic(bit)	Rx/Tx トラフィックに基づくアラート（bps）。
	Wireless Traffic(packet)	Rx/Tx トラフィックに基づくアラート（pps）。
Trap	coldStart	デバイスの coldStart トラップに基づくアラート。
	warmStart	デバイスの warmStart トラップに基づくアラート。
	linkDown	ポートの linkDown トラップに基づくアラート。
	linkUp	ポートの linkUp トラップに基づくアラート。
	authenticationFailure	SNMP 認証失敗トラップに基づくアラート。
	egpNeighborLoss	EGP Neighbor Loss トラップに基づくアラート。
	Enterprise Specific	ベンダ固有のトラップに基づくアラート。
Syslog	Syslog	指定 Syslog メッセージに基づくアラート。
sFlow	sFlow	sFlow トラフィックパケットに基づくアラート。

本画面では、様々な監視カテゴリやトラフィック、メッセージ種別（トラップ、Syslog、sFlow など）のアラームルールを設定できます。

注意 D-View8 で利用可能な監視項目は製品によって異なります。

アラームルールの追加

1. **Alarm & Notification > Monitor & Alarm Settings** をクリックします。
   デフォルトでは、「Monitor Settings」タブが表示されます。
2. 「Alarm Settings」タブを開きます。
3. 左側ツリーの「Type」の一覧から、システム定義またはユーザ定義の監視カテゴリを選択します。
4. ルールを設定するには、「+ Add」をクリックします。

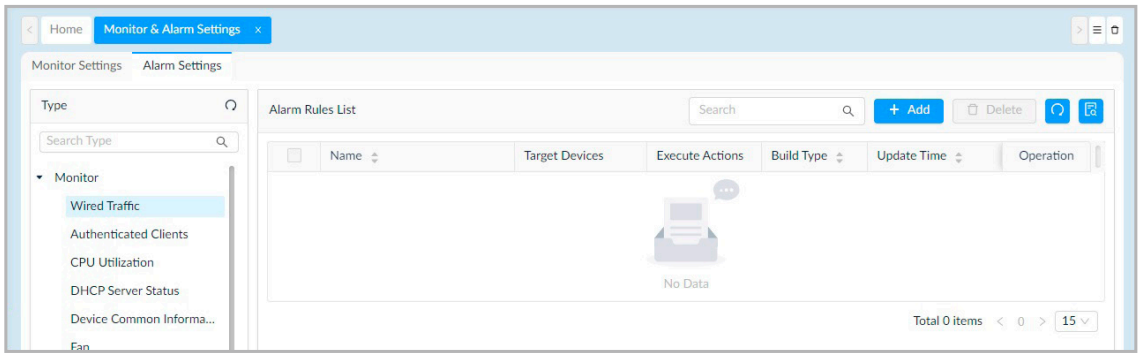


図 7-7　アラーム設定（有線トラフィック）

5. ルールによって必要な設定が異なります。以下の共通設定を定義して、ルールタスクを作成します。

項目	説明
Set Profile Information（プロファイル情報の設定）	
Basic Information	• 「Name」：アラームルールの名前を入力します。 • 「Description」：アラームルールの名前を入力します。
Rule Information	• 「Generation Conditions」：アラームの重要度（「Info」「Warning」「Critical」）毎にしきい値を設定します。しきい値の設定に関するパラメータは、監視対象の条件タイプによって異なります。 • 「Release Conditions」：アラーム解除のしきい値を設定します。
Inhibition Schedule Settings	• 「Schedule」：定義済みのスケジュールを選択するか、「Add Schedule」をクリックして新しいスケジュールを追加します。指定されたスケジュールの期間、アラームの配信が停止されます。
Analysis Source	監視対象の sFlow インタフェースおよび通信方向、アラーム基準（「Application」「DSCP」「IP」「Protocol」）を設定します。本設定は、sFlow アラームカテゴリのみで利用可能です。
Set Target Devices（ターゲットデバイスの設定）	
Set Target Devices	監視対象のデバイスとデバイスインタフェース（「Wired Traffic」監視条件を設定する場合）を設定します。

項目	説明
Set Actions（アクションの設定）	
Device Command Server Command	デバイスを選択し、「+ Add Actions」をクリックして実行するスクリプトを設定します。 このスクリプトは、アラーム送信元のほか、指定デバイスまたは D-View8 サーバで実行できます。「Device Command」または「Server Command」タブをクリックし、対象のデバイスで実行するスクリプトを設定します。デバイスでコマンドを実行するために、デバイスにログインするための資格情報とプロトコルを設定します。

6. 「>> Next」または「OK」をクリックして、次の画面に進みます。
7. ルールの定義が完了したら、「Save」をクリックしてプロファイルを保存します。設定をキャンセルするには、「Cancel」をクリックします。

指定デバイスにアラームを設定した後、デバイス毎またはポート毎（「Wired Traffic」監視条件の場合）でアラームのステータスを設定できます。

(1) **Monitoring > Device View** に移動し、システム名のリンクを使用して、デバイス情報画面に移動します。

(2) 「Port」または「Alarm」タブを選択して、ポート一覧またはアラーム設定画面に移動します。

(3) ポート一覧では、各ポートの「Alarm Switch」の ON/OFF を切り替えて、「Wired Traffic」のアラームステータスを設定できます。
アラーム設定では、特定のアラームタイプの ON/OFF を切り替えて、指定アラームのステータスを設定できます。

監視設定の表示と管理

ネットワーク監視は、「Monitor & Alarm Settings」画面の「Monitor Settings」タブで管理することができます。

監視設定の表示

1. **Alarm & Notification > Monitor & Alarm Settings** をクリックします。
2. 「Monitor Settings」タブが表示されます。
3. 「Monitor Category」の一覧から特定のカテゴリを選択して、監視対象のデバイスを表示します。

対象デバイスに対し、監視機能の有効化 / 無効化などを設定することができます。以下の手順を参照してください。

■ 監視タスクの設定：監視機能の ON/OFF

1. ターゲットデバイスを選択します。
2. ポート毎の設定に対応している項目の場合、「Selected Port(s)」にバッチタスクを適用するポート番号を入力します。
または、「Batch Select Port」をクリックして、ポップアップ表示される画面にポート番号を入力し、「Apply」をクリックします。「Selected Port(s)」に指定したポート番号が入力されます。
3. 「Edit Monitoring Status」をクリックして、選択したデバイスの指定ポートに対し、対象カテゴリの監視機能を「ON」または「OFF」に設定します。

■ 監視タスクの設定：監視間隔の設定

1. ターゲットデバイスを選択します。
2. 「Edit Interval」クリックし、ドロップダウンメニューから監視間隔を選択します。
3. 「Save」をクリックして設定を保存します。

メモ　監視ステータスを OFF にすると、関連するアラームもトリガされなくなります。

メモ　選択したカテゴリにより、設定可能なオプションは異なります。

注意　D-View8 で利用可能な監視項目は製品によって異なります。

通知の管理

通知センターには、通知ルール一覧が表示されます。トリガ条件、通知受信者、通知の停止期間などを設定できます。

通知イベントの表示と管理

1. **Alarm & Notification > Notification Center** をクリックし、「Notification Center」画面を表示します。

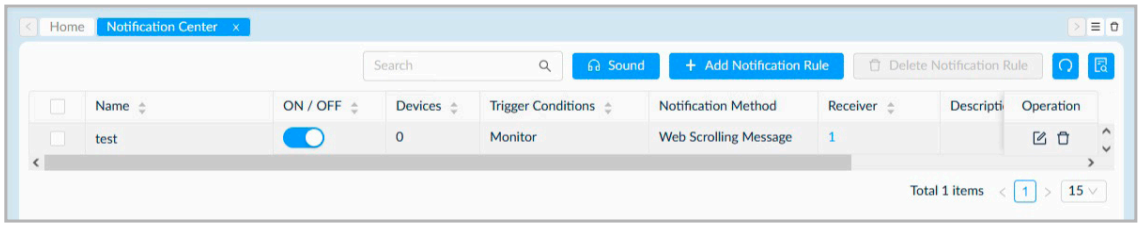


図 7-8　通知センター

表示項目：

項目	説明
Search	キーワードを入力して、エントリを検索します。
Sound	「Sound」をクリックして、通知がトリガされたときに鳴る着信音をカスタマイズします。アラームの重大度別に、内蔵の着信音を指定することができます。
Add Notification Rule	「+ Add Notification Rule」をクリックして、通知ルールを定義します。
Delete Notification Rule	エントリを選択して「Delete Notification Rule」をクリックし、通知ルールを削除します。
Refresh	（Refresh）アイコンをクリックして、テーブルの情報を更新します。
Advanced Query	（Advanced Query）アイコンをクリックして、高度な検索を開始します。エントリをフィルタリングするための条件を入力します。「Name」「ON/OFF」「Trigger Conditions」「Notification Method」で条件を指定できます。
Name	ルール名を表示します。
ON / OFF	スライドボタンをクリックして、ルールを有効または無効にします。
Devices	ルールに紐づいているデバイスの数を表示します。
Trigger Conditions	通知をトリガする監視の条件タイプ（Monitor、Trap、Syslog、Wired Traffic など）を表示します。
Notification Method	ルールの通知方法を表示します。（「Web Scrolling Message」「Email」「Execute Script」）
Receiver	通知を受信するユーザ数が表示されます。ユーザ数のリンクをクリックすると、通知を受信するユーザのユーザプロファイルを確認できます。
Description	ルールの説明を表示します。

新しいルールの追加

1. **Alarm & Notification > Notification Center** をクリックし、「Notification Center」画面を表示します。
2. 「+ Add Notification Rule」をクリックし、以下の画面を表示します。

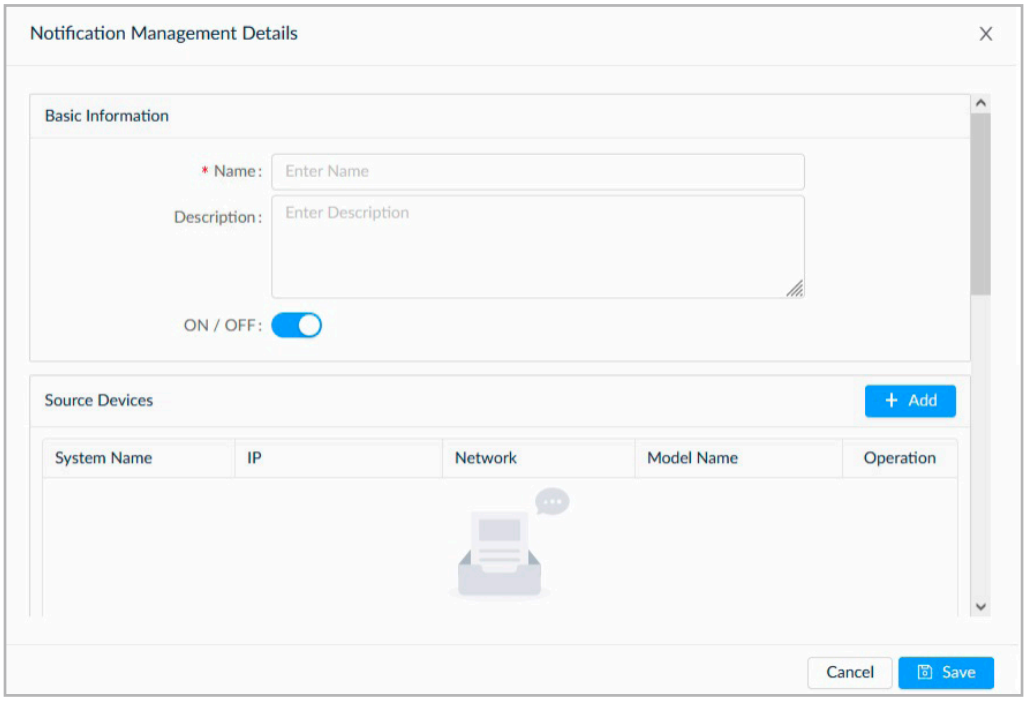


図 7-9　通知ルールの設定

3. 「Basic Information」で基本情報（名前、説明）を入力します。
4. 「ON/OFF」スライドボタンをクリックして、ルールを有効または無効にします。
5. 「Source Devices」セクションで、「+ Add」をクリックして、ターゲットデバイスの選択画面を表示します。

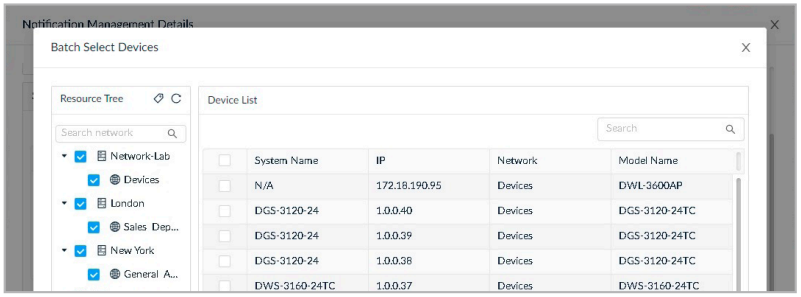


図 7-10　デバイス一括選択

6. デバイスリストから通知ルールに含めるデバイスを選択し、「OK」をクリックします。

7. 「Trigger Conditions」セクションで、通知トリガの種類を選択します。

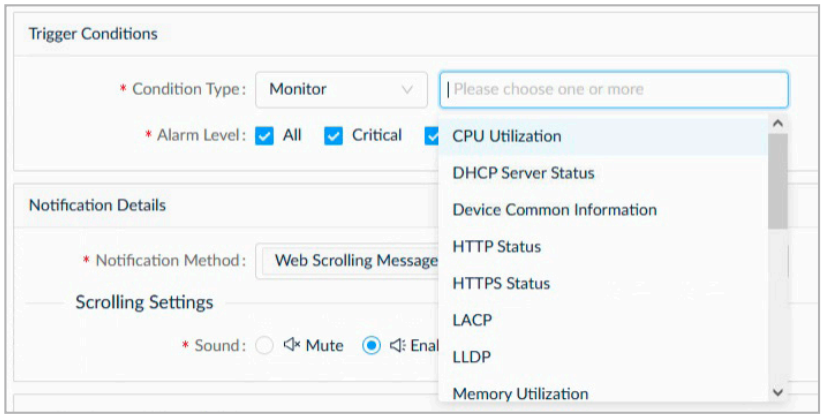


図 7-11　通知トリガの種類

詳細は、次の表を参照してください。

項目	説明
Trigger Conditions（トリガ条件）	
Condition Type	トリガ条件の種類を指定します。 • 「Monitor」：「Monitor」のアラームルールによって生成されたアラームがトリガとなり、指定された通知が送信されます。 • 「Trap」：「Trap」のアラームルールによって生成されたアラームがトリガとなり、指定された通知が送信されます。 • 「Syslog」：「Syslog」のアラームルールによって生成されたアラームがトリガとなり、指定された通知が送信されます。 • 「Wired Traffic」：「Wired Traffic」のアラームルールによって生成されたアラームがトリガとなり、指定された通知が送信されます。 「Monitor」を指定した場合、デバイスの種類に応じて利用可能な監視項目が表示されます。 以下は、スイッチの監視項目の例です。 - 「CPU Utilization」 - 「DHCP Server Status」 - 「Device Common Information」 - 「Fan」 - 「HTTP Status」 - 「LACP」 - 「LLDP」 - 「Memory Utilization」 - 「Private Port」 - 「RMON Status」 - 「Response Time」 - 「SNTP Status」 - 「SSH Status」 - 「STP Status」 - 「Safeguard Status」 - 「Syslog Status」 - 「Telnet Status」 - 「Trap Status」 - 「Wireless Access Points」 - 「Wireless Error Packets」 アラームルールを設定するには、**Alarm & Notification > Monitor & Alarm Settings > Alarm Settings** に移動し、該当ツリー / 項目を選択します。
Alarm Level	通知のトリガとなるアラームの種類を選択します。 • 「All」：すべてのアラームレベルが通知対象となります。 • 「Critical」：障害や異常を示す重大なエラー情報が通知対象となります。 • 「Warning」：問題を引き起こす可能性がある警告イベントの情報が通知対象となります。 • 「Info」：インフォメーションレベルの情報が通知対象となります。 通知を有効にするには、対応する重大度レベルのアラームを設定する必要があります。
Model	トリガ条件の種類で「Wired Traffic」を選択した場合、選択したデバイスのモデル名が表示されます。「All（すべて）」または特定のポートを選択し、トリガ条件として割り当てます。 通知を有効にするには、監視対象ポートが対応するアラームルールで設定されている必要があります。

注意 D-View8 で利用可能な監視項目は製品によって異なります。

8. 「Notification Details」セクションで、「Notification Method」項目のドロップダウンメニューを選択して、通知方法を定義します。

項目	説明
Notification Details（通知詳細）	
Notification Method	通知方法を指定します。 • 「Web Scrolling Message」：D-View8 の Web アプリケーションにログインしている場合、通知がポップアップで表示されます。 • 「Email」：通知が E メールで送信されます。 • 「Execute Script」：スクリプトを実行します。
Web Scrolling Message を選択した場合	
Sound	通知の方法として「Web Scrolling Message」を選択した場合、アラートの音設定を選択します。 • 選択肢：「Mute（ミュート / 音を消す）」「Enable Voice（音声を有効にする）」
Execute Script を選択した場合	

Command Line	通知の方法として「Execute Script」を選択した場合、実行するスクリプトを入力します。
	
	スクリプトの記述ルール：
	• '#' で始まる行は、コマンドではなくコメントと見なされます。
	• 文字列の前後に '%' を使用して、変数としてラベル付けします。例）%IP% は、IP を変数としてラベル付けします。
	• 変数の値は、対象デバイスごとに「Device Attribute」欄で指定することができます。
	• 各行には、CLI コマンドを 1 つだけ記載します。
	• デッドロック操作を防止するには、処理が停止しない CLI コマンドの使用を避けてください。例）ping10.0.0.1
	• デッドロック操作を防止するには、終了するために特別な入力エントリを必要とする CLI コマンドの使用を避けてください。例）show port
	
	サンプルスクリプト：
	`config ssh authmode password enable`
	`config ssh server contimeout 120`
	`enable SSH`
	
	変数を含むサンプルスクリプト：
	`config fdb aging_time %TimeoutSeconds%`
	
	サンプルコメント：
	`# this is a comment`

Apply Command to	スクリプトを実行する対象のデバイスを選択します。 • 「Itself」：指定した対象デバイスにスクリプトを適用します。 • 「Other Devices」：他のデバイスを指定します。
Batch Configure Attribute Values /Device Attributes	デバイス毎にログインに必要なアカウント情報および通信プロトコルを指定することが可能です。
Alarm Handling	「Acknowledge Alarm after script execution」のチェックボックスにチェックを入れて、繰り返しのスクリプト処理を終了させるためのオプションを指定します。アラームは、スクリプトの実行毎に自動的に「Acknowledge（承認済み）」ステータスになります。 • 「Number of Repetitions」：繰り返しの最大回数 (1-100）を指定します。 • 「Cycle Time」：サイクル時間（5-1440 分）を指定します。 指定したサイクル時間内で繰り返しの最大回数に達すると、自動スクリプトが停止します。

9. 「Notification Receiving Administrator」セクションで「+ Add」をクリックして、通知ユーザの選択画面を表示します。

図 7-12　通知ユーザプロファイルの選択

10. ユーザ一覧から、ルールがトリガされたときに通知を受信する管理者ユーザのプロファイルを指定します。

11. 「OK」をクリックして、ユーザを通知の対象に追加します。設定をキャンセルするには、「Cancel」をクリックします。

12. 「Notification Suspension Period（通知の停止期間）」セクションで「Schedule」のドロップダウンリストをクリックし、スケジュールを選択します。
または、「Add Schedule」をクリックして新規のスケジュールを設定します。
ここで指定した期間、通知が停止されます。

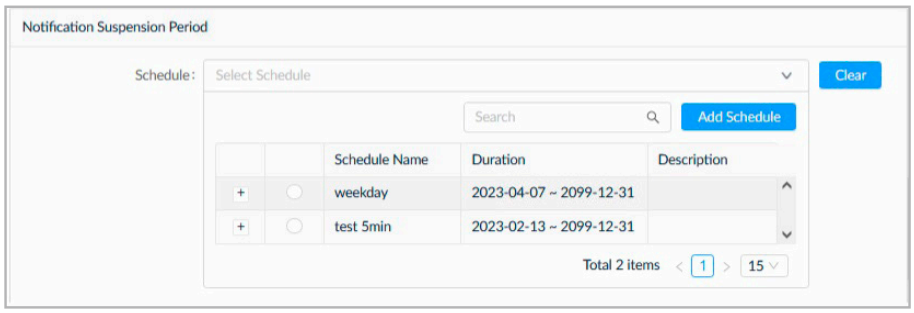


図 7-13　通知一時停止期間

メモ　**System > Scheduling > Time Range Schedule List** タブで、設定した定義済みスケジュールを確認できます。

13. 「Save」をクリックして、通知ルールを保存します。設定をキャンセルするには、「Cancel」をクリックします。

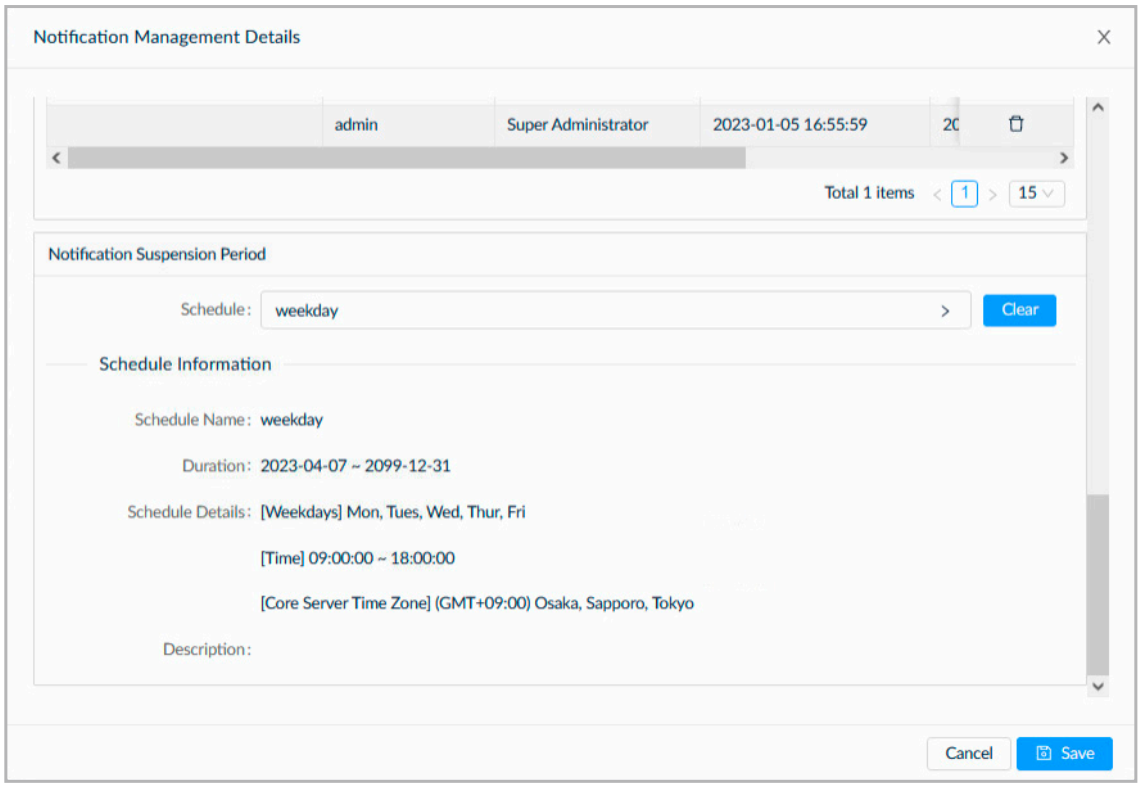


図 7-14　通知ルール

■ 通知ルールの編集・削除

作成された通知ルールは、「Operation（操作）」列の（Edit）または（Delete）アイコンをクリックして、編集または削除できます。

第 8 章　アーキテクチャトポロジの管理

トポロジ機能では、ネットワークアーキテクチャを階層マップとして表示します。

本章では、以下のトピックについて説明します。

- 「ネットワークトポロジの表示と管理」
- 「トポロジビューの作成」

ネットワークトポロジの表示と管理

階層マップを使用して、ネットワーク内のデバイスの位置を把握することができます。デバイス情報やステータス、関連するパフォーマンス統計などの情報も確認できます。

メモ　ライセンスの期限が切れると、管理ノード数の制限（D-View8 フル機能は利用可能）についてのアラートと、追加ライセンスの適用を促すメッセージが「Topology Map」画面に表示されます。ライセンスの更新手順については、P.238 の「ライセンス管理」を参照してください。

1. **Monitoring > Topology Map** をクリックします。

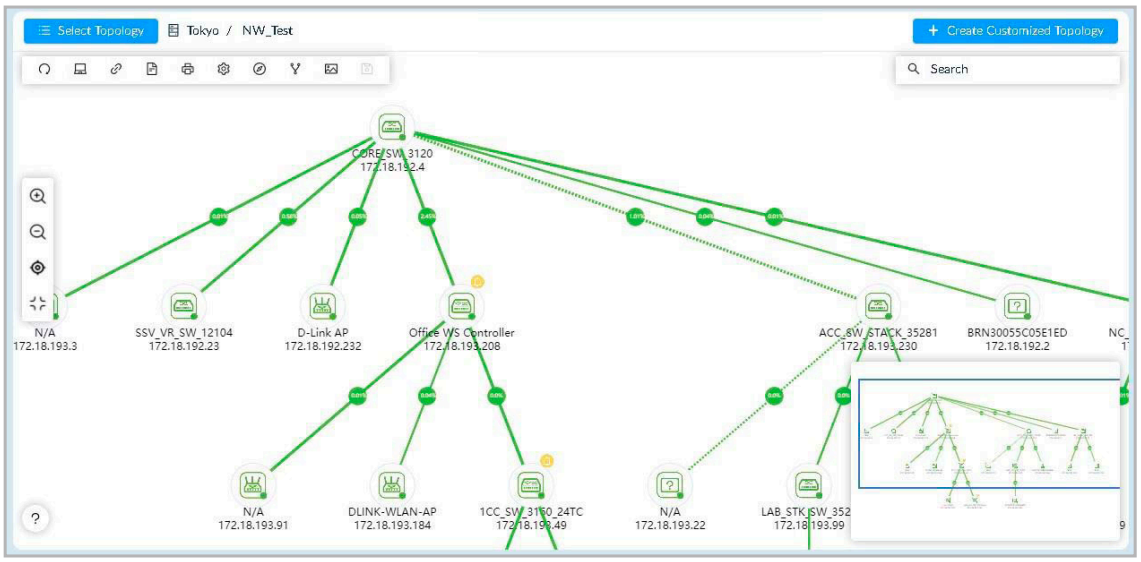


図 8-1　トポロジマップ

項目	説明
Select Topology	「Select Topology」をクリックして、「System Topology」または「Customized Topology」のリストを表示します。 検索機能を使用すると、キーワードを入力して、使用可能なマップを検索することができます。 ・「System Topology」：システムによって自動的に生成されるネットワークトポロジ。 ・「Customized Topology」：ユーザ定義のネットワークトポロジ。
Create Customized Topology	「+ Create Customized Topology」をクリックして、特定の組織 / サイト / ネットワークについて、カスタマイズされたネットワーク図を作成します。
Toolbar	**ツールバーアイコンの説明：** ・（Refresh）：画面上のトポロジを同期します。 ・（Device List）：表示中のトポロジについて、デバイスの一覧を表示します。 ・（Link List）：リンクの一覧を表示します。「Connection View」のリンク詳細画面が表示されます。

項目	説明
	• （Network overview）：検出 IP 範囲、統計グラフ（デバイスタイプ、デバイスモデル、オンライン / オフラインステータス、帯域幅など）といったネットワークステータスの概要が表示されます。 • （Export）：トポロジマップをローカルドライブ上に PNG ファイルとして保存します。 • （Topology Settings）：「Display Setting」では、トポロジ上のデバイスやリンク情報で表示する項目を選択します。「Current Topology Setting」では、現在のトポロジの表示形式を変更します。 • （Rediscover）：マップ上のデバイスをスキャンし、リンク情報を更新します。 • （Link Edit）：リンク編集機能の有効 / 無効を切り替えます。このオプションをクリックし、マップ上のデバイスをクリックしてリンクを作成します。作成したリンクは右クリックで編集または削除することができます。 • （Add Background Image）：マップに背景画像を追加します。 • （Save）：現在のトポロジマップを保存します。
Search	特定のデバイスを検索します。
Control Bar	**コントロールバーアイコンの説明：** • （Zoom In）：表示を拡大します。 • （Zoom Out）：表示を縮小します。 • （Focus on Central Node）：中央のノードにフォーカスします。中央デバイスはトポロジ設定により定義されます。 • （Zoom Fit）：作業画面に合わせてトポロジマップを表示します。
Help	? アイコンをクリックして、ヘルプ画面を表示します。 • 「Topological Legend」：トポロジマップにおけるアイコンの説明を表示します。（ステータス、デバイスタイプ、通信速度など） • 「Link Operation」：リンクを編集、削除する手順について説明を表示します。 • 「Batch Select Nodes」：複数のノードをまとめて選択する手順の説明を表示します。

2. トポロジマップでデバイスにマウスオーバーすると、当該デバイスが強調表示されます。

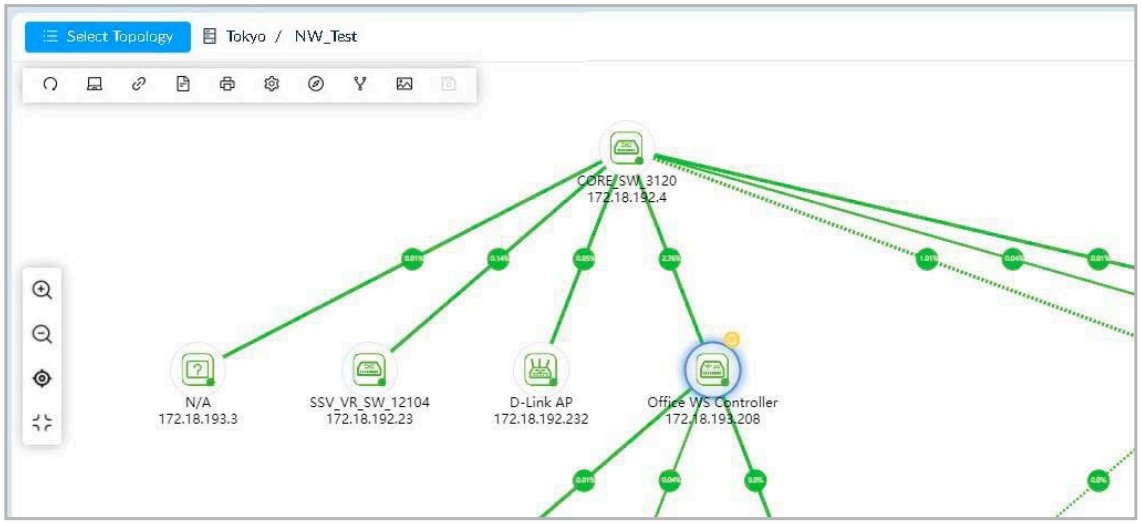


図 8-2　トポロジマップ（デバイス選択時）

3. デバイスをクリックすると、デバイス情報が表示されます。

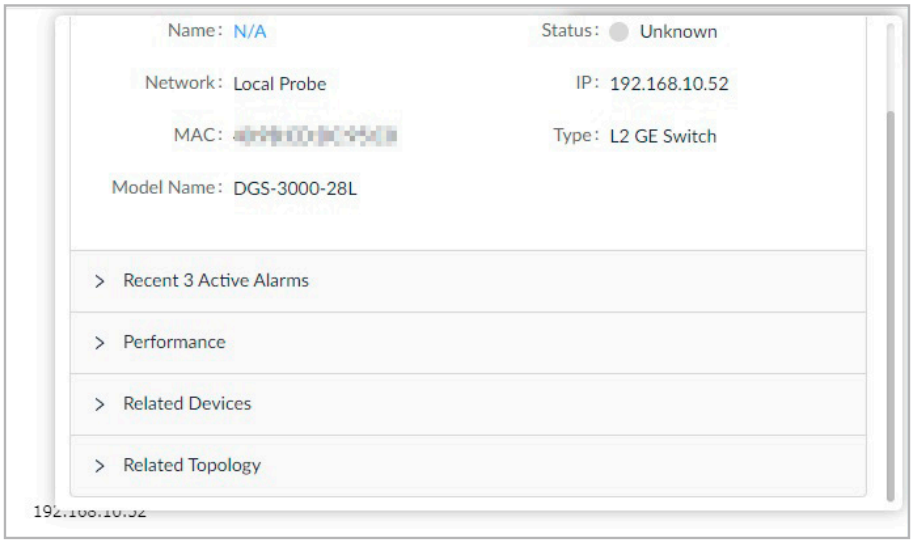


図 8-3　デバイス情報

デバイス情報では、以下の情報を確認できます。

項目	説明
Device Information	デバイス名、ステータス、ネットワーク、IP アドレス、MAC アドレス、デバイスのタイプ、およびモデル名を表示します。デバイス情報を変更するには、デバイス名のリンクをクリックしてデバイス詳細画面を開きます。
Recent 3 Active Alarms	直近の 3 つのアクティブなアラームを表示します。
Performance	CPU 使用率、可用性、メモリ使用率を表示します。
Related Devices	接続機器の情報を表示します。
Related Topology	接続されたデバイスに関連するその他のトポロジを表示します。

4. リンクをクリックすると、リンク情報画面が表示されます。

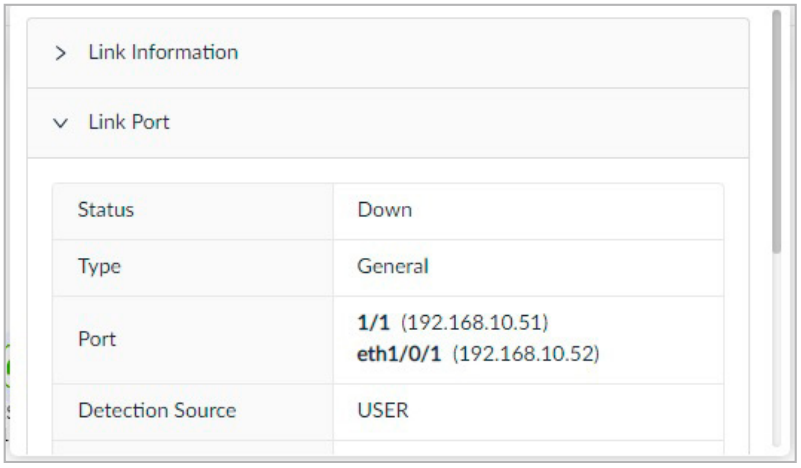


図 8-4　リンク情報

リンク情報画面では、以下の情報を確認できます。

項目	説明
Link Information	リンクを確立しているデバイスとリンクタイプを表示します。
Link Port	デバイスのリンクポート、帯域幅、使用率、Rx/Tx レートなどを表示します。
Link Alarm	このリンクのアクティビティに対して生成されたアラームを表示します。

リンクを編集するには、リンクを右クリックして「Edit Link」をクリックします。リンクのタイプ（「Normal Link」「LACP Link」「Logical Link」）およびリンクのポートを変更できます。「Normal Link（通常のリンク）」は、物理的なデータフローでワイヤとケーブルを使用し、「Logical Link（論理リンク）」は、ネットワーク内のデバイス間の物理的な接続に関係のないデータフローを示します。LACP リンクについては、デバイス情報画面で LACP のサポートと設定が確認できます。

5. 右下のナビゲーション画面を使用して、マップ上の任意のエリアに移動することもできます。

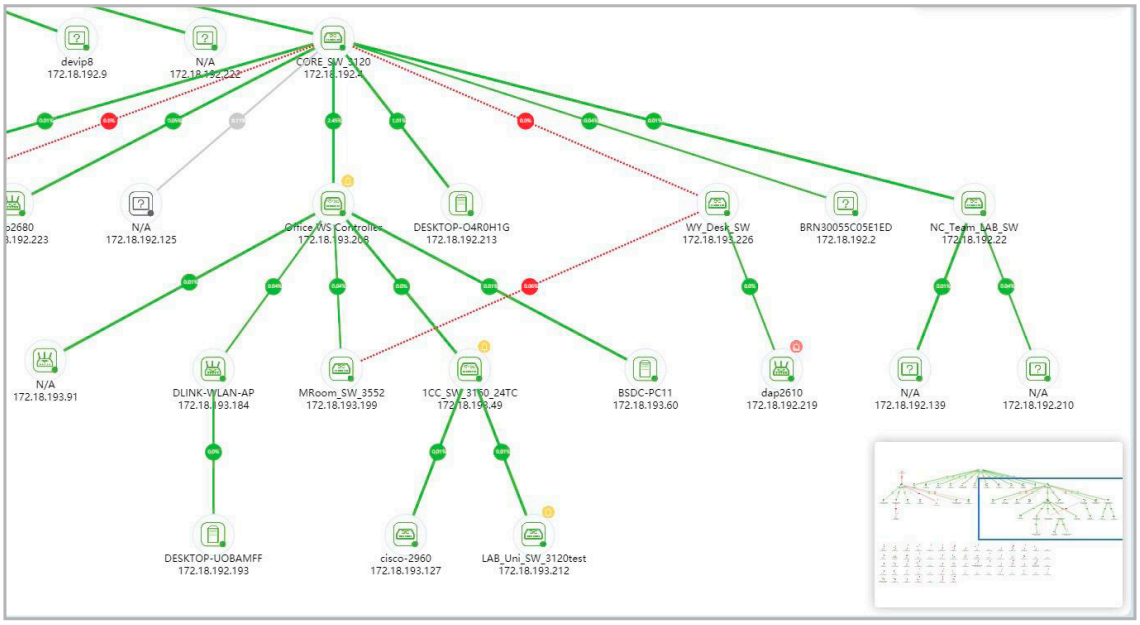


図 8-5　ナビゲーションペインの使用

トポロジビューの作成

1. **Monitoring > Topology Map** をクリックします。
2. 「+ Create Customized Topology」をクリックします。

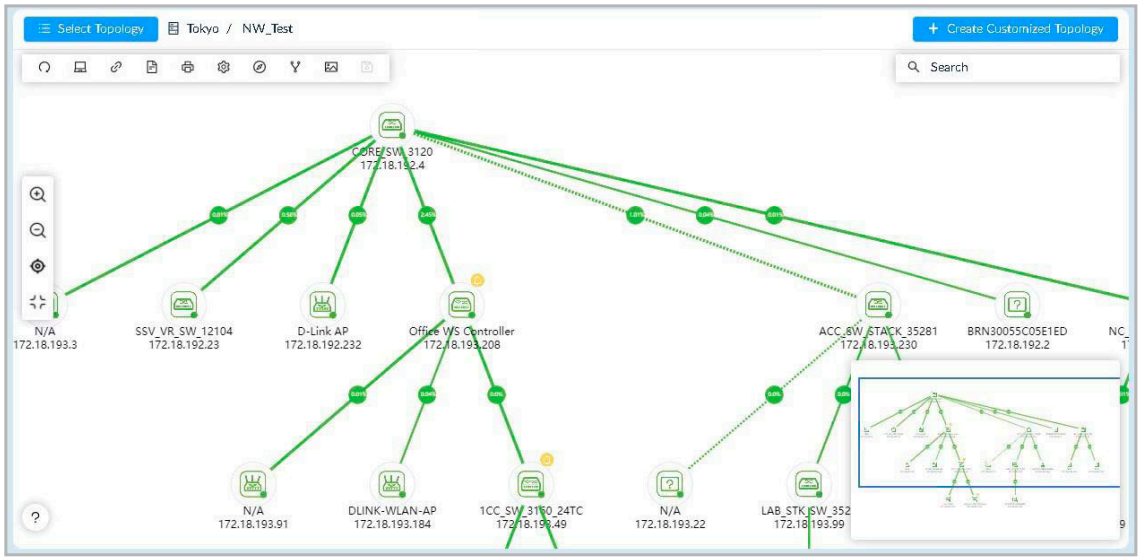


図 8-6　トポロジマップ

3. カスタムトポロジ作成画面が表示されます。

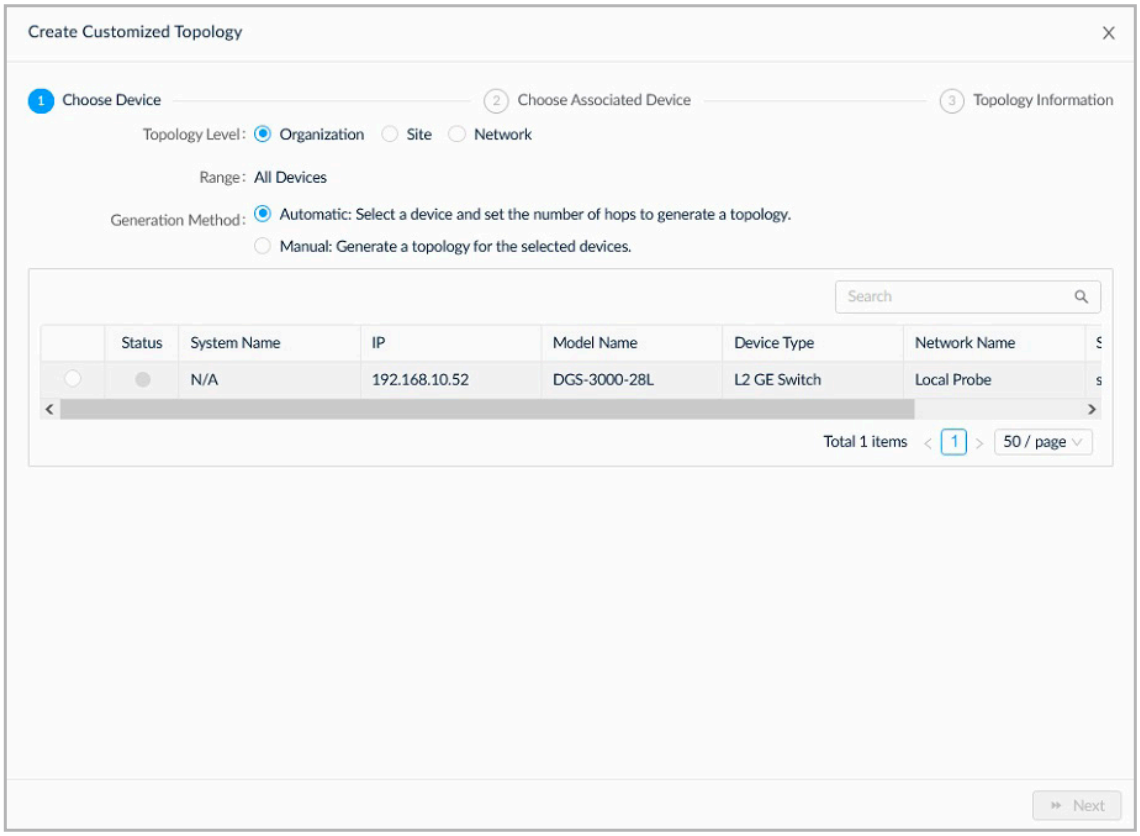


図 8-7　カスタムトポロジの作成（①デバイスの選択）

4. 「Topology Level」で、「Organization」「Site」「Network」のいずれかを選択します。
5. 「Generation Method」でトポロジを生成する方法を選択します。
   - 「Automatic（自動）」：選択したデバイスを基準デバイスとして、指定ホップ数に基づきトポロジを生成します。（初期値）
   - 「Manual（手動）」：トポロジに含めるデバイスを手動で指定します。
6. トポロジ生成方法で「Automatic」を選択した場合は、生成の基準となるデバイスを選択、「Manual」を選択した場合はトポロジに含める全てのデバイスを選択します。検索フィールドにキーワードを入力して特定のデバイスを検索することもできます。
7. 「>> Next」をクリックして、次の手順に進みます。
8. トポロジ生成方法で「Automatic」を選択した場合、「Hops of central device」のドロップダウンメニューをクリックして、基準デバイスからのホップ数（2-10）を指定します。指定ホップ数に基づき、他のデバイスが紐づくように設定されます。

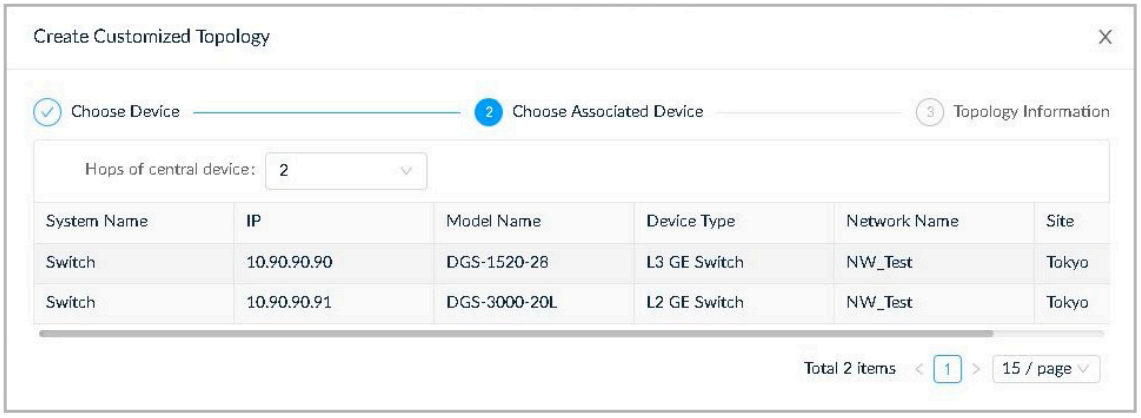


図 8-8　カスタムトポロジ（②関連デバイスの選択）

9. 「>> Next」をクリックして次の手順に進みます。前の画面に戻るには、「<< Previous」をクリックします。

10. トポロジ情報を設定します。

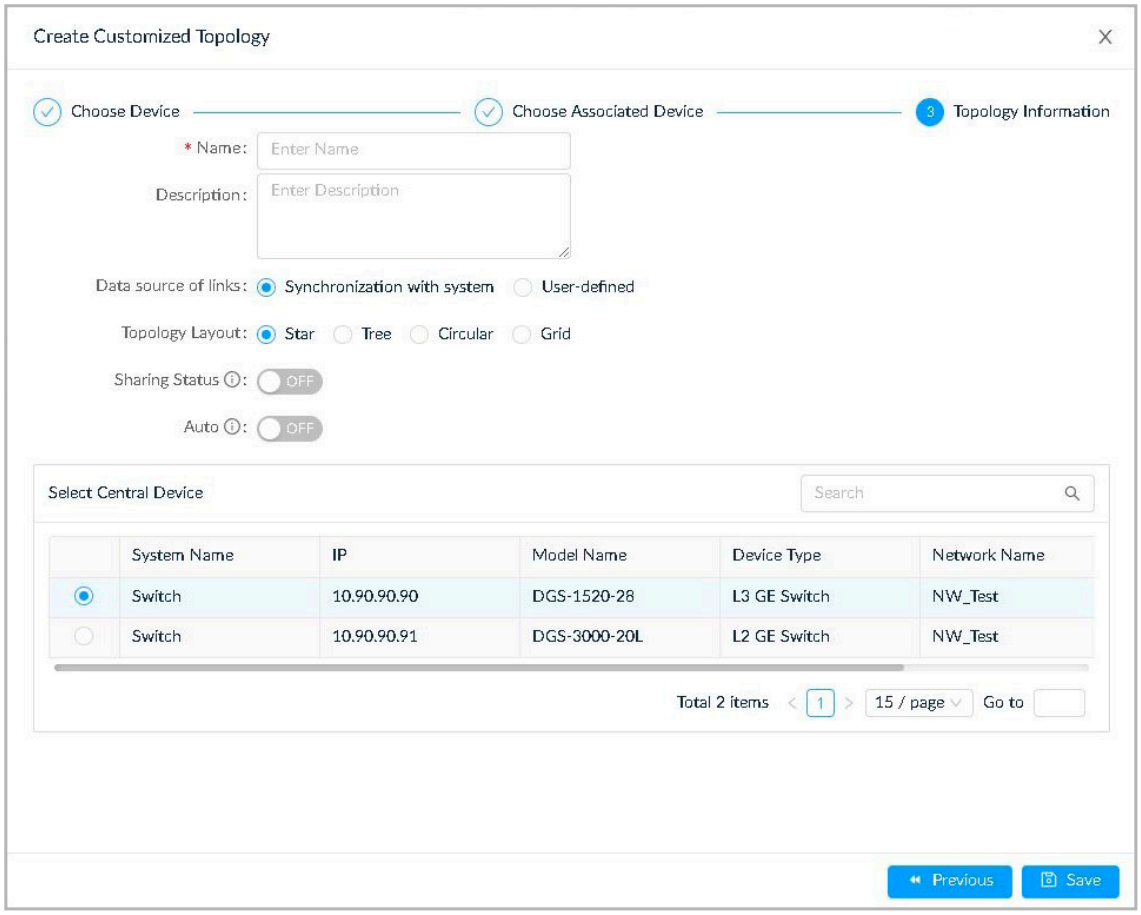


図 8-9　カスタムトポロジ（③トポロジ情報）

設定項目：

項目	説明
Name	トポロジマップの名前を入力します。
Description	マップを識別するための説明を入力します。
Data source of links	データリンクのソースを指定します。 • 「Synchronization with system（システムとの同期）」：本カスタムトポロジは、システムトポロジ（デフォルトのシステム定義トポロジ）と同じリンクデータを使用します。カスタムトポロジとシステムトポロジのリンク編集内容は、互いに同期されます。 • 「User-defined（ユーザ定義）」：本カスタムトポロジとシステムトポロジはそれぞれ異なるリンクデータを使用します。リンクの編集は互いに影響を与えません。
Topology Layout	トポロジの形のタイプを選択します。 • 選択肢：「Star（スター）」「Tree（ツリー）」「Circular（円形）」「Grid（グリッド）」
Sharing Status	スライドバーを「ON」に切り替えた場合、他の管理者に当該トポロジの表示 / 編集 / 削除のアクセス権が付与されます。 • 初期値：OFF
Auto	中心デバイスの指定方法を自動（「ON」）または手動（「OFF」）に指定します。「Auto」を「ON」に設定すると、トポロジ表示の際の中心デバイスはシステムにより自動的に選択されます。リンク数が最も多いデバイスが中心デバイスとして選択されます。 • 初期値：OFF
Select Central Device	上記の「Auto」オプションを無効化した場合、中心デバイスとして表示されるデバイスを選択します。

11. 「Save」をクリックして、トポロジマップを保存します。前の画面に戻るには、「<< Previous」をクリックします。

■ トポロジの編集・削除

作成されたカスタマイズトポロジは、編集または削除できます。

1. 「Select Topology」をクリックして、トポロジの一覧を表示します。カスタムトポロジのみ、変更または削除することが可能です。
2. 「Customized Topology」タブをクリックし、カスタムトポロジの一覧を表示します。

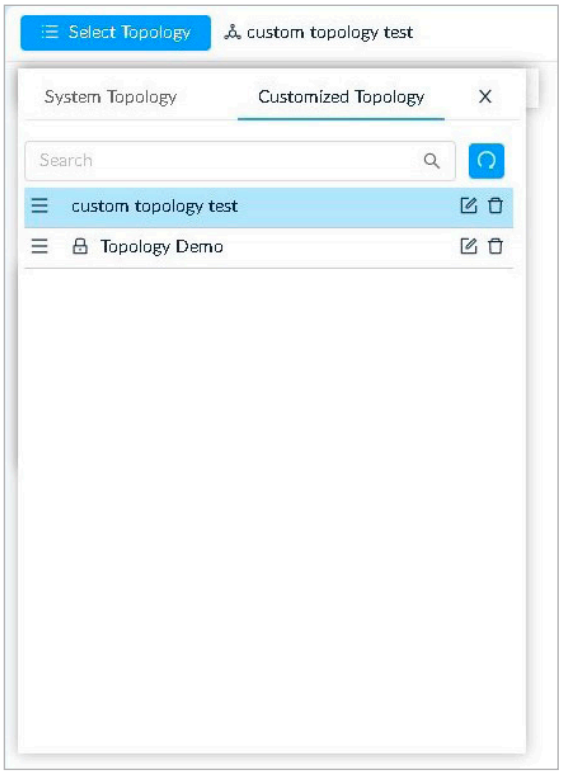


図 8-10　トポロジマップの選択

3. トポロジマップの （Edit）アイコンをクリックして、トポロジマップの設定を変更します。

   または、 （Delete）アイコンをクリックして、一覧からトポロジマップを削除します。

第 9 章　ラックグループの管理

管理者は多くの場面で、様々なデバイスが混在するネットワークにおけるデバイスの配置を体系的に把握・管理する必要があります。ラックビュー機能を使用すると、各区画のデバイス配置を効率的に表示・管理することができます。

本章では、以下のトピックについて説明します。

- 「ラックグループの追加」
- 「ラックグループの表示と変更」

ラックグループの追加

ラックはグループ毎に整理することができます。ラックおよびデバイス管理では、最初にラックグループの作成する必要があります。

1. **Monitoring > Rack View** をクリックし、ラックビューを表示します。
2. 「Group List」セクションで「Add Rack Group」をクリックします。

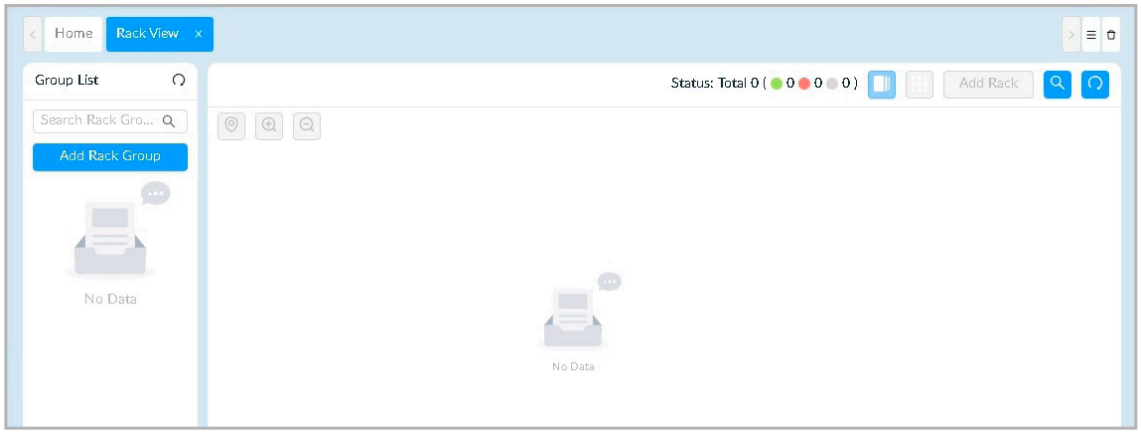


図 9-1　ラックビュー

3. 以下の画面で、グループの名前と説明を入力します。

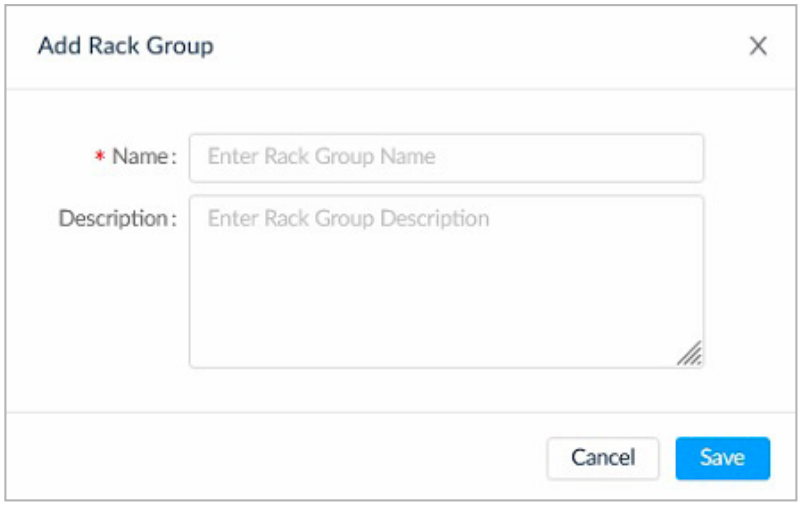


図 9-2　ラックグループの追加

4. 「Save」をクリックしてグループを作成します。設定をキャンセルするには、「Cancel」をクリックします。
5. 作成したグループラック画面が表示されます。
6. 次に、「Add Rack」をクリックして、デバイスを追加するためのラックを追加します。

7. ラックの設定を行います。

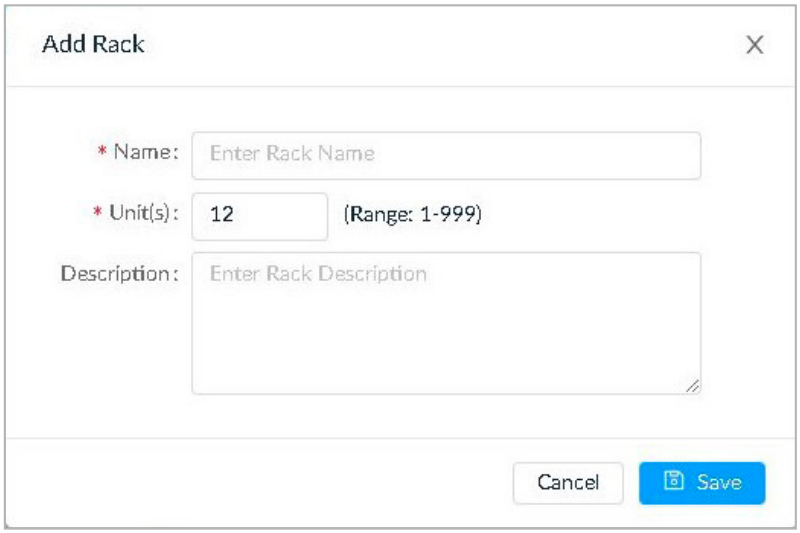


図 9-3　ラックグループへのラックの追加

設定項目：

項目	説明
Name	ラックを識別するための名前を入力します。
Unit(s)	ユニット数を入力します。「1」を指定した場合、1 デバイス分のスロットスペースが用意されます。 ・ 設定可能範囲：1-999
Description	ラックを識別するための説明を入力します。

8. 「Save」をクリックしてラックを作成します。設定をキャンセルするには、「Cancel」をクリックします。

9. ラックのスロットをクリックします。

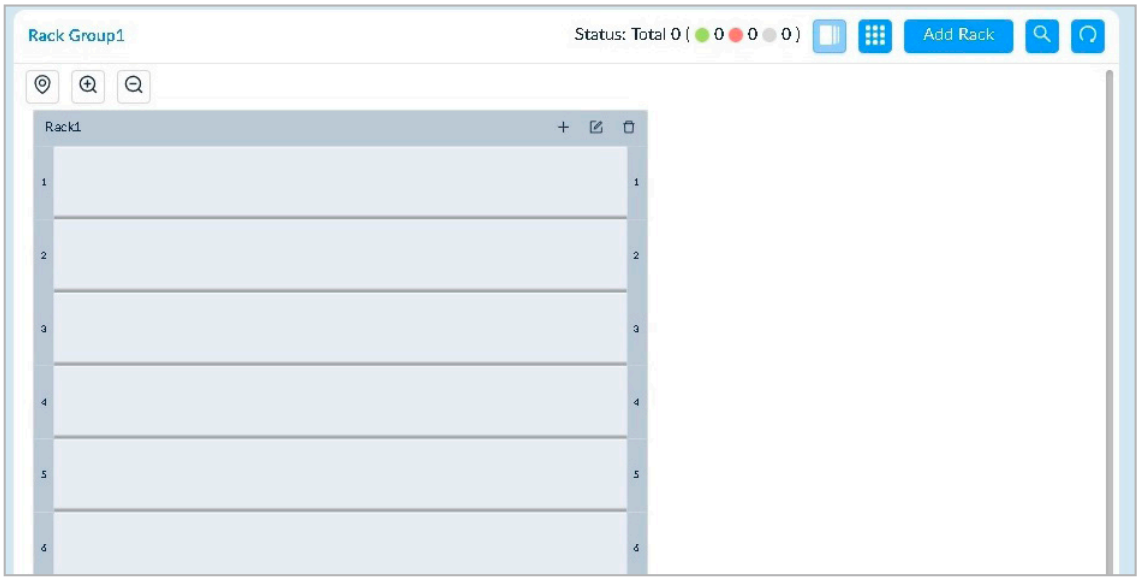


図 9-4　ラックグループ内のラック

10. スロットに追加するデバイスを選択し、「Save」をクリックします。

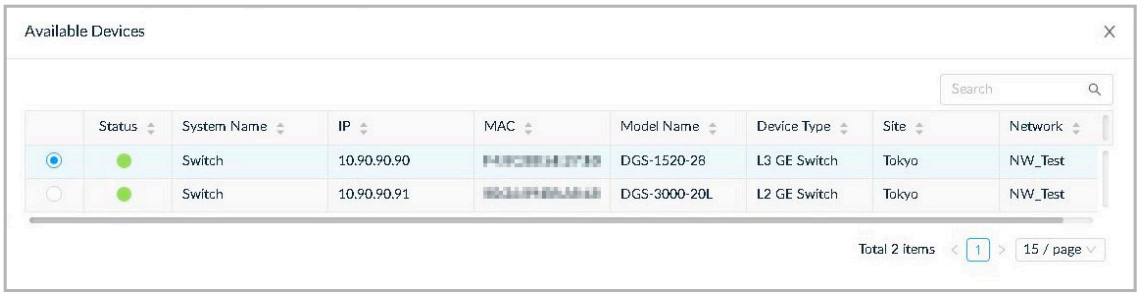


図 9-1　利用可能なデバイス

11. 選択したデバイスがラックの指定箇所に挿入されます。

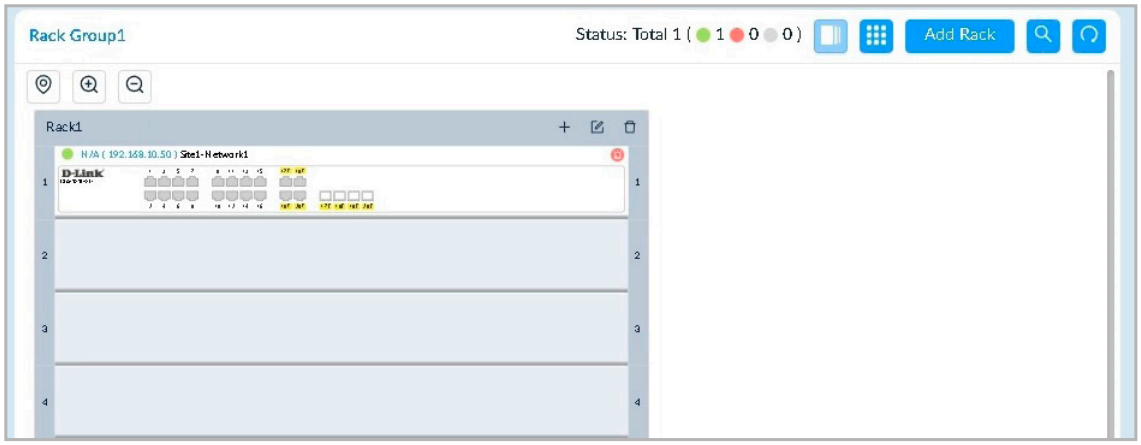


図 9-2　ラック内に配置されたデバイス

メモ　関連付けられたパネルテンプレートを持つデバイスのみ、ラックビューに表示させることができます。P.199 の「パネルテンプレートの生成」を参照してください。）

■ ラックの表示ツール

ラックグループ画面では、次のオプションを利用して表示領域を調整することができます。

- （Default）：表示倍率をデフォルトに設定します。
- （Zoom In）：表示を拡大します。
- （Zoom Out）：表示を縮小します。

■ ラックグループ内のラックを並べ替えるには：

ラックをドラッグ＆ドロップすることにより、ラックの位置を変更することもできます。

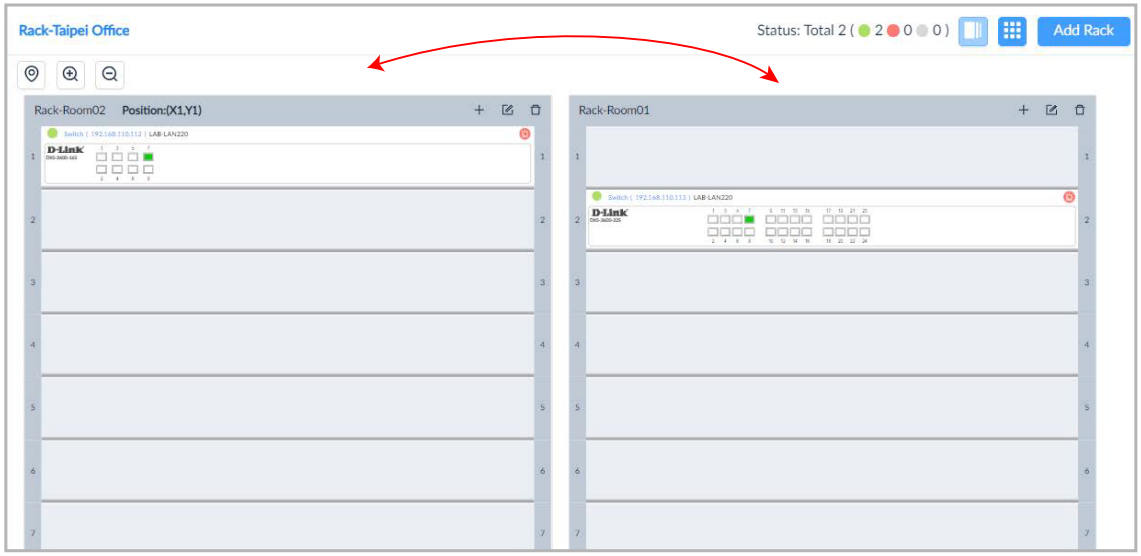


図 9-3　ラック

ラックグループの表示と変更

既存のラックグループの情報を変更します。

ラックグループの変更

1. **Monitoring > Rack View** をクリックします。
2. 左側の「Group List」にラックグループ一覧が表示されます。

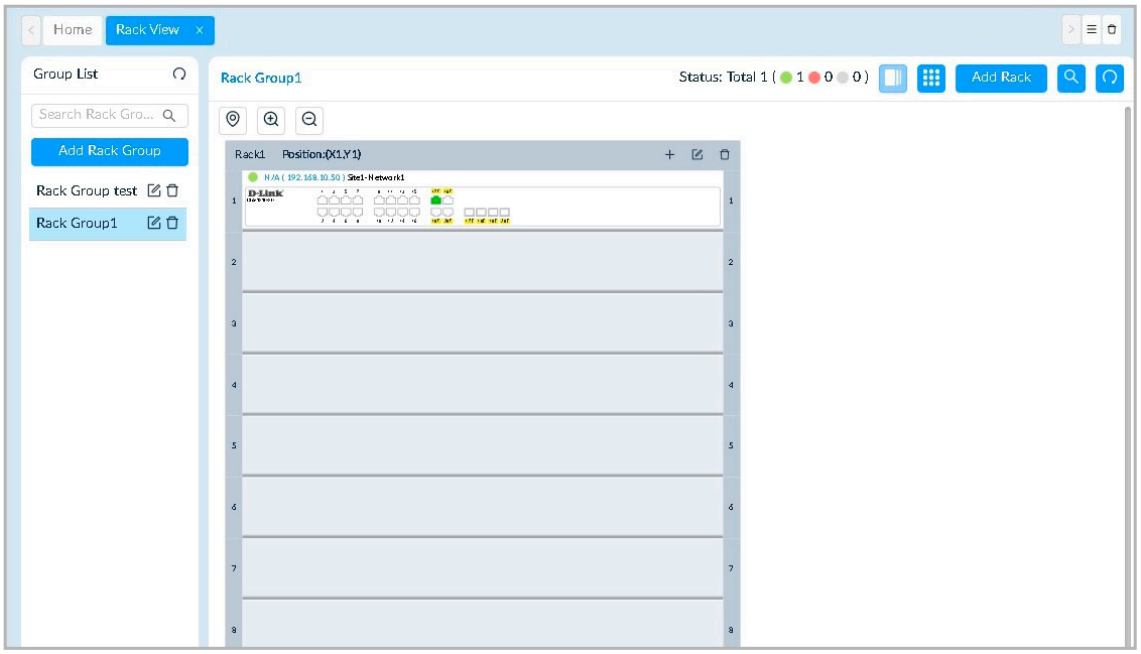


図 9-4　グループリストの表示

■ ラックグループ情報の変更

1. グループ設定を編集するには、「Group List」の （Edit）アイコンを選択します。以下の画面が表示されます。

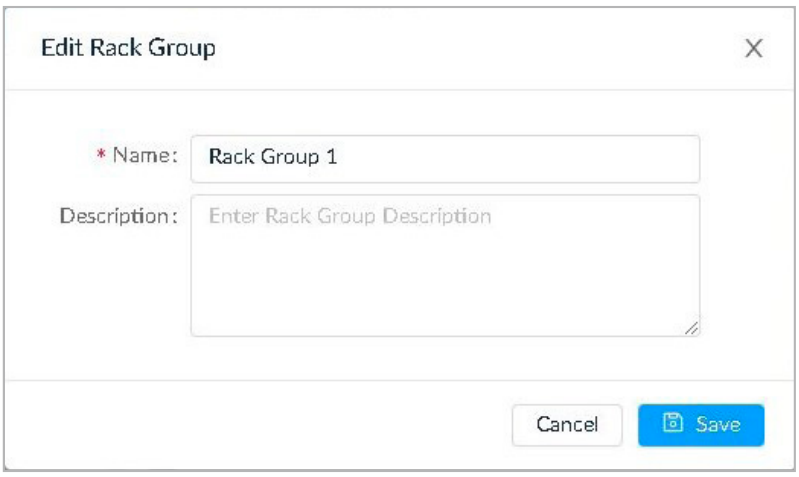


図 9-5　　ラックグループの編集

2. 「Save」をクリックして、設定内容を保存します。

■ ラックグループの削除

1. グループを削除するには、「Group List」の （Delete）アイコンを選択します。
2. 確認メッセージが表示されるので、「Yes」をクリックして削除を実行するか、「No」をクリックして操作をキャンセルします。

注意　ラックグループを削除すると、ラックグループ内のすべてのラックが同時に削除されます。

ラックの表示と変更

グループに含まれる既存のラックを変更および削除できます。

1. **Monitoring > Rack View** をクリックします。
2. 左側の「Group List」セクションにラックグループ一覧が表示されます。
3. 既存のグループを選択して、ラックグループを表示します。

■ ラック情報の変更

1. ラック情報を編集するには、ラック右上の（Edit Rack）アイコンをクリックして、ラック情報を変更します。

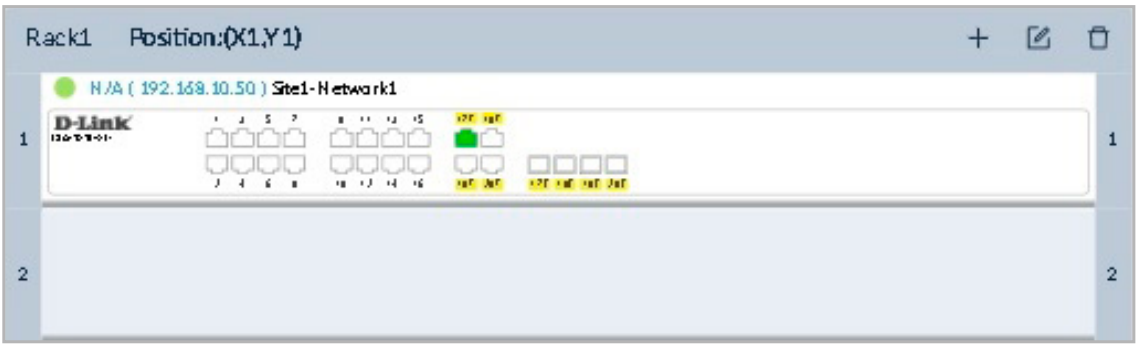


図 9-6　ラックの表示

2. 「Save」をクリックして、設定内容を保存します。

■ ラックの削除

1. グループからラックを削除するには、（Delete Rack）アイコンをクリックします。
2. 確認メッセージが表示されるので、「Yes」をクリックして削除を実行するか、「No」をクリックして操作をキャンセルします。

注意　ラックを削除すると、ラック内のすべてのデバイスが同時に削除されます。

ラック内のデバイスの表示と変更

ラックに含まれるデバイスの情報を表示、変更します。
ドラッグ & ドロップにより、ラック上のデバイスの位置を簡単に変更できます。

1. **Monitoring > Rack View** をクリックし、ラックビューを表示します。
2. 「Group List」のラックグループ一覧から既存のグループを選択し、ラックグループを表示します。

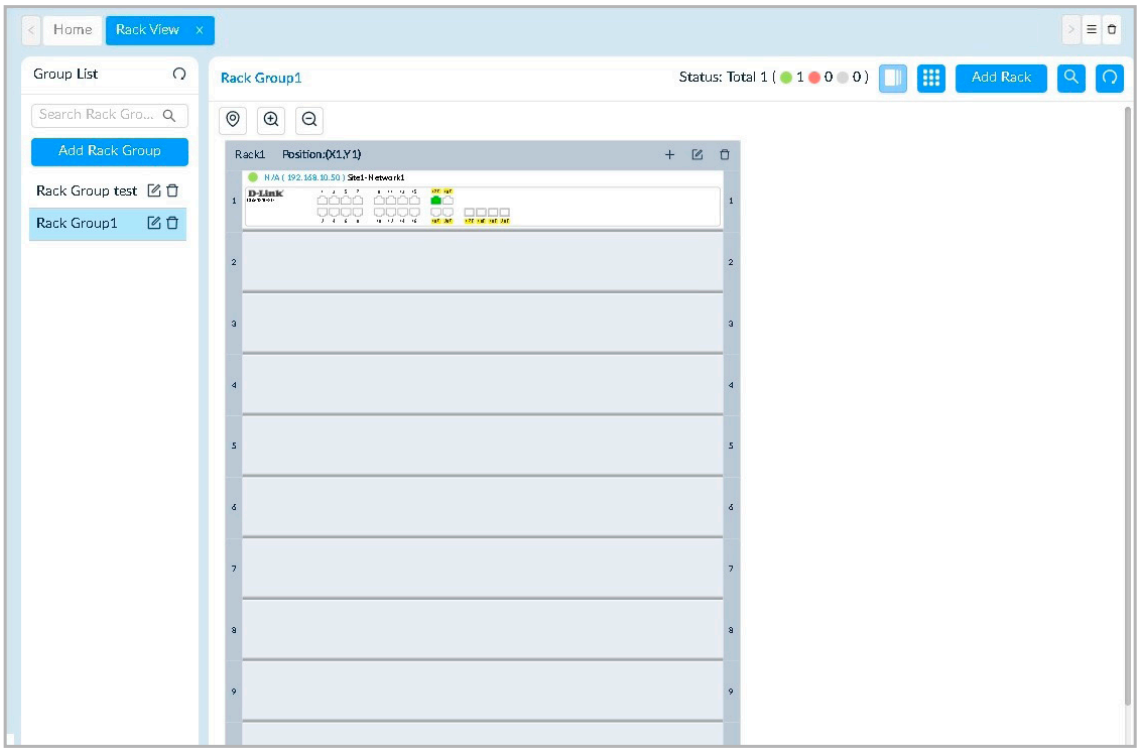


図 9-7　ラックグループの表示

3. ラックのビューから、デバイス領域をクリックします。以下のように、「View」アイコン、「Delete」アイコンが表示されます。

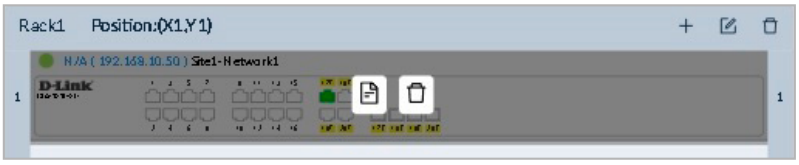


図 9-8　デバイススペースの選択

■ デバイス情報の表示

1. （View）アイコンをクリックし、デバイス情報を表示します。

以下は、D-Link スイッチの表示例です。

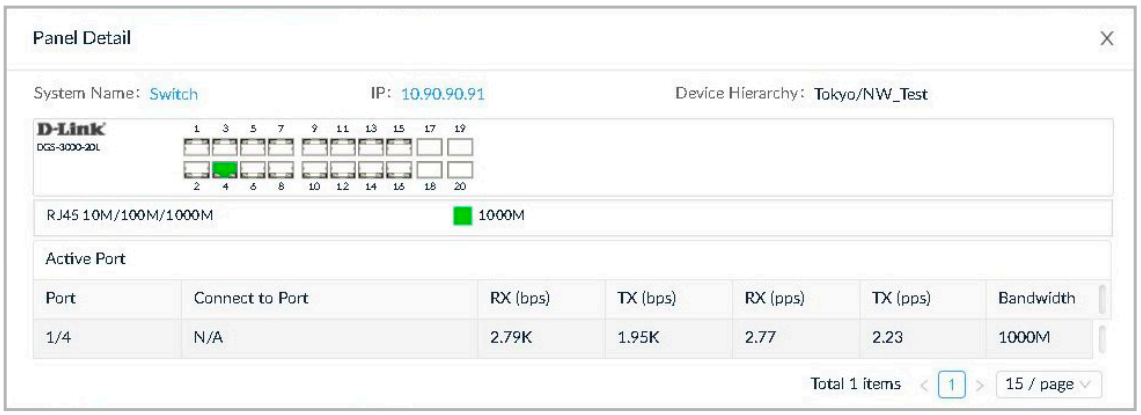


図 9-9　デバイス詳細の表示

2. 接続中（緑色）のポートの上にマウスオーバーすると、ポートの詳細が表示されます。

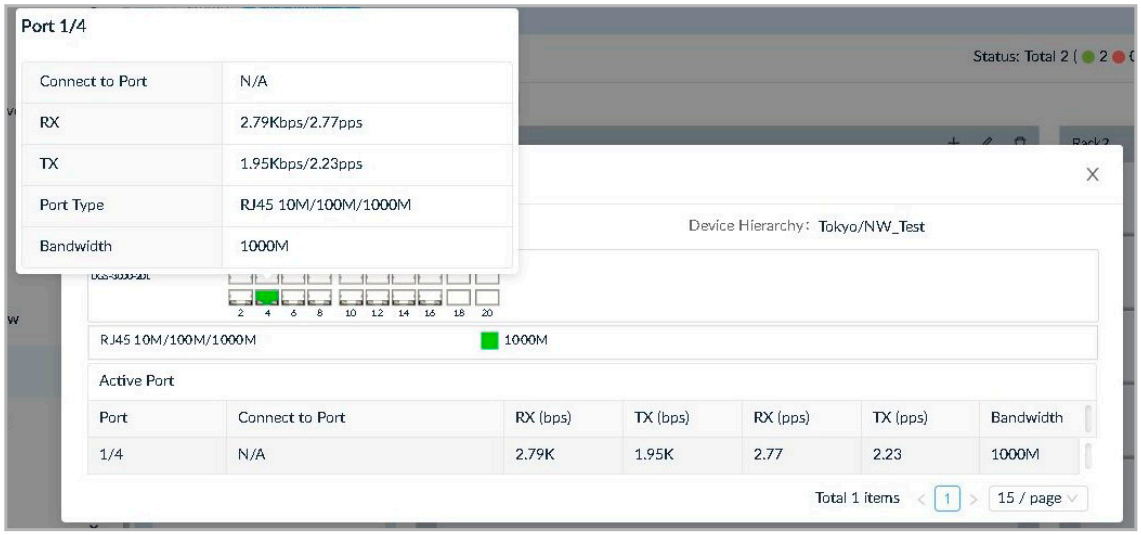


図 9-10　ポートの詳細の表示

3. IP アドレスにマウスオーバーし、「HTTP」「HTTPS」「Telnet」「SSH」のいずれかのプロトコルを選択して、デバイスの管理インタフェースを開くこともできます。

4. 「System Name（システム名）」をクリックすると、デバイス情報画面が開きます。

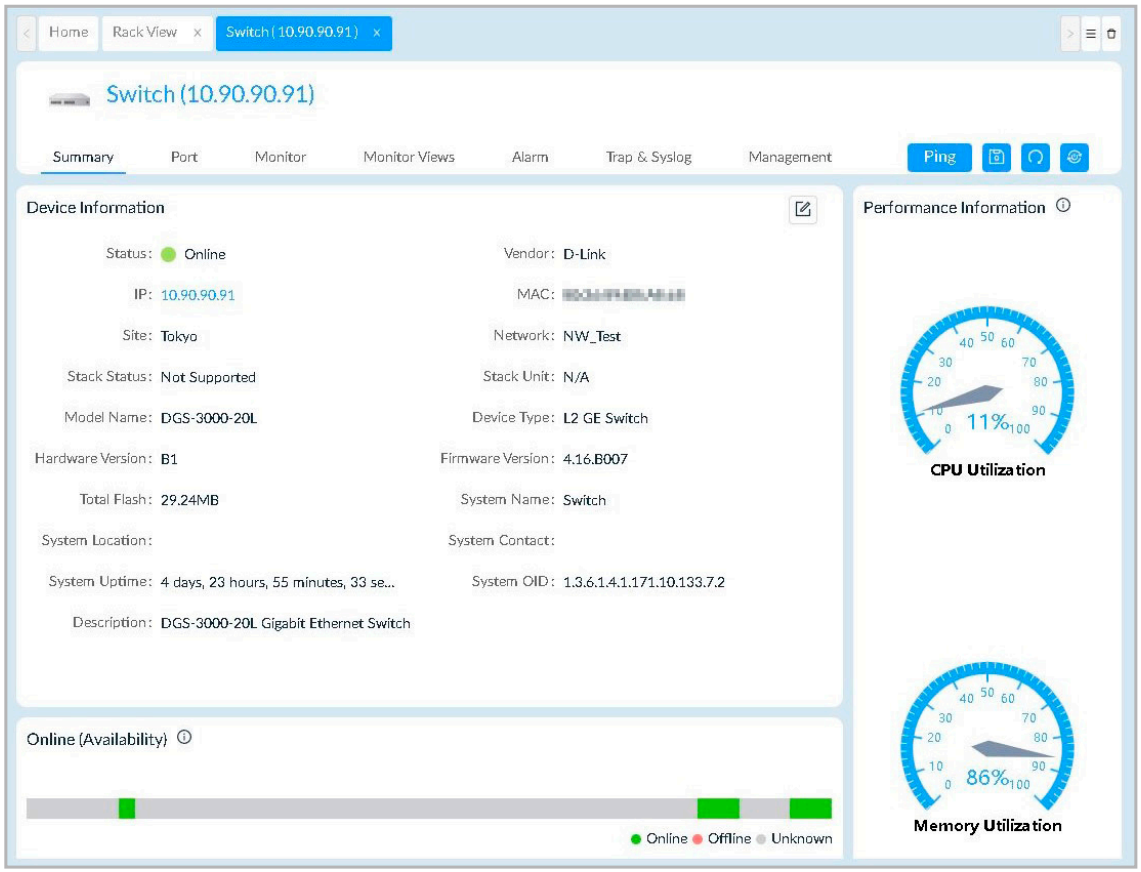


図 9-11　デバイス情報の表示

5. デバイス情報画面の詳細は、P.104 の「デバイス情報の変更」を参照してください。

■ デバイスの削除

1. ラックスペースからデバイスを削除するには、対称のデバイスをクリックした後、（Delete）アイコンをクリックします。

2. 確認メッセージが表示されるので、「Yes」をクリックして削除を実行するか、「No」をクリックして操作をキャンセルします。

■ デバイスの順序・割り当ての変更

ラックグループの表示画面で、デバイスのドラッグ & ドロップにより、デバイスの順序やラックへの割り当てを簡単に変更・整理することができます。

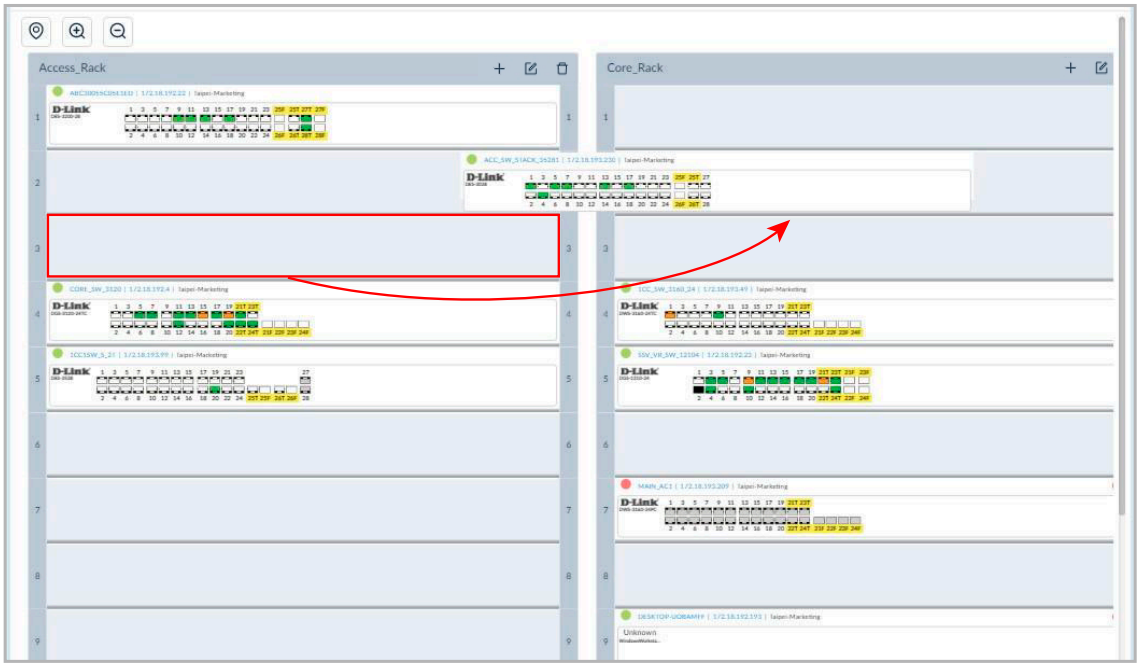


図 9-12　デバイスの割り当ての変更

第 10 章　sFlow の管理

sFlow のサンプリング技術により、高速スイッチネットワークにおけるネットワーク使用状況を可視化します。
sFlow エージェントから D-View8 に送信されたデータから、以下のような情報を取得したり、これらの使用用途に利用することができます。

- 送信元および宛先 /QoS/ アプリケーション / プロトコル / カンバセーションに関する詳細なリアルタイムデータ使用状況
- すべてのポートのトラフィックフロー
- トラフィックの問題や異常
- 潜在的なセキュリティ脅威として指定されたトラフィック
- パフォーマンス最適化に関する情報
- 課金とアカウンティング

D-View8 の sFlow 機能では、継続的な監視機能や、ネットワークパフォーマンスのレポートを利用することができます。

本章では、以下のトピックについて説明します。

- 「sFlow 監視の設定」
- 「sFlow 監視の管理」
- 「sFlow 構成テンプレートのカスタマイズ」
- 「sFlow ネットワークの監視」
- 「sFlow 監視結果の表示とエクスポート」

メモ　sFlow アナライザ機能、sFlow マッピング設定はエンタープライズ版のみサポートされます。

注意　D-View8 上の定義済み sFlow 設定は、DXS-3610 シリーズ、DXS-3400 シリーズではサポートされません。カスタムテンプレートや CLI、デバイス側の設定を利用して sFlow 設定を行い、sFlow ダッシュボードやアナライザを利用することは可能です。

sFlow 監視の設定

1. **Monitoring > Device View** をクリックし、「Device View」画面を表示します。
2. 「Managed」タブをクリックし、「Switch-All」ドロップダウンメニューから「sFlow」を選択します。

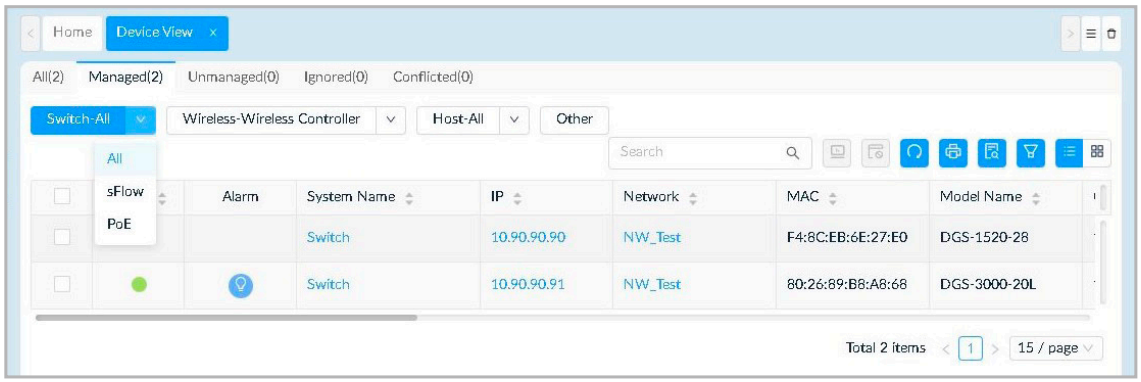


図 10-1　デバイスビュー（管理タブ）

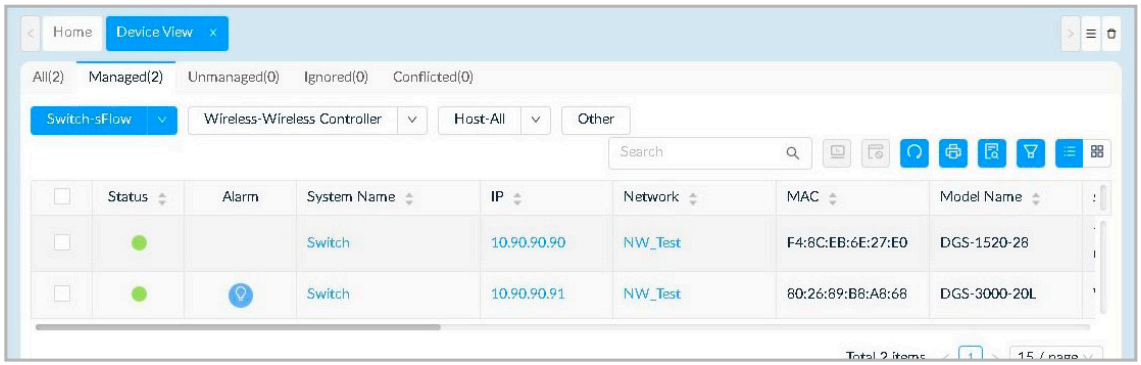


図 10-2　デバイスビュー（管理タブ /Switch-sFlow 選択）

3. 「System Name」のリンクをクリックして、デバイス情報画面を表示します。

4. 「Management」タブをクリックして、デバイスの sFlow 設定を表示します。

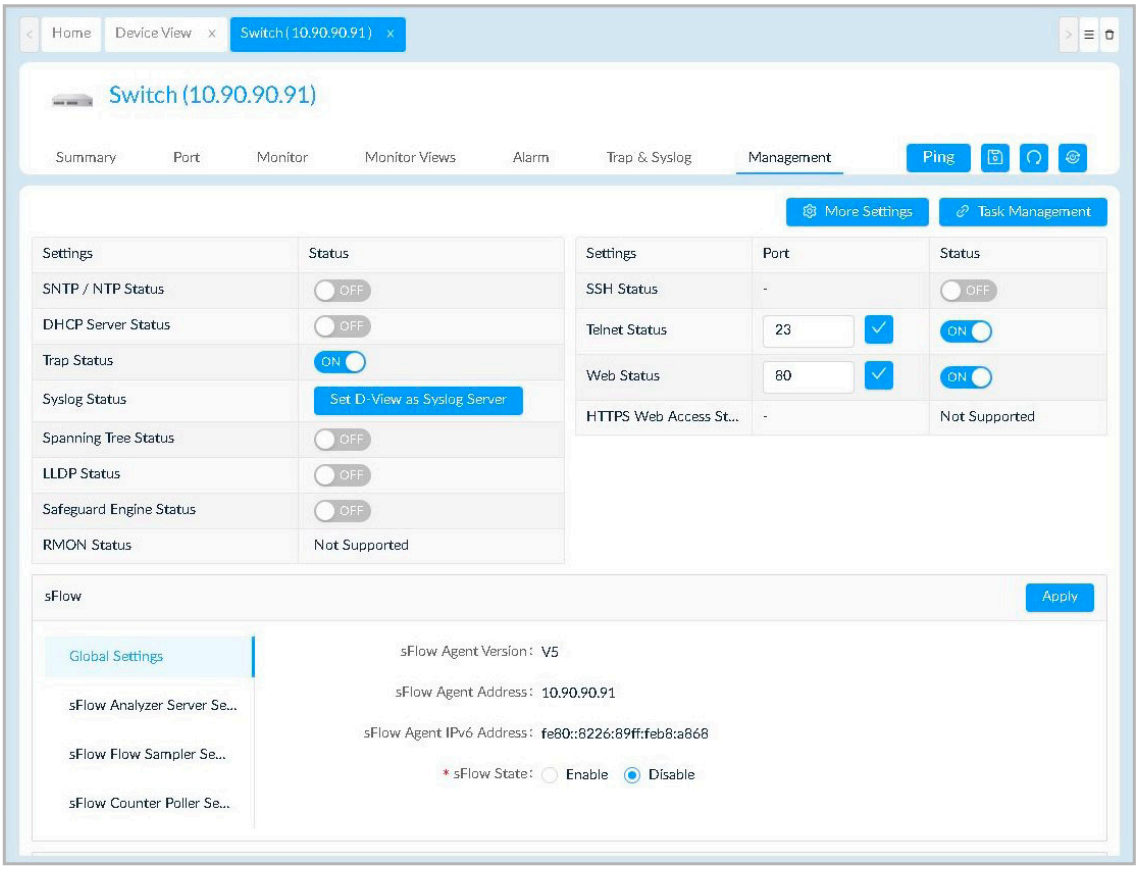


図 10-3　デバイス詳細画面（管理タブ）

メモ　デバイスの種類により、sFlow 機能のサポート可否および設定可能な項目が異なります。デバイスが sFlow に対応し、D-View8 管理画面から sFlow 設定を構成可能な場合でも、sFlow アナライザ機能を利用するにはエンタープライズ版ライセンスが必要です。（sFlow アナライザ機能については、P.195 の「sFlow ネットワークの監視」を参照してください。）

グローバル設定

5. 「sFlow」セクションで「Global Settings」タブを選択し、sFlow のグローバルステータスを設定します。

(1)　sFlow 設定を有効化するには、「sFlow State」で「Enable」を選択します。

図 10-4　sFlow グローバル設定

sFlow アナライザサーバの設定

6. 「sFlow Analyzer Server Settings」タブをクリックし、アナライザサーバの設定を行います。

(1) 「+ Add Analyzer Server」をクリックします。

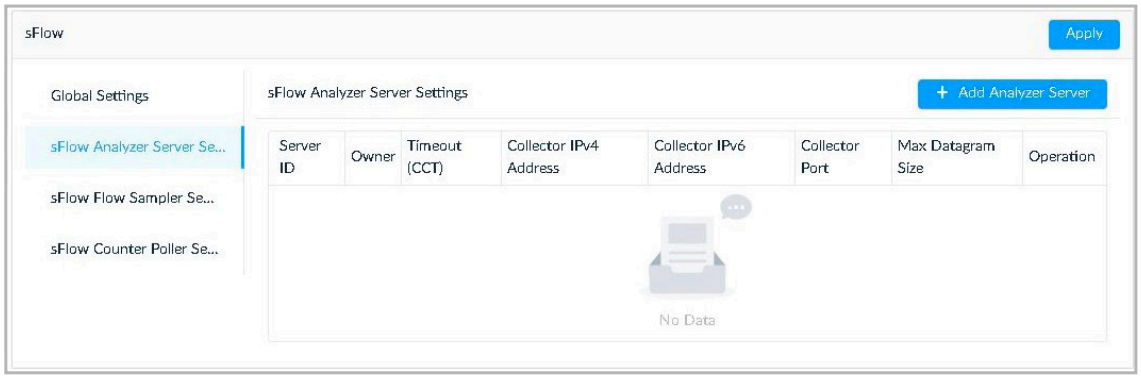


図 10-5　sFlow アナライザサーバの設定

(2) 以下の画面で、アナライザサーバの情報を入力します。

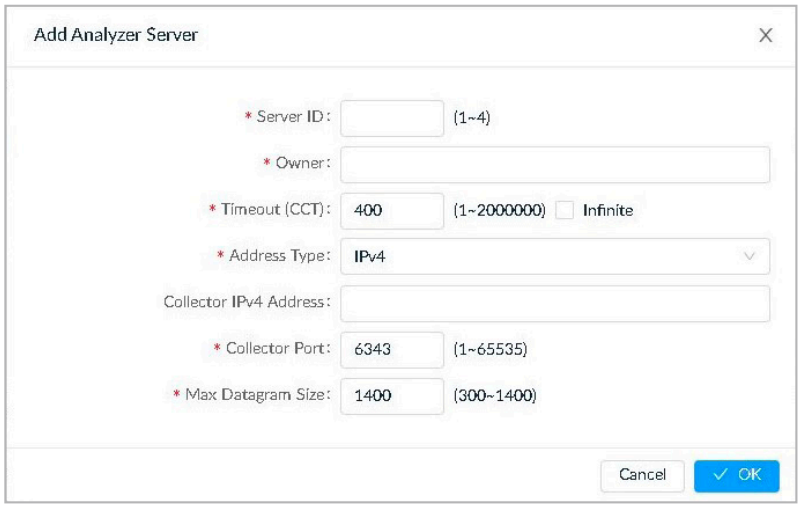


図 10-6　アナライザサーバの追加

設定項目：

項目	説明
Server ID	エントリに ID を割り当てます。
Owner	デバイスが sFlow データを送信するために使用する宛先アナライザ名を入力します。通常、この設定は D-View8 Probe サーバ IP となります。
Timeout (CCT)	コレクタのタイムアウト値を入力します。指定期間、コレクタ設定が有効となります。「Infinite」にチェックを入れると、タイムアウト設定が無効になります。
Address Type	ドロップダウンメニューをクリックして、アドレスタイプを指定します。 • 選択肢：「IPv4」「IPv6」
Collector IPv4/IPv6 Address	データ収集用のコレクタ IP アドレスを入力します。通常、この設定は D-View8 Probe サーバの IP アドレスとなります。
Collector Port	コレクタ IP アドレスに対応するポート番号を入力します。
Max Datagram Size	データパケットの最大データグラムサイズを指定します。

メモ　デバイスの種類により、sFlow 機能でサポートされる設定は異なります。

(3) 「OK」をクリックして、エントリを追加します。

sFlow フローサンプラの設定

7. 「sFlow Flow Sampler Settings」タブをクリックし、フローサンプリング方式でデータを収集するための設定を行います。

(1) 「+ Add Flow Sampler Port」をクリックします。

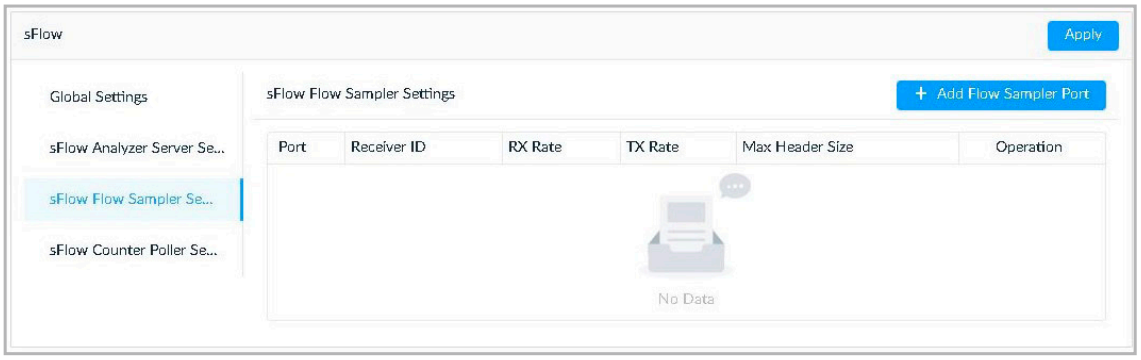


図 10-7　sFlow サンプラポートの設定

(2) 以下の画面で、sFlow サンプラポートの設定を行います。

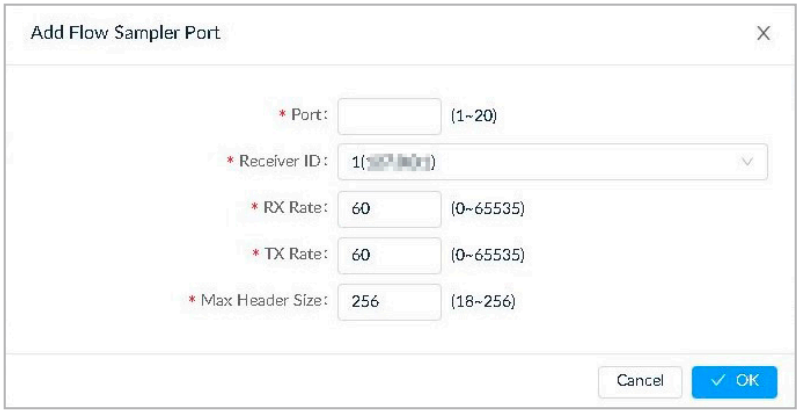


図 10-8　sFlow サンプラポートの追加

設定項目：

項目	説明
Port	sFlow データを送信するデバイスのポート番号を入力します。
Instance	各サンプリングポートのインスタンス番号を入力します。
Receiver ID	ドロップダウンメニューをクリックして、設定済みのアナライザサーバを選択します。アナライザサーバの設定については、前の手順を参照してください。
Mode	インバウンドトラフィックまたはアウトバウンドトラフィックのいずれかを選択します。
TX/RX Rate	サンプリングレートを入力します。
Max Header Size	サンプリングされたパケットから sFlow データグラムにコピーされる最大バイト数を入力します。

メモ　デバイスの種類により、sFlow 機能でサポートされる設定は異なります。

注意　DGS-1510/DGS-1520 シリーズでは、「Outbound」モードはサポートされません。

(3) 「OK」をクリックして、エントリを追加します。

sFlow カウンタポーラの設定

8. 「sFlow Counter Poller Settings」タブをクリックします。カウンタサンプリング方式でデータを収集するための設定を行います。

(1) 「+ Add Counter Poller Port」をクリックします。

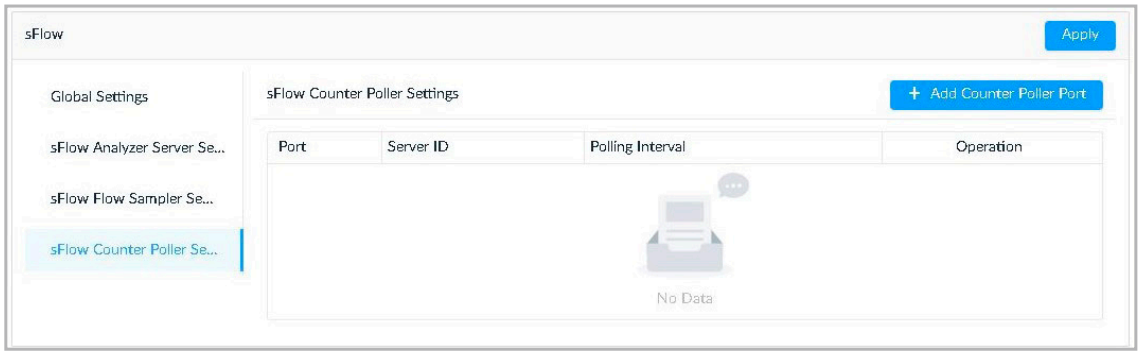


図 10-9　sFlow カウンタポーラの設定

(2) 以下の画面で、カウンタポーラポートの設定を行います。

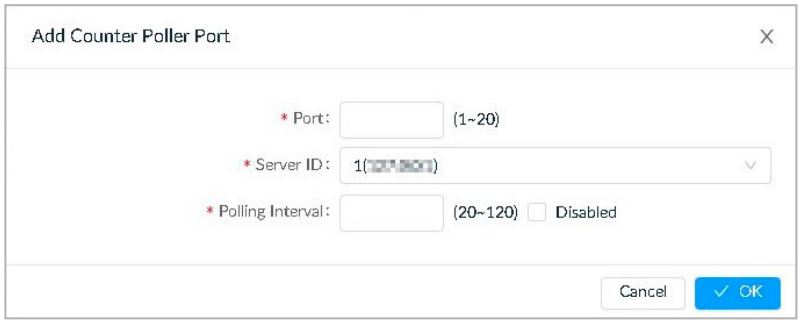


図 10-10　カウンタポーラポートの追加

項目	説明
Port	カウンタサンプルを送信するデバイスのポート番号を入力します。
Server ID	ドロップダウンメニューをクリックして、設定済みのアナライザサーバを選択します。アナライザサーバの設定については、前の手順を参照してください。
Polling Interval	カウンタポーラーサンプルの間隔となるカウンタポーリング間隔を設定します。

メモ　デバイスの種類により、sFlow 機能でサポートされる設定は異なります。

(3) 「OK」をクリックして、エントリを追加します。

9. 「sFlow」セクション右上の「Apply」をクリックして、新しい sFlow 設定を保存します。

sFlow 監視の管理

■ sFlow 監視設定の編集・削除

1. **Monitoring > Device View** をクリックし、「Device View」画面を表示します。
2. 「Managed」タブをクリックし、「Switch-All」ドロップダウンメニューから「sFlow」を選択します。
3. 「System Name」のリンクをクリックして、デバイス情報画面を表示します。
4. 「Management」タブをクリックして、デバイスの sFlow 設定を表示します。

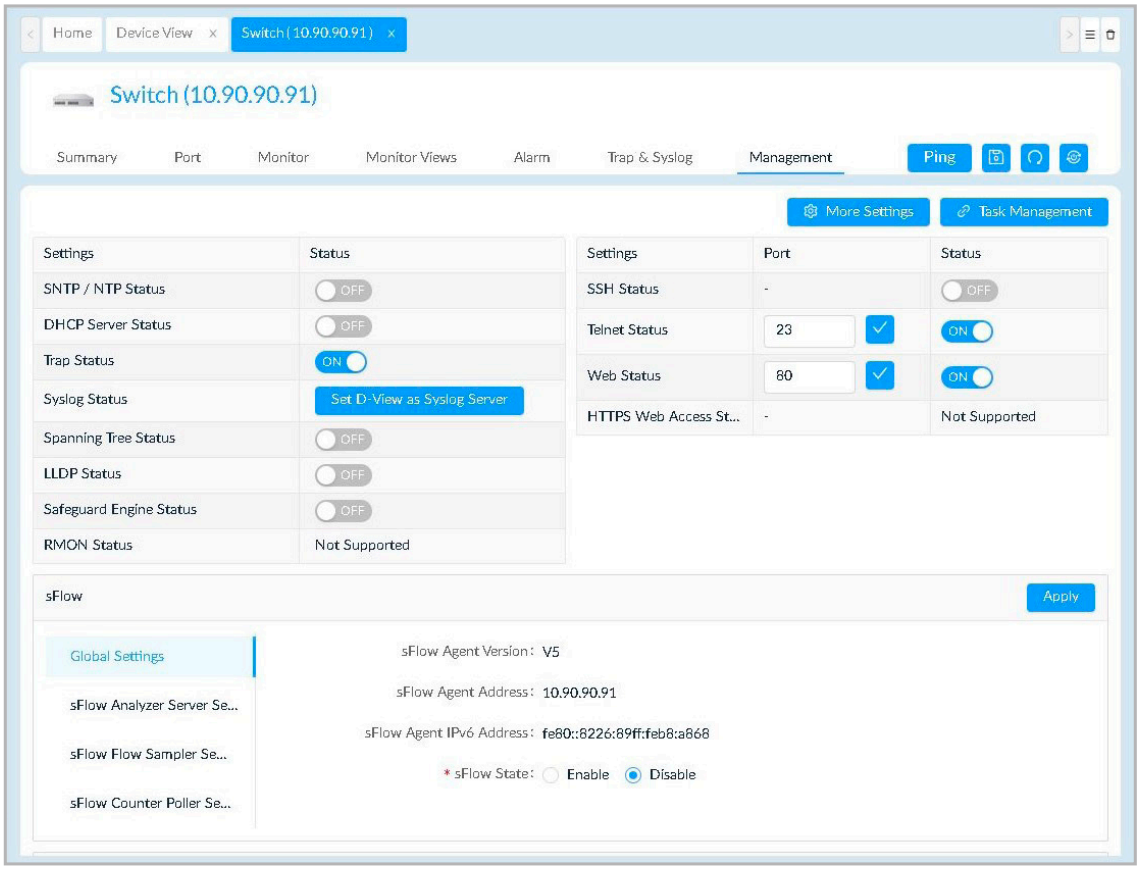


図 10-11　デバイス詳細画面（管理タブ）

5. 「sFlow」セクションで、「sFlow Analyzer Server Settings」をクリックします。

図 10-12　sFlow アナライザサーバの設定

6. 定義済みのサーバ一覧が表示されます。「Operation（操作）」列で以下のオプションを使用できます。
   - （Edit）アイコンをクリックすると、既存の設定を変更できます。
   - （Delete）アイコンをクリックすると、リストからエントリを削除できます。「Yes」をクリックし、削除処理を実行します。

メモ　「sFlow Flow Sampler Settings」と「sFlow Counter Poller Settings」タブにおいても、同様に設定を変更することができます。

sFlow 構成テンプレートのカスタマイズ

sFlow 設定をサポートするデバイスに対し、既定のテンプレートや構成設定が利用できない場合に、デバイスへの設定・管理を簡素化するためのテンプレートを作成し、sFlow 設定に役立てることが可能です。

1. **Templates > Configuration Template** をクリックし、「Configuration Template」タブを選択します。

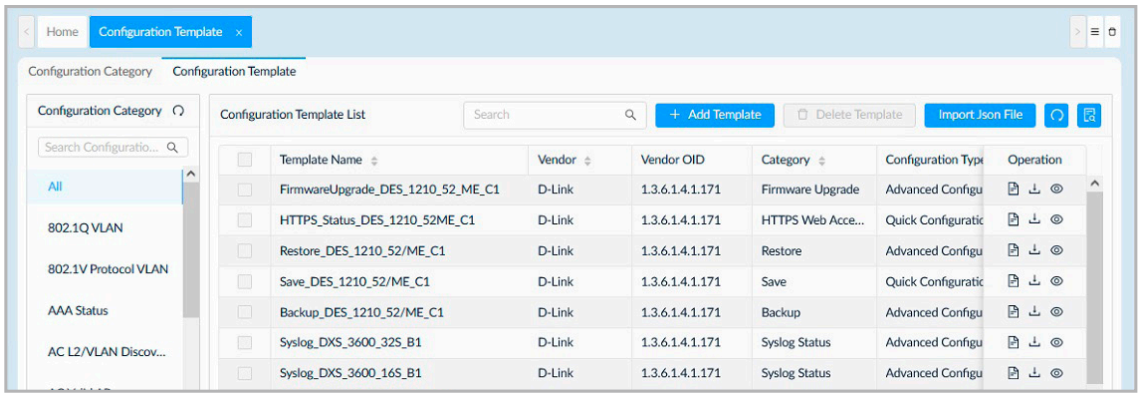


図 10-13　設定テンプレート

2. 左側ツリーより「v2_sFlow」カテゴリなどを選択し、「+ Add Template」をクリックします。以下の画面が表示されます。

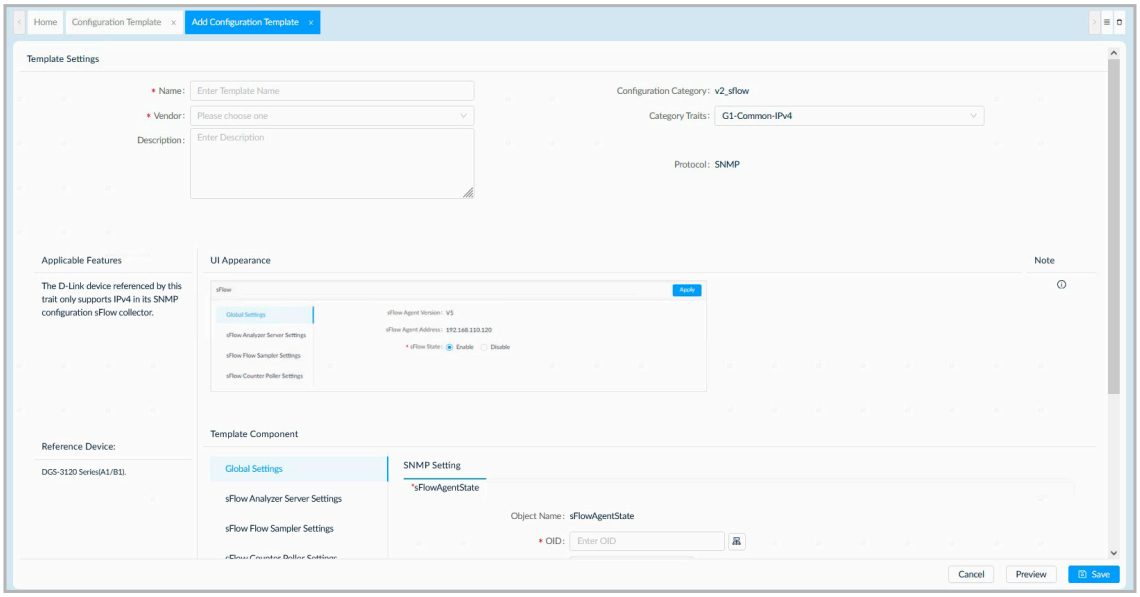


図 10-14　テンプレート設定

「Add Configuration Template」画面で、テンプレートを設定します。
設定画面用に、各項目のパラメータを調整します。

3. テンプレートの設定が完了したら、「Preview」をクリックして実際の表示内容を確認します。
4. 「Cancel Preview」をクリックして、設定画面に戻ります。
5. 「Save」をクリックしてテンプレートを保存します。設定をキャンセルするには、「Cancel」をクリックします。
6. sFlow 設定ンテンプレートの作成後、デバイステンプレートに関連付けて sFlow パラメータを設定する必要があります。（**Templates > Device Template**）。デバイステンプレートについては、P.198 の「デバイステンプレートの生成」を参照してください。

sFlow ネットワークの監視

sFlow 機能のパケットサンプリングにより、スイッチネットワークの監視や、ネットワーク使用状況とパフォーマンス監視のためのデータ収集を行います。sFlow 機能が適切に設定されると、パケットサンプリングまたはカウンタサンプリングを使用して、収集されたデータからのネットワークの監視と分析が開始されます。

メモ　本機能はエンタープライズライセンスでのみサポートされます。

■ sFlow 監視の結果表示

1. **Monitoring > sFlow Analyzer** をクリックし、sFlow アナライザを表示します。
2. パケットサンプリングを設定したポートのデバイスが左側ツリーに表示されます。利用可能なデータソースがない場合、最初に sFlow を設定し、サポートされるデバイスで sFlow サンプリングを有効にする必要があります。P.188 の「sFlow 監視の設定」及び P.194 の「sFlow 構成テンプレートのカスタマイズ」を参照してください。

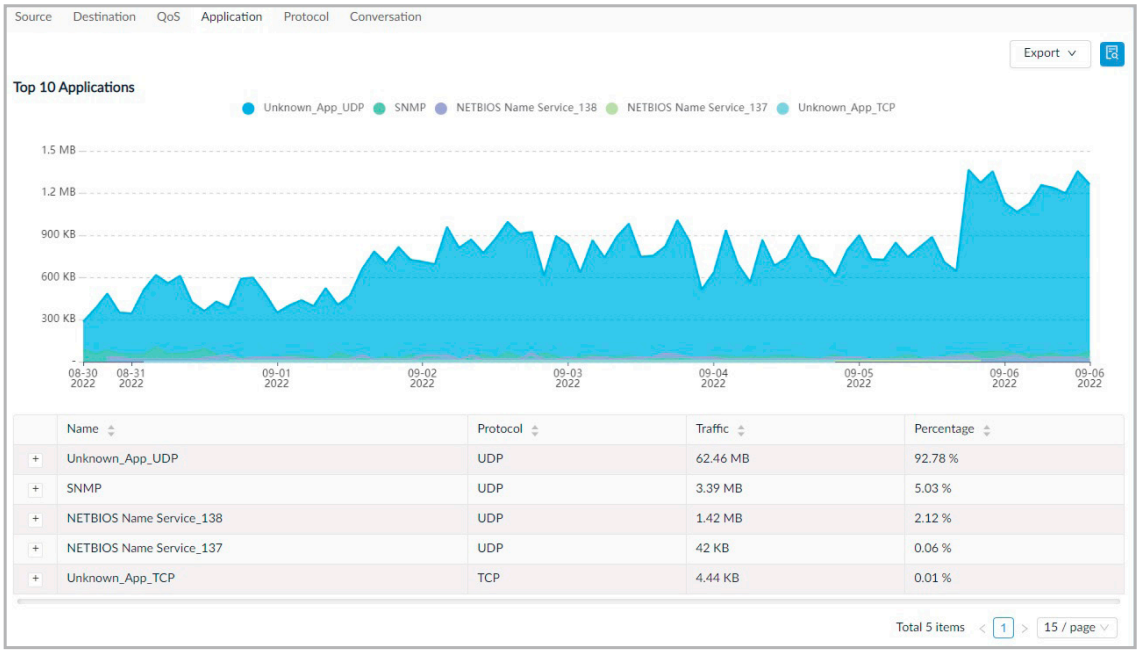


図 10-15　sFlow アナライザ

3. 以下のタブから、各カテゴリの sFlow 統計を確認できます。
   - Source
   - Destination
   - QoS
   - Application
   - Protocol
   - Conversation

■ **高度な検索**

4. 「Advanced Query」アイコンをクリックすると、フィルタ条件により、表示する時間間隔や期間などを設定できます。
以下のようなフィルタ項目を指定することもできます。カテゴリにより利用可能なオプションは異なります。

- 「Time Interval」：カウンタサンプリングの間隔を指定します。
- 「Time Period」：データ表示期間を指定します。
- 「sFlow Direction」：ポートを通過するパケットの方向（「Ingress」「Egress」「Ingress and Egress」）を選択します。
- 「Resolve DNS」：スライドバーをクリックして、DNS 解決オプションを有効または無効にします。
- 「Show Type」：ドロップダウンメニューをクリックして、表示する識別情報の種類（IP アドレスまたは MAC アドレス）を指定します。

「Search」をクリックしてクエリを開始します。「Clear」をクリックすると、初期値に戻ります。

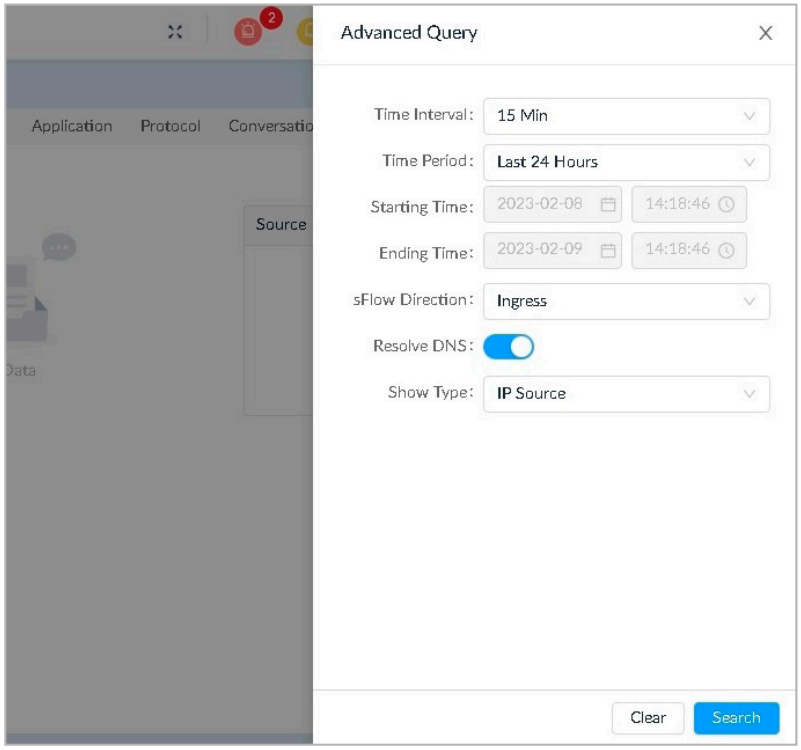


図 10-16　高度な検索

sFlow 監視結果の表示とエクスポート

sFlow 情報の条件を指定し、モニタリングソースを介して送信されたトラフィックを含む sFlow の結果を取得・分析できます。

メモ　本機能はエンタープライズライセンスでのみサポートされます。

■ sFlow 監視の結果表示

1. **Monitoring > sFlow Analyzer** をクリックし、sFlow アナライザを表示します。

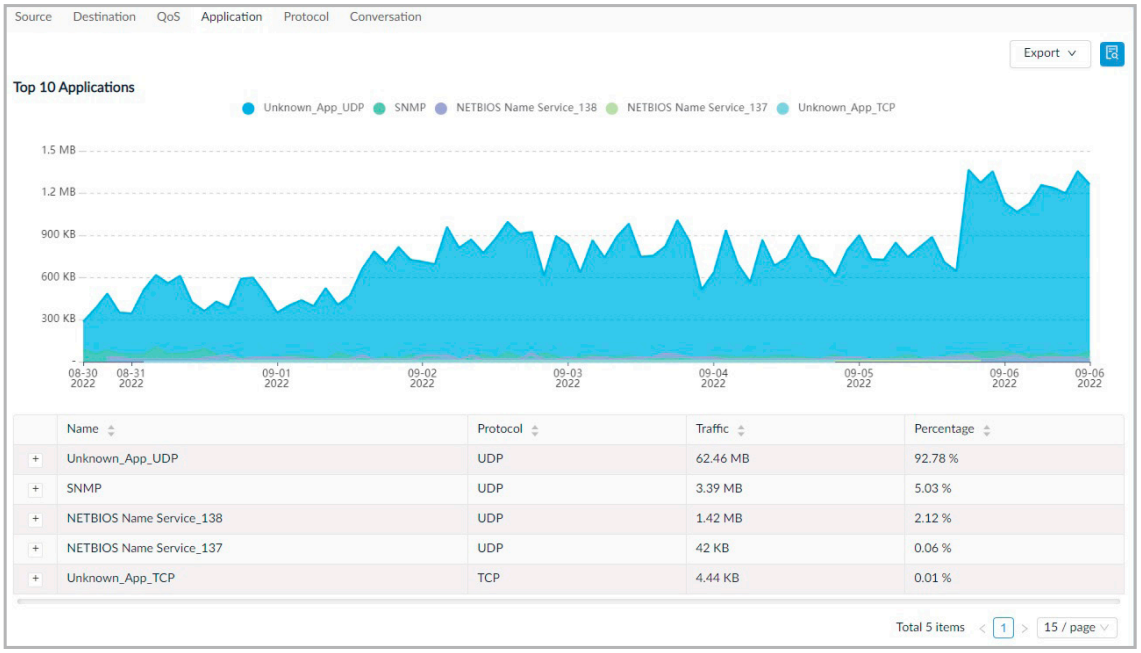


図 10-17　sFlow アナライザ

2. 以下のタブから、各カテゴリの sFlow 統計を確認できます。

項目	説明
Source	トラフィック量に基づく送信元デバイス統計情報が表示されます。デフォルトでは、上位 10 件の送信元デバイスに関する情報を表示します。 IP アドレスまたは MAC アドレスは、定義されたエイリアスで変換可能です（**System > Basic Settings > sFlow Settings** に移動し、「IP Alias Mapping」または「MAC Address Mapping」タブを選択します）。
Destination	トラフィック量に基づく宛先デバイス統計情報が表示されます。デフォルトでは、上位 10 件の宛先デバイスに関する情報を表示します。 宛先を IP アドレスまたは MAC アドレスで表示するように選択することもできます。IP アドレスまたは MAC アドレスは、設定されたエイリアスで変換可能です（**System > Basic Settings > sFlow Settings** に移動し、「IP Alias Mapping」または「MAC Address Mapping」タブを選択します）。
QoS	トラフィック量に基づく QoS 統計情報が表示されます。上位 10 件の QoS を表示します。 DSCP は sFlow 設定で定義されます（**System > Basic Settings > sFlow Settings** に移動し、「DSCP Mapping」タブを選択します）。
Application	トラフィック量に基づくアプリケーション統計情報が表示されます。上位 10 件のアプリケーションに関する情報が表示されます。 アプリケーションとエイリアス間のマッピングについては、に移動し、「Application Mapping」タブを選択し設定します。
Protocol	トラフィック量に基づくプロトコル統計情報が表示されます。
Conversation	デバイス間のカンバセーション一覧を表示します。

■ 監視結果のエクスポート

3. 監視結果をファイルにエクスポートするには、右上の「Export」ドロップダウンメニューをクリックし、エクスポートファイルの種類として以下のオプションを選択します。
   - 「PDF」
   - 「Excel」
   - 「CSV」

   データはブラウザの所定のダウンロードフォルダに保存されます。

第 11 章　テンプレート機能

テンプレートを使用すると、デバイスの監視・構成タスクをすばやくセットアップし、特定のデバイスモデル間で一貫した設定を行うことができます。監視および設定タスクに加えて、デバイスのプロビジョニングにも効率的です。

本章では、以下のトピックについて説明します。

- 「デバイステンプレートの生成」
- 「デバイスベンダとデバイスタイプの管理」
- 「パネルテンプレートの生成」
- 「監視テンプレートの生成」
- 「設定テンプレートの生成」

デバイステンプレートの生成

デバイステンプレートは、構成および監視のプロビジョニングに役立ちます。

デバイステンプレートの追加

1. **Templates > Device Template** に移動します。

1. 既存のテンプレート画面が開いている場合は、「Add Device Template」をクリックして新規テンプレート入力画面を表示します。

2. 以下の情報を入力します。

項目	説明
Template Information	
Model Name	設定するモデル名を入力します。
Device Type	ドロップダウンメニューからデバイスタイプを選択します。または、右側の「New」をクリックして、新しいデバイスタイプを追加します。デバイスタイプの詳細は、**Templates > Device Support** を参照してください。
Vendor Name	ドロップダウンメニューからベンダ OID を持つベンダを選択します。または、右側の「New」をクリックして、新しいベンダを追加します。ベンダの詳細は、**Templates > Device Support** を参照してください。
SOID	デバイスのシステム OID を入力します。右側の「Search」をクリックして、デバイス IP およびその他の SNMP 接続パラメータを使用して特定のデバイス SOID を検索することもできます。
Hardware Version	デバイスのハードウェアバージョンを入力します。
Extended Information	デバイスに追加のプロパティを設定します。

各種テンプレートの紐づけ

パネルテンプレート、監視テンプレート、設定テンプレートをデバイステンプレートに関連付ける場合は、次の手順を実行します。

■　パネルテンプレート

「Associate Panel Template」をクリックして、パネルテンプレートをモデルに関連付けます。カスタマイズしたパネルテンプレートを作成することも可能です。パネルテンプレートの詳細は、以下のセクション P.199 の「パネルテンプレートの生成」を参照してください。

■　監視テンプレート

「Associate Monitor Template」をクリックして、監視テンプレートをモデルに関連付けます。カスタマイズした監視カテゴリ及び監視テンプレートを作成することも可能です。監視テンプレートの詳細は、以下のセクション P.200 の「監視テンプレートの生成」を参照してください。監視テンプレートがモデルに関連付けられている場合は、その監視ステータスを制御したり、ポーリング間隔を編集したりできます。P.167 の「監視設定の表示と管理」を参照してください。

■　設定テンプレート

「Configuration」タブに移動し、「Associate Configuration Template」をクリックして、設定テンプレートをモデルに関連付けます。カスタマイズした設定カテゴリ及び設定テンプレートを作成することも可能です。設定テンプレートの詳細は、以下のセクション P.201 の「設定テンプレートの生成」を参照してください。設定テンプレートがモデルに関連付けられている場合は、バッチ設定に使用することができます。P.139 の「設定プロファイルの追加」及び P.118 の「バッチ設定」を参照してください。

注意　管理対象デバイスに関連付けられているシステム定義テンプレートの一部は、まだ検証プロセス中であり、正常に動作しない場合があります。サポートされている製品及びバージョンの一覧は、P.13 の「サポートされる製品」を参照してください。

3. 「Save」をクリックして、定義したデバイステンプレートを保存します。

デバイスベンダとデバイスタイプの管理

ベンダとデバイスタイプはデバイスの主要なプロパティです。これらは、多くの設定項目や検索条件で使用されます。

ベンダおよびデバイスタイプの追加

■ ベンダの追加

1. **Templates > Device Support > Vendor** に移動し、「+ Add Vendor」をクリックします。
2. 以下の情報を入力します。

項目	説明
Vendor Name	ベンダ名を入力します。
Vendor OID	ベンダに対応する OID（オブジェクト識別子）を入力します。

■ デバイスタイプの追加

1. **Templates > Device Support > Device Type** に移動し、「+ Add Device Type」をクリックします。
2. 以下の情報を入力します。

項目	説明
Device Type Name	デバイスタイプ名を入力します。
Device Category	デバイスカテゴリを選択します。新規のデバイスカテゴリを作成する場合は、「Device Category」タブに移動し設定します。
Description	デバイスタイプの説明を入力します。

■ エントリの編集・削除

作成されたベンダまたはデバイスタイプは、「Operation（操作）」列の （Edit）または （Delete）アイコンをクリックして、編集または削除できます。

パネルテンプレートの生成

パネルテンプレートは、ポート、コネクタ、ベンダロゴを含む前面パネルの表示用に設定します。

パネルテンプレートの追加

1. **Templates > Panel Template** に移動し、「+ Add Template」をクリックします。
2. 以下の情報を入力します。

項目	説明
Panel Detail	
Template Name	テンプレートの名前を入力します。
Description	テンプレートの簡単な説明を入力します。
Panel Diagram	
Vendor Logo	パネルのロゴ画像をアップロードします。ファイルは、2MB 未満で JPG または PNG である必要があります。
Panel Height	パネルの高さを選択します。 • 選択肢：「1」「2」（U）
Panel Width	パネルの幅を選択します。 • 「Full width」「2/3 width」「Customized（0.1-1 の 10 進数）」
Port Numbering Rule	ポートの番号付けのルールを選択します。 • 選択肢：「Vertical numbering scheme（縦並び）」「Horizontal numbering scheme（横並び）」
Port Starting Number	ポートの開始番号を入力します。
Port Start ifIndex	ポートのインタフェースインデックスの開始番号を入力します。

3. パネルにポートを追加するには、対象のポート種類の外観のアイコンを、指定したポートにドラッグ＆ドロップします。
   選択したポートを右クリックし、「Bind port type」からポートタイプ（RJ45 10M/100M など）を指定します。

その他、必要に応じて以下の設定を行います。

■ **ポートのラベル付け**
ポートにラベルを付けるには、配置したポートをクリックして「Port Name」に名前を入力します。

■ **ポートの再配置**
配置したポートをドラッグ＆ドロップして再配置できます。

■ **ポートのグループ化**
「Draw a box to」ドロップダウンメニューから「group/ungroup」を選択します。
クリックしながらポートを囲むと、指定箇所が 1 つのユニットとしてグループ化されます。指定を繰り返して、複数のグループを作成することができます。

4. 「Save」をクリックして、パネルテンプレートのポートレイアウトを保存します。

監視テンプレートの生成

監視テンプレートは、監視機能の設定に役立ちます。

監視カテゴリの追加

監視テンプレートを作成する前に、最初に監視カテゴリを追加する必要があります。

1. **Templates > Monitor Template** に移動し、「Monitor Category」タブをクリックします。
2. 「+ Add Category」をクリックします。
3. 以下の情報を入力します。

項目	説明
Category Information	
Category Name	カテゴリ名を入力します。
Units	設定する単位を選択します。
Protocol	構成のプロトコルを選択します。 • 選択肢：「SNMP」「HTTP(S)」「WMI」
Line Chart	監視結果をグラフ表示する折れ線グラフ機能の有効 / 無効を設定します。 **Monitoring > Device View** から対象デバイスのシステム名のリンクをクリックしてデバイス情報画面を開き、**Monitor > Customized Monitor** を開いて追加した監視結果を確認できます。
Description	カテゴリの簡単な説明を入力します。
Data Source Definition	
Name/Value Type	「+ Add」をクリックして、データソースの名前と値タイプを定義します。

4. 「Save」をクリックして、監視カテゴリを保存します。

監視テンプレートの追加

1. **Templates > Monitor Template** に移動し、「Monitor Template」タブをクリックします。
2. 左側の監視カテゴリ一覧から目的のカテゴリを選択します。
3. 「+ Add Monitor Template」をクリックします。
4. 以下の情報を入力します。

項目	説明
Basic Information	
Template Name	テンプレートの名前を入力します。
Monitor Category	選択したカテゴリが表示されます。カテゴリを選択し直すこともできます。
Vendor Name	ドロップダウンメニューからベンダ OID を持つベンダを選択します。または、「New」をクリックして、新しいベンダを追加します。ベンダの詳細は、**Templates > Device Support** を参照してください。
Monitoring Interval	監視するポーリング間隔を選択します。 • 選択肢：「60」「300」「600」「1800」「7200」（秒） • 初期値：60（秒）
Description	テンプレートの簡単な説明を入力します。

項目	説明
Data Source Definition	
Name/OID	監視対象デバイスから取得する特定のデータオブジェクトについて OID を定義します。 「+ New」をクリックして新規のデータソースを設定することができます。
Script	
Data Process Script	追加したデータソースの値を Groovy で処理するスクリプトを入力します。

5. 「Save」をクリックして、監視テンプレートを保存します。

■ テンプレートのデバイスへの紐づけ

作成したテンプレートは、デバイスモデルに関連付けることができます。監視テンプレートをデバイスに関連付けた後、定義済みのシステムメトリックを使用してデバイスを監視するように設定できます。

- デバイステンプレートの設定：**Templates > Device Template**
- アラームおよび監視の設定：**Alarm & Notification > Monitor & Alarm Settings**

■ 監視機能の設定

デバイスごとに監視機能を有効または無効にすることもできます。
Monitoring > Device View に移動し、システム名のリンクからデバイス情報画面を開きます。次に「Monitor」タブをクリックし、「Monitoring Settings」ボタンをクリックします（P.104 の「デバイス情報の変更」参照）。

設定テンプレートの生成

設定テンプレートは、一貫したデバイス構成管理に役立ちます。設定テンプレートの枠組みとなる、使用可能な設定カテゴリの一覧が提供されます。

設定カテゴリの確認

設定テンプレートのベースとなる、設定カテゴリの内容を表示します。

設定テンプレートは設定テンプレートタブから追加することができますが、デバイスの管理機能（デバイスの再起動、アップグレードなど）については本画面からカテゴリを選択し、テンプレートを作成することもできます。

注意　設定カテゴリの追加は未サポートです。

1. **Templates > Configuration Template** に移動し、「Configuration Category」タブをクリックします。
2. 機能別にカテゴリが用意されています。

項目	説明
v2_firmware_upgrade	デバイスのファームウェアアップグレード用設定カテゴリです。
v2_backup	デバイスのコンフィグレーションファイルのバックアップ用カテゴリです。
v2_restore	デバイスのコンフィグレーションファイルのリストア用カテゴリです。
v2_reboot	デバイスの再起動用カテゴリです。
v2_save	デバイスのコンフィグレーション保存用カテゴリです。
v2_sFlow	デバイスの sFlow 設定用カテゴリです。

メモ　上記の「v2...」という名前のカテゴリでは、定義済みの「Category Traits」を利用することができます。（「Operation」列の （View）アイコンをクリック→「View Configuration Category」画面を開く）

- 「Category Traits」のドロップダウンメニューから選択したデバイスの特性により、設定する SNMP オブジェクトやコンポーネントが異なります。
- 対象モデルに設定テンプレートを追加する前に、MIB ブラウザなどの SNMP ツールを使用して SNMP オブジェクトの有効性を検証する必要があります。選択したカテゴリの SNMP オブジェクト構成が対象モデルに合致しない場合、そのカテゴリを使用することはできません。

メモ　そのほかのシステム定義テンプレートは、スケジュールタスクのバッチ設定で利用することができます（P.117 の「バッチ構成による複数ネットワークの管理」参照）。

3. 「Operation」列の （View）アイコンをクリックし、設定カテゴリの定義済みテンプレートを表示します。
設定が必要な以下の項目が表示されます。

- コンポーネント（SNMP オブジェクト名、値タイプ）、そのレイアウトビュー

メモ　「v2...」という名前の設定カテゴリでは、選択したタイプに基づいてテンプレートを追加することができます。既に同じタイプの設定テンプレートがデバイスに紐づいている場合（「Backup」「Firmware_Upgrade」「Reboot」「Save」「Restore」など）、これら「v2」バージョンのテンプレートを追加する必要はありません。（※システム定義のテンプレートの紐づけを解除することはできません。）

4. 「+ Add Template」をクリックして、このカテゴリの新しいテンプレートを作成します。「Configuration Template」タブからテンプレートを追加することも可能です（次項参照）。
5. 選択した設定カテゴリのテンプレートデザイン画面が表示されます。ここで、「Category Traits」を選択し直すことも可能です。
6. SNMP オブジェクトの OID、値タイプなどを指定します。
7. 「Save」をクリックして、設定テンプレートを保存します。
8. 「Configuration Template」タブを選択します。「Operation」列の （View）アイコンをクリックし、作成テンプレートを確認することができます。

設定テンプレートの追加

1. **Templates > Configuration Template** に移動し、「Configuration Template」タブをクリックします。
2. 左側の設定カテゴリ一覧からカテゴリを選択します。
3. 右上の「+ Add Template」をクリックします。
4. 以下の情報を入力します。

項目	説明
Template Settings	
Name	テンプレートの名前を入力します。
Configuration Category	選択したカテゴリが表示されます。
Vendor	ドロップダウンメニューからベンダ OID を持つベンダを選択します。
Category Traits	ドロップダウンメニューからデバイスの特性を選択します。設定カテゴリ毎に、異なる特性が表示されます。 ・「Applicable Features」に設定の手順と要件が表示されます。 ・「Reference Device」に本特性が実装されているデバイスが表示されます。 ・「UI Appearance」に実際のレイアウトが表示されます。 ・「Template Component」に使用する SNMP 項目が表示されます。
Description	テンプレートの簡単な説明を入力します。
Protocol	設定に使用するプロトコルとして「SNMP」が表示されます。
Engineering View	
画面下部にあるテンプレートデザインセクションでは、例えば SNMP 項目のようなコンポーネントの設定が可能です。OID や関連付けられた値タイプを入力します。	

メモ　名前の 頭に「v2」が付く設定カテゴリ、v2_Backup、v2_Firmware_ Upgrade、v2_Reboot、v2_Restore、v2_Save、および v2_sFlow は、使用する SNMP オブジェクトが適切に設定されている場合、かつ SNMP ツールの SNMP コマンドを使用してその有効性のテストが済んでいる場合のみ正常に実行されます。同じタイプの設定テンプレート（Backup、Firmware_Upgrade、Reboot、Save、Restore、sFlow など）が既に関連付けられているデバイスでは、更新された v2 バージョンを新たに追加する必要はありません。（※システム定義のテンプレートの紐づけを解除することはできません。）

メモ　上記のテンプレート作成は、名前の 頭に v2 が付く設定カテゴリにのみ適用されます。スケジュールタスクで利用可能な、名前の頭に v2 が付かないバッチ設定用の設定テンプレートを作成する場合は、P.117 の「バッチ構成による複数ネットワークの管理」を参照してください。

5. 「Save」をクリックして、設定テンプレートを保存します。

■ テンプレートのデバイスへの紐づけ

作成したテンプレートは、デバイスモデルに関連付けることができます。設定テンプレートをデバイスに関連付けた後、構成の変更や設定に使用できます。**Configuration > Batch Configuration** でバッチ設定を行います。詳細は、P.137 の「設定タスク（実行ジョブ）の追加」および P.118 の「バッチ設定」を参照してください。

■ デバイス設定の利用

これらのテンプレート設定は、以下の機能で利用することができます。（P.104 の「デバイス情報の変更」参照）

(1) **Monitoring > Device View** に移動し、対象モデルのシステム名のリンクからデバイス情報画面を開きます。

(2) 「Management」タブでは以下の機能を使用することができます。

項目	説明
（Save to Device）	実行中のコンフィグレーションをブートアップコンフィグレーションに保存します。 v2_save テンプレートに紐づいている場合、v2_save テンプレートを介して実行されます。テンプレートでは、次のようなデバイスに対し設定が定義されています。 • 実行中のコンフィグレーションおよびスタートアップコンフィグレーションの両方にアドレスを指定する必要のあるデバイス、また、MIB ノードの異なる 2 つのコンフィグレーションファイルを持つデバイス
（Reboot）	デバイスの再起動を行います。 v2_reboot テンプレートに紐づいている場合、v2_reboot テンプレートを介して実行されます。
Firmware Upgrade セクションの （Upload button）	ファームウェアのアップグレードを行います。 v2_firmware_upgrade に紐づいている場合、v2_firmware_upgrade テンプレートを介して実行されます。テンプレートでは、次のようなデバイスに対し設定が定義されています。 • 1 つまたは 2 つのイメージファイルを持ち、ブートアップファイルの指定を行う必要のあるデバイス、また、アップグレード後に自動的に再起動されるデバイス
Configuration File Backup / Restore セクション	バックアップ / リストアを実行します。 v2_backup および v2_restore テンプレートに紐づいている場合、v2_backup および v2_restore テンプレートを介して実行されます。テンプレートでは、次のようなデバイスに対し設定が定義されています。 • 特定のファイル名を必要とする、もしくは必要としない、1 つまたは 2 つのコンフィグレーションファイルを持つデバイス、また、TFTP 経由のファイルのバックアップ / リストアで異なるコマンドを要するデバイス
sFlow セクション	各種 sFlow 設定を行います。 v2_sFlow に紐づいている場合、v2_sFlow テンプレートを介して提供されます。テンプレートでは、次のような設定が定義されています。 • IPv4 アドレスタイプのみ対応の sFlow コレクタ、IP v4 と IPv6 両方のアドレスタイプに対応の sFlow コレクタ、アドレスタイプ選択（IPv4 または IPv6）に対応する sFlow コレクタ、グローバル on/off 設定なしの設定

デバイス情報画面の各種機能についての詳細は、P.104 の「デバイス情報の変更」を参照してください。

第 12 章　レポート機能

レポート機能では、組み込みのパラメータ項目を設定し、表示内容をカスタマイズしたレポートを生成することができます。必要に応じて、1 回のみのレポートまたはスケジュールとして表示および生成できます。

本章では、以下のトピックについて説明します。

- 「レポートの管理」
- 「スケジュールレポートとマイレポートの作成」
- 「スケジュールレポート / マイレポートの表示と削除」

レポートの管理

レポートテンプレート

D-View8 には、サポートされているデバイスの定義済みレポートテンプレートが用意されています。様々な監視項目やレポートを利用することができます。

デフォルトのテンプレートと、使用可能なレポートのタイプは以下の通りです。

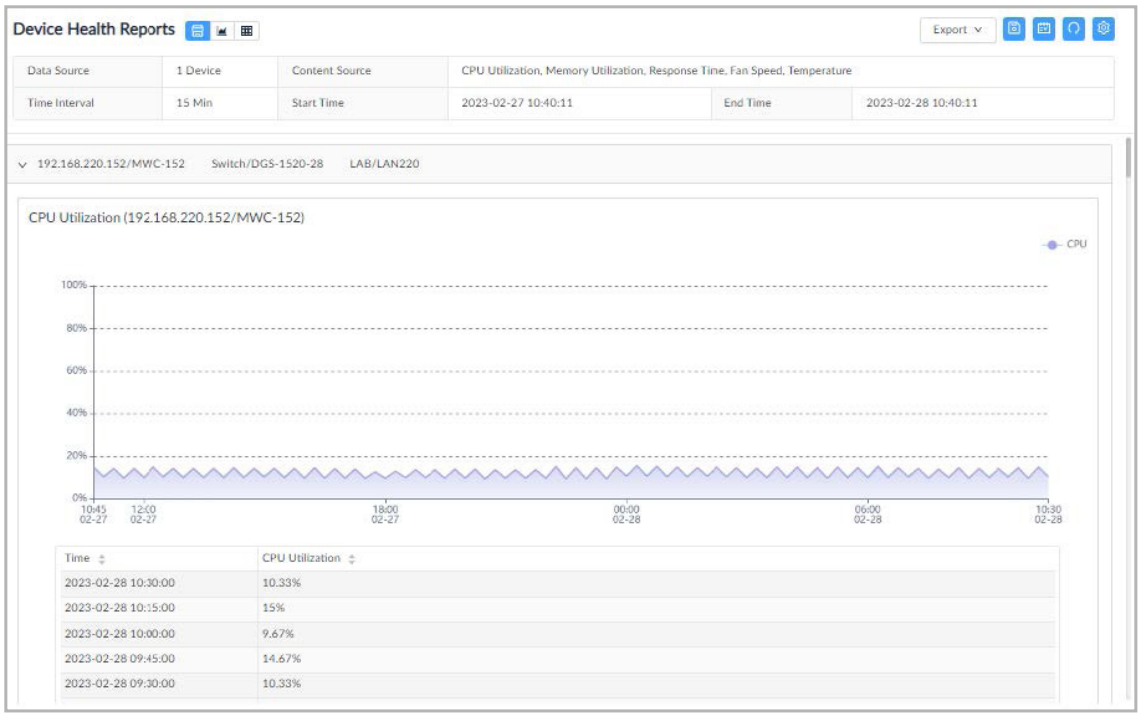


図 12-18　レポートテンプレートの表示

レポート種別	カテゴリ	レポート名	レポート内容
General Reports	Device Reports	Device Health	CPU 使用率、メモリ使用率、応答時間、ファン速度、温度を表示します。
		Trap	トラップイベントを表示します。
		Syslog	Syslog メッセージを表示します。
		Device Top N	次のパフォーマンスインジケータに関する、選択したデバイスの上位 10 件のデバイス統計を表示します。 • CPU 使用率、メモリ使用率、応答時間、Tx/Rx トラフィック、トラップおよび Syslog メッセージ
	Wired Interface Reports	Wired Traffic	選択したデバイスのすべてのインタフェースの Rx/Tx トラフィック統計を表示します。
		Wired Throughput Top N	選択したデバイスの上位 10 件のデバイスポートの Rx/Tx トラフィック統計を表示します。
	Wireless Reports	Wireless Client Count	選択した無線デバイスの無線クライアント数が表示されます。
		Wireless Traffic	選択した無線デバイスの無線トラフィックを表示します。
	Advanced Reports	Inventory	デバイスカテゴリとモデルに関する、選択したデバイスの分布を表示します。

レポート種別	カテゴリ	レポート名	レポート内容
Scheduled Reports	One Time	—	指定した時刻に生成される自動レポート。
	Recurrent	—	指定した時刻に繰り返し生成される自動レポート。
My Reports	My Reports	—	「General Reports」から選択したレポートの保存済みスナップショット。

レポートの生成

D-View8 には、様々なカテゴリやサマリ目的に対応した多数のテンプレートが用意されています。テンプレートを選択し、ネットワークの管理や維持に役立つレポートを簡単に生成できます。

1. **Reports > General Reports** をクリックします。
2. 左側のレポート一覧から、対象のレポートを選択します。

   以降の設定例では、「Device Health Reports（デバイスの正常性レポート）」を使用します。

図 12-19　レポートテンプレート（デバイスの正常性）

3. 最初にレポートパラメータを設定する必要があります。「The report parameters are required, click HERE to configure.」のリンクをクリックして、レポートの設定を行います。

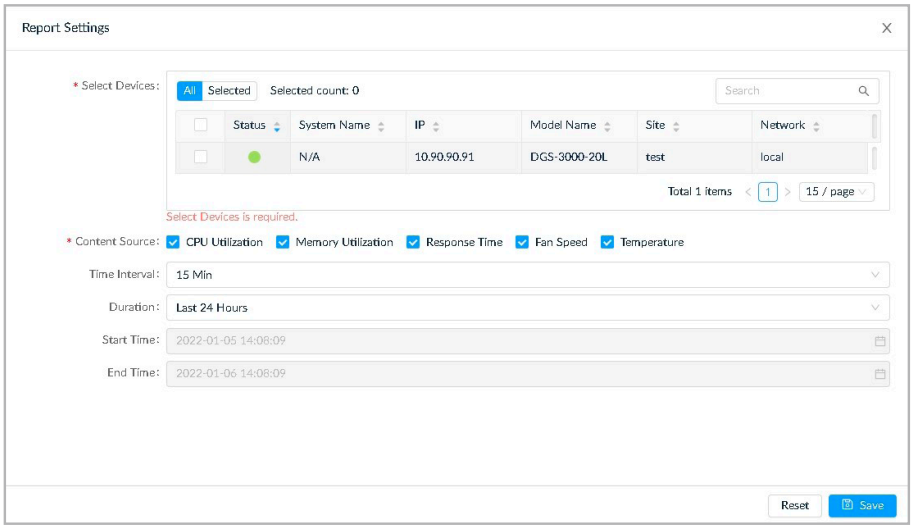


図 12-20　レポートパラメータの設定

4. 次の設定を行います。

項目	説明
Select Devices	デバイス一覧からデバイスを選択します。検索フィールドを使用して、「System Name」「IP」「Model Name」「Site」「Network」によりデバイスを検索することもできます。このカテゴリでは、1 つのレポートに最大 15 個のデバイスを含めることができます。
Content Source	レポートデータの項目を選択します。 • 選択肢：「CPU Utilization」「Memory Utilization」「Response Time」「Fan Speed」「Temperature」

項目	説明
Time Interval	データの間隔を指定します。 • 選択肢：「Minimum interval configured」「15 Min」「2 Hour」「8 Hour」「1 Day」
Duration	ドロップダウンメニューをクリックして、レポートの取得期間を設定します。 • 選択肢:「Last Hour」「Last 6/12/24 Hours」「Today」「Yesterday」「Last 7/30/90 days」「This Week」「Last Week」「This Month」「Last Month」「Customized」
Start Time	「Duration」で「Customized」を選択した場合は、開始日を設定します。
End Time	「Duration」で「Customized」を選択した場合は、終了日を設定します。

メモ　利用可能な設定項目およびそのパラメータは、レポートの種類や選択肢によって異なります。

5. 「Save」をクリックしてレポートを作成します。パラメータをリセットするには、「Reset」をクリックします。

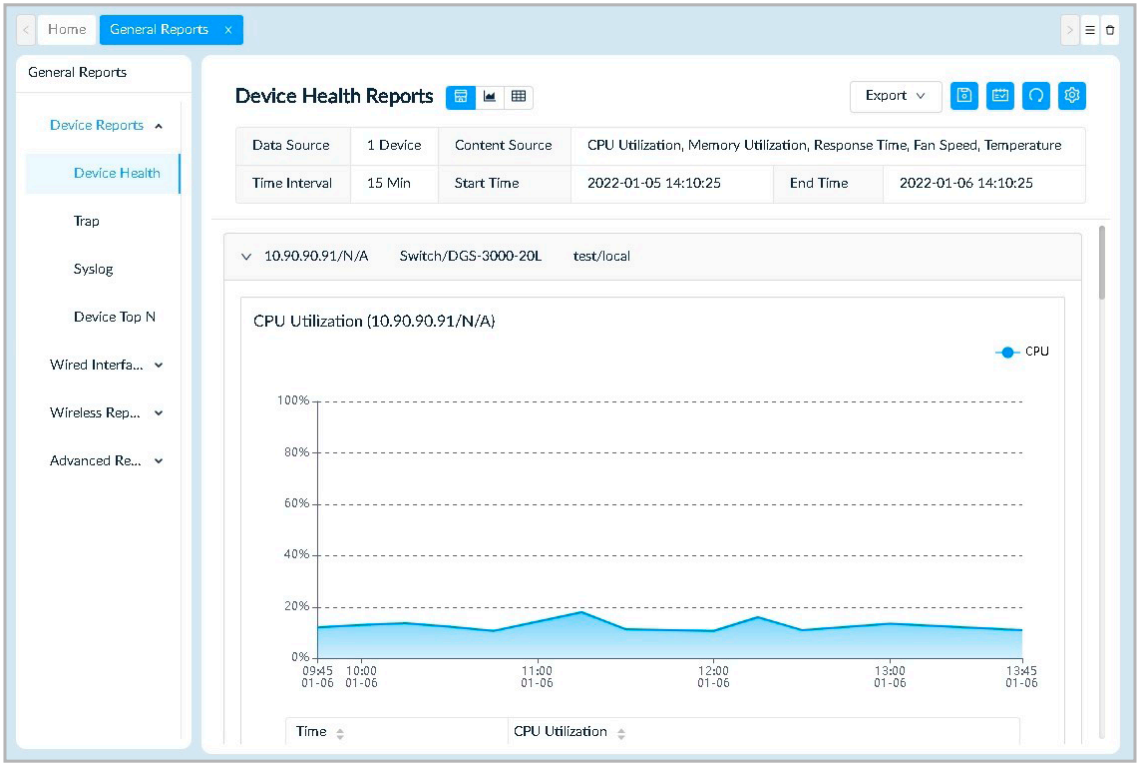


図 12-21　作成されたレポート（デバイスの正常性）

■ データ表示形式の変更

レポートデータは、デフォルトの形式（グラフ / テーブル）、またはグラフのみ、テーブルのみで表示できます。

画面上部の アイコンをクリックして、データ表示形式を指定します。

レポートの変更と削除

テンプレートはそのままで、レポートを削除することができます。
レポートの削除により生成データも削除されるため、レポートを削除する前に、エクスポート機能を使用してレポートを保存することをお勧めします。

1. **Reports > General Reports** をクリックします。
2. レポート一覧から以対象のレポートを選択します。
   以降の設定例では、「Device Health Reports（デバイスの正常性レポート）」を使用します。レポートが生成済みであるものとします。

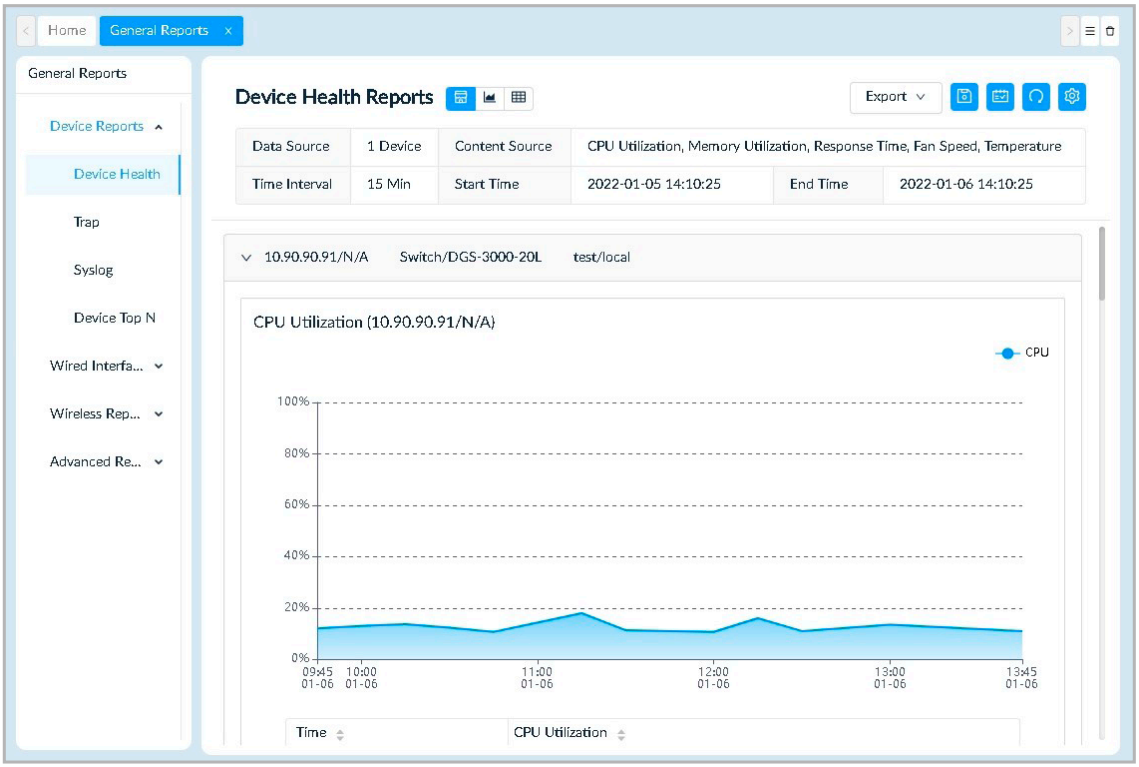


図 12-22　デバイスの正常性レポート

3. 右上の （Report Settings）アイコンをクリックし、レポート設定画面を開きます。

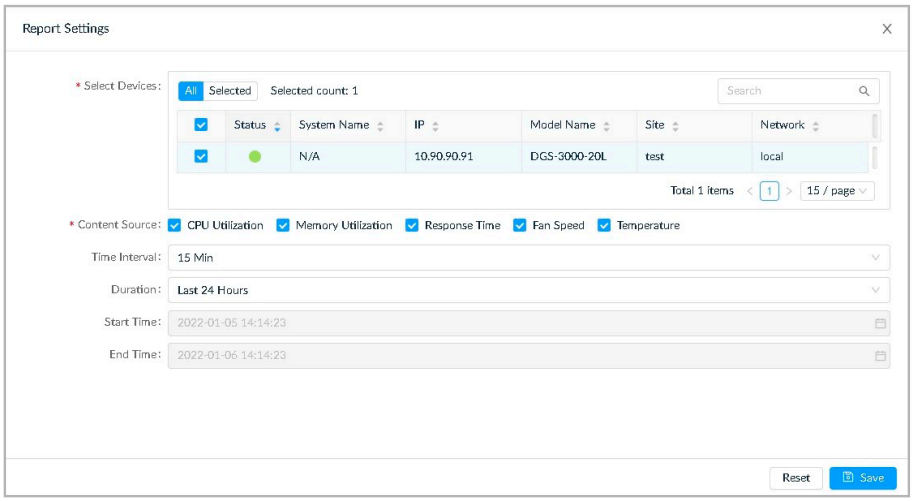


図 12-23　レポート設定

■ レポート設定の変更

4. レポート内容を変更し、「Save」をクリックします。

■ レポートの削除

5. 設定をリセットするには、「Reset」をクリックします。レポート及びデータが削除されます。

ページ右上の ✕ アイコンをクリックするか、アクティブな画面の外側をクリックして元の画面に戻ることができます。

レポート設定例

ここでは、Syslog レポートを例にレポートの設定方法を説明します。

■ Syslog レポートの生成

レポートの組み込みテンプレートを使用して Syslog レポートを生成する方法について示します。

1. **Reports > General Reports** をクリックします。
1. 「Device Reports」配下の「Syslog」を選択し、「The report parameters are required, click HERE to configure.」のリンクをクリックします。
2. デバイス一覧からデバイスを選択します。システム上でログを収集するためには、管理対象デバイスに対し D-View8 を Syslog サーバとして設定する必要があります。
   (1) **Monitoring > Device View** に移動し、デバイスのシステム名のリンクをクリックしてデバイス情報画面を開きます。
   (2)「Management」タブをクリックして、「Syslog Status」を ON に設定します。
3. 期間を設定するには、「Duration」ドロップダウンメニューをクリックして、レポートの期間（「Last Hour」「Last 6/12/24 hours」「Today」「Yesterday」「Last 7 Days」「This Week」「Last Week」「Last 30 Days」「This Month」「Last Month」「Customized」）を指定します。カスタマイズする場合は、開始 / 終了日時を選択します。
4. 「Save」をクリックして、生成されたレポートを表示します。
   設定をクリアするには、「Reset」をクリックします。

■ レポート表示形式の変更

「Syslog Reports」の横の ボタンで、レポートの表示を変更します。

- 「Show All（すべて）」「Show Chart only（グラフ形式のみ）」「Show Table only（表形式のみ）」

■ Syslog レポートのハイライト説明の設定

右上の「Add Syslog Description」をクリックし、Syslog メッセージを設定することができます。
定義された Syslog メッセージはレポート内にハイライトテキストとして表示されます。ハイライトテキストにカーソルを合わせると、該当ログの発生数や重大度レベルを確認することができます。

1. Syslog の説明を追加するには、「Add Syslog Description」をクリックします。
2. Syslog の説明を入力します。「Syslog Description」の文字列は、特定のログイベントを示すログのキーワード（「Syslog Keyword」）に関連付けられたハイライトテキストとして表示されます。
3. 「Save」をクリックします。
   定義された説明は、**Alarm & Notification > Trap & Syslog Editor > Syslog Editor** にも一覧表示されます。

Syslog Description を使用した Syslog レポートは、以下のように表示されます。なお、テキストが大きいほど、定義したシステムログの発生回数が多いことを意味します。

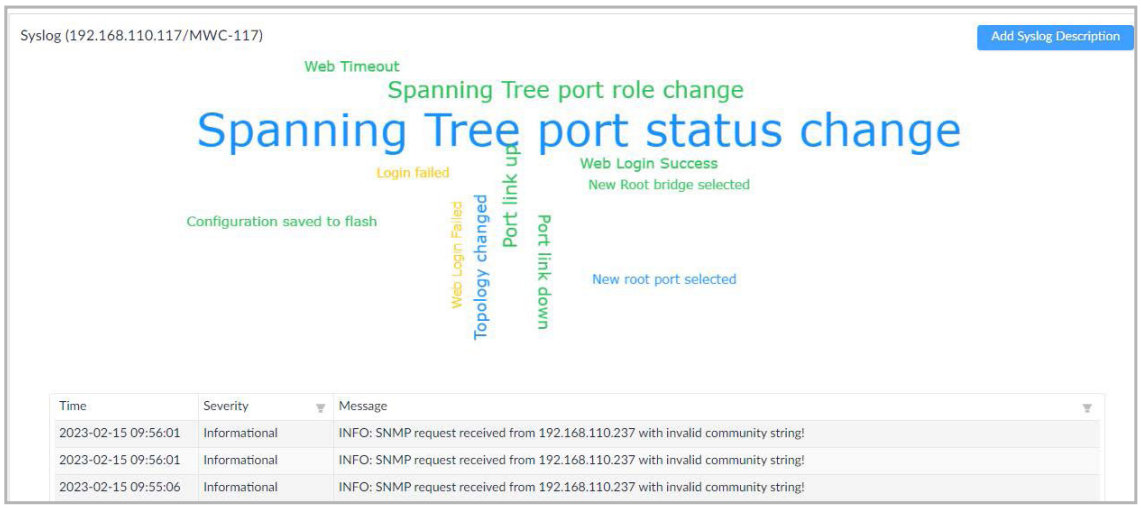


図 12-24　Syslog レポート

トラップレポートでは、Syslog レポートと同様に、トラップイベントを示す OID 説明のハイライトテキストが表示されます。詳細は、P.163 の「トラップエディタ機能」を参照してください。

スケジュールレポートとマイレポートの作成

既存のレポートテンプレートから、スケジュールされたレポートまたはマイレポートを作成できます。

- スケジュールされたレポート：1 回のみ / 繰り返しのスケジュールレポートを作成することができます。
- マイレポート：レポートテンプレートから生成したレポートを保存することができます。

スケジュールレポートの作成

1. **Reports > General Reports** をクリックします。

メモ　スケジュールレポートに設定するには、既存のレポートが存在する必要があります。詳細は、「レポートの生成」セクションを参照してください。

2. レポート一覧からカテゴリ（「Device Reports」「Wired Interface Reports」「Wireless Reports」「Advanced Reports」）を選択し、対象のレポート画面を開きます。以下の例では、「Wired Interface Reports」の「Wired Traffic」カテゴリを使用しています。

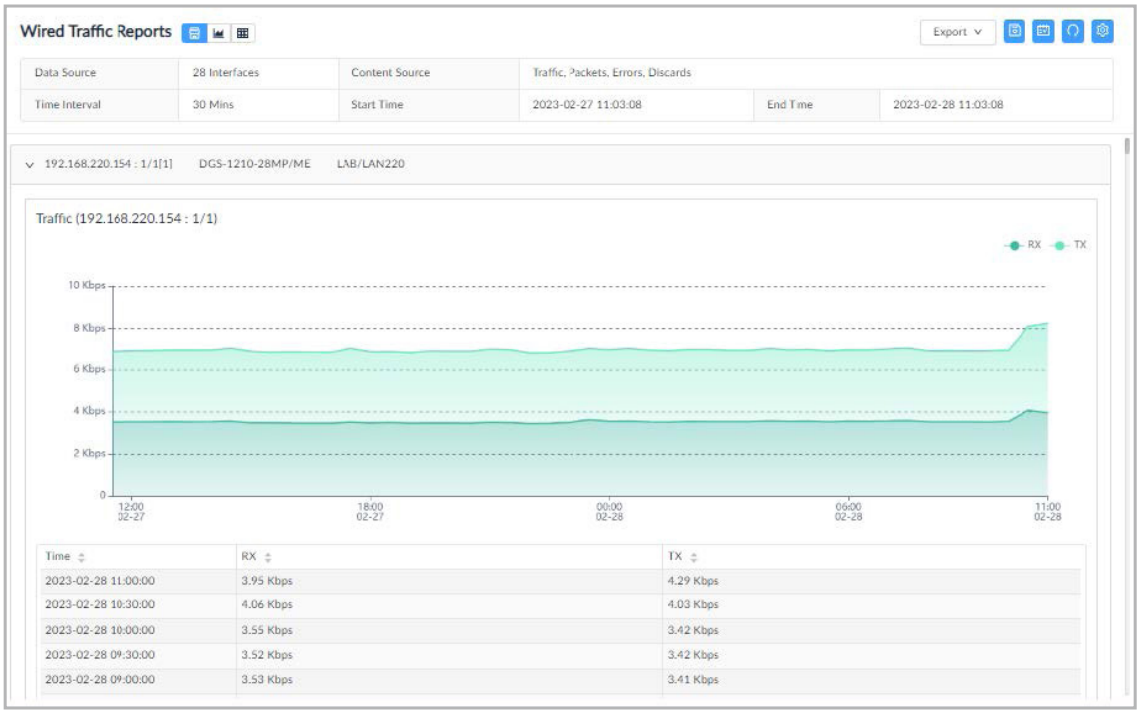


図 12-1　有線トラフィックレポート

注意　最適なシステムパフォーマンスを維持するため、ユーザごとに 500 個のレポート作成が上限となっています。制限を超えると、FIFO ルールに基づいてエントリが削除されます。

3. 右上の （Upgrade to Scheduled Reports）アイコンをクリックします。

4. 「Upgrade to Scheduled Reports」画面で必要な情報を入力します。

項目	説明
Basic Information	
Report Name	レポートの名前を入力します。
Description	レポートを識別するための説明文を入力します。
Schedule Information	
Schedule Type	レポートのスケジュールサイクルを選択します。 • 選択肢：「One Time（1 回）」「Recurrent（繰り返し）」 - 「Specify Generation Time」：「One Time」を選択した場合、タスクを実行する日時を指定します。 - 「Schedule」：「Recurrent」を選択した場合、「スケジュールリストから定義済みのスケジュールを選択します。または、「Add Schedule」をクリックして新しいスケジュールを定義します。

項目	説明
	新規のスケジュールを設定する場合、以下の頻度を設定できます。指定した時刻に 1 回、または複数の異なる時刻にレポートタスクを実行します。 • 「Daily」:実行するデイリー間隔を選択します。「1」を指定した場合、タスクを毎日実行します。「2」を指定した場合、タスクを 2 日ごと（1 日おき）に実行します。 • 「Weekly」：実行間隔を週単位で選択します。「1」を指定した場合、毎週指定した曜日にタスクを実行します。「2」を指定した場合、隔週（1 週間おき）にタスクを実行します。 • 「Monthly」：タスクを実行する月と日付を指定します。 • 「Specific Days」：タスクを実行する年月日を指定します。

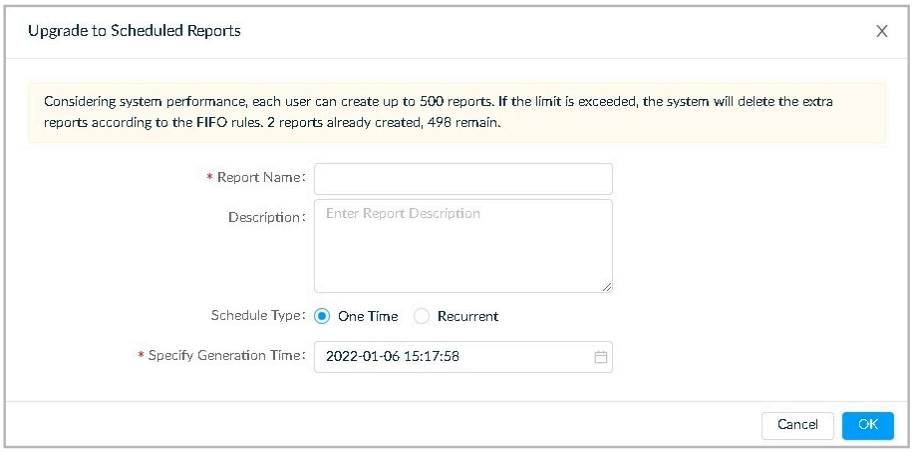


図 12-2　スケジュールレポートへのアップグレード

5. 「OK」をクリックして、スケジュールレポートを生成します。設定をキャンセルするには、「Cancel」をクリックします。

6. **Reports > Scheduled Reports** を選択して、作成されたスケジュールレポートを表示します。
   - 「One Time」タブ：スケジュールが「One Time（1 回）」に指定されているレポートが表示されます。
   - 「Recurrent」タブ：スケジュールが「Recurrent（繰り返し）」に指定されているレポートが表示されます。

図 12-3　スケジュールレポートの一覧

マイレポートの作成

1. **Reports > General Reports** をクリックします。
2. レポート一覧からカテゴリ（「Device Reports」「Wired Interface Reports」「Wireless Reports」「Advanced Reports」）を選択し、対象のレポート画面を開きます。
3. マイレポートとして保存するには、「General Reports」の該当レポート画面で （Save to My Reports）アイコンをクリックします。
4. 「Save to My Reports」画面で必要な情報を入力します。
   - 「Report Name」：レポートの名前を入力します。
   - 「Description」レポートを識別するための説明文を入力します。

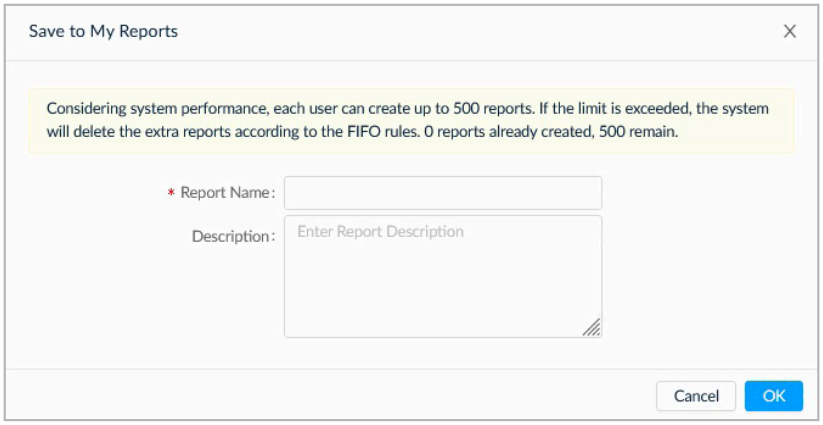


図 12-4　マイレポートへの保存

5. 「OK」をクリックして、マイレポートとして保存します。設定をキャンセルするには、「Cancel」をクリックします。
6. **Reports > My Reports** を選択して、マイレポートを表示します。

図 12-5　マイレポートの一覧

スケジュールレポート / マイレポートの表示と削除

スケジュールレポートまたはマイポートに設定したレポートを削除します。
すべてのレポートは、保持されている期間、表示できます。

■ スケジュールレポートの表示または削除

1. **Reports > Scheduled Reports** をクリックします。
2. 「One Time」または「Recurrent」タブをクリックして、スケジュールレポートの一覧を表示します。
3. レポートを表示するには、「Operation」列から （View report）アイコンをクリックします。

   レポートを削除するには、「Operation」列から （Delete this report）アイコンをクリックします。

■ マイレポートの表示または削除

1. **Reports > My Reports** をクリックし、マイレポートとして保存されたレポートの一覧を表示します。
2. レポートを表示するには、「Operation」列から （View report）アイコンをクリックします。

   レポートを削除するには、「Operation」列から （Delete this report）アイコンをクリックします。

第 13 章　ユーザとセキュリティプロファイルの管理

セキュリティプロファイルを使用して、ユーザ毎に D-View8 の各機能の利用権限を効率的に管理できます。

本章では、以下のトピックについて説明します。

- 「ユーザ役割の種類と機能毎のアクセス権限」
- 「認証の資格情報」
- 「ユーザプロファイルの管理」

ユーザに対し、機能の制限が可能なだけでなく、サイトやネットワークへのアクセス権限も設定することができます（P.218 の「ユーザプロファイルの追加」を参照）。

ユーザ役割の種類と機能毎のアクセス権限

ユーザ役割の種類

D-View8 には、以下のユーザ役割が定義されています。
「Organization Administrator」「Site Administrator」「Network Administrator」の役割を、各ユーザに割り当てることができます。

ユーザ役割：

項目	説明
「Super Administrator（スーパーアドミニストレータ）	このユーザは、ライセンスおよびシステムアップグレードを含む、すべての機能を実行できます。
Organization Administrator（組織管理者）	このユーザは、組織全体のユーザおよびセキュリティプロファイルの管理を含む、すべての管理機能を実行できます。
Site Administrator（サイト管理者）	このユーザは、割り当てられたサイトに対し管理機能を実行できます。
Network Administrator（ネットワーク管理者）	このユーザは、割り当てられたネットワークに対し管理機能を実行できます。

アクセス権限の詳細

各機能に対するアクセス権限の詳細は下記の通りです。
System > User Management の「Role Privileges」タブから確認することができます。

機能		Super Administrator（スーパーアドミニストレータ）	Organization Administrator（組織管理者）	Site Administrator（サイト管理者）	Network Administrator（ネットワーク管理者）
Dashboard（ダッシュボード）					
Analysis					
Analysis	Overview	Read and Write	Read and Write	Read and Write	Read Only
	Switch	Read and Write	Read and Write	Read and Write	Read Only
	Wireless	Read and Write	Read and Write	Read and Write	Read Only
	Host	Read and Write	Read and Write	Read and Write	Read Only
	sFlow	Read and Write	Read and Write	Read and Write	Read Only
	PoE	Read and Write	Read and Write	Read and Write	Read Only
Customized Dashboard		Read and Write	Read and Write	Read and Write	Read Only
Monitoring（モニタ）					
Network Discovery		Read and Write	Read and Write	Read Only	Read Only
Device View		Read and Write	Read and Write	Read and Write	Read and Write
Interface View		Read and Write	Read and Write	Read and Write	Read and Write
Topology Map		Read and Write	Read and Write	Read and Write	Read Only
Connection View		Read and Write	Read and Write	Read and Write	Read and Write
Rack View		Read and Write	Read and Write	Read and Write	Read Only
sFlow Analyzer		Read and Write	Read and Write	Read and Write	Read and Write
Device Group		Read and Write	Read and Write	Read and Write	Read and Write
Configuration（設定）					
Batch Configuration	Quick Configuration	Read and Write	Read and Write	Read and Write	Read and Write
	Advanced Configuration	Read and Write	Read and Write	Read and Write	Read and Write

機能		Super Administrator（スーパーアドミニストレータ）	Organization Administrator（組織管理者）	Site Administrator（サイト管理者）	Network Administrator（ネットワーク管理者）
Task Management	Current Task	Read and Write	Read and Write	Read and Write	Read and Write
	Historical Task	Read and Write	Read and Write	Read and Write	Read and Write
Firmware Management		Read and Write	Read and Write	Read and Write	Read and Write
Configuration Management	Backup	Read and Write	Read and Write	Read and Write	Read and Write
	Restore	Read and Write	Read and Write	Read and Write	Read and Write
File Management		Read and Write	Read and Write	Read and Write	Read and Write
Alarm & Notification（アラーム & 通知）					
Alarm	Active Alarms	Read and Write	Read and Write	Read and Write	Read and Write
	Historical Alarms	Read and Write	Read and Write	Read and Write	Read and Write
Trap & Syslog	Trap	Read and Write	Read and Write	Read and Write	Read Only
	Syslog	Read and Write	Read and Write	Read and Write	Read and Write
Trap & Syslog Editor	Trap Editor	Read and Write	Read and Write	Read and Write	Read Only
	Syslog Editor	Read and Write	Read and Write	Read and Write	Read Only
Monitor & Alarm Settings	Monitor Settings	Read and Write	Read and Write	Read and Write	Read and Write
	Alarm Settings	Read and Write	Read and Write	Read and Write	Read and Write
Notification Center		Read and Write	Read and Write	Not Available	Not Available
Templates（テンプレート）					
Device Template		Read and Write	Read and Write	Not Available	Not Available
Device Support	Vendor	Read and Write	Read and Write	Not Available	Not Available
	Device Category	Read and Write	Read and Write	Not Available	Not Available
	Device Type	Read and Write	Read and Write	Not Available	Not Available
Panel Template		Read and Write	Read and Write	Not Available	Not Available
Monitor Template	Monitor Category	Read and Write	Read and Write	Not Available	Not Available
	Monitor Template	Read and Write	Read and Write	Not Available	Not Available
Configuration Template	Configuration Category	Read and Write	Read and Write	Not Available	Not Available
	Configuration Template	Read and Write	Read and Write	Not Available	Not Available
Reports（レポート）					
General Reports		Read and Write	Read and Write	Read and Write	Read and Write
Schedule Reports		Read and Write	Read and Write	Read and Write	Read and Write
My Reports		Read and Write	Read and Write	Read and Write	Read and Write
Tools（ツール）					
MIB Browser		Read and Write	Read and Write	Read Only	Read Only
MIB Compiler		Read and Write	Read and Write	Not Available	Not Available
ICMP Ping		Read and Write	Read and Write	Read and Write	Read and Write
SNMP Test		Read and Write	Read and Write	Read and Write	Read and Write
Trace Route		Read and Write	Read and Write	Read and Write	Read and Write
CLI		Read and Write	Read and Write	Read and Write	Read and Write
File Comparison		Read and Write	Read and Write	Read and Write	Read and Write
System（システム）					
Basic Settings	Organization	Read and Write	Read and Write	Not Available	Not Available
	Mail Server Settings	Read and Write	Read and Write	Not Available	Not Available
	Forward Trap	Read and Write	Read and Write	Not Available	Not Available
	Forward Syslog	Read and Write	Read and Write	Not Available	Not Available
	REST API	Read and Write	Read and Write	Read and Write	Read and Write
	Credentials	Read and Write	Read and Write	Not Available	Not Available
	sFlow Settings	Read and Write	Read and Write	Not Available	Not Available
	System Preferences	Read and Write	Read and Write	Read and Write	Read and Write
User Management	Users	Read and Write	Read and Write	Read Only	Not Available
	Role Privileges	Read and Write	Read and Write	Not Available	Not Available
	AD Server	Read and Write	Read and Write	Not Available	Not Available
	RADIUS Server	Read and Write	Read and Write	Not Available	Not Available
Scheduling		Read and Write	Read and Write	Read Only	Read Only

機能		Super Administrator（スーパーアドミニストレータ）	Organization Administrator（組織管理者）	Site Administrator（サイト管理者）	Network Administrator（ネットワーク管理者）
Server Management	Probe	Read and Write	Read and Write	Not Available	Not Available
	Core Server	Read and Write	Read and Write	Not Available	Not Available
	Web Server	Read and Write	Read and Write	Not Available	Not Available
D-View 8 Log	User Operation Log	Read Only	Read Only	Read Only	Read Only
	System Log	Read Only	Read Only	Read Only	Read Only
	Device Maintenance Log	Read Only	Read Only	Read Only	Read Only
D-View 7 Upgrade（D-View8 v2.x ではサポートされません）		Read and Write	Not Available	Not Available	Not Available
About		Read and Write	Read Only	Read Only	Read Only

認証の資格情報

管理ユーザのアクセス権限は、ユーザプロファイルおよび役割により決定されます。ログイン認証については、次の 3 つの認証方式がサポートされます。

- ローカル認証
- RADIUS 認証
- AD 認証

AD サーバ認証

D-View8 に AD ドメインを利用してログインするための設定を行います。AD ノードの設定には、以下の情報が必要です。

- ドメイン名
- ドメインコントローラアドレス

AD サーバの追加

1. **System > User Management** に移動し、「AD Server」タブをクリックして以下の画面を表示します。
2. 「+ Add AD Server」をクリックします。

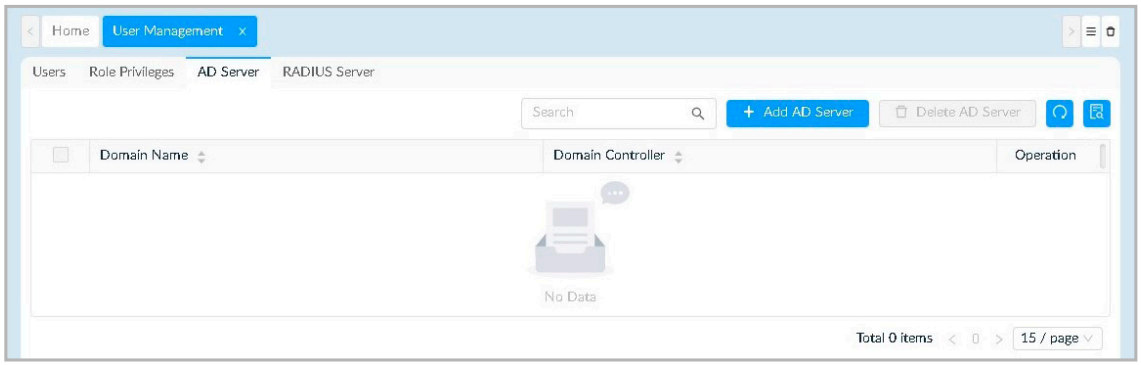


図 13-6　AD サーバ

3. 「Add AD Server」画面で、AD サーバのドメイン名とコントローラ情報を入力します。

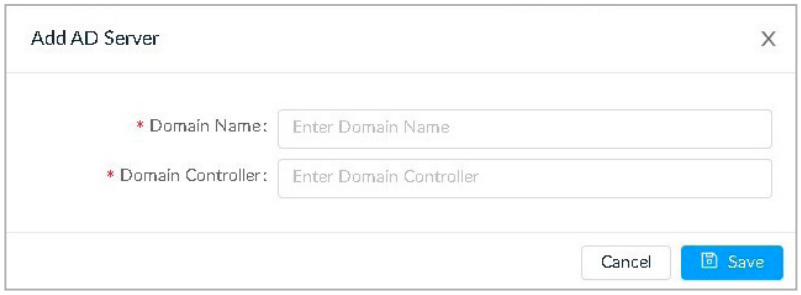


図 13-7　AD サーバの追加

4. 「Save」をクリックして設定を確定します。設定をキャンセルするには、「Cancel」をクリックします。

AD サーバの表示と変更

1. **System > User Management** に移動し、「AD Server」タブをクリックしてＡＤサーバ一覧を表示します。

   検索フィールドを使用して、ドメイン名またはコントローラ情報でエントリを検索できます。

   または、（Advanced Query）アイコンをクリックして、高度な検索機能を利用します。

2. エントリを編集するには、「Operation」列の（Edit）アイコンをクリックします。

   エントリを削除するには、「Operation」列の（Delete）アイコンをクリックします。

RADIUS サーバ認証

D-View8 に RADIUS サーバを利用してログインするための設定を行います。

RADIUS サーバの設定

1. **System > User Management** に移動し、「RADIUS Server」タブをクリックします。
2. 以下の設定を行います。

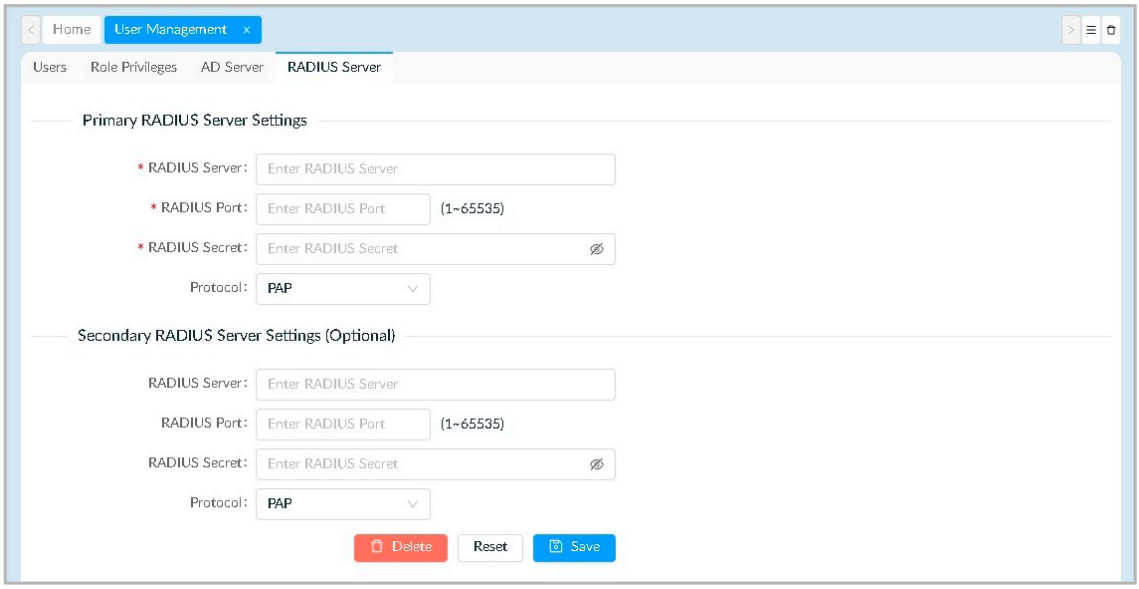


図 13-8　RADIUS サーバの設定

設定項目：

項目	説明
Primary RADIUS Server Settings（プライマリ RADIUS サーバ設定）	
RADIUS Server	リモート RADIUS サーバの IP アドレスを入力します。
RADIUS Port	RADIUS サービスのポート番号を入力します。
RADIUS Secret	RADIUS サーバとの通信で使用する認証および暗号化キー文字列を入力します。RADIUS サーバで定義されている暗号化鍵と一致する必要があります。
Protocol	RADIUS サーバで使用する認証スキームを入力します。 • 「PAP」：パスワード認証プロトコル。 • 「CHAP」：チャレンジハンドシェイク認証プロトコル。 • 「MSCHAP」：Microsoft チャレンジハンドシェイク認証プロトコル。 • 「MSCHAP2」：ピア間の相互認証を追加した Microsoft チャレンジハンドシェイク認証プロトコル 2。
Secondary RADIUS Server Settings (Optional)（セカンダリ RADIUS サーバ設定（オプション））	
RADIUS Server	リモート RADIUS サーバの IP アドレスを入力します。
RADIUS Port	RADIUS サービスのポート番号を入力します。
RADIUS Secret	RADIUS サービスで使用される認証および暗号化キー文字列を入力します。RADIUS サーバで定義されている暗号化鍵と一致する必要があります。
Protocol	RADIUS サーバで使用する認証スキームを入力します。 • 「PAP」：パスワード認証プロトコル。 • 「CHAP」：チャレンジハンドシェイク認証プロトコル。 • 「MSCHAP」：Microsoft チャレンジハンドシェイク認証プロトコル。 • 「MSCHAP2」：ピア間の相互認証を追加した Microsoft チャレンジハンドシェイク認証プロトコル 2。

注意　「MSCHAP」「MSCHAP2」はサポートされません。

3. 「Save」をクリックして、設定内容を保存します。
   変更内容をリセットするには、「Reset」をクリックします。保存済みの設定に戻ります。

保存済みの設定内容を削除するには、「Delete」をクリックしします。

ユーザプロファイルの管理

D-View8 では、役割ベースのアクセス制御を行います。プロファイルを使用してユーザを作成、管理します。ユーザプロファイルは、ユーザ名、パスワード、指定された役割に関連付けられた権限で構成されます。
各役割の機能権限を確認するには、**System > User Management** に移動し、「Role Privileges」タブを選択します。

ユーザプロファイルの追加

1. **System > User Management** をクリックし、「Users」タブを開きます。
2. 「+ Add User」をクリックします 。

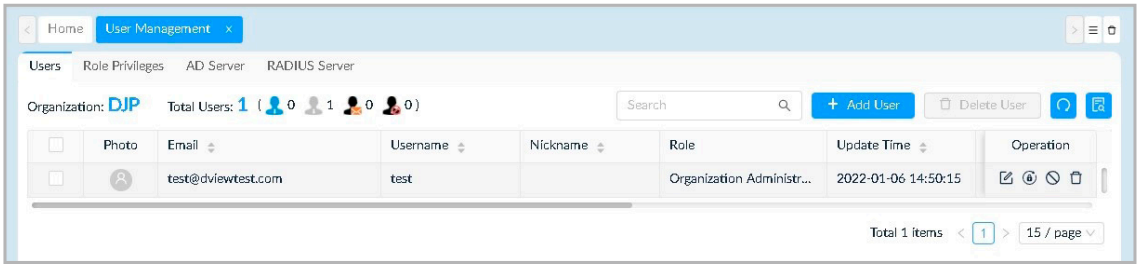


図 13-9　ユーザ管理

3. 以下の画面で、ユーザプロファイルの設定を行います。

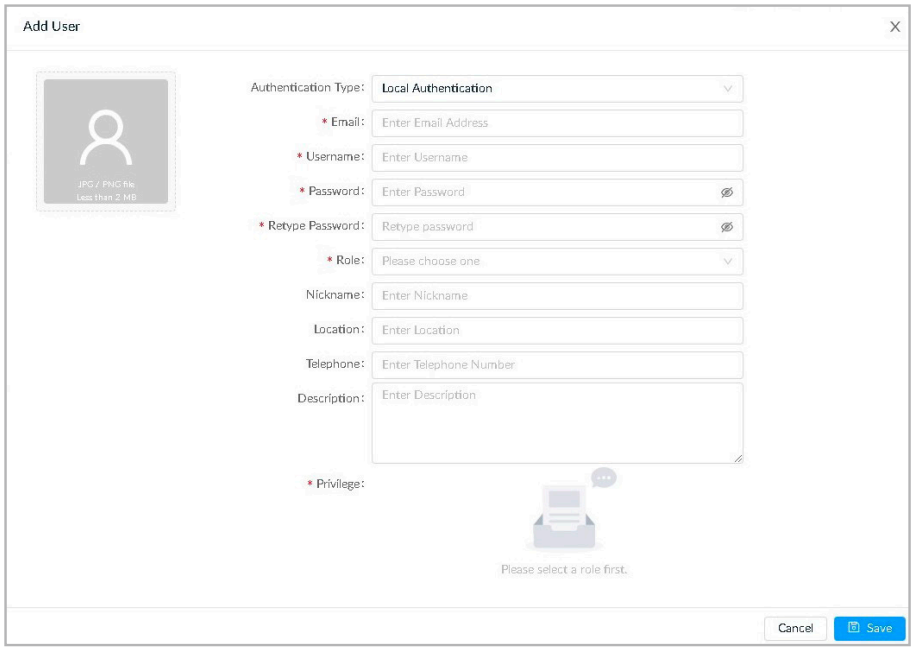


図 13-10　ユーザの追加

4. アバターアイコンをクリックして、プロフィール画像として使用する JPG/PNG ファイルをアップロードします。
5. 次の情報を設定します。

項目	説明
Authentication type	認証方式を選択します。 • 選択肢：「Local Authentication」「RADIUS Authentication」「AD Authentication」
AD Server	「AD Authentication」を選択した場合は、使用する AD サーバを選択します。
Email	プロファイルの電子メールアドレスを入力します。
Username	プロファイルのユーザ名を入力します。
Password	「Local Authentication」を指定した場合、パスワードを設定します。パスワードは、数字と文字両方を含む 6 文字以上の英数字である必要があります。記号も使用できます。
Retype Password	確認用にパスワードを再度入力します。
Role	プロファイルのセキュリティロール（役割）を選択します。 • 選択肢：「Organization Administrator」「Site Administrator」「Network Administrator」
Nickname	ニックネームを入力します。（オプション）
Location	プロファイルの場所を入力します。（オプション）

項目	説明
Telephone	プロファイルの電話番号を入力します。（オプション）
Description	プロファイルの識別に役立つ説明を入力します。（オプション）
Privilege	「Role」の種類に基づいて、ユーザが読み取り権限または読み書き権限でアクセス可能となる組織、サイト、またはネットワークを選択します。 読み取り権限を持つユーザは、管理対象ネットワーク階層下の資産情報を取得することができますが、設定の変更はできません。 この「Privilege」では、ネットワークまたはサイトへのアクセスを制御し、「Role」では、システム操作を実行するためのグループ化された権限セットを制御します。詳細は、P.213 の「ユーザ役割の種類と機能毎のアクセス権限」を参照してください。

6. 「Save」をクリックしてプロファイルを作成します。設定をキャンセルするには、「Cancel」をクリックします。
   - プロファイルが作成されると、システムは設定された E メールアドレスにアクティベーションメールを送信します。
   - オプションで、手動でアクティベーションメールを送信することもできます。
   - アカウントのユーザは、新たなパスワードの設定が必要となります。

■ 手動でアクティベーション E メールを送信する

アクティベーションメール認証が未処理の場合、手動でメールを再送することができます。

7. （Send Activation Email）アイコンをクリックして、定義されたメールアカウントにメールを配信します。

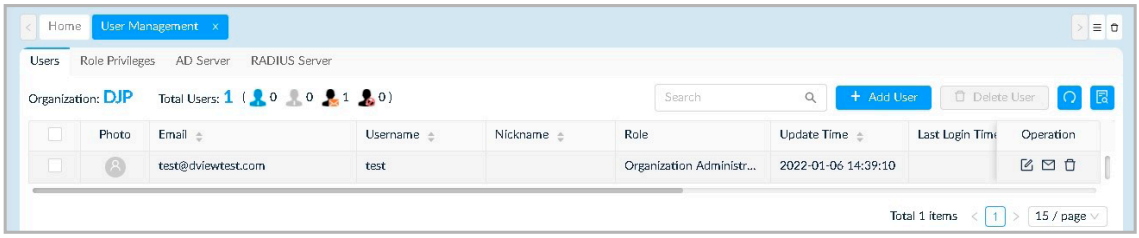


図 13-11　手動でのメール送信

メール経由でのアクティベーション処理が完了すると、定義されたユーザプロファイルを使用して D-View8 にアクセスできるようになります。

ユーザプロファイルの変更または削除

1. **System > User Management** をクリックします。

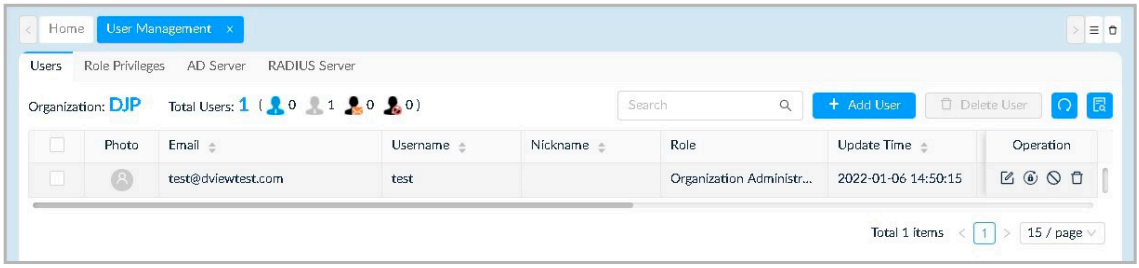


図 13-12　ユーザ一覧

2. 「Operation」列には以下の項目が表示されます。

項目	説明
（Edit）	プロファイル情報を変更します。
（Send Activation Email）	アクティベーションのリンクを含むアカウント招待メールを送信します。Super Administrator のみ使用できます。本機能は、システムによるメールアカウントのアクティベーション処理が未完了である場合に実行することができます。
（Reset Password）	プロファイルの新しいパスワードを生成します。生成された新しいパスワードは、プロファイルの E メールに送信されます。Reset Password 機能は、ユーザアカウントが有効化されている場合のみ使用できます。
（Disable）	対象のユーザアカウントを非アクティブ化します。Disable 機能はユーザが有効化されている場合のみ使用できます。
（Activated）	対象のユーザアカウントをアクティブ化します。または、（Edit）ボタンをクリックして「Edit User」ページを開き、Activated ボタンをクリックしてアクティブ化することもできます。無効化されている場合に実行することができます。
（Delete）	このユーザアカウントを削除します。

第 14 章　グローバル設定の管理

システム全体の管理と通信に使用するグローバル設定を構成します。

本章では、以下のトピックについて説明します。

- 「組織の設定」
- 「メールサーバ設定」
- 「トラップ転送の設定」
- 「Syslog 転送の設定」
- 「REST API キーの生成」
- 「接続プロトコルの認証情報の設定」
- 「sFlow 設定のセットアップ」
- 「システム環境設定」
- 「スケジュール機能」
- 「ライセンス管理」
- 「D-View8 ログ」

組織の設定

組織情報は、「Basic Settings」画面で確認することができます。タイムゾーン、ロゴ、組織名などを定義できます。
組織情報は、ネットワーク検出とその後のネットワークアーキテクチャの表示に必要です。

1. **System > Basic Settings** をクリックします。デフォルトでは「Organization」タブが表示されます。

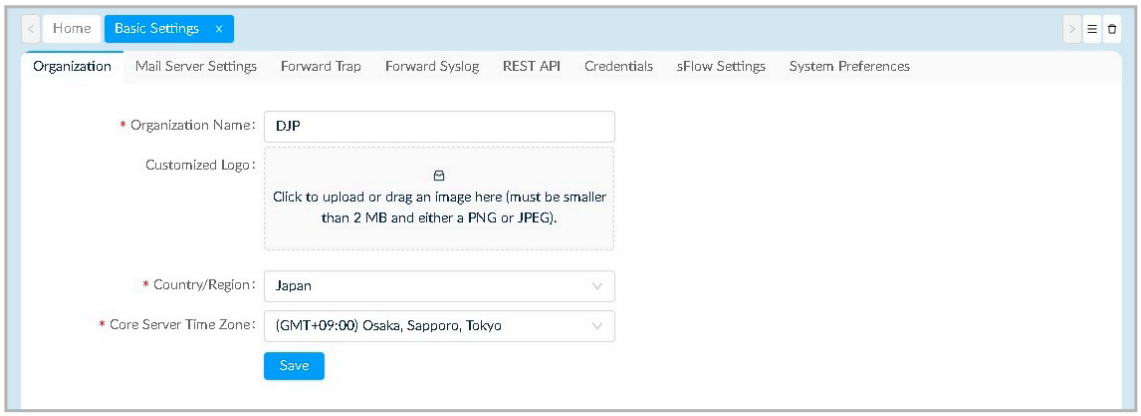


図 14-13　組織の設定

2. 次の情報を定義します。

項目	説明
Organization Name	組織の名前を入力します。
Customized Logo	アップロードする画像を選択します。（JPEG または PNG 形式、2MB 未満）
Country/Region	組織の属する国を選択します。「Japan」から変更しないでください。
Core Server Time Zone	指定した国に対応するタイムゾーンを選択します。

3. 「Save」をクリックして、組織設定を保存します。

メールサーバ設定

メール通知を利用するには、メールサーバの設定が必要です。

1. **System > Basic Settings** をクリックします。
2. 「Mail Server Settings」タブを選択し、以下の画面を表示します。

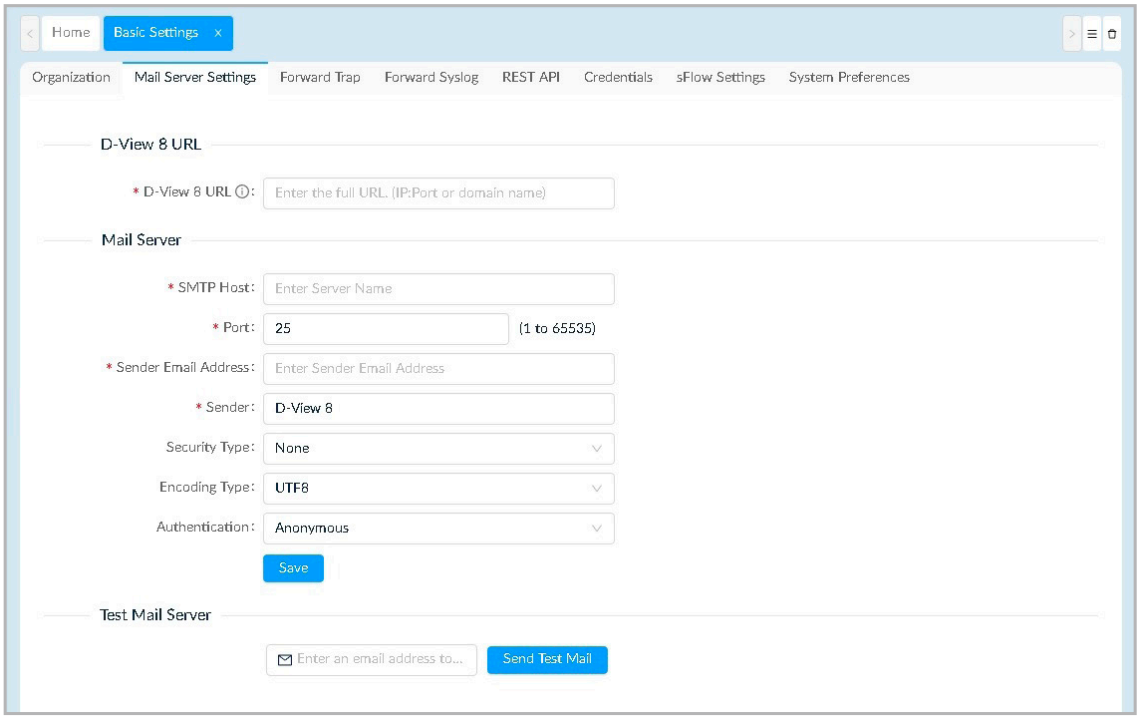


図 14-14　メールサーバ設定

3. 次の情報を定義します。

項目	説明
D-View 8 URL	
D-View 8 URL	この URL は、ユーザアカウントの E メール検証リンクおよびパスワードリセット時の E メールで使用されます。
Mail Server	
SMTP Host	SMTP サーバのアドレスを入力します。
Port	SMTP サーバのポート番号を入力します。
Sender Email Address	送信元メールアドレスを入力します。
Sender	送信者として使用する名前を入力します。
Security Type	ドメインのセキュリティプロトコルを選択します。 • 選択肢：「None」「SSL」
Encoding Type	SMTP 通信の転送エンコーディングを選択します。 • 選択肢：「UTF8」「ASCII」
Authentication	SMTP サーバで認証が必要かどうかを選択します。 • 選択肢：「Anonymous」「SMTP Authentication」
Username	SMTP サーバへのアクセス権を持つユーザ名を入力します。 「Authentication」で「SMTP Authentication」を選択した場合に指定する必要があります。
Password	SMTP ユーザのパスワードを入力します。 「Authentication」で「SMTP Authentication」を選択した場合に指定する必要があります。

注意 D-View8 の SMTP サーバとして Gmail を使用する場合、Google アカウントで 2 段階認証プロセスを有効化して、アプリパスワードを設定する必要があります。

4. 「Save」をクリックして、メールサーバの設定を保存します。

メールサーバの設定テスト

(1) 「Test Mail Server」セクションの電子メールアドレス欄に、テスト電子メールの送信先となる電子メールアドレスを入力します。
(2) 「Send Test Mail」をクリックします。
(3) テストメールが受信されているかどうかを確認します。メールを受信しなかった場合は、メールサーバの設定に誤りがないか確認してください。

トラップ転送の設定

SNMP トラップ転送機能を使用すると、指定したサーバ宛先にトラップを転送できます。

1. **System > Basic Settings** をクリックします。
2. 「Forward Trap」タブを選択し、以下の画面を表示します。

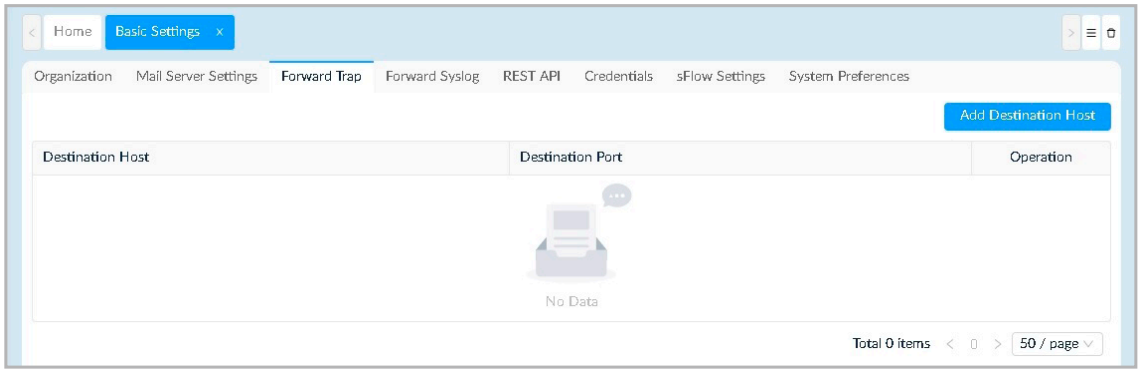


図 14-15　トラップ転送

3. 「Add Destination Host」をクリックします。

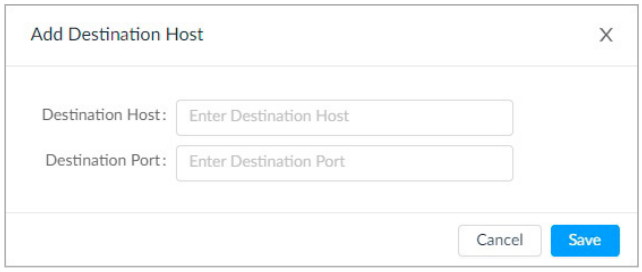


図 14-16　宛先ホストの追加

4. 宛先ホスト（IPv4 または IPv6 アドレス）とポート番号を入力して、トラップ宛先を定義します。
5. 「Save」をクリックして、トラップ宛先を保存します。
   設定をキャンセルするには、「Cancel」をクリックします。

■ エントリの編集 / 削除

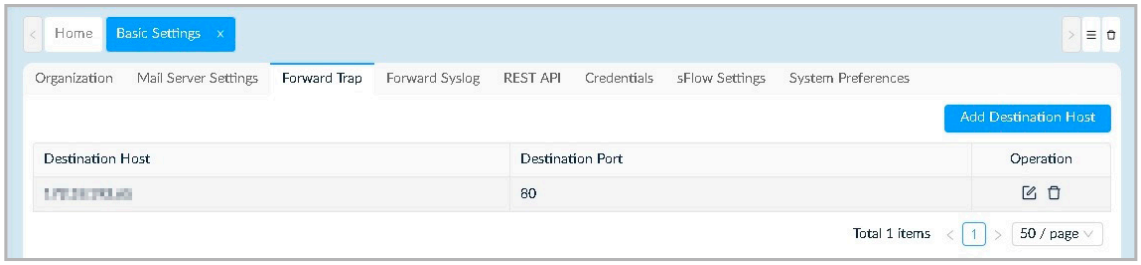


図 14-17　トラップ転送の宛先一覧

エントリの編集

(1) 「Operation」列の （Edit）アイコンを選択して、トラップ転送エントリの設定を変更します。

(2) 「Save」をクリックして、設定を保存します。

エントリの削除

(1) 「Operation」列の （Delete）アイコンを選択して、トラップ転送エントリを削除します。

(2) 確認メッセージが表示されます。エントリを削除する場合は「Yes」、キャンセルする場合は「No」をクリックします。

Syslog 転送の設定

外部 Syslog サーバに Syslog メッセージを送信するための設定を行います。

1. **System > Basic Settings** をクリックし、「Forward Syslog」タブを選択します。

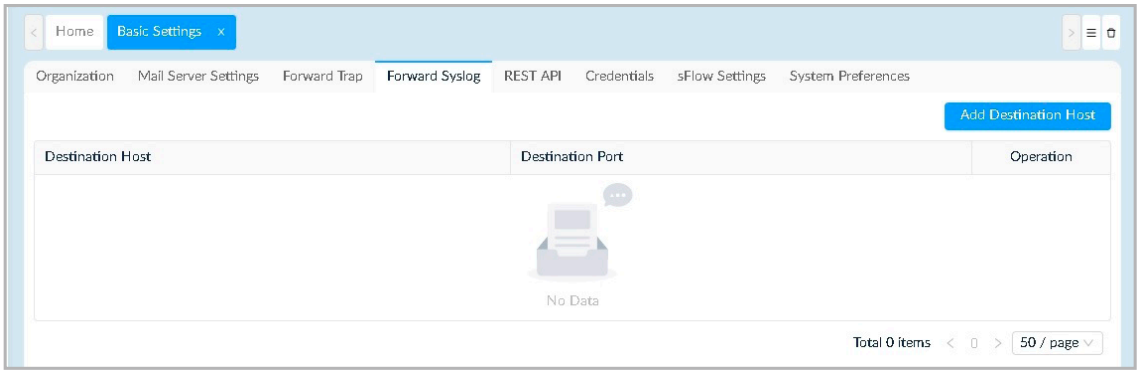


図 14-18　Syslog 転送

2. 「Add Destination Host」をクリックします。

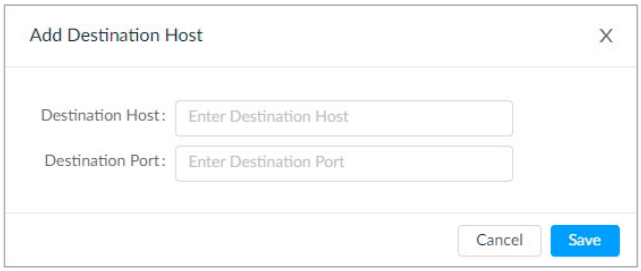


図 14-19　宛先ホストの追加

3. 宛先ホスト（IPv4 または IPv6 アドレス）とポート番号を入力して、Syslog 宛先を定義します。
4. 「Save」をクリックして、Syslog 宛先を保存します。
   設定をキャンセルするには、「Cancel」をクリックします。

■ エントリの編集 / 削除

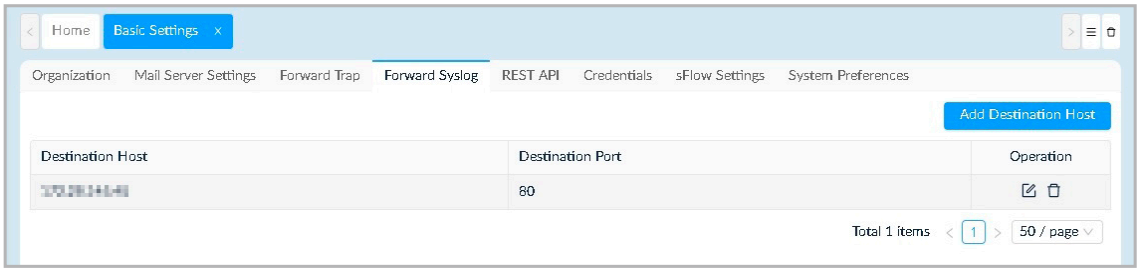


図 14-20　Syslog 転送の宛先一覧

エントリの編集

(1) 「Operation」列の （Edit）アイコンを選択して、Syslog 転送エントリの設定を変更します。

(2) 「Save」をクリックして、設定を保存します。

エントリの削除

(1) 「Operation」列の （Delete）アイコンを選択して、Syslog 転送エントリを削除します。

(2) 確認メッセージが表示されます。エントリを削除する場合は「Yes」、キャンセルする場合は「No」をクリックします。

REST API キーの生成

REST API 認証では、D-View8 のすべての REST API 接続に HTTPS を使用します。サードパーティ製アプリケーションが API を介してアクセスするために、認証が必要です。

メモ　本機能はエンタープライズ版のみサポートされます。

1. **System > Basic Settings** をクリックします。
2. 「REST API」タブを選択して、以下の画面を表示します。

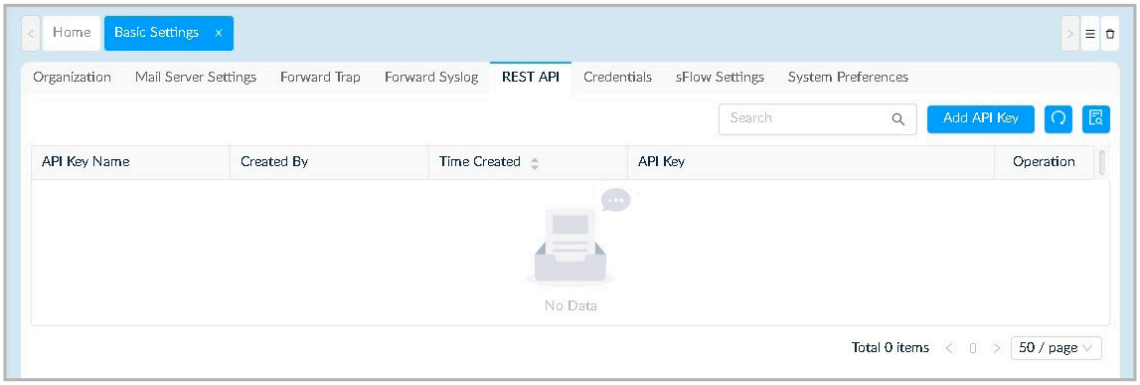


図 14-21　REST API

3. 「Add API Key」をクリックし、以下の画面を表示します。

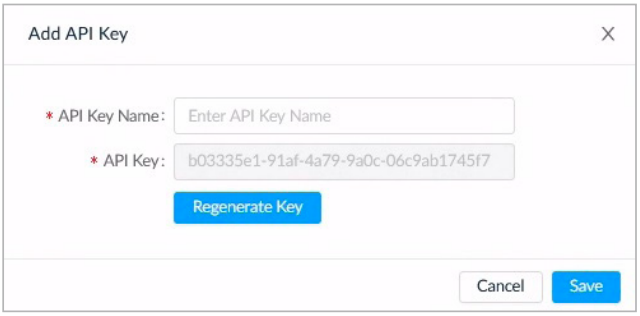


図 14-22　API キーの追加

4. 「API Key Name」欄に、API を識別するための名前を入力します。
5. 新しい鍵の値を生成するには、「Regenerate Key」をクリックします。
6. 「Save」をクリックして、REST API キーを保存します。設定をキャンセルするには、「Cancel」をクリックします。
REST API キーは、「Operation」列から無効化 / 有効化 / 削除することができます。

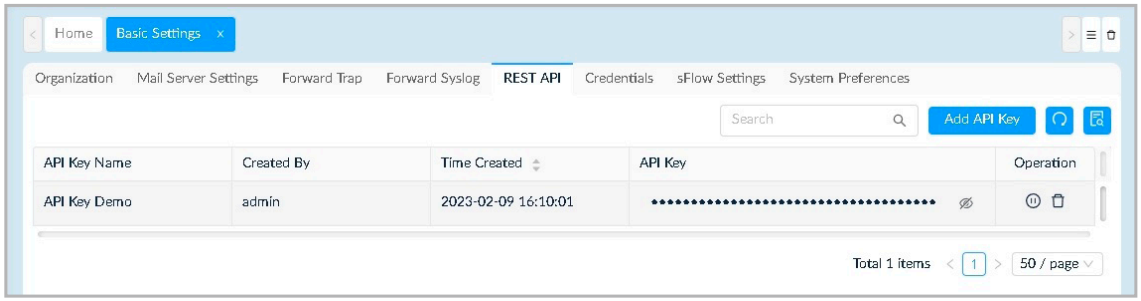


図 14-23　REST API

接続プロトコルの認証情報の設定

SNMP 認証プロファイル

SNMP 認証情報により、SNMP 互換デバイスへのアクセスを管理します。認証情報の定義を保存しておくと、システムによるネットワーク検出でネットワークデバイスをスキャンする際に便利です（**Monitoring > Network Discovery**）。ネットワーク検出の詳細は、P.96 の「ネットワークの検出」を参照してください。

1. **System > Basic Settings** をクリックします。
2. 「Credentials」タブを選択して、以下の画面を表示します。デフォルトでは「SNMP Credentials」タブが表示されます。

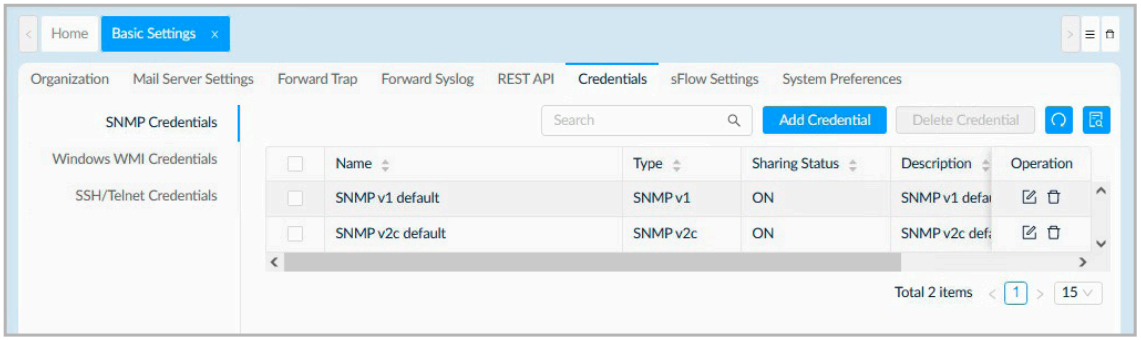


図 14-24　SNMP 認証情報

3. 「Add Credential」をクリックし、以下の画面を表示します。

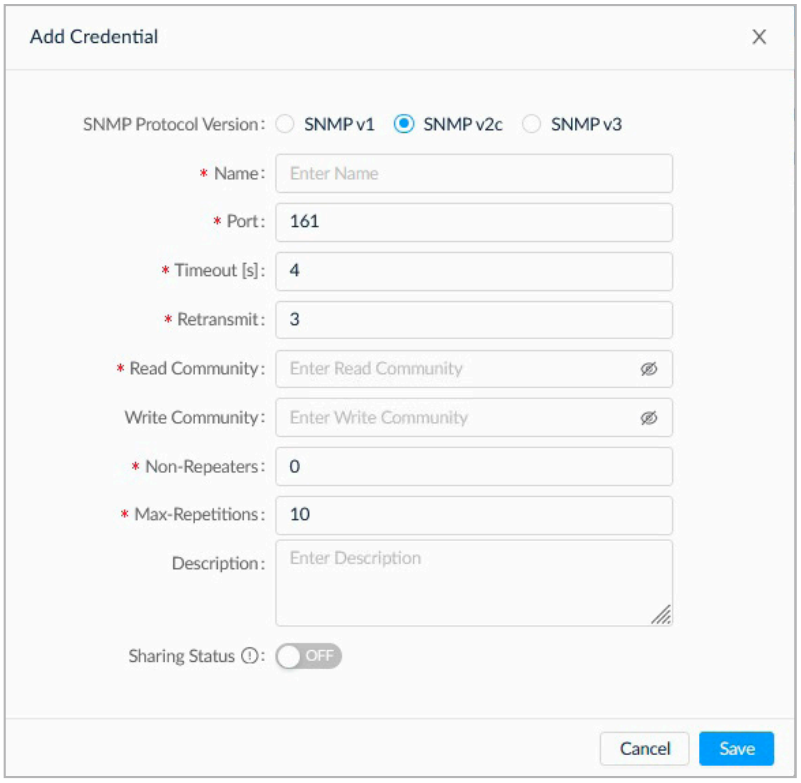


図 14-25　SNMP プロファイルの追加

4. SNMP バージョン（「SNMP v1」「SNMP v2c」「SNMP v3」）を選択します。デフォルトでは、D-View8 は SNMPv2c を使用します。
5. 選択したバージョンに応じて、以下の設定を行います。

「SNMPv1」を選択した場合

項目	説明
Name	プロファイルの名前を入力します。
Port	SNMP ポート番号を入力します。
Timeout [s]	タイムアウト時間を入力します。 • 初期値：4（秒）

項目	説明
Retransmit	リトライ回数を入力します。 ・ 初期値：3
Read Community	読み取り用の認証文字列を入力します。 ・ 初期値：public
Write Community	書き込み用の認証文字列を入力します。 ・ 初期値：private
Description	プロファイルを識別するための説明を入力します。（オプション）
Sharing Status	他のネットワークとの共有を有効または無効にします。 許可された役割を持つ他の管理者がこの SNMP 設定を表示および編集できるようにします。

「SNMPv2c」を選択した場合

項目	説明
Name	プロファイルの名前を入力します。
Port	SNMP ポート番号を入力します。
Timeout [s]	タイムアウト時間を入力します。 ・ 初期値：4（秒）
Retransmit	リトライ回数を入力します。 ・ 初期値：3
Read Community	読み取り用の認証文字列を入力します。
Write Community	書き込み用の認証文字列を入力します。
Non-Repeaters	単一の Get Next インスタンスで返されるオブジェクトの上限数を入力します。 ・ 初期値：0
Max-Repetitions	各変数に対して実行される Get Next 処理の数を入力します。 ・ 初期値：10
Description	プロファイルを簡単に識別するための説明を入力します。（オプション）
Sharing Status	他のネットワークとの共有を有効または無効にします。 許可された役割を持つ他の管理者がこの SNMP 設定を表示および編集できるようにします。

「SNMPv3」を選択した場合

項目	説明
Name	プロファイルの名前を入力します。
Port	SNMP ポート番号を入力します。
Timeout [s]	タイムアウト時間を入力します。 ・ 初期値：4（秒）
Retransmit	リトライ回数を入力します。 ・ 初期値：3
Non-Repeaters	単一の Get Next インスタンスで返されるオブジェクトの上限数を入力します。 ・ 初期値：0
Max-Repetitions	各変数に対して実行される Get Next 処理の数を入力します。 ・ 初期値：10
User Name	SNMPv3 ユーザ名を入力します。
Context Name	SNMPv3 エンティティの識別子として機能するコンテキスト名を入力します。（オプション）
Security Level	セキュリティレベルを選択します。 ・「authPriv」：認証と暗号化を使用します。（初期値） ・「authNoPriv」：認証を使用します。暗号化は使用しません。 ・「noAuthNoPriv」：認証も暗号化も使用しません。
Authentication Protocol	認証プロトコルを選択します。 ・「MD5」：ユーザを認証するための 128 ビットのハッシュ値を生成します。 ・「SHA」：ユーザを認証するための 160 ビットのハッシュ値を生成します。
Authentication Password	認証プロトコルで使用されるパスワードを入力します。
Privacy Protocol	暗号化プロトコルを選択します。 ・「DES」：DES アルゴリズムを使用してデータを暗号化します。 ・「AES」：AES アルゴリズムを使用してデータを暗号化します。
Privacy Password	データの暗号化に使用する暗号化パスワードを入力します。
Description	プロファイルを簡単に識別するための説明を入力します。（オプション）
Sharing Status	他のネットワークとの共有を有効または無効にします。 許可された役割を持つ他の管理者がこの SNMP 設定を表示および編集できるようにします。

6. 「Save」をクリックしてプロファイルを作成します。設定をキャンセルするには、「Cancel」をクリックします。

■ エントリの編集 / 削除

SNMP プロファイルは、「Operation」列から（Edit）または（Delete）をクリックして、変更または削除できます。

または、プロファイル一覧からエントリを選択して、「Delete Credential」をクリックすることで削除することもできます。

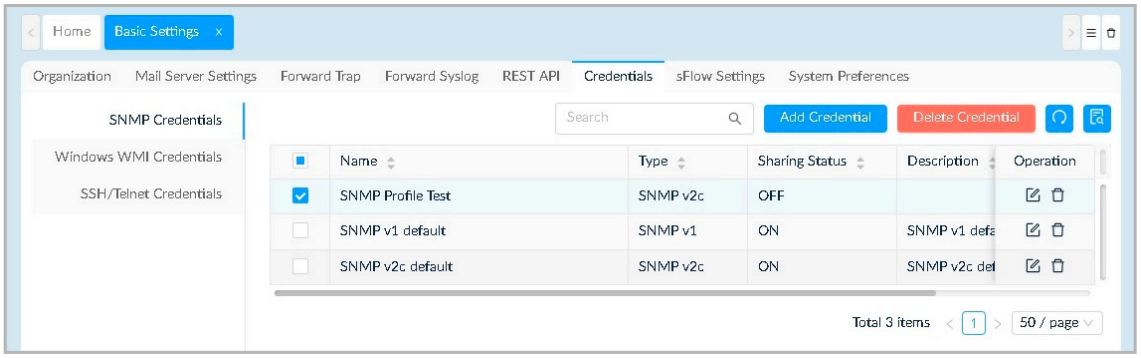


図 14-26　SNMP プロファイルの削除

WMI 認証プロファイル

Windows Management Instrumentation（WMI）は、Microsoft Windows システムでリモートシステムの情報を取得するために使用されます。本機能を使用するには、適切な権限が必要です。定義済みの資格情報は、ネットワーク検出でネットワークデバイスを検出するときに使用することができます（**Monitoring > Network Discovery**）。

1. **System > Basic Settings** をクリックします。
2. 「Credentials」タブを表示して、「Windows WMI Credentials」をクリックします。

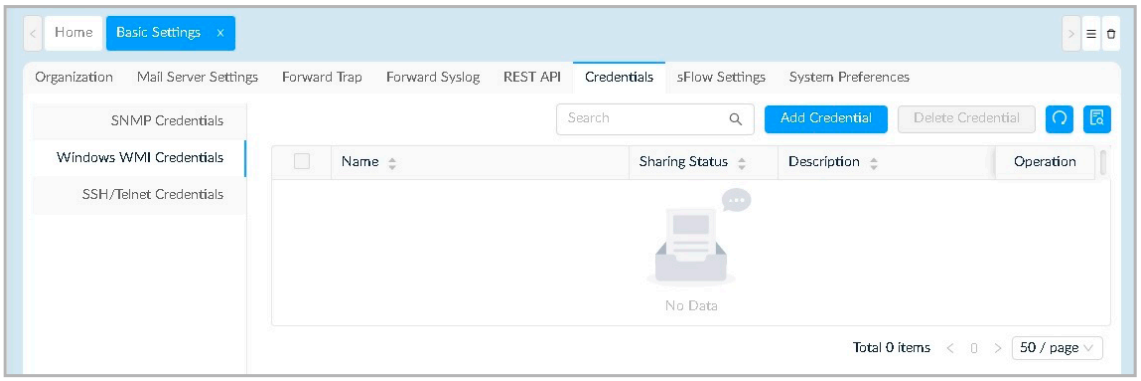


図 14-27　WMI 認証情報

3. 「Add Credential」をクリックし、以下の画面を表示します。

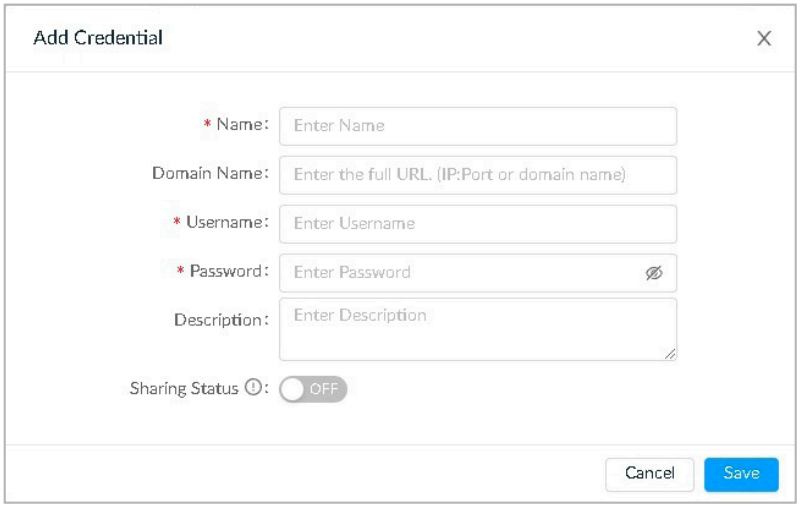


図 14-28　WMI プロファイルの追加

4. 以下の設定を行います。

項目	説明
Name	プロファイルの名前を入力します。
Domain Name	Windows ドメイン名を入力します。
User Name	Windows システム管理者権限を持つユーザ名、または WMI データにアクセスする権限を持つユーザアカウントを入力します。
Password	上記ユーザアカウントのパスワードを入力します。
Description	プロファイルを簡単に識別するための説明を入力します。
Sharing Status	他のネットワークとの共有を有効または無効にします。 組織内で権限のある他の管理者がこのプロファイルを表示または変更できるようにします。

5. 「Save」をクリックしてプロファイルを作成します。設定をキャンセルするには、「Cancel」をクリックします。

■ エントリの編集 / 削除

WMI プロファイルは、「Operation」列から（Edit）または（Delete）をクリックして、変更または削除できます。

または、プロファイル一覧からエントリを選択して、「Delete Credential」をクリックすることで削除することもできます。

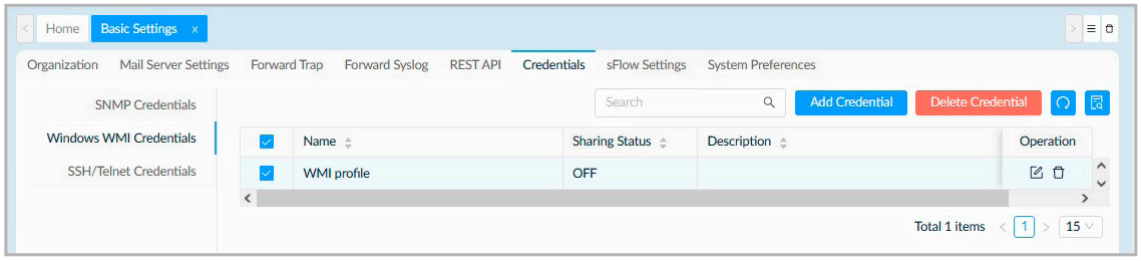


図 14-29　WMI プロファイルの削除

SSH/Telnet 認証プロファイル

SSH/Telnet 認証の資格情報を定義します。
SSH と Telnet は、D-View8 サーバのリモート管理を可能にします。通信ポートとアクセス権限を設定する必要があります。

（メモ）　本設定は現在のバージョンではサポートされません。（他の機能で使用することができません。）

1. **System > Basic Settings** をクリックします。
2. 「Credentials」タブを表示して、「SSH/Telnet Credentials」をクリックします。

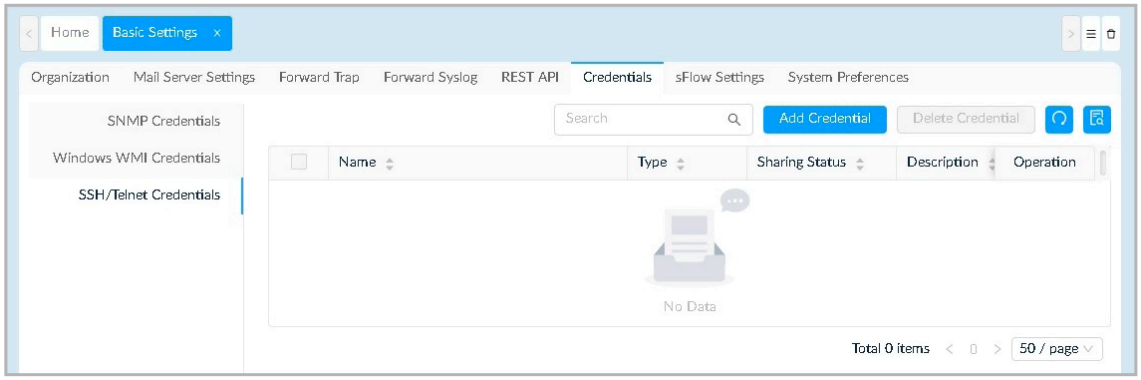


図 14-30　SSH/Telnet 認証情報

3. 「Add Credential」をクリックし、以下の画面を表示します。

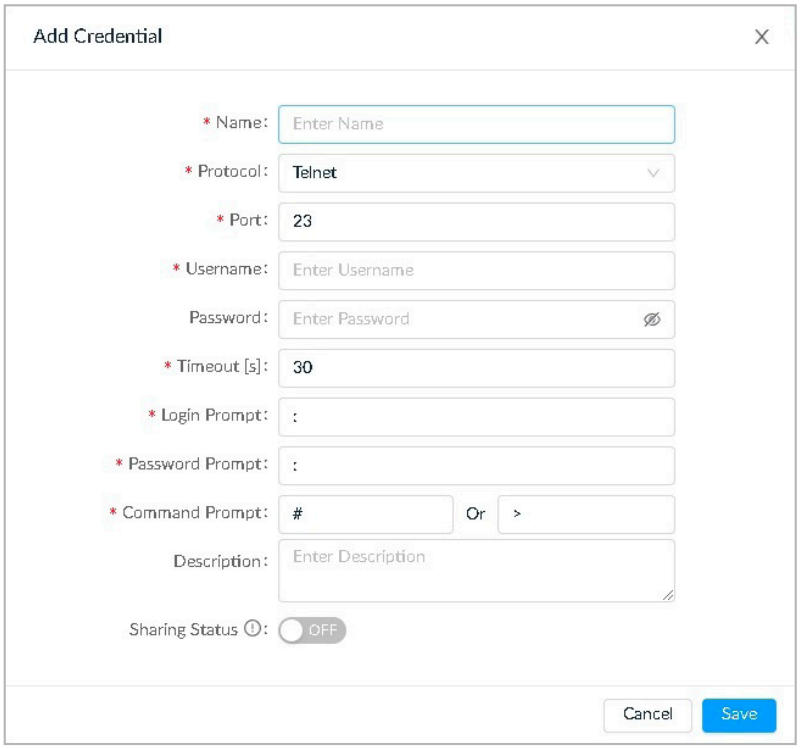


図 14-31　SSH/Telnet プロファイルの追加

4. 以下の設定を行います。

項目	説明
Name	プロファイルの名前を入力します。
Protocol	リモート管理に使用する通信プロトコルを選択します。 • 選択肢：「Telnet」「SSH」
Port	上記プロトコルで使用するポート番号を指定します。
User Name	サーバへのアクセスに必要なユーザ名を入力します。
Password	上記ユーザのパスワードを入力します。
Timeout [s]	セッションのタイムアウト時間（秒）を指定します。
Login Prompt	ログイン時に表示されるプロンプトを指定します。
Password Prompt	パスワード入力時にコマンドラインに表示されるプロンプトを指定します。
Command Prompt	コマンド入力時にコマンドラインに表示されるプロンプトを指定します。
Description	プロファイルを簡単に識別するための説明を入力します。
Sharing Status	他のネットワークとの共有を有効または無効にします。 組織内で権限のある他の管理者がこのプロファイルを表示または変更できるようにします。

5. 「Save」をクリックしてプロファイルを作成します。設定をキャンセルするには、「Cancel」をクリックします。

■ エントリの編集 / 削除

SSH/Telnet プロファイルは、「Operation」列から（Edit）または（Delete）をクリックして、変更または削除できます。

または、プロファイル一覧からエントリを選択して、「Delete Credential」をクリックすることで削除することもできます。

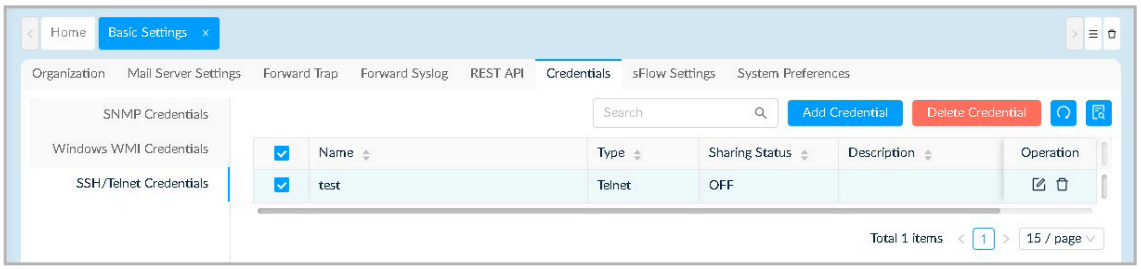


図 14-32　SSH/Telnet プロファイルの削除

sFlow 設定のセットアップ

D-View8 の sFlow 設定を使用すると、アプリケーションとネットワークリソースの効率的な管理を行うことができます。
本画面では、アプリケーションやDSCP名のマッピング設定を行います。sFlowアナライザ（**Monitoring > sFlow Analyzer**）でサンプリングされたパケットからのトラフィックを監視する際に役立ちます。

（メモ）　本機能はエンタープライズ版のみサポートされます。

■ sFlow 設定の表示

1. **System > Basic Settings** をクリックします。
2. 「sFlow Settings」タブをクリックし、以下の画面を表示します。

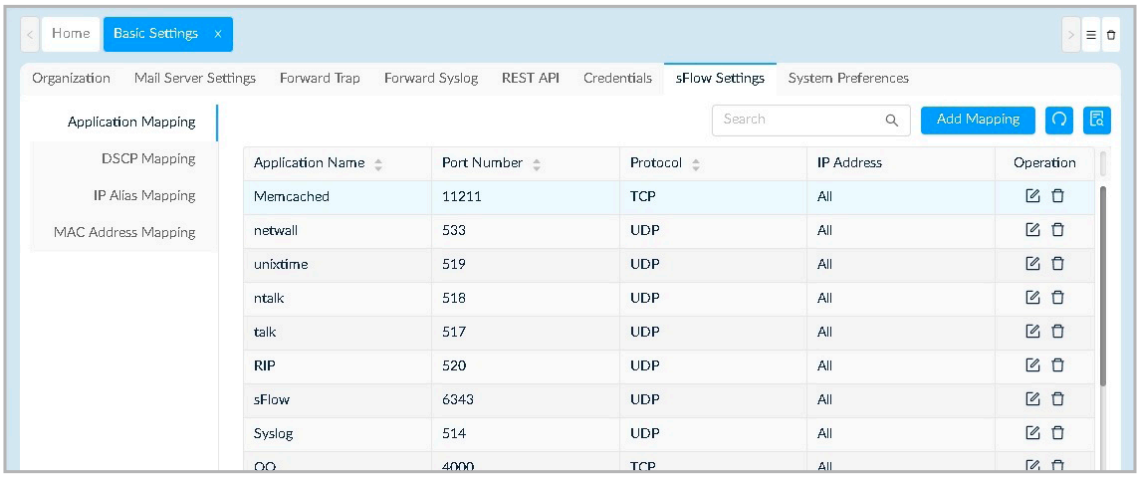


図 14-33　sFlow 設定

本画面では、以下のマッピングオプションが利用可能です。

- アプリケーションマッピング
- DSCP マッピング
- IP エイリアスマッピング
- MAC アドレスマッピング

アプリケーションマッピング

収集したデータのアプリケーションを適切に識別できるように設定します。

■ アプリケーションマッピングの設定

1. **System > Basic Settings** をクリックします。
2. 「sFlow Settings」タブを開き、「Application Mapping」をクリックします。

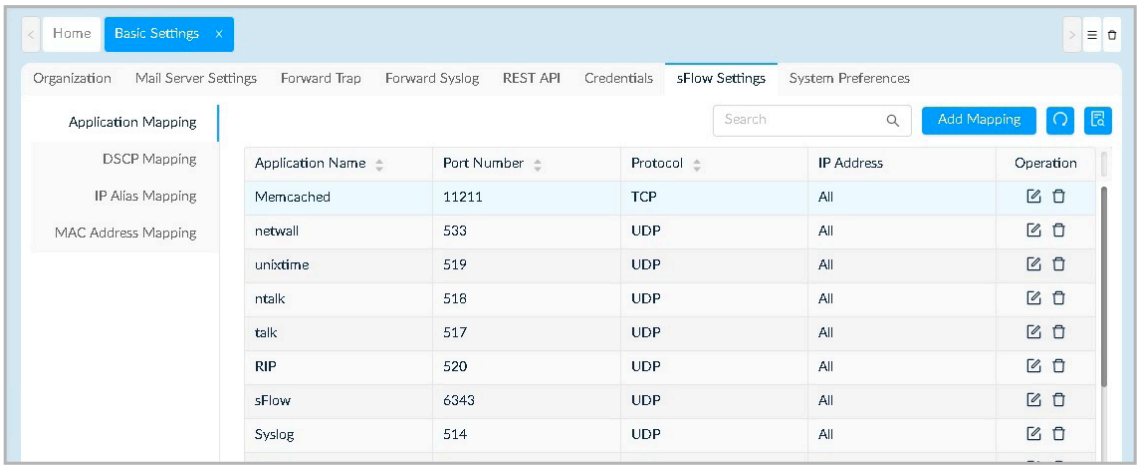


図 14-34　sFlow 設定（アプリケーションマッピング）

3. 「Add Mapping」をクリックし、マッピングルールを設定します。

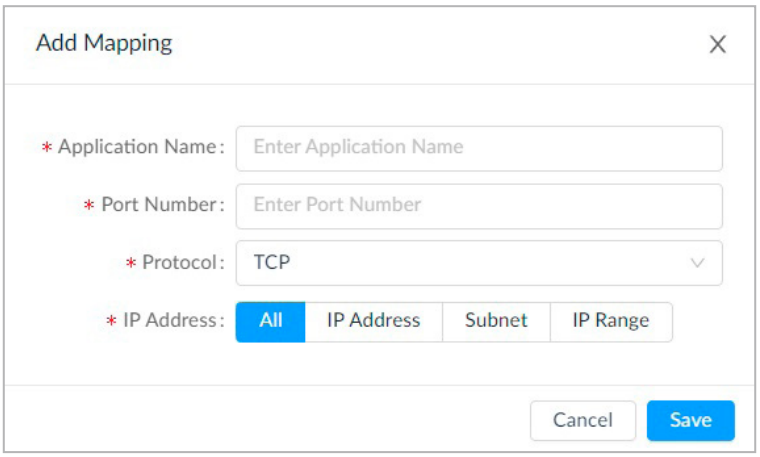


図 14-35　マッピングの追加

項目	説明
Application Name	アプリケーション名を入力します。
Port Number	ポート番号を入力します。
Protocol	ドロップダウンメニューを選択してプロトロルを選択します。 • 選択肢：「TCP」「UDP」
IP Address	IP アドレスの指定方法を選択して、フローデータのアドレス範囲を指定します。 • 選択肢：「All」「IP Address」「Subnet」「IP Range」

4. 「Save」をクリックしてアプリケーションマッピングルールを作成します。設定をキャンセルするには、「Cancel」をクリックします。

DSCP マッピング

QoS で使用される定義済み DSCP（Differentiated Services Code Point）の sFlow マッピングを表示します。

1. **System > Basic Settings** をクリックします。
2. 「sFlow Settings」タブを開き、sFlow 設定画面を表示します。

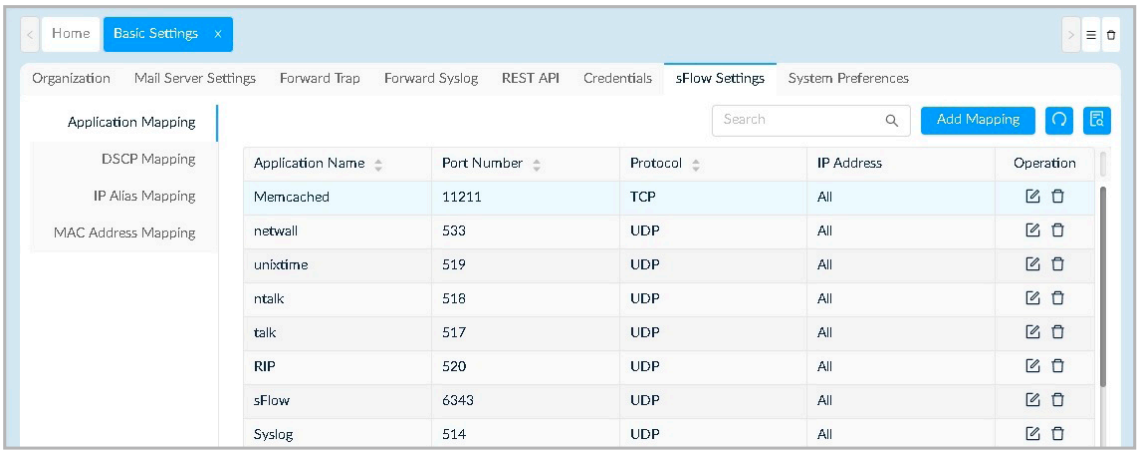


図 14-36　sFlow 設定（アプリケーションマッピング）

3. 「DSCP Mapping」をクリックします。DSCP 名と対応する値が表示されます。

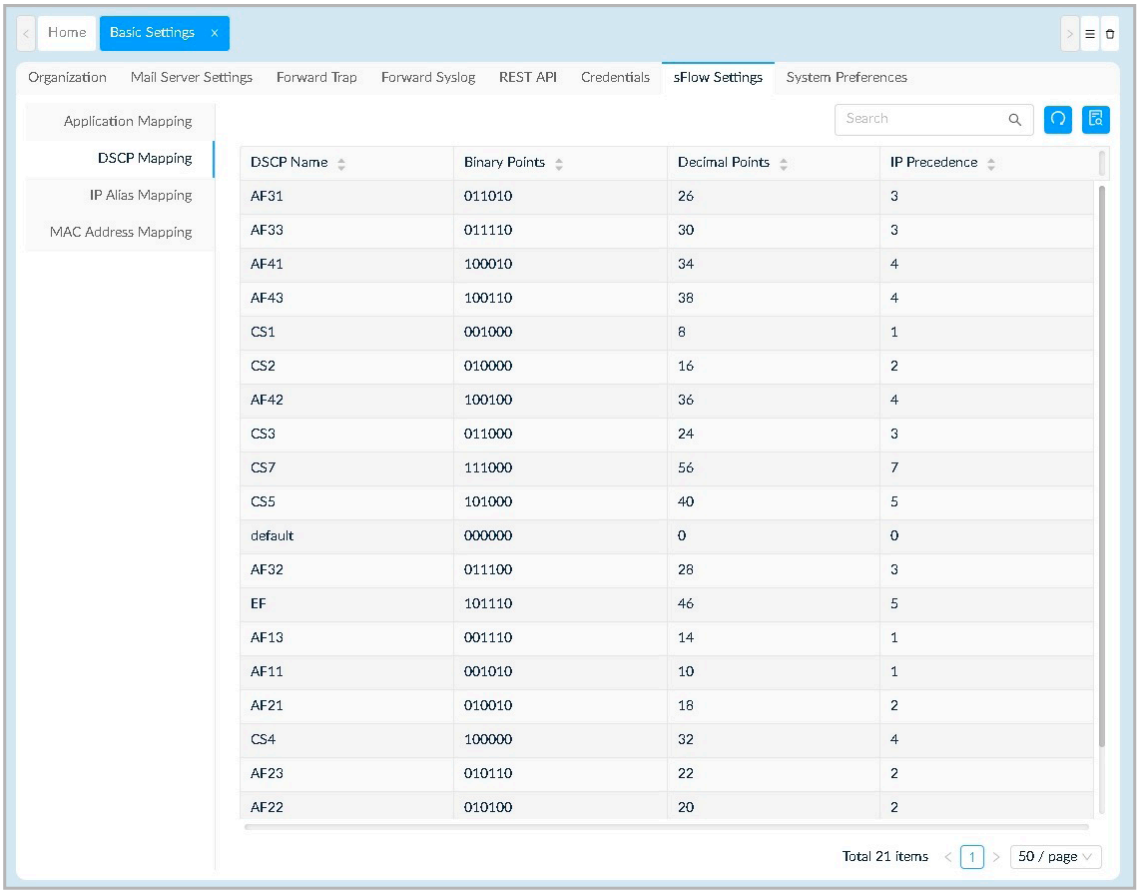


図 14-37　sFlow 設定（DSCP マッピング）

IP エイリアスマッピング

収集データの IP アドレスを定義された名前で識別できるように設定します。

1. **System > Basic Settings** をクリックします。
2. 「sFlow Settings」タブを開き、sFlow 設定画面を表示します。

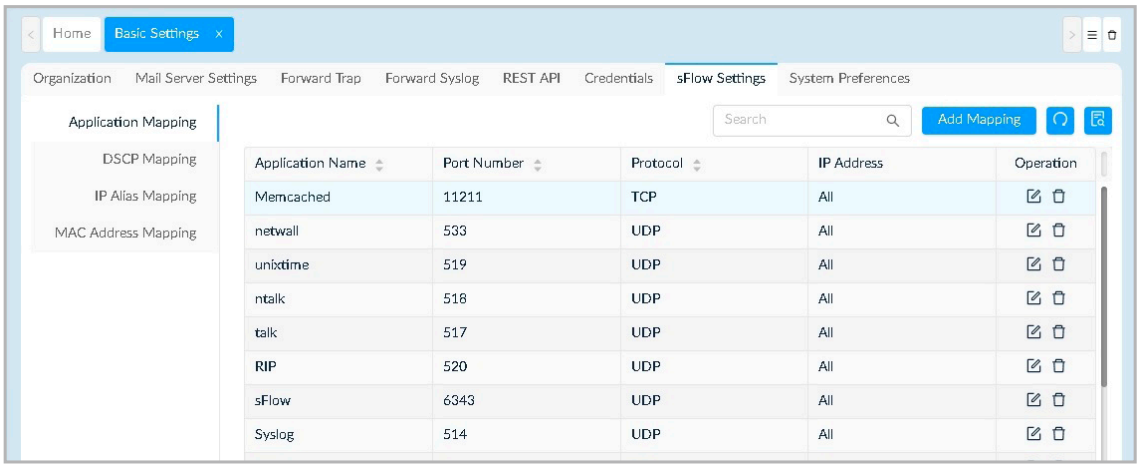


図 14-38　sFlow 設定（アプリケーションマッピング）

3. 「IP Alias Mapping」をクリックし、IP エイリアスマッピング画面を表示します。

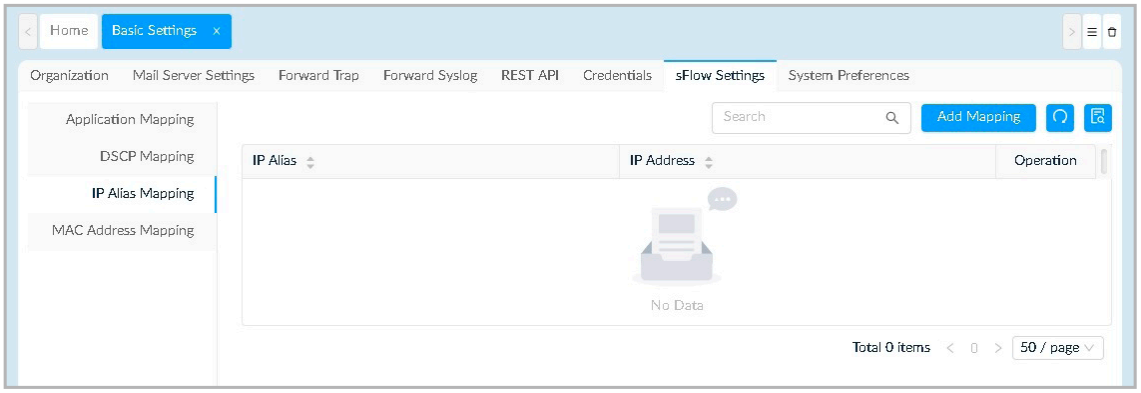


図 14-39　sFlow 設定（IP エイリアスマッピング）

4. 「Add Mapping」をクリックし、以下の画面を表示します。

図 14-40　マッピングの追加

5. IP エイリアスと IP アドレスを入力して、フローデータのエイリアスと IP アドレスのマッピングエントリを定義します。
6. 「Save」をクリックして、IP エイリアスマッピングルールを作成します。設定をキャンセルするには、「Cancel」をクリックします。

MAC アドレスマッピング

収集データの MAC アドレスを定義された名前で識別できるように設定します。

1. **System > Basic Settings** をクリックします。
2. 「sFlow Settings」タブを開き、sFlow 設定画面を表示します。

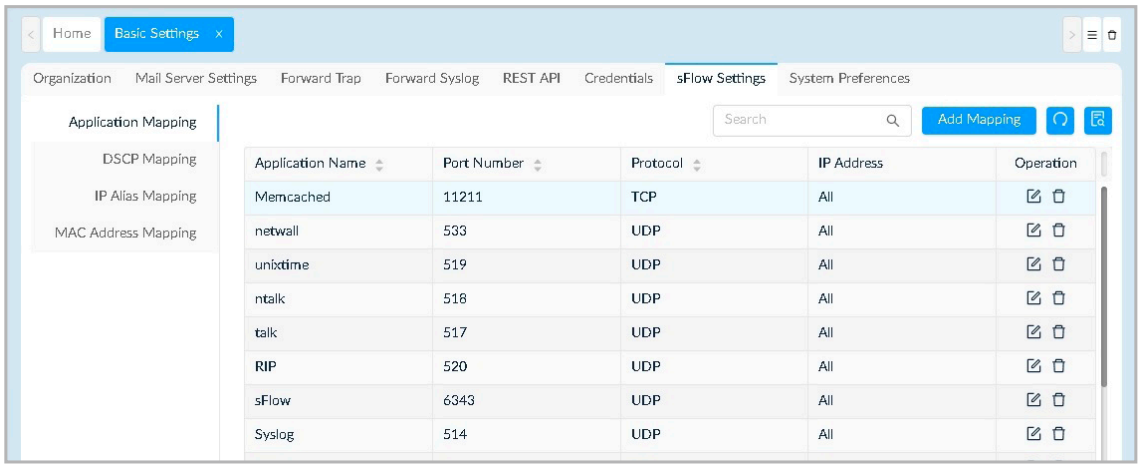


図 14-41　sFlow 設定（アプリケーションマッピング）

3. 「MAC Address Mapping」をクリックし、MAC アドレスマッピング画面を表示します。

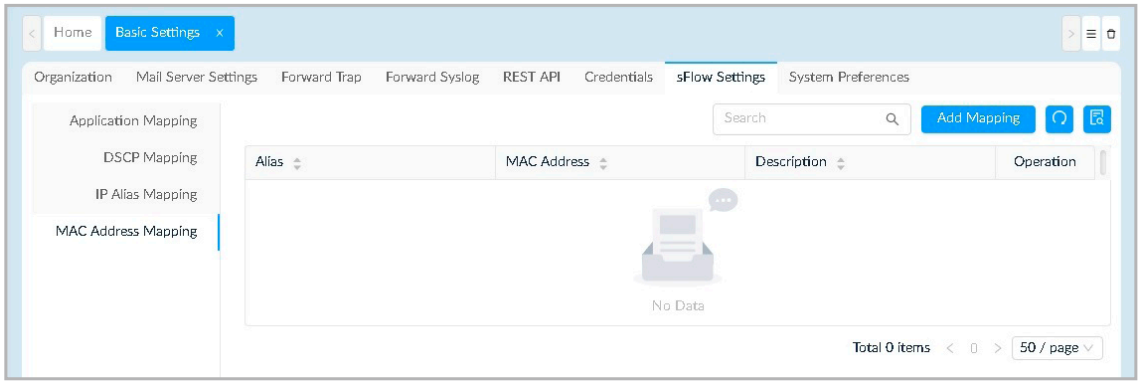


図 14-42　sFlow 設定（MAC アドレスマッピング）

4. 「Add Mapping」をクリックし、以下の画面を表示します。

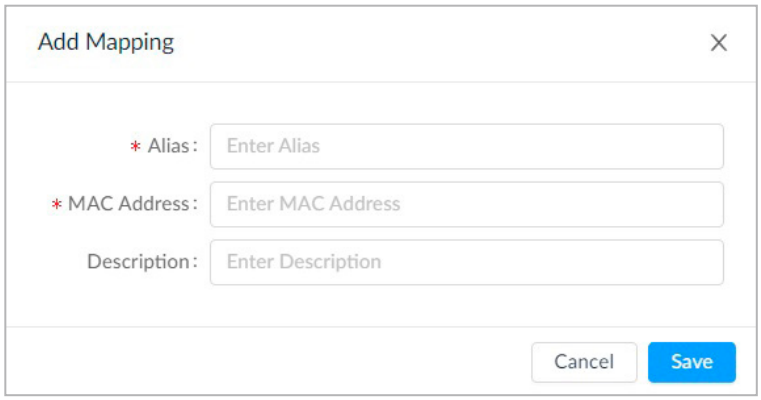


図 14-43　マッピングの追加

5. エイリアス、MAC アドレスを入力して、エイリアスと MAC アドレスのマッピングエントリを定義します。
6. 「Save」をクリックして、MAC アドレスマッピングルールを作成します。設定をキャンセルするには、「Cancel」をクリックします。

システム環境設定

インタフェースの全体レイアウトのテーマ、およびテーブル（表）の設定を行います。

1. **System > Basic Settings** をクリックし、「System Preferences」タブを選択します。

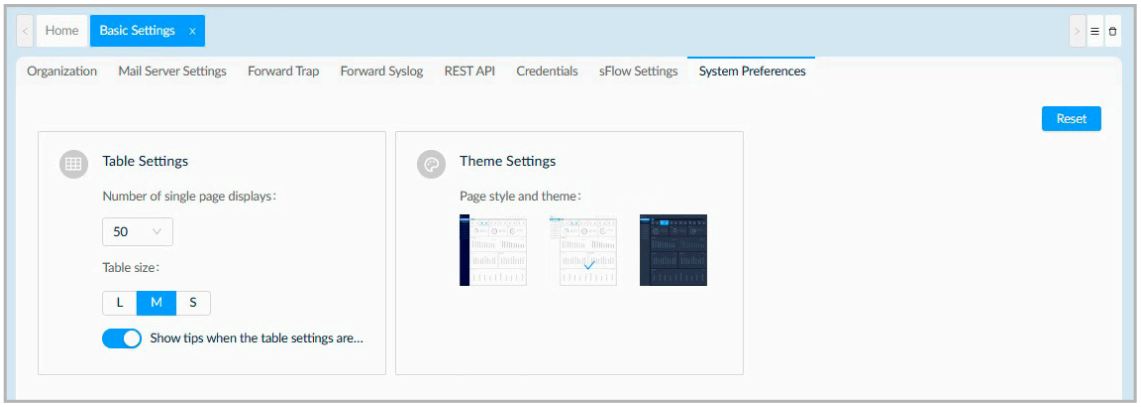


図 14-44　システム環境設定

2. 各セクションで、テーブルおよびテーマの設定を行います。

■ Table Settings（テーブル設定）

項目	説明
Number of single page displays	D-View8 で表示されるテーブルについて、1 ページあたりの項目（行）の表示数を選択します。 • 選択肢：「50」「100」「200」 • 初期値：「50」
Table size	D-View8 で表示されるテーブルについて、表示サイズを設定します。 • 選択肢：「L（Large）」「M（Middle）」「S（Small）」 • 初期値：「M」
Show tips when the table settings are modified	ON にした場合、各画面でテーブルの項目表示数を変更した時に、システム全体に同じ設定を適用するかどうかメッセージが表示されます。

■ Theme Settings（テーマ設定）

項目	説明
Page style and theme	インタフェースに適用する定義済みのテーマを選択します。 背景が暗い / 明るいモード、または左側のメインメニューのみ暗いモードに設定することができます。

元の設定にリセットするには、「Reset」ボタンをクリックします。すべてのテーブルとテーマ設定がデフォルト状態にリセットされます。

スケジュール機能

スケジュール機能で定義される、指定期間や繰り返しのスケジュールに従って、スケジュールに対応している各種機能を自動化することができます。

スケジュールオプションには、「Recurrent」と「Time Range」の 2 種類があります。
- 「Recurrent（繰り返し）」：ネットワーク検出、タスク、設定のバックアップと復元、スケジュールされたレポートで利用できます。
- 「Time Range（時間範囲）」：アラーム設定と通知ルールで利用できます。

繰り返しのスケジュールの設定

1. **System > Scheduling** に移動し、「Recurrent Schedule List」タブを開きます。
2. 「Add Schedule」をクリックし、以下の設定を行います。

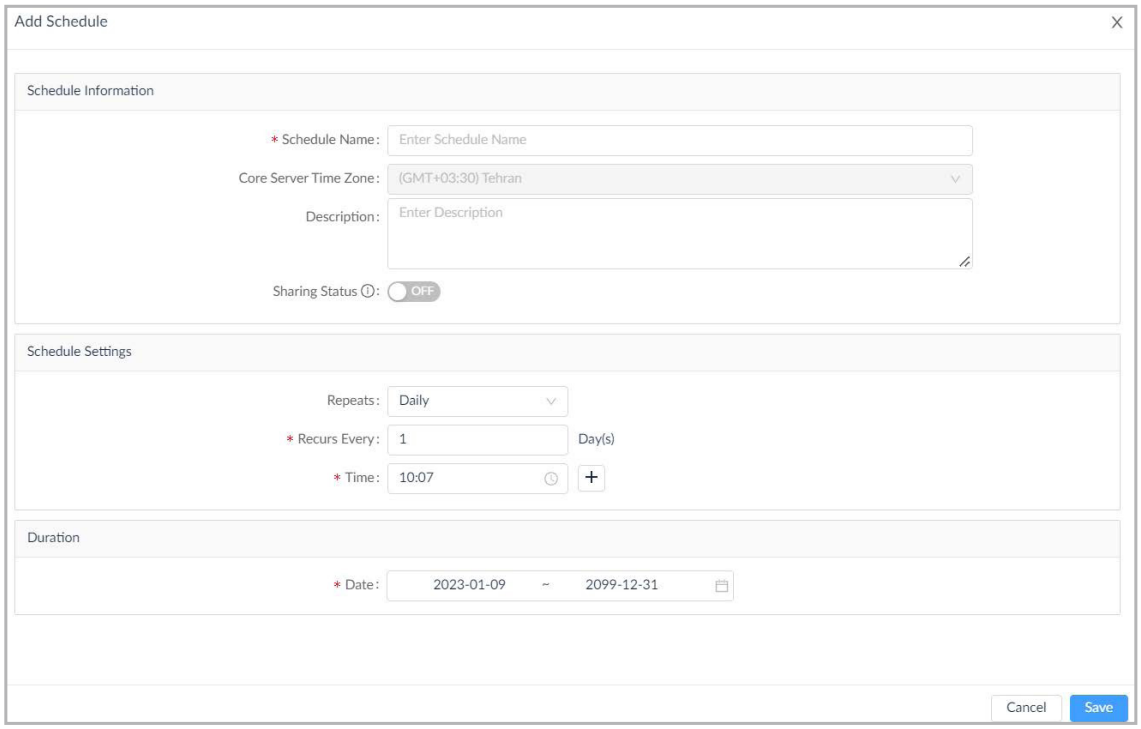


図 14-45　スケジュールの追加

設定項目：

項目	説明
Schedule Information	
Schedule Name	スケジュールの名前を入力します。
Core Server Time Zone	「Basic Settings」画面の「Organization」タブで設定されているコアサーバタイムゾーンが表示されます。
Description	スケジュールの簡単な説明を入力します。
Sharing Status	他のネットワークとの共有を有効または無効にします。 許可された役割を持つ他の管理者がこのスケジュール設定を表示および編集できるようにします。
Schedule Settings	
Repeats	スケジュールの頻度（単位）を選択します。 • 「Daily」「Weekly」「Monthly」「Specific Days」
Recurs Every/ Repeat Month/ Repeat On	スケジュールの頻度を設定します。 • 「Daily」：実行するデイリー間隔を選択します。「1」を指定した場合、タスクを毎日実行します。「2」を指定した場合、タスクを 2 日ごと（1 日おき）に実行します。 • 「Weekly」:実行間隔を週単位で選択します。「1」を指定した場合、毎週指定した曜日にタスクを実行します。「2」を指定した場合、隔週（1 週間おき）にタスクを実行します。 • 「Monthly」：タスクを実行する月と日付を指定します。 • 「Specific Days」：タスクを実行する年月日を指定します。
Time	スケジュールの時刻（24 時間表記、<hh:mm> 形式）を選択します。複数設定すると、異なる時刻に同じタスクを実行できます。
Duration	
Duration	有効期間となる開始日と終了日を選択します。

タイムレンジスケジュールの設定

1. **System > Scheduling** に移動し、「Time Range Schedule List」タブを開きます。
2. 「Add Schedule」をクリックし、以下の設定を行います。

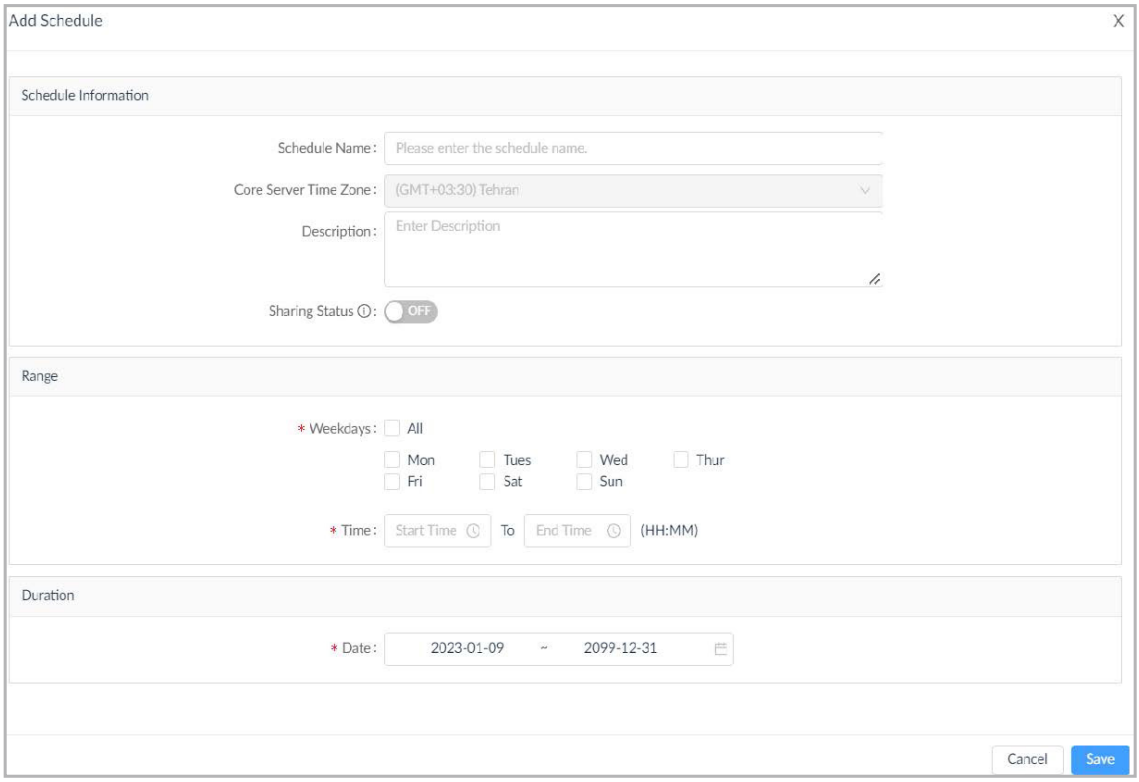


図 14-46　スケジュールの追加

設定項目：

項目	説明
Schedule Information	
Schedule Name	スケジュールの名前を入力します。
Core Server Time Zone	「Basic Settings」画面の「Organization」タブで設定されているコアサーバタイムゾーンが表示されます。
Description	スケジュールの簡単な説明を入力します。
Sharing Status	他のネットワークとの共有を有効または無効にします。 許可された役割を持つ他の管理者がこのスケジュール設定を表示および編集できるようにします。
Range	
Weekdays	曜日を選択します。
Time	スケジュールの時間帯（24 時間表記、<hh:mm> 形式）を選択します。
Duration	
Duration	有効期間となる開始日と終了日を選択します。

ライセンス管理

製品の表示

D-View8 の製品およびライセンスの情報は、「About」画面で確認できます。

メモ　ライセンス画面を表示できるのは、「Super Administrator」権限の管理者のみです。

1. **System > About** に移動します。
2. 製品およびソフトウェア情報が表示されます。

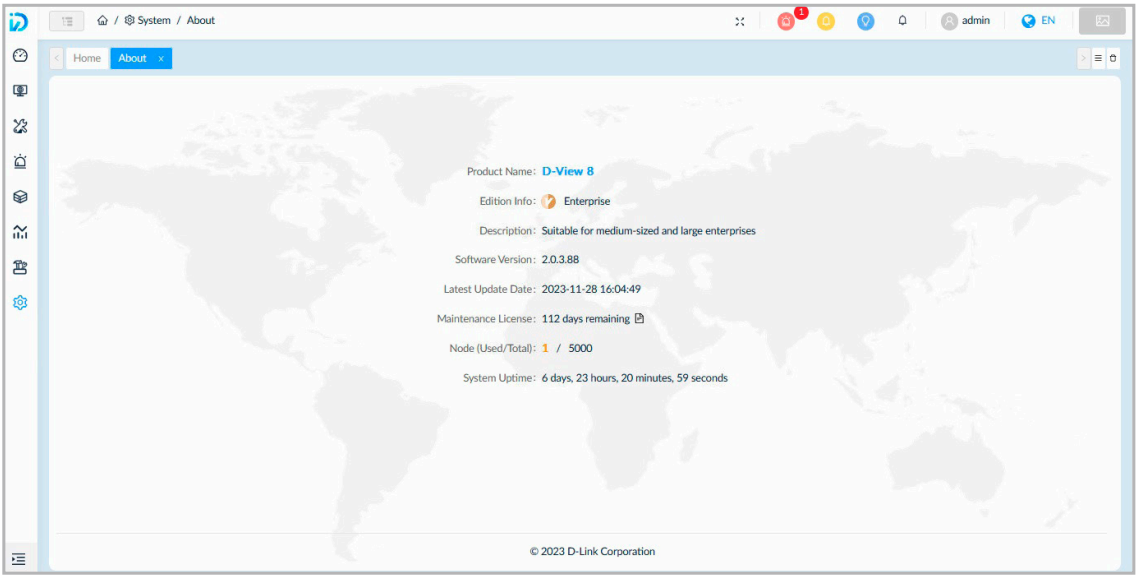


図 14-47　製品およびソフトウェア情報

設定項目：

項目	説明
Product Name	製品名（D-View8）が表示されます。
Edition Info	エディション情報（Standard または Enterprise）が表示されます。
Description	製品の簡単な説明が表示されます。
Software Version	システムの現在のソフトウェアバージョンが表示されます。
Latest Update Date	システムが最後に更新された日付が表示されます。
Maintenance License	ライセンス有効期間の残り日数が表示されます。
Node (Used/Total)	現在の管理ノード数 / サポートされる合計ノード数が表示されます。
System Uptime	システムが稼働している時間（日数 / 時間 / 分 / 秒）が表示されます。

3 か月間の試用期間を過ぎると、有効なライセンスで製品のアクティベーションを行うようにメッセージが表示されます。

製品購入時のアクティベーション

1. **System > About** に移動します。
2. 製品名として表示されている D-View8 の横にある「Activation」リンクをクリックし、製品アクティベーションプロセスを開始します。

図 14-48　アクティベーション

3. 「ADD LICENSE」画面が表示されます。

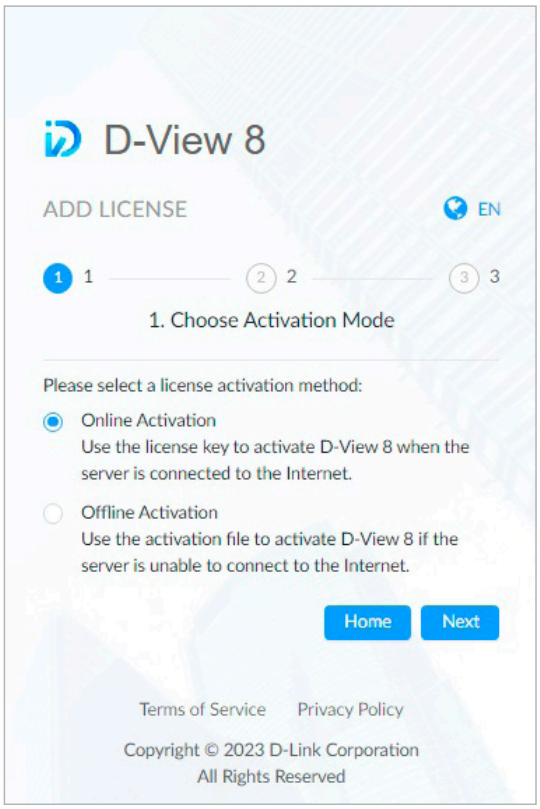


図 14-49　ライセンスの追加

4. 次のいずれかの方法を選択します。

項目	説明
Online Activation	ライセンスキーを使用して D-View8 をアクティブ化します。サーバはインターネットに接続されている必要があります。「Next」をクリックして続行し、画面の手順に従ってプロセスを完了します。この方法では、購入したライセンスのライセンスキーを入力します。
Offline Activation	アクティベーションファイルを使用して D-View8 をアクティブ化します。サーバはインターネットに接続されている必要はありません。この方法では、D-View8 オフラインアクティベーションツールにより生成されたアクティベーションファイルをアップロードします。

■ オフラインアクティベーション時のアクティベーションファイル生成手順

オフラインアクティベーションでは、以下の手順で D-View8 オフラインアクティベーションツールを実行し、生成されたアクティベーションファイルを D-View8 サーバにアップロードします。

メモ　D-View8 オフラインアクティベーションツールは D-Link Japan 製品サイトからダウンロードしてください。

メモ　D-View8 オフラインアクティベーションツールはインターネットに接続可能な PC 上で実行する必要があります。

1. D-View8 オフラインアクティベーションツールの実行ファイルをダブルクリックして、プログラムを起動します。
2. 「License Type」ドロップダウンリストから「Standard/Enterprise License」を選択します。
3. 「License Key」に、購入したライセンスのライセンスキーを入力します。
4. 「Bound MAC」に D-View8 サーバの MAC アドレスを入力します。（ライセンスキーはサーバのハードウェアに関連付けられます。）
5. 「Browse」をクリックしてアクティベーションファイルの出力ディレクトリを指定します。
6. 「Generate」をクリックして、アクティベーションファイルを生成します。

製品ライセンス情報の表示

1. **System** > **About** に移動します。
2. 「Maintenance License」項目の をクリックして、製品とメンテナンスライセンスの情報を表示します。

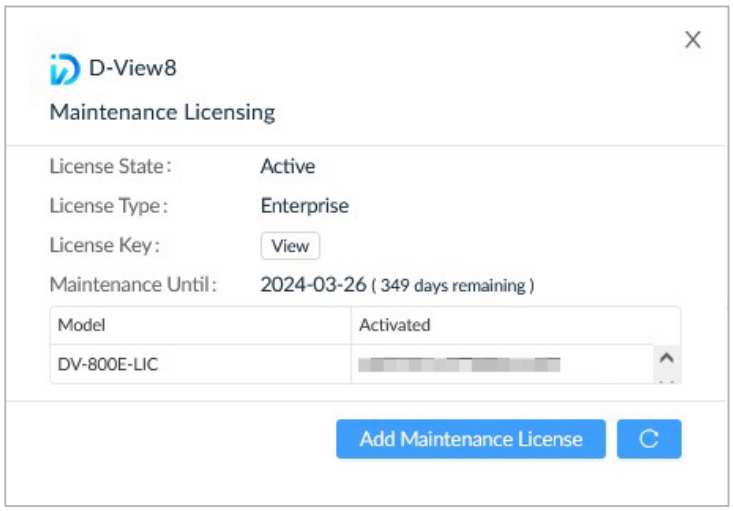


図 14-50　メンテナンスライセンス情報

項目	説明
License State	製品ライセンスのステータス（アクティブまたは非アクティブ）が表示されます。
License Type	ライセンスの種類（Standard または Enterprise）が表示されます。
License Key	「View」をクリックすると、購入したライセンスキーが下部に表示されます。
Maintenance Until	ライセンスの期限とライセンス期限切れまでの日数が表示されます。購入したすべてのライセンスの合計日数になります。

メモ　製品アクティベーションの最初の 1 年間が経過すると、新しいメンテナンスライセンスを購入するようにメッセージが表示されます。

追加メンテナンスライセンスのアクティベーション

最初にご購入いただくスタンダード版またはエンタープライズ版ライセンスには、1 年間のフリーメンテナンスサポートが付いています。フリーメンテナンスサポート期間が過ぎると、管理ノードは 30 台に制限されます。スタンダード版またはエンタープライズ版のメンテナンスサポート（上限管理数までの D-View8 機能サポート）を継続して利用するには、追加ライセンスをご購入いただく必要があります。

1. **System > About** に移動します。
1. 「Maintenance License」項目の をクリックして、製品とメンテナンスライセンスの情報を表示します。
1. 「Add Maintenance License」をクリックし、ライセンスアクティベーションプロセスを開始します。
2. 「ADD ANNUAL LICENSE」画面が表示されます。

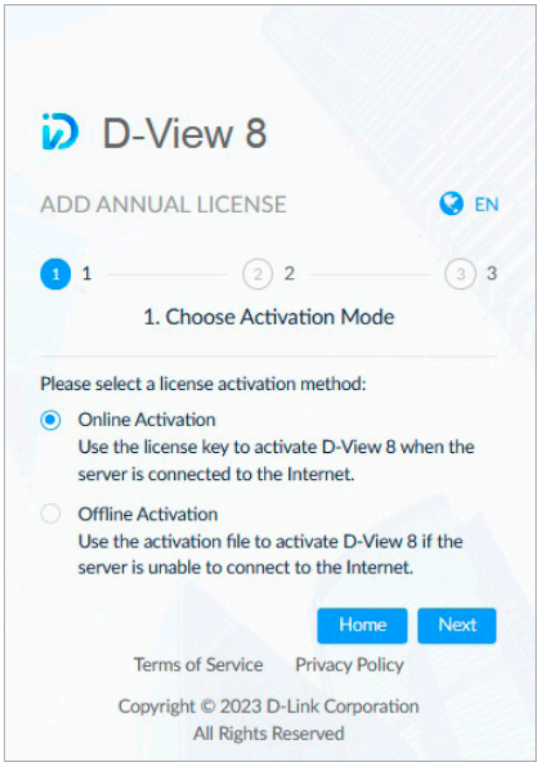


図 14-51　年間ライセンスの追加

3. 次のいずれかの方法を選択します。

項目	説明
Online Activation	ライセンスキーを使用してメンテナンスサービスで D-View8 を再アクティブ化します。サーバはインターネットに接続されている必要があります。「Next」をクリックして続行し、画面の手順に従ってプロセスを完了します。この方法では、購入したライセンスのライセンスキーを入力します。
Offline Activation	アクティベーションファイルを使用してメンテナンスサービスで D-View8 を再アクティブ化します。サーバはインターネットに接続されている必要はありません。「Download the current activation file」をクリックしてアクティベーションファイルをダウンロードし、再アクティベーションファイルを生成します。

■ オフラインアクティベーション（メンテナンスライセンス追加）時のアクティベーションファイル生成手順

オフライン再アクティベーションでは、D-View8 サーバからアクティベーションをダウンロードした後、以下の手順で D-View8 オフラインアクティベーションツールを実行し、生成された新しいアクティベーションファイルを D-View8 サーバにアップロードします。

メモ　D-View8 オフラインアクティベーションツールは D-Link Japan 製品サイトからダウンロードしてください。

メモ　D-View8 オフラインアクティベーションツールはインターネットに接続可能な PC 上で実行する必要があります。

1. D-View8 オフラインアクティベーションツールの実行ファイルをダブルクリックして、プログラムを起動します。
2. 「License Type」ドロップダウンリストから「Annual Maintenance License」を選択します。
3. 「License Key」に、購入したライセンスのライセンスキーを入力します。
4. 「Current AC File」で「Browse」をクリックして、上記「ADD ANNUAL LICENSE」画面でダウンロードした ac ファイルを指定します。
5. 「Generate」をクリックして、新しいアクティベーションファイルを生成します。

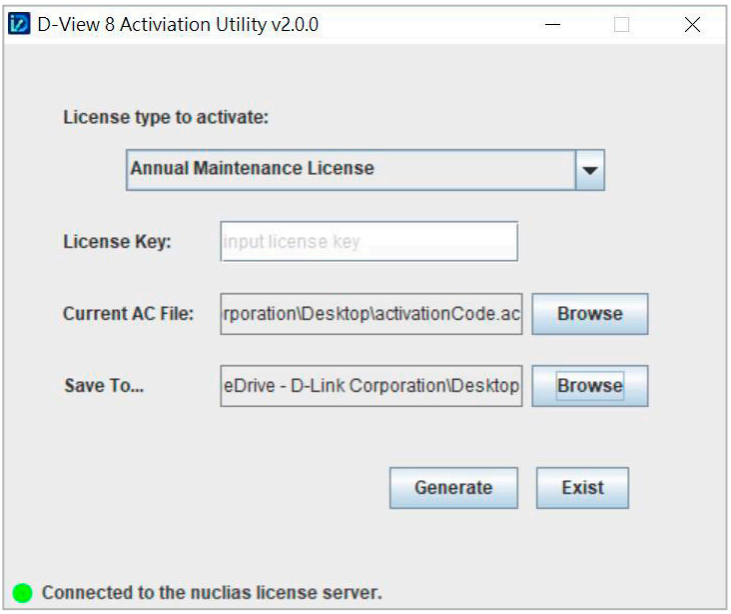


図 14-52　オフラインアクティベーション

注意　メンテナンスライセンスの有効期限が近づくと、有効期限の 30 日前に有効期限が近いライセンスが通知されます。

ライセンス有効期限のリマインダー

有効期限の 7 日前に再びリマインダーを設定することができます。適切なタイミングで次の画面のように通知メッセージが表示されます。その後、有効期限の 3 日前に再びリマインドするように選択できます。

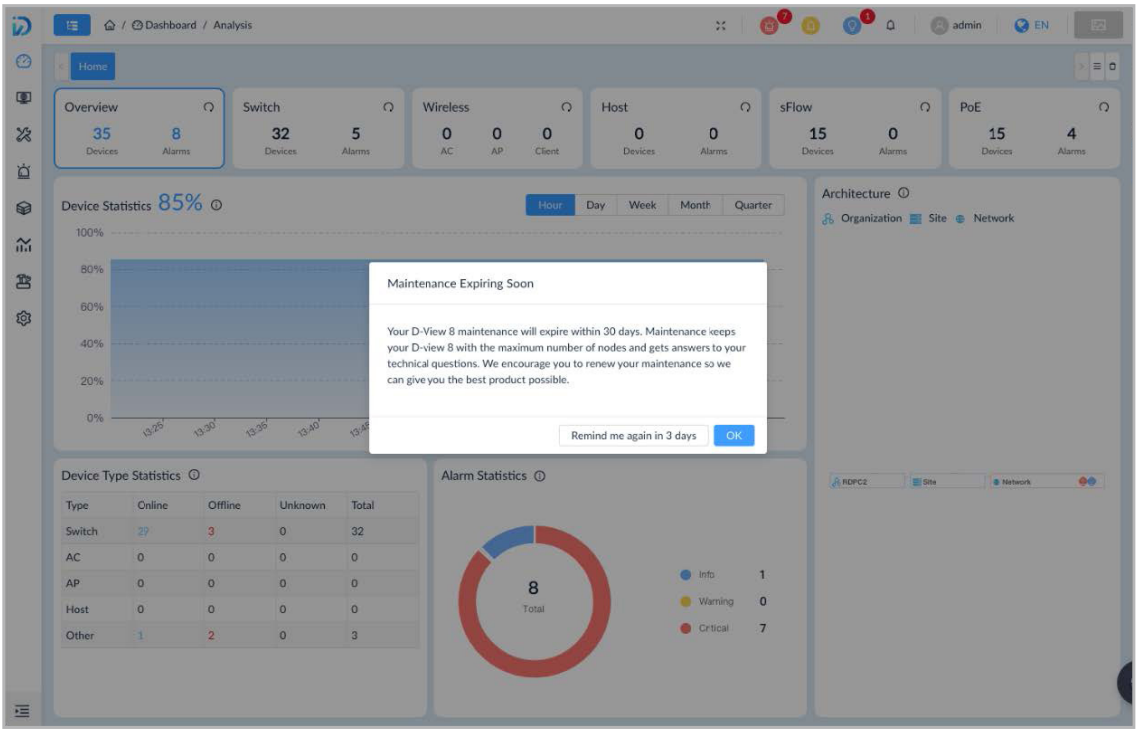


図 14-53　スケジュール

メンテナンスライセンスの有効期限が切れると、システムからアラートが通知されます。D-View8 Web アプリケーションの以下の画面にメッセージが表示されます。

- Dashboard > Analysis
- Monitoring > Device View
- Monitoring > Topology Map
- Configuration > Bach Configuration
- Configuration> Firmware Management
- Configuration > Configuration Management

D-View8 ログ

「D-View8 Log」画面には、以下の種類のログが表示されます。

- 「User Operation Log」タブ：ユーザが実行した管理操作とタスクに関連するログが表示されます。
- 「System Log」タブ：システムのサービスと Probe エージェントのアクティビティに関連するログが表示されます。
- 「Device Maintenance Log」タブ：管理対象デバイスに対し実行した操作に関連するログが表示されます。

ログは、デバイスの正常性の分析、ネットワーク接続のトラブルシューティング、およびネットワークセキュリティのテストに使用できます。
これらの D-View8 ログは、管理対象デバイスによって生成されるデバイスの「Syslog」とは異なります（**Alarm & Notification > Trap & Syslog**）。

メモ　許可されたレベルのネットワーク階層のアクティビティに関連するログのみを表示できます。

ユーザ操作ログの表示

1. **System > D-View 8 Log** 移動します。
2. 「User Operation Log」タブを選択します。ログエントリには次の情報が含まれます。

項目	説明
Log Time	ユーザアクティビティのタイムスタンプが表示されます。
Terminal Type	D-View8 サーバとの接続に使用するデバイスとインタフェースが表示されます。
User	ユーザ名が表示されます。
Operation Object	ユーザが操作したオブジェクト / メニューカテゴリが表示されます。
Detail	操作の詳細なアクティビティが表示されます。

システムログの表示

1. **System > D-View 8 Log** 移動します。
2. 「System Log」タブを選択します。ログエントリには次の情報が含まれます。

項目	説明
Log Time	システムアクティビティのタイムスタンプが表示されます。
Log Type	サーバアクティビティの簡単な説明が表示されます。
Server	影響を受けるサーバと IP アドレスが表示されます。
Detail	サーバアクティビティの詳細情報が表示されます。

デバイスメンテナンスログの表示

1. **System > D-View 8 Log** 移動します。
2. 「Device Maintenance Log」タブを選択します。ログエントリには次の情報が含まれます。

項目	説明
Log Time	デバイス操作アクティビティのタイムスタンプが表示されます。
Result	デバイス操作の結果が表示されます。
Configuration Type	操作の設定カテゴリが表示されます。
Function	機能名が表示されます。
System Name	デバイスのシステム名が表示されます。
Model Name	デバイスのモデル名が表示されます。
IP	デバイスの IP アドレスが表示されます。
User	オペレータのユーザ名が表示されます。
Site	デバイスのネットワークサイトが表示されます。
Network	デバイスのネットワークが表示されます。

■ エントリの検索・エクスポート

これらのログは、時間またはアクティビティなどでフィルタできます。

フィルタを作成するには、右上の（Advanced Query）アイコンをクリックします。ログのタイムスタンプ、機能、構成タイプ、システム名、IP アドレス、ユーザ名などを使用してアクティビティを指定できます。
指定の条件で絞り込まれたエントリ一覧について、CSV ファイルとしてエクスポートできます。

第 15 章　各種ツール

D-View8 で提供される便利なツールを使用して、ネットワークを効率的に管理することができます。これらのツールでは、パケットが通過するノードからの送信データと応答を使用し、ネットワークのボトルネックのトラブルシューティングに利用することができます。

本章では、以下のトピックについて説明します。

- 「MIB ブラウザ」
- 「MIB コンパイラツール」
- 「ICMP Ping の実行」
- 「SNMP テストの実行」
- 「Trace Route の実行」
- 「CLI からのネットワーク管理の設定」
- 「コンフィグレーションファイルの比較」

MIB ブラウザ

MIB ブラウザでは、サポートされているデバイスから SNMP 情報を取得できます。SNMP 対応デバイスにポーリングを行い、読み取り可能な形式でデバイス情報を取得できます。

メモ　本機能はエンタープライズ版のみサポートされます。

SNMP データの取得

1. **Tools > MIB Browser** をクリックし、以下の画面を表示します。

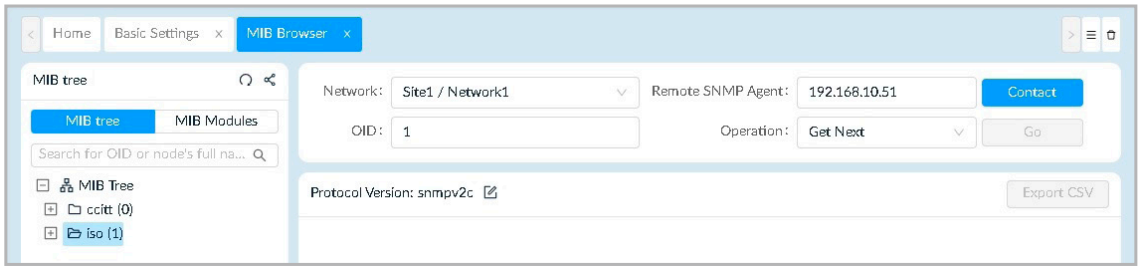


図 15-1　MIB ブラウザ

■ SNMP データの取得

2. SNMP 接続パラメータを指定します。
   - 「Network」：ドロップダウンメニューをクリックして、ネットワークを選択します。
   - 「Remote SNMP Agent」：管理デバイスを選択、またはリモート SNMP エージェントのアドレスを入力します。
3. 「Contact」をクリックして、リモート SNMP エージェントとの接続を開始します。
4. OID オブジェクトを指定します。
   - 「OID」：OID 番号を指定します。
     「OID」は、「MIB tree」のセクションで、次のいずれかの方法を使用して特定の MIB を検索し、指定することもできます。
     - 「MIB tree」タブをクリックして、特定のオブジェクトを選択します。このタブには、MIB オブジェクトが階層構造で表示されます。
     - 「MIB Modules」をクリックして、特定のノードエントリを選択します。MIB ファイルが一覧にない場合は、ファイルをアップロードしてコンパイルできます（**Tools > MIB Compiler**）
     - 検索フィールドに特定の OID を入力して、オブジェクトまたはノードを参照します。
5. 「Operation」：ドロップダウンメニューをクリックして、実行する操作を選択します。
   - 「Get」：値を取得します。
   - 「Get Next」：テーブル内の変数を順番に取得します。
   - 「Get Bulk」：「Get Next Request」に設定された繰り返し上限数まで値を取得します。
   - 「Walk」：一連の SNMP Get Next 操作を実行します。
   - 「Table View」：表形式オブジェクトで表示します。
   - 「Instance View」：関連する複数のオブジェクトインスタンスを表示します。
   - 「Set ...」：OID の値を設定します。
6. 「Go」をクリックして指定したオブジェクトの検索を開始します。

7.　結果はメインの表示ペインに表示されます。

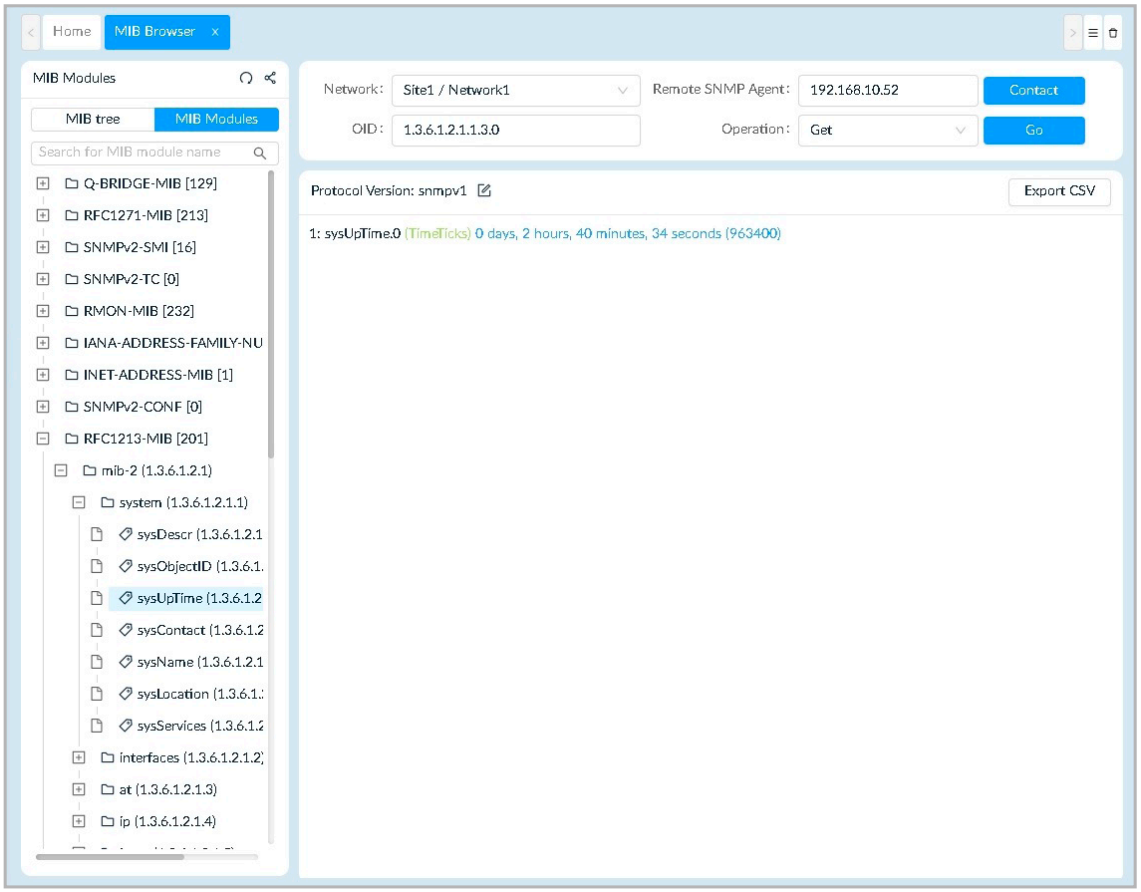


図 15-2　SNMP 操作の実行

■　データのエクスポート

8.　MIB データは、CSV 形式でローカルフォルダにダウンロードできます。「Export CSV」をクリックして、ダウンロードを開始します。

■　SNMP 認証情報の変更

OID オブジェクトにアクセスするための SNMP 認証情報は、（SNMP Protocol Preference）アイコンをクリックして変更できます。

「SNMP Protocol Preference」画面で、プロトコル設定を変更します。

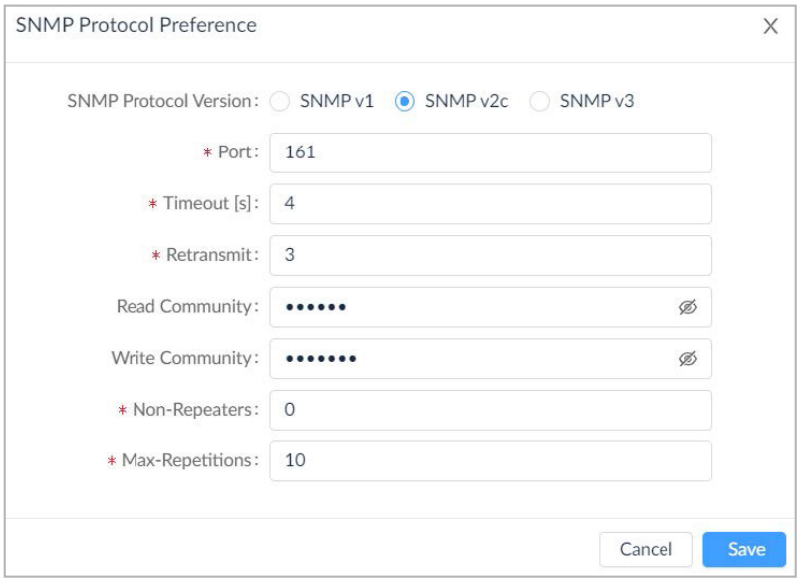


図 15-3　SNMP プロトコル設定

設定の詳細は P.225 の「SNMP 認証プロファイル」を参照してください。

MIB コンパイラツール

MIB コンパイラを使用すると、SNMP 対応デバイスの管理機能を拡張させることができます。SNMP オブジェクトを追加すると、オブジェクトの検出と MIB ツリーへの表示が可能になります。適切な形式の標準または拡張 MIB のコンパイルが可能です。不正な形式の MIB は受け付けません。

コンパイルされた MIB は MIB ブラウザで読み込み、利用することができます。

メモ　本機能はエンタープライズ版のみサポートされます。

MIB ファイルの追加

MIB ブラウザに MIB ファイルをアップロードできます。

1. **Tools > MIB Compiler** をクリックします。デフォルトでは「Compile Page」タブが表示されます。

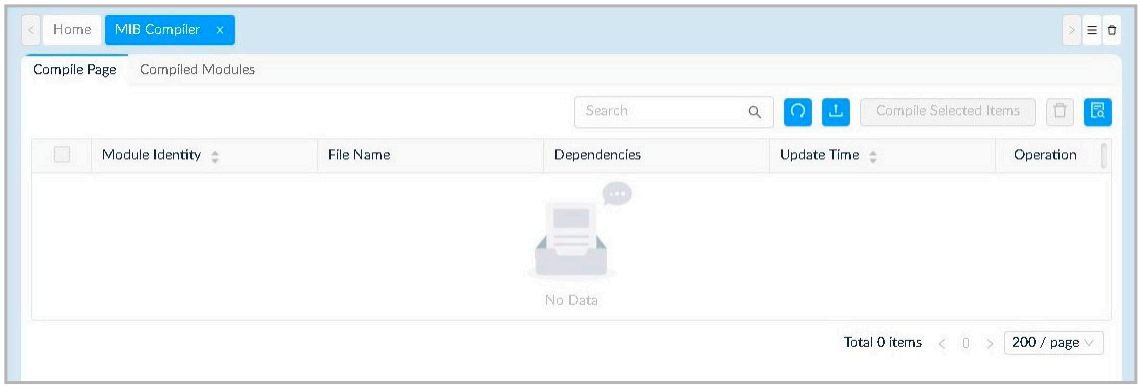


図 15-4　MIB コンパイラ

2. （Upload MIB files）アイコンをクリックします。

3. 「Select Files」をクリックして、MIB ファイルを指定しアップロードします。
   または、「Select Directory」をクリックします。指定したフォルダ配下にあるすべてのファイルが選択されます。

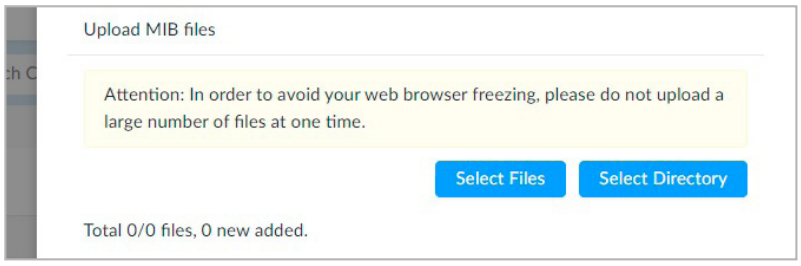


図 15-5　MIB ファイルのアップロード / ディレクトリの選択

ファイル選択後、ファイルの一覧とアップロードステータスが表示されます。

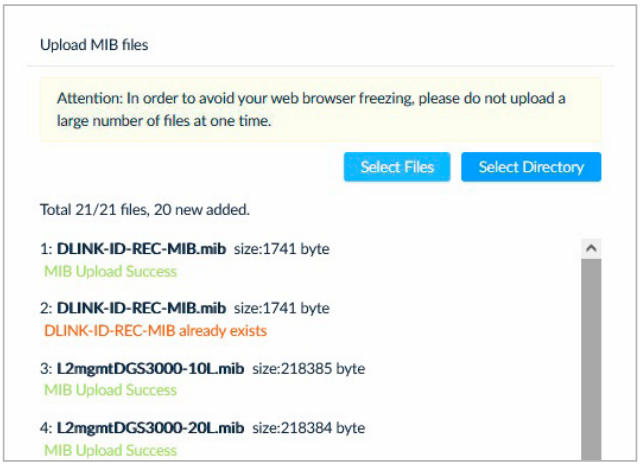


図 15-6　アップロードステータス

MIB ファイルのコンパイル

アップロード済みの MIB ファイルをコンパイルして、MIB ブラウザで利用できるようにします。

1. **Tools > MIB Compiler** をクリックし、「Compile Page」タブを選択します。

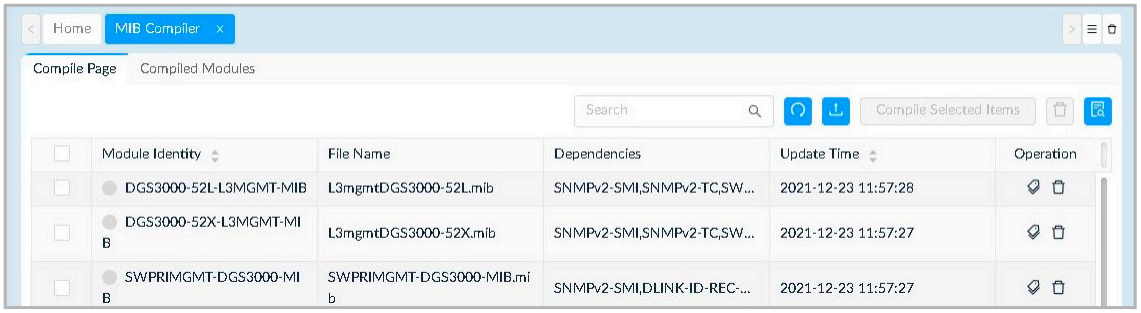


図 15-7　MIB コンパイル

2. 以下のいずれの方法でコンパイルを開始します。
   - 一覧からオブジェクトを選択して「Compile Selected Items」をクリックします。
   - 「Operation」列の （Compile）アイコンをクリックします。

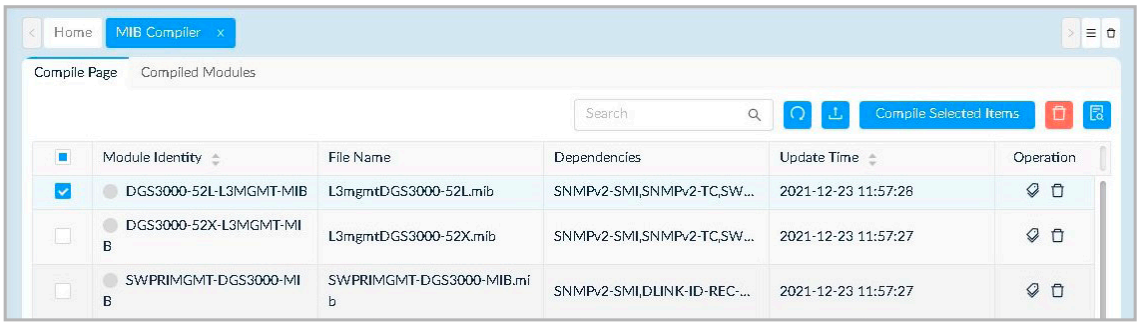


図 15-8　選択項目のコンパイル

MIB が正常にコンパイルされると、「Compiled Modules」タブ配下に表示され、MIB ブラウザからもアクセスできるようになります。

ICMP Ping の実行

ネットワークデバイスに Ping を実行し、接続性を診断することができます。

1. **Tools > ICMP Ping** をクリックし、以下の画面を表示します。

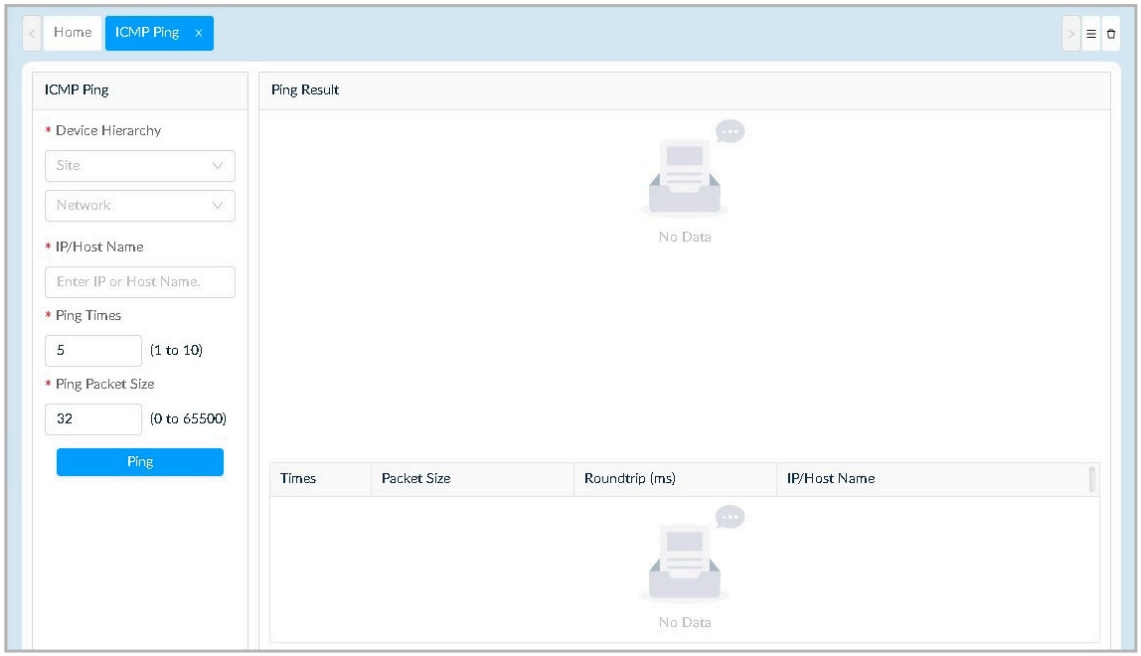


図 15-9　ICMP Ping

2. 「ICMP Ping」セクションで、次の情報を入力します。

項目	説明
Device Hierarchy	ドロップダウンメニューをクリックして、サイトおよびネットワークを選択します。
IP/Host Name	宛先デバイスの IP アドレスまたはホスト名を入力します。
Ping Times	Ping テストを実行する回数を入力します。 • 設定可能範囲：1-10 • 初期値：5
Ping Packet Size	echo リクエストメッセージのサイズを指定します。 • 初期値：32（bytes）

3. 「Ping」をクリックしてテストを開始します。

4. 「Ping Result」に Ping 結果が表示されます。

図 15-10　Ping 結果の表示

SNMP テストの実行

SNMP テストを使用すると、検出されたデバイスを監視し、ネットワークの問題を解決したり、システム正常性の問題を特定したりできます。SNMPv1、v2c でテストする場合は、SNMP コミュニティ文字列を指定する必要があります。SNMPv3 の場合は、ユーザ名と認証および暗号化（プライバシー）のパラメータを指定する必要があります。

1. **Tools > SNMP Test** をクリックし、以下の画面を表示します。

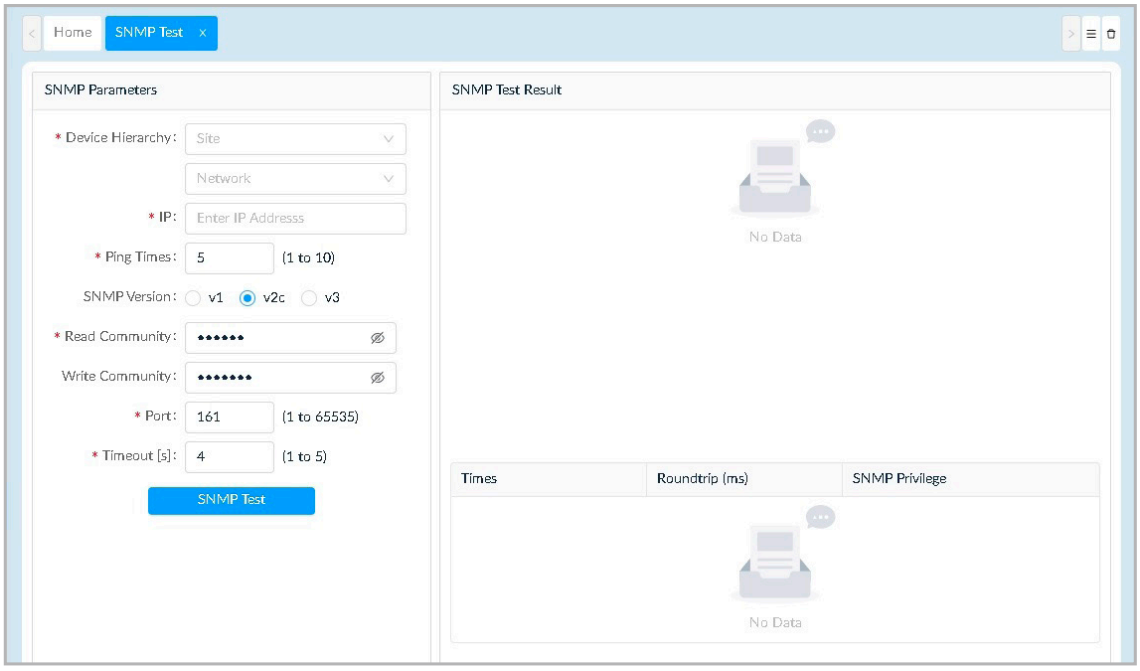


図 15-11　SNMP テスト

2. 「SNMP Parameters」セクションで、次の情報を入力します。

項目	説明
Device Hierarchy	ドロップダウンメニューをクリックして、サイトとネットワークを選択します。
IP	デバイスの IP アドレスを入力します。
Ping Times	Ping テストを実行する回数を入力します。 • 設定可能範囲：1-10
SNMP Version	SNMP バージョンを選択します。 • 選択肢：「v1」「v2c」「v3」
Non-Repeaters（SNMPv3 のみ）	単一の Get Next インスタンスで返されるオブジェクトの上限数を入力します。
Max-Repetitions（SNMPv3 のみ）	各変数に対して実行される Get Next 処理の数を入力します。
User Name（SNMPv3 のみ）	SNMP v3 で使用するユーザ名を入力します。
Context Name（SNMPv3 のみ）	必要に応じて、SNMP v3 のコンテキスト名を入力します。アクセス制限を含む MIB 内のオブジェクトインスタンスの名前付きサブセットを定義します。
Security Level（SNMPv3 のみ）	認証と暗号化を使用するかどうかを指定します。 • 「authPriv」：認証と暗号化を使用します。（初期値） • 「authNoPriv」：認証を使用します。暗号化は使用しません。 • 「noAuthNoPriv」：認証も暗号化も使用しません。 認証を使用する場合は、認証プロトコル（MD5 または SHA）とパスワードを指定します。 暗号化を使用する場合は、暗号プロトコル（DES または AES）とパスワードを指定します。
Read Community（SNMPv1/v2c のみ）	読み取り用のコミュニティ文字列を指定します。
Write Community（SNMPv1/v2c のみ）	書き込み用のコミュニティ文字列を指定します。
Port	対象デバイスのポート番号を入力します。 • 設定可能範囲：1-65535 • 初期値：161
Timeout(s)	タイムアウト時間を入力します。 • 設定可能範囲：1-5（秒） • 初期値：4（秒）

3. 「SNMP Test」をクリックしてテストを開始します。

4. 「SNMP Test Result」に結果が表示されます。

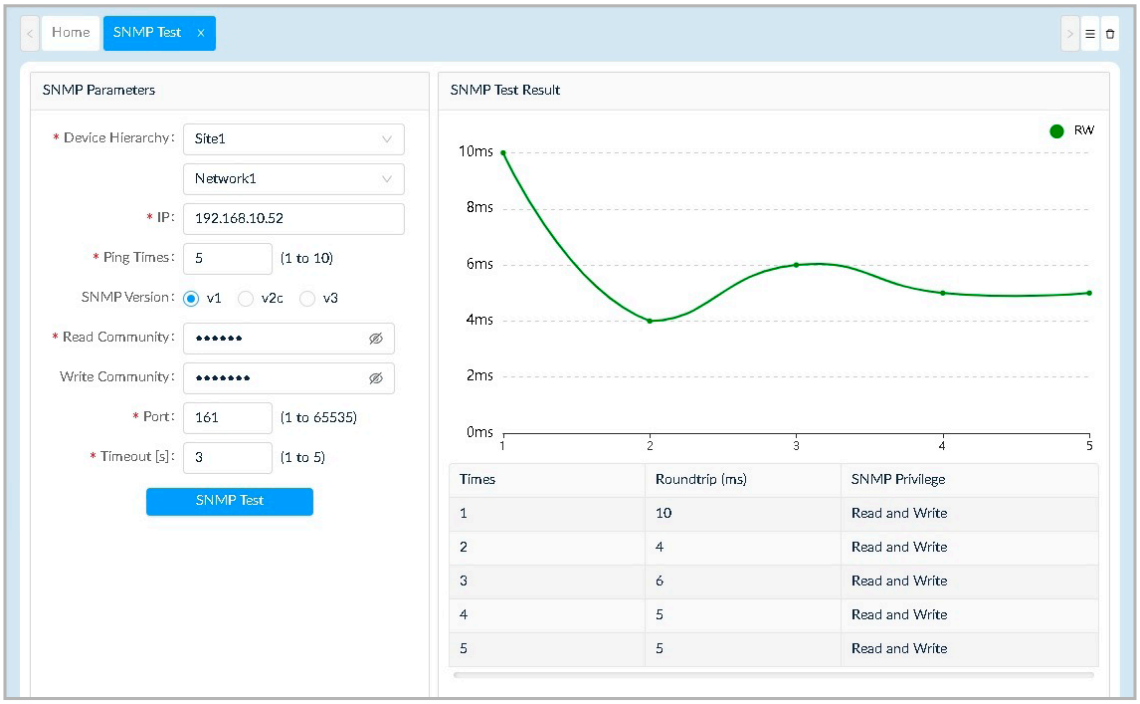


図 15-12　SNMP テスト結果

Trace Route の実行

トレースルートテストを実行し、対象デバイスへのネットワーク経路の診断に役立てることができます。

1. **Tools > Trace Route** をクリックし、以下の画面を表示します。

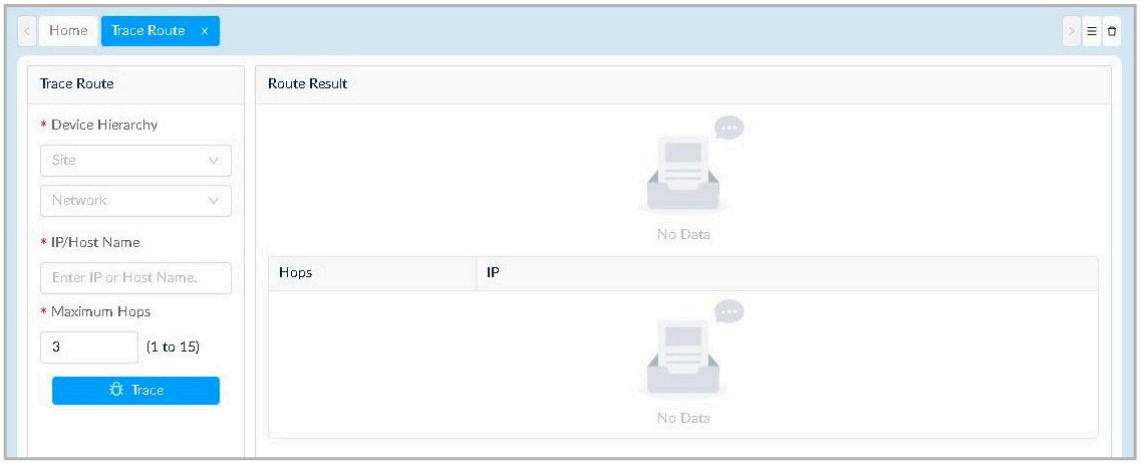


図 15-13　トレースルート

2. 「Trace Route」セクションで、次の情報を入力します。
   - 「Device Hierarchy」：ドロップダウンメニューをクリックして、サイトおよびネットワークを選択します。
   - 「IP/Host Name」：宛先デバイスの IP アドレスまたはホスト名を入力します。
   - 「Maximum Hops」：トレースルートパケットが通過できる最大ホップ数（1-15）を入力します。
3. 「Trace」をクリックしてテストを開始します。
4. 「Route Result」に結果が表示されます。

図 15-14　トレースルートの結果

CLI からのネットワーク管理の設定

D-View8 から CLI（コマンドラインインタフェース）を使用してデバイスにアクセスし、ネットワーク設定および管理を行うことができます。

■ セッションの作成

1. **Tools > CLI** をクリックし、以下の画面を表示します。
2. 「Session List」セクションで、「Add New Session」をクリックします。

図 15-15　CLI

3. 以下の画面で CLI 接続パラメータを設定します。

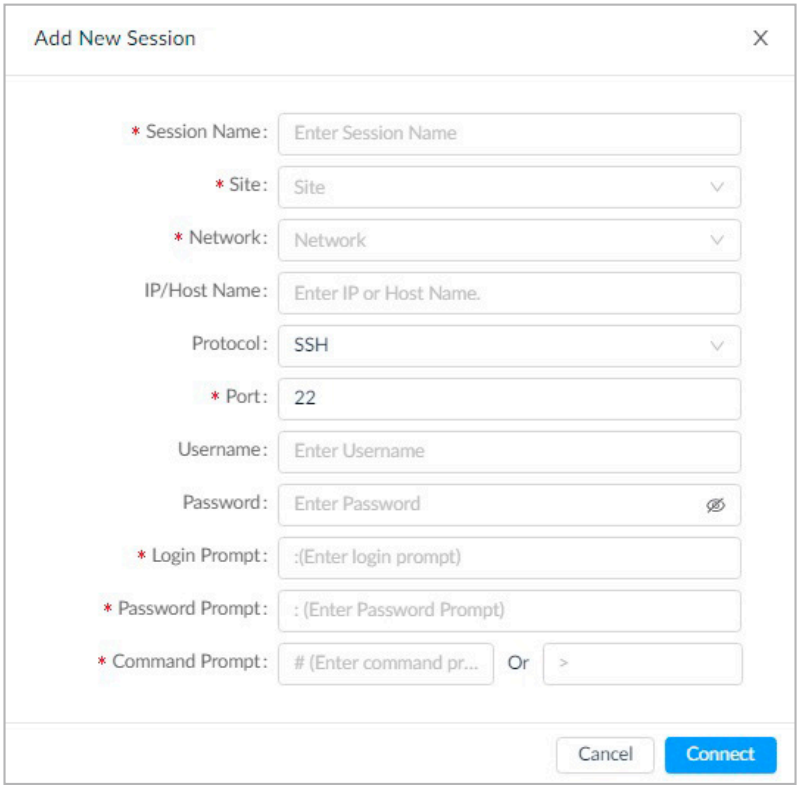


図 15-16　セッションの追加

設定項目：

項目	説明
Session Name	CLI 接続を定義する名前を入力します。
Site	ドロップダウンメニューをクリックして、対象のサイトを選択します。
Network	ドロップダウンメニューをクリックして、対象のネットワークを選択します。
IP/Host Name	接続先デバイスの IP アドレスまたはホスト名を入力します。
Protocol	ドロップダウンメニューをクリックして、接続プロトコルを選択します。 • 選択肢：「SSH」「Telnet」
Port	Telnet または SSH サービスのポート番号を入力します。
Username	デバイスにアクセスする権限を持つユーザ名を入力します。
Password	ユーザのパスワードを入力します。
Login Prompt	ログイン時に表示されるプロンプトを指定します。
Password Prompt	パスワード入力時にコマンドラインに表示されるプロンプトを指定します。

項目	説明
Command Prompt	コマンド入力時にコマンドラインに表示されるプロンプトを指定します。

4. 「Connect」をクリックして、接続を開始します。設定をキャンセルするには、「Cancel」をクリックします。
5. 定義済みの CLI 接続が「Session List」に表示され、接続時はメインの表示ペインで接続画面が開きます。

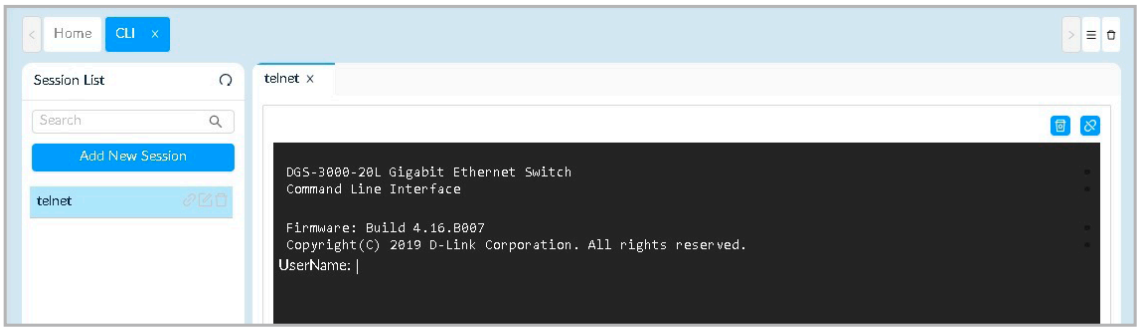


図 15-17　CLI セッション

注意 DXS-1210/B1 シリーズへ接続した場合、「r」で終わる文字列を入力し Tab キーを押下すると、デバイスのハングアップを招きます。タブキーを使用しないようにしてください。

■ セッションの終了

6. セッションを終了するには、（Disconnect）アイコンをクリックします。

■ 定義済みセッションへの接続 / 編集 / 削除

7. 定義済みのセッションに対する操作を行うには、以下のアイコンをクリックします。

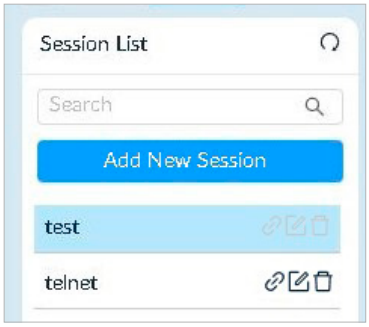


図 15-18　CLI 接続エントリ

- （Connect）：接続を開始します。
- （Edit）：「Edit Session」画面を開き、接続設定を編集します。
- （Delete）：エントリを削除します。

コンフィグレーションファイルの比較

ファイル比較ツールでは、2 つのコンフィグレーションファイルを比較することができます。比較できるのはテキストファイルのみです。

1. **Tools > File Comparison** をクリックし、以下の画面を表示します。

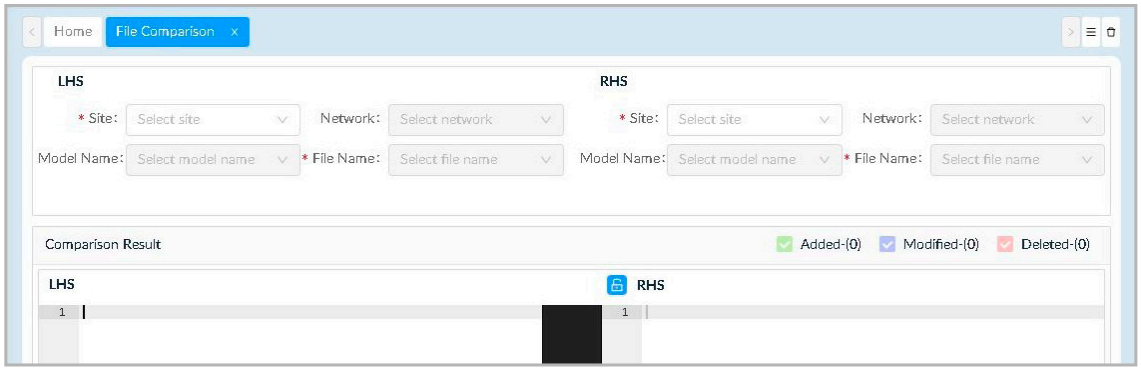


図 15-19　ファイル比較

2. サイト、ネットワークを選択します。必要に応じて、デバイスモデルにより条件をフィルタします。
3. 比較するコンフィグレーションファイルを指定します。
4. 比較結果が表示されます。

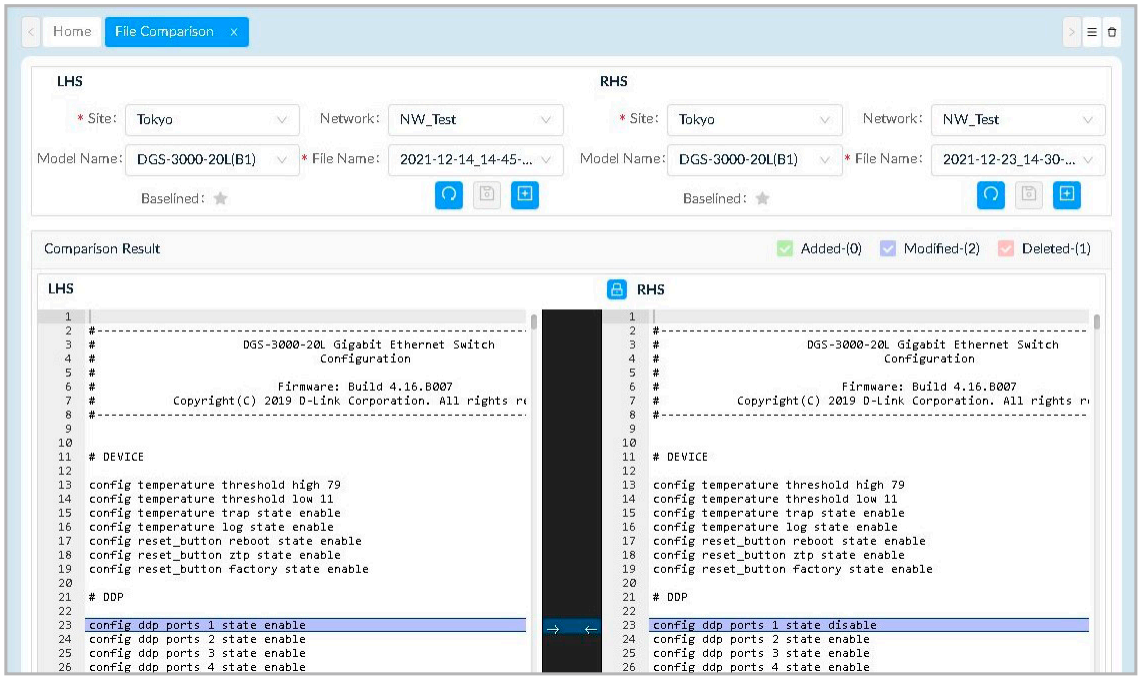


図 15-20　ファイル比較結果

比較結果では、変更箇所が種類毎に色付きでハイライト表示されます。

- 緑色：追加されたテキスト、紫色：変更されたテキスト、赤色：削除されたテキストの削除の違いが表示されます。

■ ファイルの編集とアップロード

ファイルは、本画面で直接編集して新しいコンフィグレーションファイルとして保存し、サーバにアップロードできます。ファイルの編集後、（Save as）アイコンをクリックして保存、アップロードします。アップロードされたすべてのコンフィグレーションファイルとファームウェアファイルの一覧は、**Configuration > File Management** から確認できます。

■ リストア

（Restore to Device）アイコンをクリックし、現在表示されているファイルを使用してリストアジョブを実行またはスケジュールできます。すべてのリストアジョブのステータスは、**Configuration > Configuration Management > Restore** から確認できます。

第 16 章　付録

付録 A：クラスタ構成のインスト―ルシナリオ（Windows サーバ 5 台構成）

D-View8 は、3 台または 5 台構成のサーバクラスタの中に配備することができます。
本章では、「Windows サーバ 5 台を使用したクラスタ構成」について説明します。

メモ　Windows サーバを 3 台使用した場合のインストール手順については、P.25 の「D-View8 サーバのインストール（Windows サーバ / クラスタ構成）※エンタープライズ版のみ」を参照してください。

MongoDB レプリカセットとは別に、2 台のサーバに D-View8 server サービスをインストールします。

クラスタ構成図

本シナリオにおけるクラスタ構成図は以下の通りです。

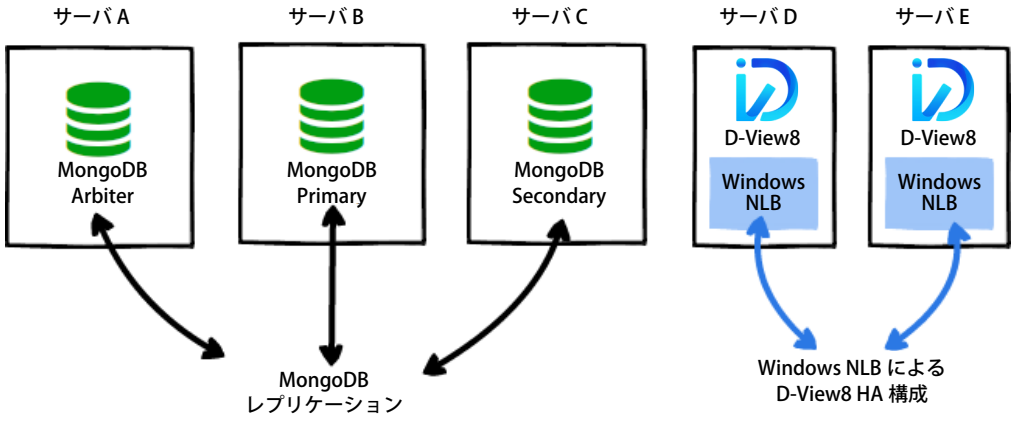


図 16-21　クラスタ構成図

サーバ構成

5 台の Windows サーバ構成は以下の通りです。

Windows サーバ構成例

項目	サーバ A	サーバ B	サーバ C	サーバ D	サーバ E
IP アドレス	192.168.1.205	192.168.1.203	192.168.1.204	192.168.1.201	192.168.1.202
OS ※	Windows 10 Windows Server 2016 Windows Server 2019	Windows 10 Windows Server 2016 Windows Server 2019	Windows 10 Windows Server 2016 Windows Server 2019	Windows Server 2016 Windows Server 2019	Windows Server 2016 Windows Server 2019
MongoDB レプリカセット役割	Arbiter	Primary	Secondary	—	—
NLB 設定	—	—	—	仮想 IP： 192.168.1.200	仮想 IP： 192.168.1.200

※いずれかの OS を想定

クラスタ構築手順

手順 1 ：MongoDB クラスタのインストール

MongoDB データベースをインストールし、データベースクラスタでデータの冗長性を有効にする手順について説明します。
以下の手順に従い、サーバ A、サーバ B、サーバ C にそれぞれ MongoDB をインストールします。

1. D-Link Japan のサイトから D-View8 MongoDB インストールパッケージをダウンロードします。
2. D-View8 MongoDB のインストーラをダブルクリックし、セットアップウィザードを開始します。
「Next >」をクリックして次に進みます。

図 16-22　セットアップウィザードの開始

3. 使用許諾画面が表示されます。「I Agree」をクリックし、使用許諾に同意します。

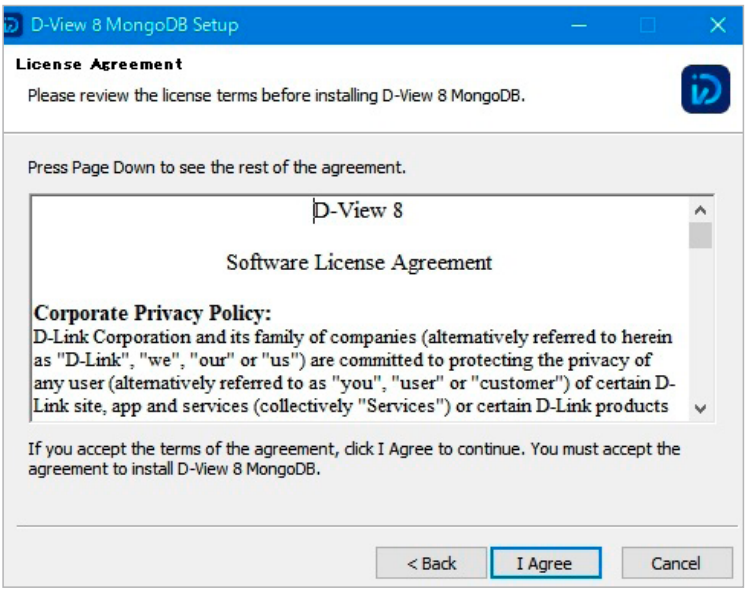


図 16-23　使用許諾への同意

4. 「Connection Configuration」画面で、MongoDB の設定を行います。

(1) 以下のパラメータを設定します。
- 「MongoDB Type」:「Replication」を選択します。
- 「MongoDB」: サーバ接続用に設定される MongoDB ポート番号を入力します。

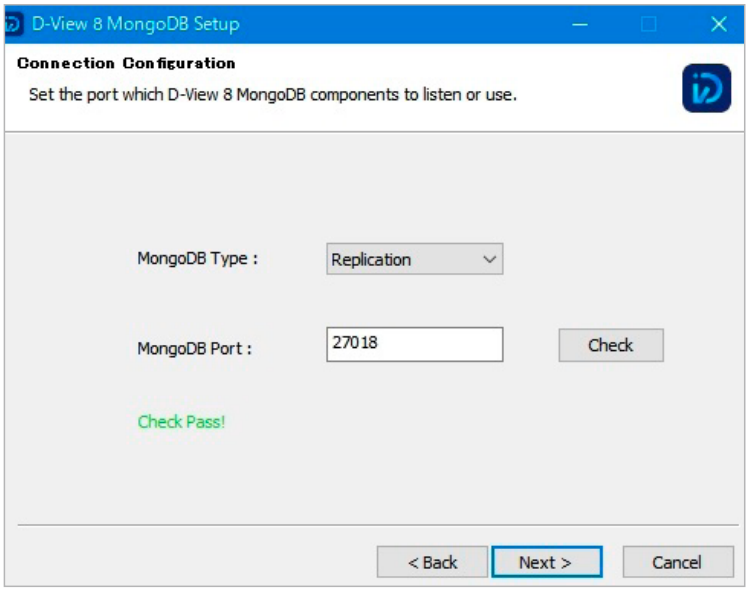


図 16-24　接続設定（MongoDB タイプの設定）

(2) 設定をテストするには、「Check」をクリックします。
正しく設定されている場合は、「Check Pass!」が表示されます。テストが失敗した場合は、ポート設定を見直してください。

(3) 「Next >」をクリックして先へ進みます。

5. インストールディレクトリを指定し、「Install」をクリックします。

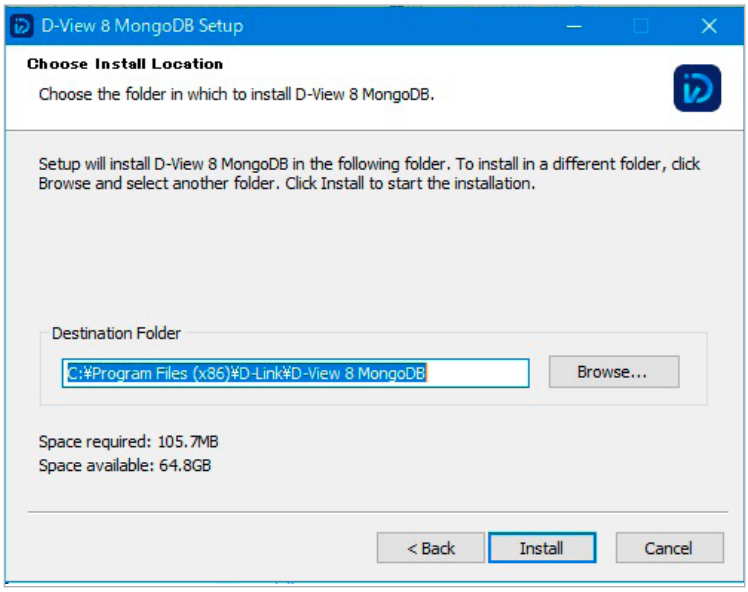


図 16-25　インストールディレクトリの選択

6. D-View8 MongoDB のインストールが開始され、進捗状況が表示されます。

7. インストール完了後、「Close」をクリックします。

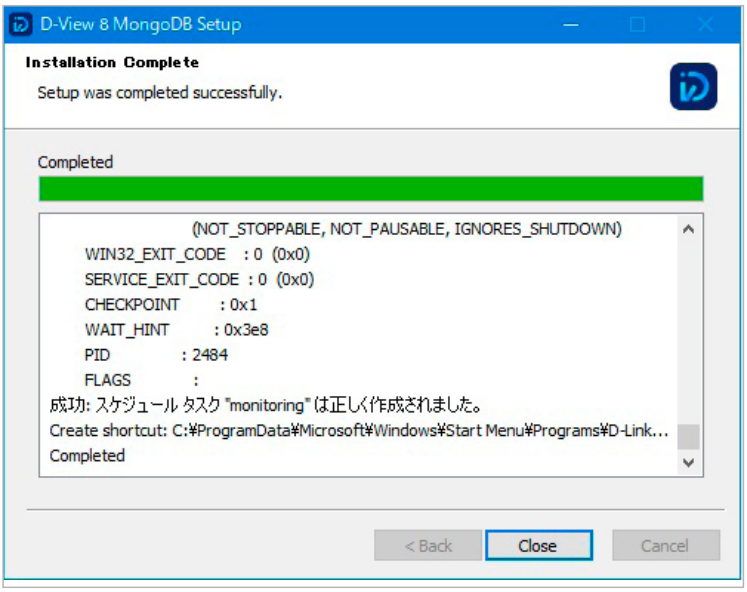


図 16-26　インストール完了

手順 2：D-View8 のインストール

以下の手順に従い、データベースサーバ以外の追加サーバ（ここではサーバ D、サーバ E）にそれぞれ D-View8 アプリケーションをインストールし、それらを MongoDB クラスタに接続します。

1. D-Link Japan のサイトから D-View8 インストールパッケージをダウンロードします。
2. D-View8 のインストーラをダブルクリックし、セットアップウィザードを開始します。
   「Next >」をクリックします。

図 16-27　セットアップウィザードの開始

3. 使用許諾画面が表示されます。
   「I Agree」をクリックし、使用許諾に同意します。

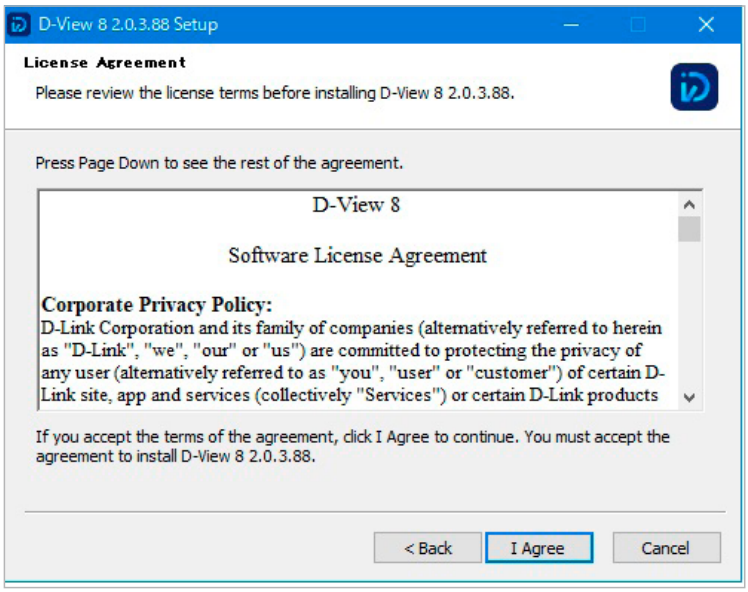


図 16-28　使用許諾への同意

4. D-View8 のインストールディレクトリを指定します。
「Next >」をクリックします。

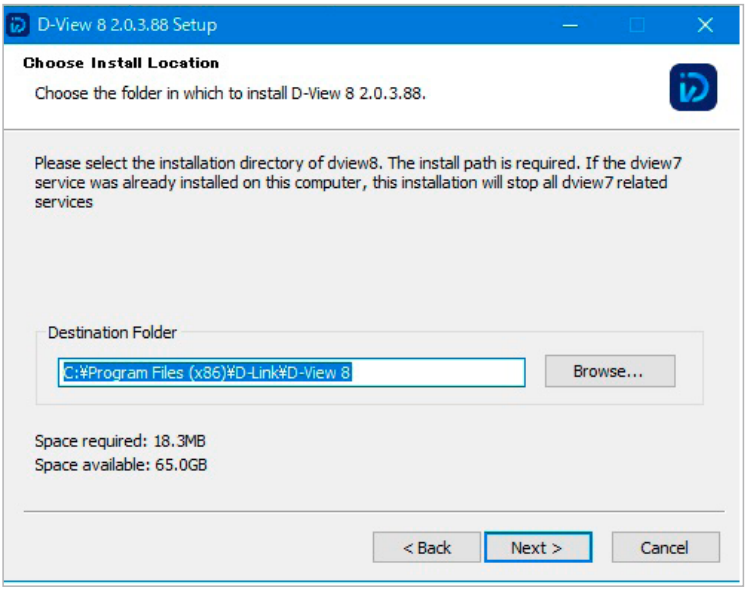


図 16-29　インストールディレクトリの選択

5. 「Connection Configuration」画面で、MongoDB の設定を行います。

(1) 以下のパラメータを設定します。
- 「MongoDB Type」:「Replication」を選択します。
- 「Server IP」:当該サーバの IP アドレスを入力します。
- 「Web Port」:Web アクセス用のポート番号を入力します。
- 「Core Port」:コアサーバのポート番号を入力します。
- 「Probe Port」:プローブ接続用のポート番号を入力します。

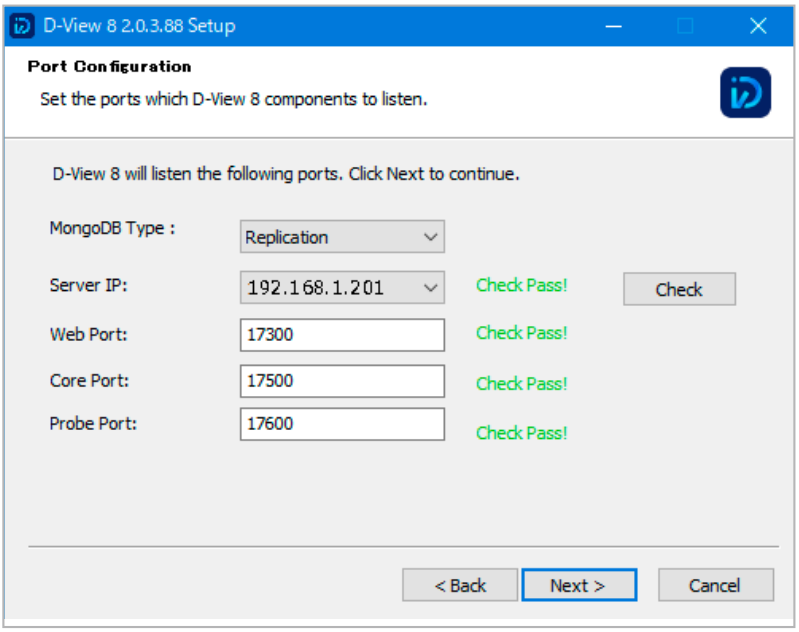


図 16-30　ポート構成（サーバ D の例）

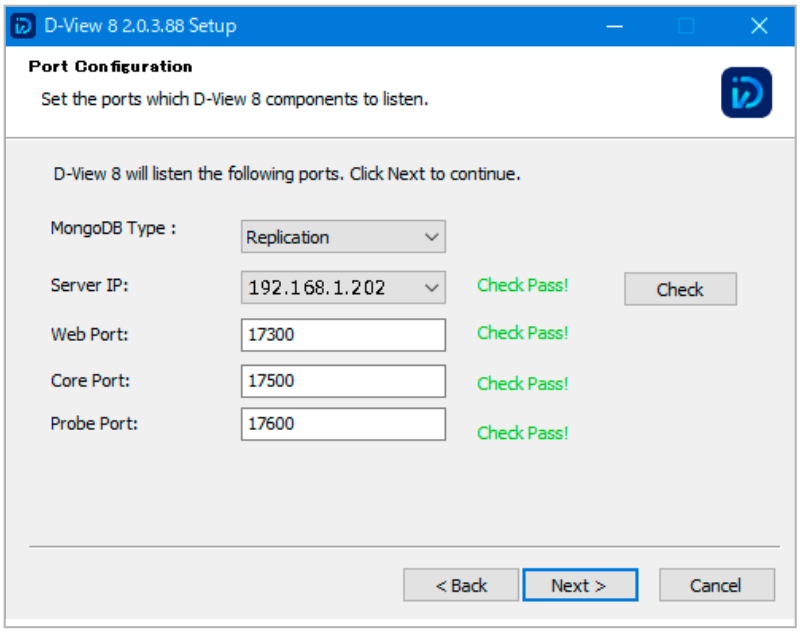


図 16-31　ポート構成（サーバ E の例）

(2)　設定をテストするには、「Check」をクリックします。
正しく設定されている場合は、「Check Pass!」が表示されます。テストが失敗した場合は、設定内容を見直してください。

(3)　「Next >」をクリックして先へ進みます。

6.　「MongoDB Database Configuration」画面で、MongoDB レプリカセットとの接続設定を行います。

(1)　以下のパラメータを設定します。
- 「Primary/Secondary/Arbiter」：MongoDB レプリカセットとなる各サーバの IP アドレスとポート番号を入力します。

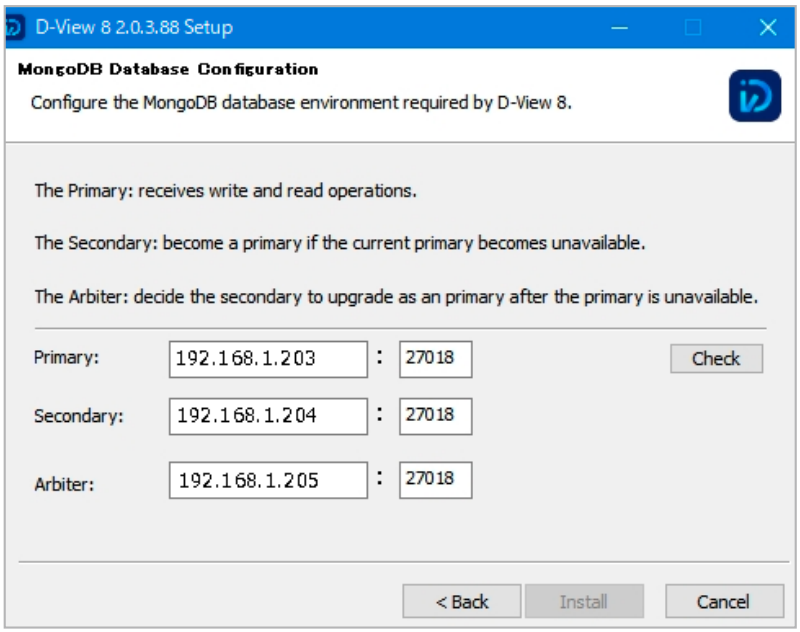


図 16-32　MongoDB 設定

(2)　設定をテストするには、「Check」をクリックします。
正しく設定されている場合は、「Check Pass!」が表示されます。テストが失敗した場合は、設定内容を見直してください。

(3)　「Install」をクリックしてインストールを開始します。

7.　「Finish」をクリックし、セットアップウィザードを終了します。

以上の設定により、Web ブラウザから D-View8 サーバにアクセスできるようになります。

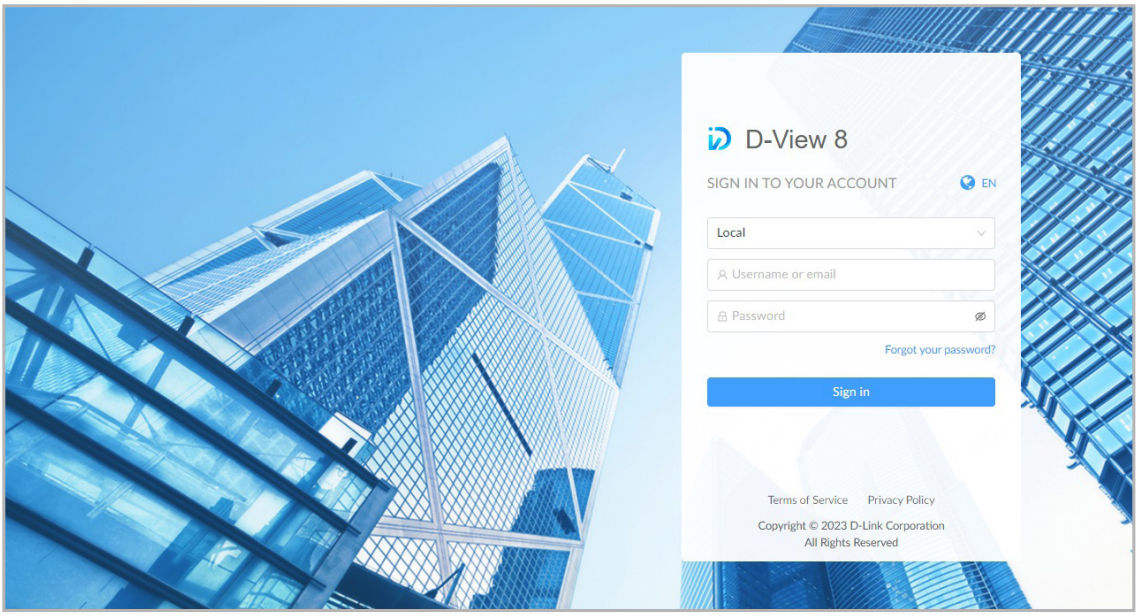


図 16-33　D-View8 ログイン画面

手順 3：NLB のセットアップ

本アプリケーションでは、サーバのロードバランシング（負荷分散）がサポートされています。
同じサブネット内で 2 台のサーバを負荷分散用に構成します。本セクションでは、5 台のサーバ構成のうち、2 台の D-View8 サーバ上で NLB を設定する手順を説明します。

1. サーバ D とサーバ E に、Windows のサーバーマネージャーから「ネットワーク負荷分散マネージャー」をインストールします。

■ NLB の設定（サーバ D）

2. 「ネットワーク負荷分散クラスター」を右クリックして、「新しいクラスター」を選択します。

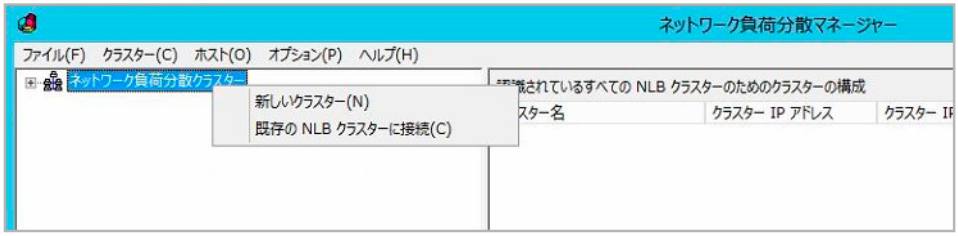


図 16-34　ネットワーク負荷分散マネージャー

3. 「新しいクラスター：接続」画面で、以下の設定を行います。
   - 「ホスト」:「192.168.1.201」を入力し、「接続」をクリックします。

図 16-35　新しいクラスタ接続のセットアップ

4. 「新しいクラスター：ホスト パラメーター」画面で、「次へ >」をクリックして先へ進みます。

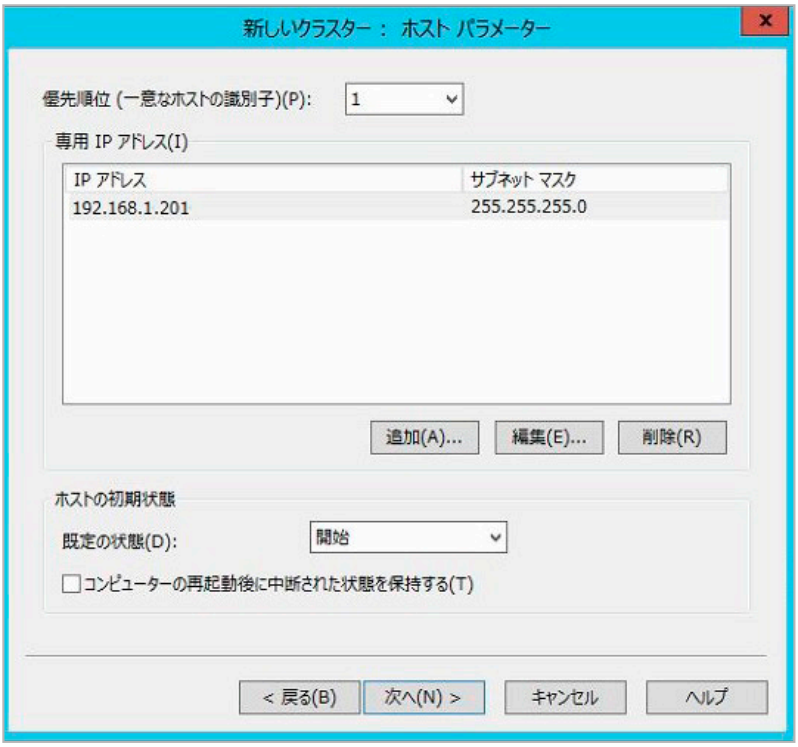


図 16-36　ホストパラメーターの設定

5. 「新しいクラスター：クラスター IP アドレス」画面で、「追加 ...」ボタンをクリックします。
「IP アドレスの追加」画面で、クラスタ IP およびネットマスクとして使用する仮想 IP アドレスとネットマスクを入力します。

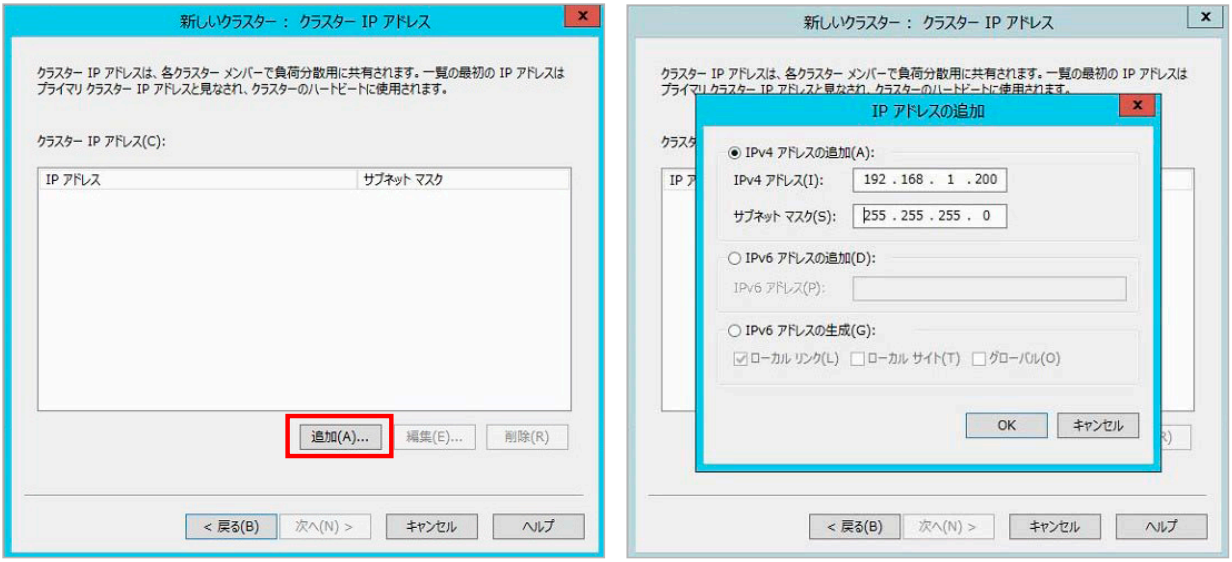


図 16-37　クラスタ IP の設定

6. 「新しいクラスター：クラスター パラメーター」画面で、以下の設定を行います。
   - 「クラスタ操作モード」:「マルチキャスト」を選択し、パフォーマンスを最適化します。

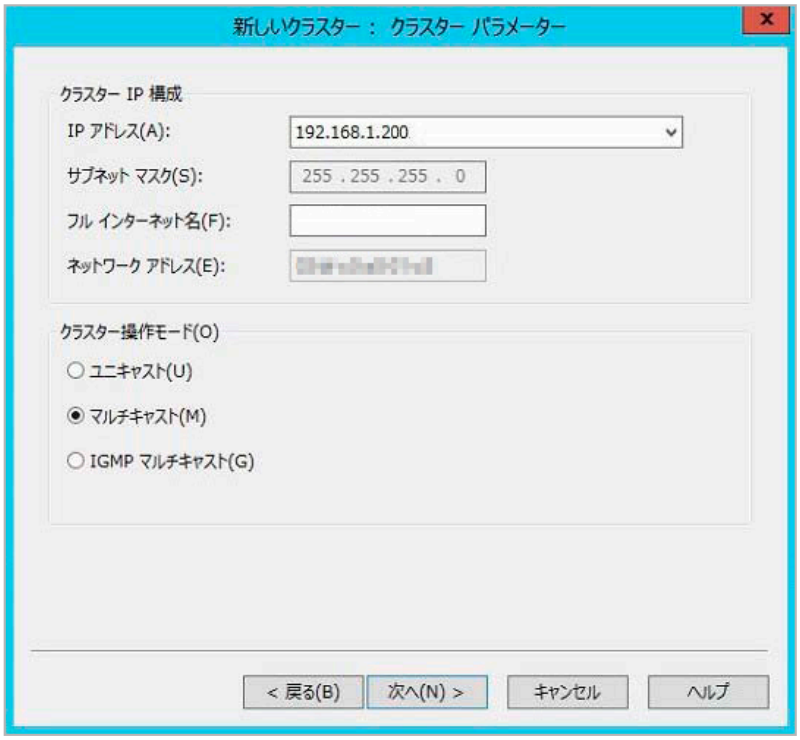


図 16-38　クラスターパラメータの設定

7. 「新しいクラスター：ポートの規則」で定義済みのポートの規則を選択し、「編集 ...」をクリックします。
   「ポートの規則の追加と編集」画面で、「フィルターのモード」に「複数ホスト」を選択し、「アフィニティ」を「なし」に指定します。

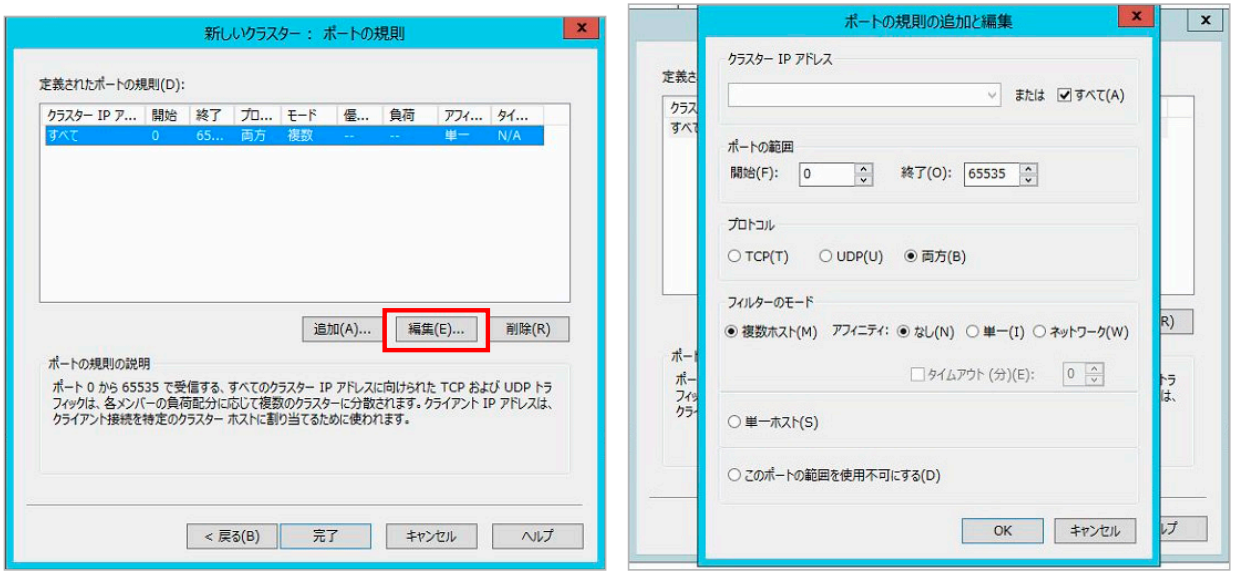


図 16-39　ポートの規則

8. 「OK」→「完了」をクリックして、クラスタの編集を完了します。

以上の手順により、NLB クラスタが作成されます。

図 16-40　ポートの規則

次に、このクラスタにサーバ E を追加します。

9. クラスタノードを右クリックして、「ホストをクラスターに追加」をクリックします。

図 16-41　ホストをクラスタに追加

10. 「ホストをクラスターに追加：接続」画面で、「ホスト」にサーバ E の IP アドレス（例：192.168.1.202）を入力し、「接続」をクリックします。

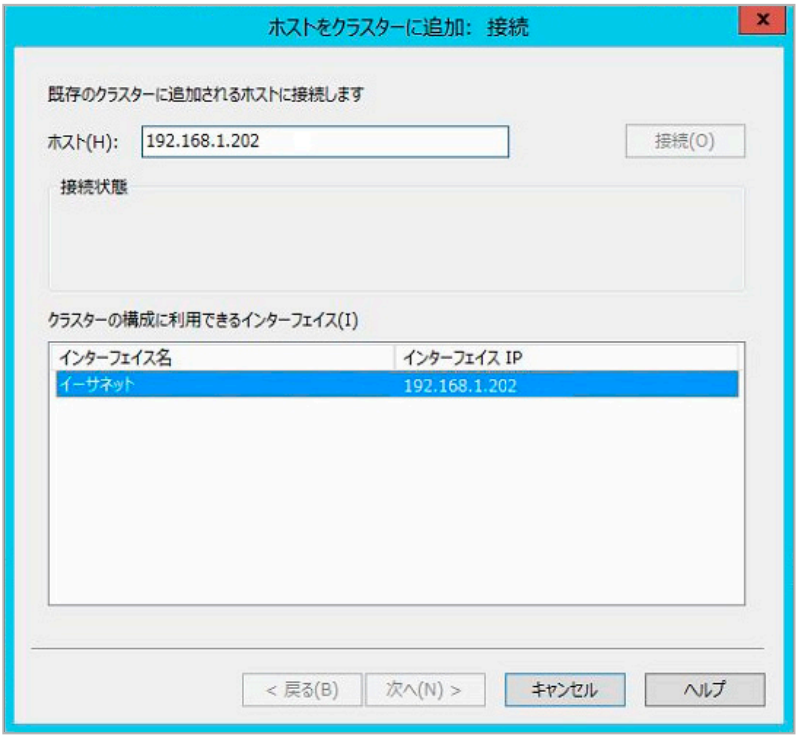


図 16-42　ホストをクラスタに追加

11.「ホストをクラスターに追加：ホスト パラメーター」画面で、「次へ >」をクリックして先へ進みます。

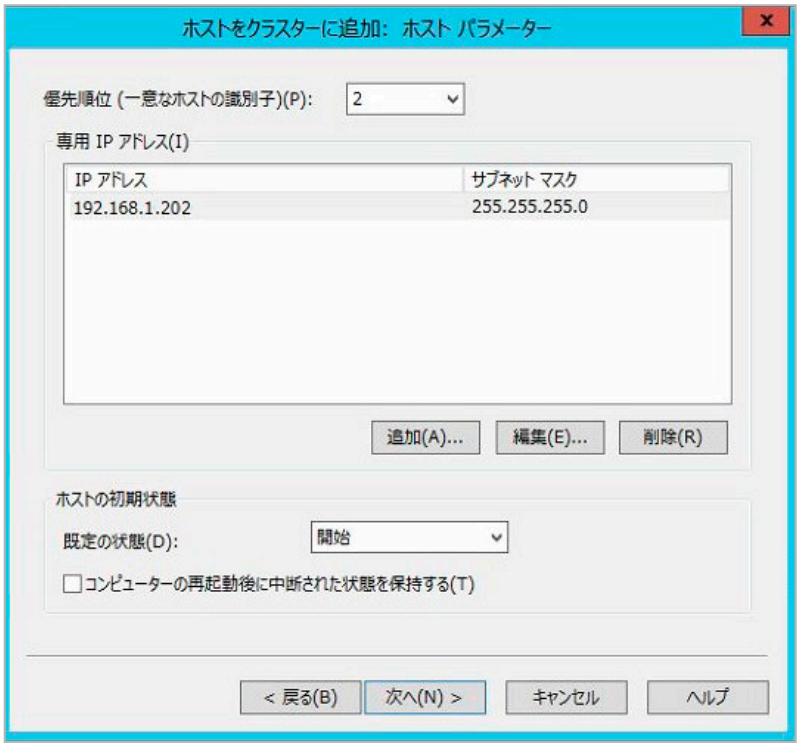


図 16-43　ホストパラメーターの設定

12.「ホストをクラスターに追加：ポートの規則」画面で、「完了」をクリックします。

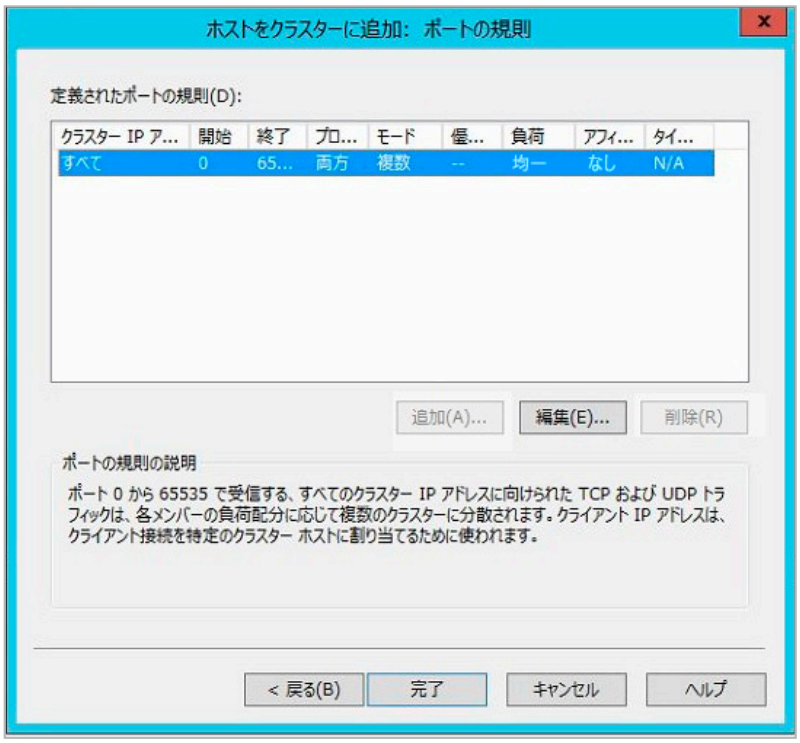


図 16-44　ポートの規則

以上の設定により、サーバ D とサーバ E で構成されるクラスタが作成されます。

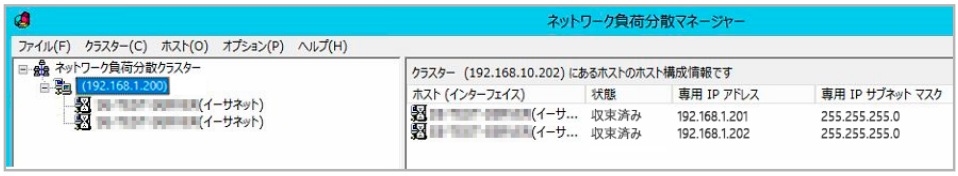


図 16-45　ネットワーク負荷分散クラスタ

クラスタ IP アドレスを使用して D-View8 にアクセスすることができます。

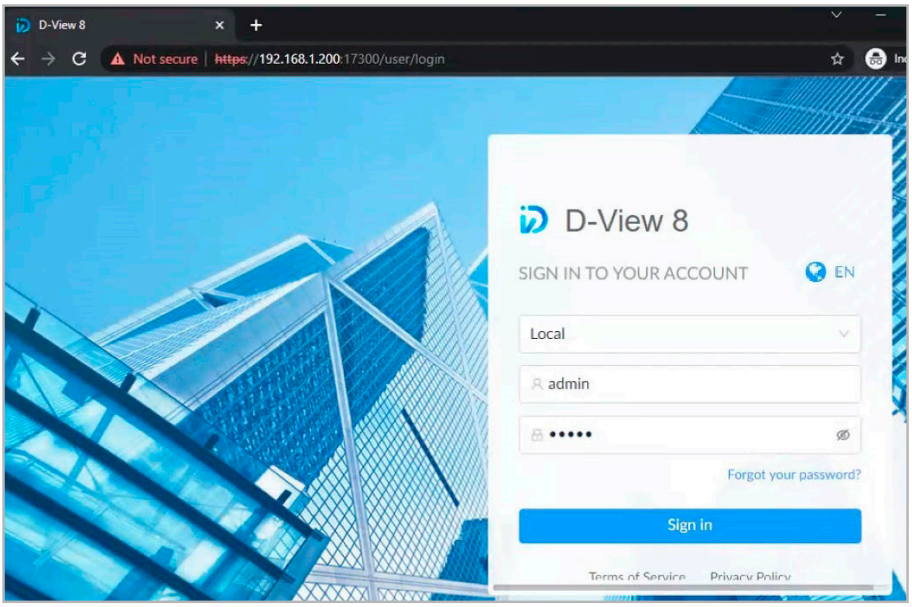


図 16-46　D-View8 ログイン画面

■ サーバ E での NLB 管理

サーバ E で NLB クラスタを管理する場合は、次の手順を実行します。

1. 「ネットワーク負荷分散クラスター」を右クリックして、「既存の NLB クラスターに接続」を選択します。

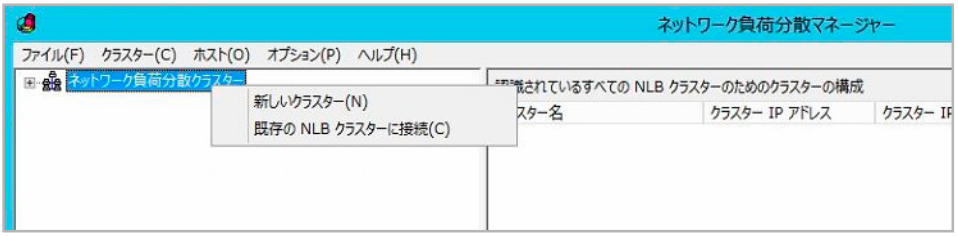


図 16-47　ネットワーク負荷分散マネージャー

2. 「既存のクラスターに接続：接続」画面で、NLB クラスタ IP「192.168.1.200」を入力し、「接続」ボタンをクリックします。

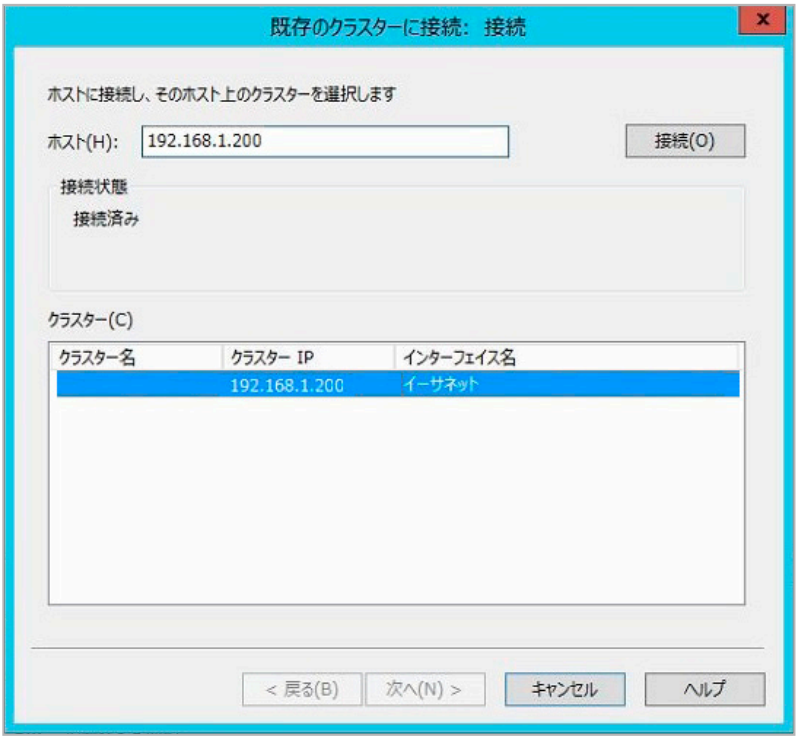


図 16-48　既存のクラスタに接続

- サーバ E で NLB クラスタ情報を確認できます。

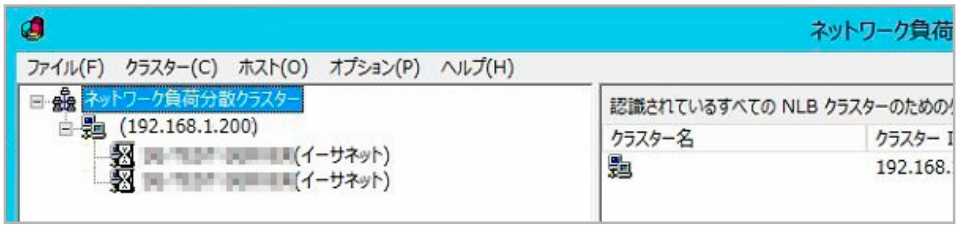


図 16-49　ネットワーク負荷分散クラスタ