

スピーディなセキュリティ問題の解決に

IDsentrieは、Active DirectoryやOpenLDAP上のユーザID管理操作を一つにまとめるID管理機能をサポートしています。管理者はIDシリーズのGUIから一度操作するだけで、複数のディレクトリサーバに存在するユーザID情報を更新することができます。統合された認証機能では、ハイパフォーマンスなRADIUSとDHCP認証機能をサポートしています。DHCP認証では、従来必要だった認証スイッチが不要となるため、低コストで端末認証環境を構築することができます。



- 統合ID管理
- RADIUS/DHCP認証
- IDトラッキング機能
- エンドユーザ向けパスワード管理ポータル

IDsentrieの主な機能

製品特徴：

- アイデンティティ&アクセス管理 (IAM) をシンプルに実現するアプライアンスソリューション
- 手作業によるフォレンジックを省いて迅速な問題解決を可能にするインスタントIP-to-IDマッピング
- パスワード復旧やアカウント更新に関わるコストを削減するユーザセルフヘルプサービス
- シンプルなサインオン環境とコンプライアンス体制を強化するアカウントデータ同期機能
- 洗練されたセキュリティを提供する統合認証機能
- ネットワークの問題解決と法規制への対応を支援するアイデンティティベースのレポートテイング/ロギング

▶ 簡単なID特定を実現する
インスタントIP-to-IDサービス

IPアドレスやMACアドレスと、ユーザのID情報を簡単にマッピングするユニークなソリューションを提供します。IDsentrieのIP-to-IDサービスは、これまで手動で行ってきたIPアドレス/MACアドレスとユーザID情報とのマッチング作業を自動化します。IT担当者は、セキュリティリスクを発見した際、その原因となるユーザの特定を迅速に行うことが可能になります。IP-to-IDサービスは、ユーザID情報を入手するための複数の方法をサポートしており、既存のセキュリティ環境、ネットワーク、アプリケーションとシームレスに統合することができます。

▶ ユーザセルフヘルプサービスによる
パスワード復旧とアカウント情報更新

エンドユーザは、パスワードの復旧とアカウント情報の更新をヘルプデスクや、IT担当者の助けを必要とせずに行うことができます。セルフヘルプサービスは、サポートの負荷やコストを削減するだけでなく、パスワードとそのほかのアカウント情報を同期することにより、アカウント管理をよりシンプルにします。パスワードポリシーコントロールや、パスワード更新通知機能を使用することにより、異なるプラットフォームのデバイスに存在するアカウントのパスワードポリシーを統一化させ、より強固なパスワードセキュリティを実現することができます。

▶ Unified Identity Manager(UIM)による
アカウントの集中統合管理

複数のデバイスに登録されているユーザ情報を管理しやすいバーチャルディレクトリに統合することにより、ユーザアカウント管理をシンプルにします。

UIMを使用することにより、複数のサーバに対するユーザアカウントの作成・削除・更新・有効化・無効化を一回の操作で行うことができます。少ないリソースで、全てのデバイス进行操作することが可能となりますので、より正確で安全性の高いID管理環境を構築することができます。

▶ シンプルなサインオン環境を実現する
ネットワーク認証機能

IDsentrieは、高速なRADIUS認証、802.1X認証、DHCP認証サービスを提供します。IDsentrieに内蔵したデータベースによるユーザアカウント管理の他に、プロキシ機能を使用して、外部デバイスの既存アカウントを使用することもできます。

IDsentrieのネットワーク認証コンポーネントは、VPN機器や、ワイヤレス装置、スイッチ/ルータ、ファイアウォールのようなデバイスに対して、認証サービスの集中管理サービスを提供します。DHCP認証機能では、Web認証を使用したDHCP方式の検疫ソリューションを提供します。サブリカントを持たないゲストアクセスに対してもWebによる分かりやすい認証環境を提供し、認証に失敗したユーザのネットワークアクセスを防御します。

▶ DHCP認証/検疫・ゲストアクセスサービス

IDsentrieは、Web認証を使用したDHCP方式の検疫機能をサポートしています。認証に失敗したユーザーを、検疫用のネットワークに隔離することにより、権限のないネットワークアクセスを防ぎます。手軽にWeb認証用のアカウントを発行・管理できる管理用Webインタフェースを使用することにより、来客用等のアカウント管理のみをIT担当者以外に委任することができます。

一般企業は、IDsentrieを導入することにより、運用コストと管理負荷を軽減し、セキュリティと法規制対策を改善することができます。IT部署は、IP-to-IDサービスで問題に直接関係するユーザをピンポイントで把握することが可能となり、少ない負荷で迅速にトラブルシュートを行うことができます。システム管理者は、UIMを使用することにより、同時に複数のデバイスに存在するユーザアカウントの集中管理が可能となり、管理作業の生産性が向上します。従業員は、セルフヘルプサービスを使用することにより、パスワード復旧時においてもアカウント停止やヘルプデスク担当者のサポートが不要となるため、業務効率が向上します。ネットワーク認証や、無許可アクセスを防ぐアクセスコントロールサービスにより、ネットワーク全体のセキュリティはさらに向上します。IDsentrieの充実したレポートテイング、監査機能は、完全な可視性を提供し、IT部署の作業効率を向上させます。

» RADIUS認証プロトコルサポート

- PAP, CHAP, MS-CHAP Version 1, 2
- EAP 802.1X方式:
MD5, LEAP, PEAP, MS-CHAPv2, SIM, TLS,
TTLS, GTC, OTP
- EAP 証明書管理

» RADIUS機能

- レルムエイリアスサポート
- レルムベースの認証コントロール
- ユーザ毎マルチポリシー
- ユーザ毎マルチパスワード
- ユーザ毎NASベースポリシー
- グループ-ポリシー設定
- グループ-デフォルトプロファイル設定
- グループ-レベルアクセスコントロール
- グループ-デバイスアクセスコントロール
- グループ-NASオペレーション
- 利用時間ポリシーコントロール
- スケジュールグループポリシーコントロール
- アカウント利用時間制限機能
- アカウントリングフォーマットサポート:
Cisco TACACS, Free RADIUS, Livingston, MERIT v2

» IP-to-IDマッピングサービス

- IP-ID, MAC-IP, ホスト名
- ユニバーサルIDリゾルバ
Universal Identity Resolver (UIR)
- サードパーティ製品へのID情報提供 (XML-API)
- 内部RADIUS/DHCPのイベントモニタ
- 多くのサードパーティ製品のイベントモニタ (VPN、
ファイアウォール、スイッチ/ルータ、DHCPサーバ、
アプリケーションサーバ等)
- 標準サポート (Check Point, Cisco,
Netscreen/Juniper, Fortinet, SonicWALL)
- あらゆるテキストを構文解析できるジェネリックパーサ機能
- シスログ・ログファイルからのイベント取得機能
(NEC EnterpriseDirectoryServerサポート)
- ID情報を付加したレポート作成機能
- ログイン活動の表示
- 閾値設定によるアラート機能
- スケジュール設定可能な外部サーバへの保存機能

» 管理機能

- セキュアWeb GUI (HTTP, HTTPS)
- SSH, Telnet, RS-232 シリアルコンソール
- アドバンスドコマンドラインインタフェース (CLI)
- SNMPv1, v2
- 暗号化パスワード
- セキュアアップデート、バックアップ、リストア
- 多言語サポート
◆ 日本語、英語、簡体字、繁体字中国語、韓国語
- アクティブ・スタンバイ構成による冗長化機能

» RADIUS RFC 準拠

- RFC 2548-MS Vendor Attributes
- RFC 2619-Auth Server MIB
- RFC 2621-Acct Server MIB
- RFC 2716-PPP EAP TLS
- RFC 2759-MS PPP CHAPv2
- RFC 2809-Compulsory Tunneling
- RFC 2865-RADIUS
- RFC 2866-RADIUS Accounting
- RFC 2867-Accounting Modifications
- RFC 2868-Attributes for Tunneling
- RFC 2869-RADIUS Extensions
- RFC 2882-NAS Requirements

» LDAP RFC 準拠

- RFC 2251-LDAPv3 Protocol
- RFC 2255-URL Format
- RFC 2829-Auth Methods
- RFC 2830-TLS Extensions
- RFC 3377-Technical Specs

» ID管理機能

- サードパーティ製デバイス内アカウントの集中管理機能
- 集中パスワードポリシー強制機能
- アカウントパスワード&データ同期
- カスタマイズ可能な編集画面
- カスタマイズ・新規追加が可能な属性マッピング機能
- CSV(UTF-8, Shift-JIS)によるスケジューリングインポート機能
- CSVエクスポート機能
- Sudo/Sudoユーザエイリアスサポート
- ゲストユーザアクセスコントロール
- デバイス間アカウントコピー・移動機能

» Webベースユーザセルフヘルプポータル機能

- パスワードポリシー強制
- パスワード期限メール通知
- パスワード管理・復旧
- ユーザプロフィール管理
- 段階的なセキュリティチャレンジ
- セルフヘルプアクティビティログ採取 (監査用)
- 利用状況のレポート機能
- ユーザ自身による複数アカウントの一括更新
- セルフヘルプ利用状況のメール通知機能
◆ アカウントロック/解除
◆ 作業状況通知 (成功・失敗<閾値設定可能>):
パスワード再設定、パスワード変更、プロフィールアクセス

» データストアサポート

- ID管理対象サーバ
◆ 内部RADIUSデータベース
◆ Windows 2000 SP4 Active Directory
◆ Windows 2003 SP2 Active Directory
◆ eDirectory 8.7.x (Netware, Linux)
◆ eDirectory 8.8 (Linux)
◆ iPlanet version 5.1, SunOne 5.2
◆ openLDAP 1.6, 2.2
◆ Open Directory 10.3.9, 10.4
◆ Linux Redhat Enterprise 3, 4
◆ HPUNIX 11iv2, v3
◆ Solaris 8, 9, 10
◆ Fedora Core version 3, 4, 5
◆ FreeBSD 6.1
◆ NetBSD 3
◆ SCO Open Server 5.0.7
◆ Oracle SQL 10g, 9i
◆ MS SQL 2000
◆ MS SQL 2005 SP1
◆ mySQL 5.1.x, 5.0.x, 4.x (Linux)
◆ Sybase ASE 12.5.1
◆ PostgreSQL 8.1.9, 7.4.6
◆ Lotus Domino Server 7.0.2, 6.5
- RADIUS連携サーバ
◆ Windows NT ドメイン
◆ RSA Authentication Manager 6.0
◆ Kerberos V5

» DHCP機能

- 認証DHCP機能
- 高速DHCPサーバ機能
- Microsoft Network Access Protection (NAP)
エンフォースポイント
- Webベースのゲストアクセスポータル
- 詳細なリソースレポート
- ID情報との統合
- ブラックリスト通知機能

» キャパシティ

UIMデバイス数:	400
UIMユーザー数:	10,000
RADIUSユーザー数:	10,000
IP to IDイベント数:	1,000万
IP to ID保存期間:	30日
ログエントリ数:	50万

ハードウェア仕様

モデル	IDsentry 1100
ギガビット・カッパー (10/100/1000 BASE-T)	4
管理インターフェース (専用) (10/100/1000 BASE-T)	1
コンソールポート	○
電源ユニット	250W シングルユニット, AC 100 ~ 240V, 50 ~ 60Hz
最大消費電力	131W
ラックサイズ	1U
動作環境	動作温度: 0 ~ 40°C 湿度: 5% ~ 95% (結露無きこと)
サイズ	44.45mm (高さ) x 439.42mm (幅) x 424.18mm (奥行)
重量	7.3 kg
規格準拠	FCC Class A, UL, CE, TUV, CB, VCCI, RoHS 対応

●仕様は予告無く変更することがあります。最新の情報は弊社WEBサイトでご確認下さい。 ●本書で使用した登録商標および商標はそれぞれの所有者の資産です。



A10ネットワークス株式会社

〒105-0001 東京都港区虎ノ門4-3-20 神谷町MTビル16階
TEL: 03-5777-1995 FAX: 03-5777-1997
Email: jinfo@a10networks.com
http://www.a10networks.co.jp

お問い合わせ