H3C iMC EIA

エンドユーザーインテリジェントアクセス

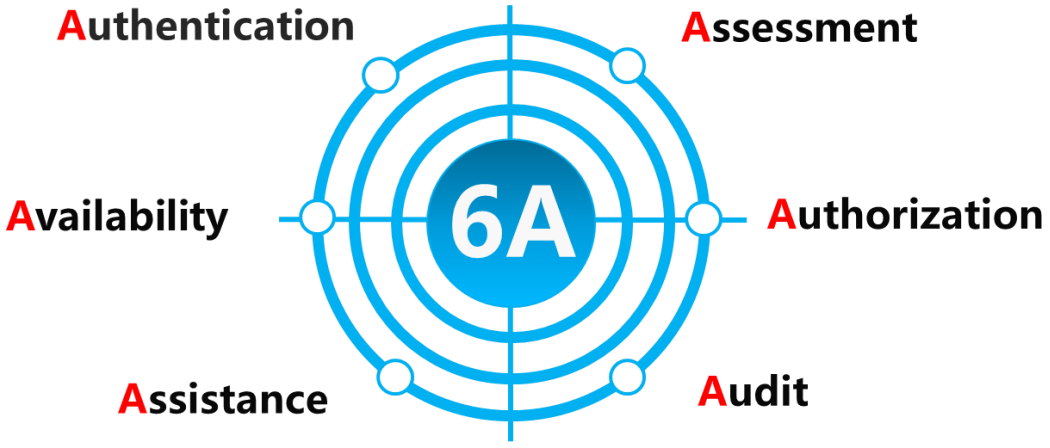
リリース日:2019年10月

New H3Cテクノロジー(株)

H3C iMCエンドユーザーインテリジェントアクセス

製品の概要

H3C IMC End-user Intelligent Access(EIA)は、セキュアなアクセス管理ソリューションとして、有線、無線、VPNなどのネットワークインフラストラクチャで構築された企業ネットワークにおいて、エンドポイントのネットワークアクセスを管理します。EIAは、ユーザーロール、デバイスタイプ、アクセス時間、アクセス場所などの基準に基づいてアクセスシナリオを定義することをサポートし、厳密なネットワークアクセス制御を行います。企業ネットワークの統一的な運用・保守要件に対応して、さまざまなアクセス方法、豊富なエンドポイントタイプ、さまざまなユーザーロールを管理し、セキュリティポリシーを確実に実行します。



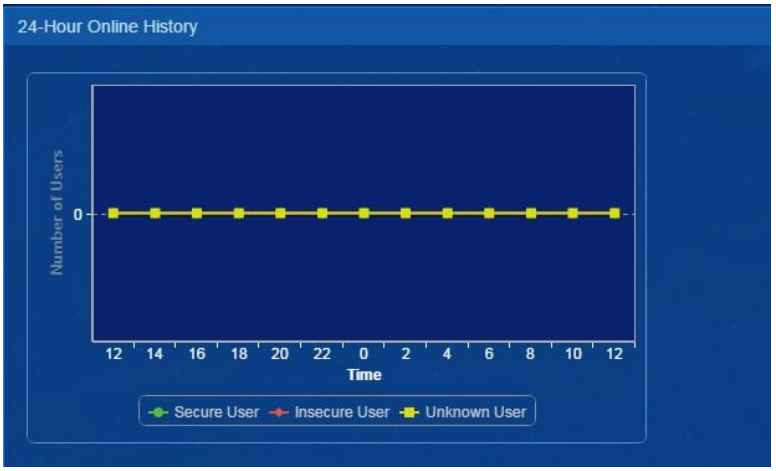
EIA機能

機能とメリット

デバイス管理とユーザーリソース管理の一元化

ネットワークデバイスの集中管理に加えて、EIAは基本ユーザーを維持します。

(ユーザー名、識別ID、担当者アドレス、電話番号、電子メールアドレスおよびユーザーグループを含む)および追加のユーザー情報を一元的に管理できます。管理者は、ネットワーク操作のニーズに応じてユーザー情報をカスタマイズできます。たとえば、管理者は、大学ネットワークの場合は学生IDと成績をカスタマイズし、企業ネットワークの場合は部門と職階をカスタマイズできます。



リソース管理

デバイスとユーザーのグループ管理

EIAでは、デバイスとユーザーのグループ化がサポートされています。管理者は、同じ属性を持つユーザーをグループに割り当て、グループ管理権限をオペレータに割り当てます。また、管理者はアクセスサービスをユーザーグループに割り当てることで、ユーザーグループ内のユーザーのネットワークアクセスを管理します。

ユーザー管理とネットワークデバイス管理の統合

デバイス管理とユーザー管理の統合により、管理者はより効率的に操作を実行できます。オンラインユーザーリストは、基本デバイス情報、アラームおよびパフォーマンスステータスなど、オンラインユーザーのアクセスデバイスに関する情報を表示するためのインターフェースを提供します。管理者は、アクセスデバイスを選択してユーザーに対してアクションを実行できます。たとえば、アクセスデバイスを選択して、デバイス上のすべてのアクセスユーザーを強制的にオフラインにできます。

異なるアプリケーションシナリオのための複数のアクセスおよび認証方法

- ユーザーは、さまざまなアクセス方法(802.1XやVPNアクセスなど)を使用してネットワークにアクセスできます。
- 認証方式(PAP、CHAP、EAP-MD5、EAP-TLS、PEAPなど)は、さまざまなアプリケーションシナリオのセキュリティ要件を満たします。
- ユーザーとデバイスIPアドレス、アクセスポート、VLAN、ユーザーIPアドレス、およびハードウェア情報(MACアドレスなど)とのバインディングにより、認証セキュリティが強化され、アカウントの損失や無効なアクセスが防止されます。
- Windowsドメインコントローラおよび LDAP対応のサードパーティー製電子メールシステムとの統合認証により、複数認証を回避できます。
- Endpoint Admission Defense(EAD)ソリューションと連携することで、セキュリティポリシーに準拠したユーザーエンドポイントだけがネットワークにアクセスできるようになります。
- ポータル認証は、H3C INode DCおよびPCクライアントをサポートしています。ポータル認証ページをカスタマイズして、サードパーティーシステムのホームページに埋め込むことができます。認証ページは、ポートグループ、SS IDおよびエンドポイントオペレーティングシステムに基づいてプッシュできます。

厳格な権限制御と強化されたユーザーアクセス管理

- ユーザーベースの特権制御ポリシーは、さまざまなユーザーのネットワークアクセス特権を定義します。
- 同時一とプロキシサービス禁止の設定は、特定のユーザーによる過剰なネットワークリソースの使用を効果的に回避します。
- 最大アイドル時間の設定をサポートします。
- ユーザーACLベースおよびVLANベースの制御により、ユーザーが外部の違法なWebサイトや機密データのある内部サーバにアクセスできないようにします。
- ユーザーIPアドレス割り当てポリシーにより、IPアドレスのセキュリティと一意性が保証されます。
- 管理者がネットワークアクセスの時間範囲と場所を設定した後、ユーザーは設定されたネットワークだけにアクセスできます。
- EIAでは、内部情報の漏洩を防ぐために、複数のNICの使用とダイヤルインアクセス方式を制限しています。
- EIAでは、ユーザーは専用クライアントを使用する必要があり、自動クライアントアップグレードが強制されます。これにより、クライアントのセキュリティが確保されます。

エンドポイントユーザーの強力な監視と管理

- EIAでは、オンラインユーザーへのリアルタイムクエリがサポートされており、管理者は不正ユーザーを強制的にオフラインにすることができます。
- ブラックリスト機能は、悪意を持ってパスワードを推測したユーザーをブラックリストに追加し、MACアドレスまたはIPアドレスによって不正行為の原因を追跡します。
- EIAでは、システムアップグレード前のネットワーク切断通知や、悪意のあるパスワード攻撃が検出された場合のパスワード保護通知など、重要なイベントが発生したときにユーザーにアクセスするための管理者通知の送信がサポートされています。
- 認証失敗ログは、管理者が認証失敗の理由を特定するのに役立ちます。

シンプルなメンテナンスオペレーション

- サービスベースのユーザー分類管理と、認証バインディングポリシー、セキュリティポリシー、およびアクセス権限をサービスに統合することにより、メンテナンス操作が簡素化され、ネットワーク管理が統一されます。
- EIAは、オペレータがアクセスユーザーに対して集中管理操作を実行するための、使いやすいWebインターフェースを提供します。
- アクセスユーザーは、アカウントに申し込み、セルフサービスセンターでユーザー情報を照会および変更できます。これにより、アクセス効率が向上し、管理者のワークロードが軽減されます。

さまざまなゲストアカウントの作成方法

EIAゲスト管理は、アプリケーションシナリオに基づいて、次のゲスト作成方法を提供します。

公共の場におけるSMS認証方式

公共の場所では、ゲストは電話番号を使用してアカウントを登録し、SMSメッセージを介してパスワードを取得してネットワークに迅速にアクセスできます。ワークフローは次のとおりです。

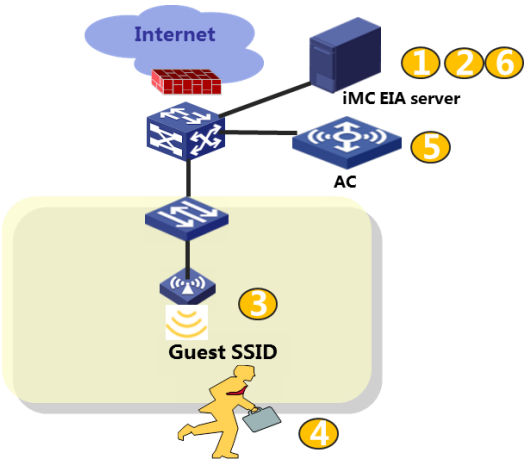
1) ゲストマネージャは、EIAサーバでゲストアクセスポリシーとアカウントパラメータ(有効期間を含む)を設定します。
2) ゲストがゲストSSIDに接続しようとします。
3) ゲストは、プッシュされたWeb認証ページに電話番号を入力し、「パスワード取得」をクリックします。

4) EIAサーバは、この電話番号のゲストアカウントを自動的に作成し、ゲストアクセスポリシーとアカウント有効期間をアカウントに割り当てます。
5) EIAサーバは、SMSメッセージゲートウェイを介してSMSメッセージでゲストにアカウントとパスワードを送信します。
6) ゲストは、SMSメッセージを受信した後、Web認証ページでパスワードを入力します。
7) 認証を通過したゲストは、アクセスポリシーで定義されたネットワークリソースにアクセスできます。
8) EIAサーバは、期限切れのゲストアカウントを定期的に削除します。

受付担当者によるアカウント作成

この方法は、ゲストアカウントが特定の受付担当者(警備員、フロントデスクトップ受付担当者、従業員など)によって管理されている場合に適用されます。ワークフローは次のとおりです。

1) ゲスト受付はセルフサービスセンターにログインし、ゲストアカウントを作成し、アクセスポリシーと有効期間をアカウントに割り当てる。
2) EIAサーバは、アカウントとパスワードを電子メールまたはSMSメッセージでゲストに送信します。
3) ゲストはゲストSSIDに接続しようとします。
4) ゲストは、プッシュされたWeb認証ページでアカウントとパスワードを入力します。
5) 認証を通過したゲストは、アクセスポリシーで定義されたネットワークリソースにアクセスできます。
6) EIAサーバは、期限切れのゲストアカウントを定期的に削除します。

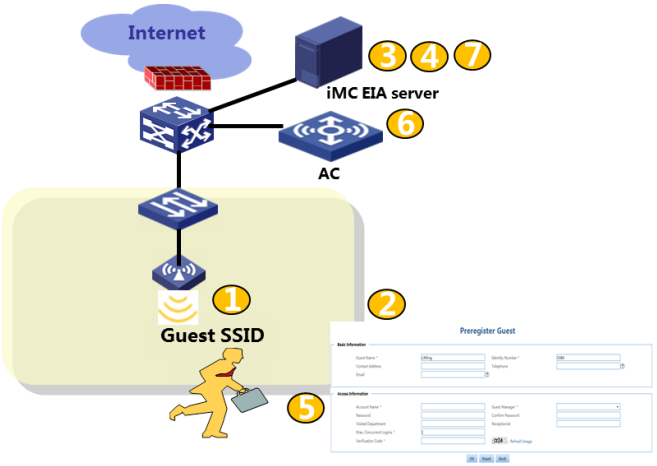


受付担当者によるアカウント作成

ゲストによるセルフサービスアカウントの作成

ゲストはこの方法を使用してアカウントに応募し、ゲストの受付担当者が応募を承認します。ワークフローは次のとおりです。

1) ゲストがゲストSSIDに接続しようとします。
2) ゲストは、プッシュされたWeb認証ページで「ゲストの事前登録」をクリックし、アカウント情報を入力し、事前登録ページでゲストの受付担当者を選択します。
3) ゲスト受付はセルフサービスセンターにログインし、アクセスポリシーと有効期間をゲストに割り当てる。
4) アカウントが有効になると、EIAは電子メールまたはSMSメッセージでアカウントをゲストに送信します。
5) ゲストは再びゲストSSIDに接続しようとし、プッシュされたWeb認証ページにアカウントとパスワードを入力します。
6) 認証を通過したゲストは、アクセスポリシーで定義されたネットワークリソースにアクセスできます。
7) EIAサーバは、期限切れのゲストアカウントを定期的に削除します。



ゲストによるアカウントの作成

QRコード認証方式

ゲストは、インテリジェントエンドポイントを使用して特定のQRコードをスキャンし、アカウントの作成とネットワークアクセスを迅速化できます。ゲスト認証には、次のタイプのQRコードを使用できます。

認証用QRコード

1) ゲストマネージャは、セルフサービスセンターにゲストアカウントを作成し、QRコードを生成します。
2) ゲストはQRコードをスキャンして認証します。

承認用QRコード

1) ゲストがWebサイトにアクセスすると、ゲストは自動事前登録のページに誘導され、そのページにQRコードも自動的に生成されます。
2) ゲストマネージャはQRコードをスキャンして承認ページに入り、ゲストアカウントを承認します。
3) アカウントが承認された後、ゲストはネットワークにアクセスできます。

その他の方法

EIAは、企業のWeChat公式プラットフォームと通信するための豊富なSDKインターフェースをサポートしている。ゲストは、企業のWeChat公式アカウントに従うことで、企業のワイヤレスネットワークにアクセスできる。

複数のSMSメッセージ通知方法

SMSメッセージの送信には、次の方法を使用できます。

- SMSメッセージゲートウェイ。
- EIAがWebインターフェースを介して通信するサードパーティーSMSメッセージゲートウェイ。EIAが
- カスタマイズされたインターフェースを介して通信するカスタマーSMSメッセージプラットフォーム。

統合されたアクセスデバイス管理とシンプルな操作およびメンテナンス

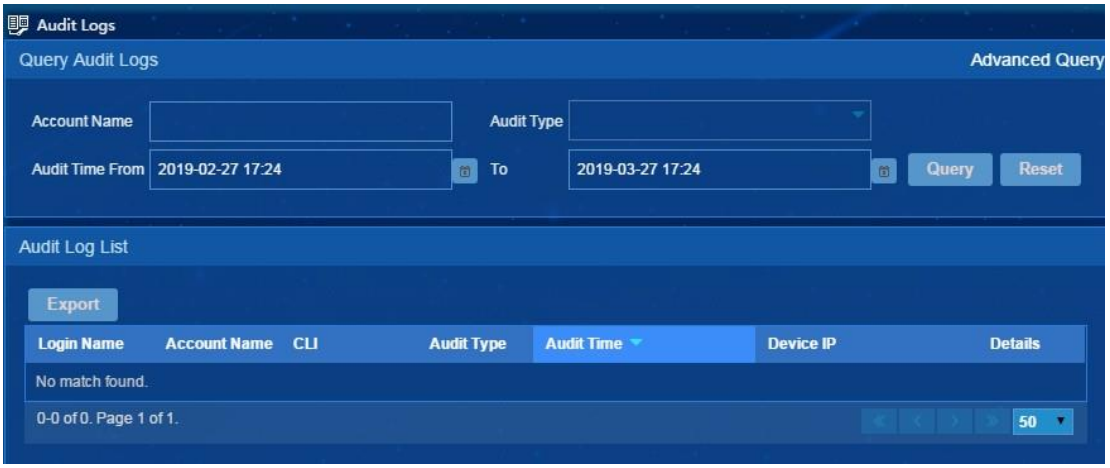
- EIAは、IMC ACLマネージャソリューションと連携して、アクセスデバイス上でACLを設定します。管理者は、アクセスデバイスを選択し、デバイス用のACLを設定できます。アクセスデバイスのACL展開情報は、アクセスデバイスリストに表示されます。
- EIAには、アクセスデバイスの詳細(基本的なデバイス情報、アラーム、パフォーマンスステータスなど)を照会するためのリンクがあります。
- 管理者は、トポロジ管理機能を使用してアクセスデバイスを管理できます。トポロジにはアクセスデバイスが表示され、管理者はこれらのデバイスに関する情報を表示できます。また、トポロジ上のアクセスデバイスを非アクセスデバイスに設定することもできます。

デバイスユーザー用のシナリオベースの許可ポリシー管理

- EIAは、シナリオに基づいて認可ポリシーを割り当てます。シナリオは、デバイスロケーション、デバイスタイプおよびアクセス時間範囲の組み合せです。管理者は、さまざまなシナリオのデバイスユーザーに対してシェルプロファイルおよびコマンドセットを定義できます。
- EIAでは、デバイスユーザーのネットワークアクセス時間範囲を制御するために、固定またはフレキシブルアクセス時間範囲の設定がサポートされています。
- シェルプロファイル設定では、特権レベル、アクセスACL、アクセス期間など、デバイスユーザーのグローバルアトリビュートを定義します。
- コマンドセットコンフィギュレーションでは、デバイスユーザーが使用できるコマンドを定義します。

デバイス管理動作の詳細なロギングと監査

- 認証ログには、ログイン名、ログイン結果、失敗理由、認証時間、ログインデバイスのIPアドレス、ユーザーのIPアドレス、特権レベル、ログインアクション、認証タイプ、サービスタイプなど、デバイスユーザーのデバイスログイン情報が記録されます。
- 承認ログは、ログイン承認およびコマンド承認イベントを監視します。ログイン承認が有効な場合、TACACS+Authentication Manager(TAM)サーバは、正常なログインユーザーに対してログインレベルを承認し、承認ログにイベントを記録します。コマンド承認が有効な場合、TAMサーバは、デバイスユーザーがコマンドを実行したときにコマンドの実行権限を持っているかどうかを判断し、コマンド承認ログを保持します。
- TAMサーバは、デバイスユーザーログイン、ログインデバイス、デバイスユーザーの動作を記録します。監査ログには、ログイン名、監査タイプ、監査時刻、デバイスIP、エンドポイントユーザーIP、コマンドなどの情報が記録されます。



監査ログ

ネットワーク運用のインテリジェントな広告プッシュ

IMCプラットフォームを使用すると、EIAはユーザーIDおよびアクセス場所に基づいてユーザーに広告をプッシュできます。アクセスユーザーはより簡単かつ迅速に情報を取得できます。また、EIAはサードパーティーの広告プラットフォームと連携して、ネットワーク操作のニーズを満たすこともできます。

高パフォーマンスの認証プロセスと大規模なデータベースストレージ

認証機構の最適化、パケット処理の簡易化、メモリ制御の効率化により、1秒間に1万人以上のユーザーからの認証要求を、認証ピーク時に同時に処理することができます。また、データベースの性能の最適化とサービス処理の正確な制御により、数百万人のユーザーに関するデータの統計収集やサービス処理を効率的に行うことができます。

仕様

項目		仕様
ハードウェア プラットフォーム	PCサーバ	Xeon 2.4 G(以上)、メモリサイズ4 GB以上、ハードディスクサイズ80 GB以上、オプティカルドライブ48台、100 M NIC、解像度1024×768、サウンドカード
	PCクライアント	基本周波数≥1.8 GHz、メモリサイズ≥512 MB、ハードディスクサイズ≥20 GB、48xオプティカル ドライブ、100 M NIC、解像度1024×768、サウンドカード

項目		仕様
オペレーティングシステム	ウィンドウ	IMC EIAサーバ:Windows Server 2012/2016 64ビット データベース:SQL Server 2012 SP2/2014/2016 Enterprise 64ビット
	Linux	IMC EIAサーバ:Red Hat Enterprise Linuxバージョン7.3/7.4 64ビット データベース:Oracle 11g/12c 64ビット

注文情報

プロダクトID	説明
SWP-IMC7-EIA	H3C iMC、エンドユーザーインテリジェントアクセスコンポーネント
LIS-IMC7-EIAA-50	H3C iMC、エンドユーザーインテリジェントアクセスコンポーネント、50ライセンス
LIS-IMC7-EIAB-200	H3C iMC、エンドユーザーインテリジェントアクセスコンポーネント、200ライセンス
LIS-IMC7-EIAC-500	H3C iMC、エンドユーザーインテリジェントアクセスコンポーネント、500ライセンス
LIS-IMC7-EIAD-2000	H3C iMC、エンドユーザーインテリジェントアクセスコンポーネント、2000ライセンス
LIS-IMC7-EIAE-5000	H3C iMC、エンドユーザーインテリジェントアクセスコンポーネント、5000ライセンス

The Leader in Digital Solutions

New H3C Technologies Co., Limited
Beijing Headquarters
Tower 1, LSH Center, 8 Guangshun South Street, Chaoyang District, Beijing, China
Zip: 100102
Hangzhou Headquarters
No.466 Changhe Road, Binjiang District, Hangzhou, Zhejiang, China ,Zip: 310052
Tel: +86-571-86760000

http://www.h3c.com