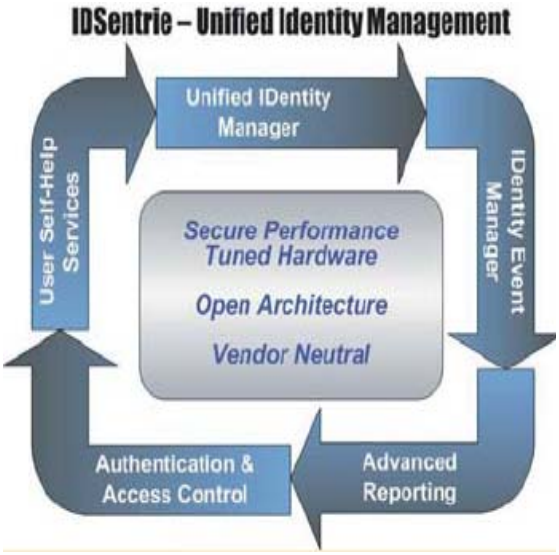
A10 IDsentrie 系列的產品介紹

〝沒有身份識別，沒有資訊安全〞，資訊安全是一個複雜而涵蓋多種安全設備、網路行為分析設備、及網路基礎設備的系統，當大量的日誌、告警產生時，想要在這些眾多訊息中及時跟踪問題是非常有挑戰性的工作，尤其是當這些訊息都只提供 MAC 或 IP 地址而缺乏實質的身份訊息時。如果能在網路中加入身份識別與連接管理功能，則不僅能符合更嚴格的審計法規，能有效跟踪現有網路系統的諸多事件，及時解決問題，同時也能產生更多帶有身份訊息的記錄與報表。

IDsentrie 提供完整身份識別與連接管理(IAM)功能，能在既有環境中將安全、網路與身份識別緊密融合，滿足 IT 人員在網路身份識別與連接管理上方面的需求。
A10 IDsentrie 系列分為兩個型號：

●A10 IDsentrie 2000 適用於中、大型企業用戶
●A10 IDsentrie 1000 適用於中、小型企業用戶

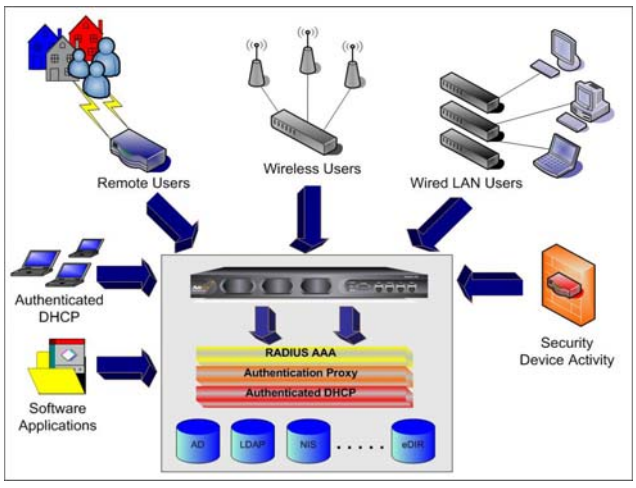


IDsentrie™ 系列的主要 IAM 功能組件：

●業界最強的 RADIUS 認證伺服器 (AAA)
●RADIUS 及 LDAP 認證代理 (Proxy)
●統一身份管理引擎 (UIM)
●用戶自助式服務 (Self-Help)
●基于身份的事件管理引擎 (IEM)
●IP-to-ID 即時身份解析服務 (UIR)
●高級報表(Reporting)
●Authenticated DHCP 伺服器

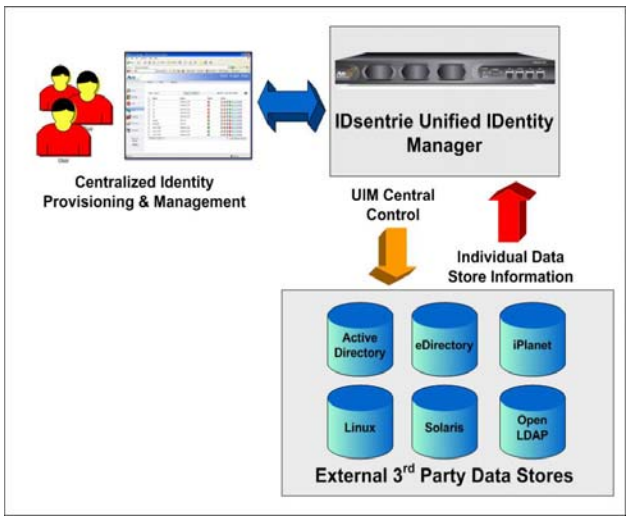
基于標准的 RADIUS 認證伺服器（AAA）

IDsentrie™的RADIUS認證伺服器支援多種認證協議及多種第三方目錄及數據存儲，爲企業的本地服務(Wired LAN)以及各種接入服務（如 802.1x、Wireless、撥接、VPN 等）提供安全認證服務，同時它還可以提供認證代理服務，方便用戶使用既有目錄中的的帳戶訊息。



統一身份管理引擎（UIM）

統一身份管理引擎通過把不同目錄中的帳戶訊息集中到一個便於管理的虛擬目錄下，來簡化企業對帳戶的管理。它滿足了企業對帳戶訊息進行集中統一管理的需求。這樣，帳戶訊息就能夠很快地被同步到所有目錄中，極大程度地提高整個網路系統的安全性和可靠性。統一身份管理引擎不但爲企業降低了網路系統的管理負擔，而且完全避免了由于網路的複雜性，所導致IT人員的操作失誤給企業帶來的重大損失，同時也強化了企業對內部身份訊息的管理。

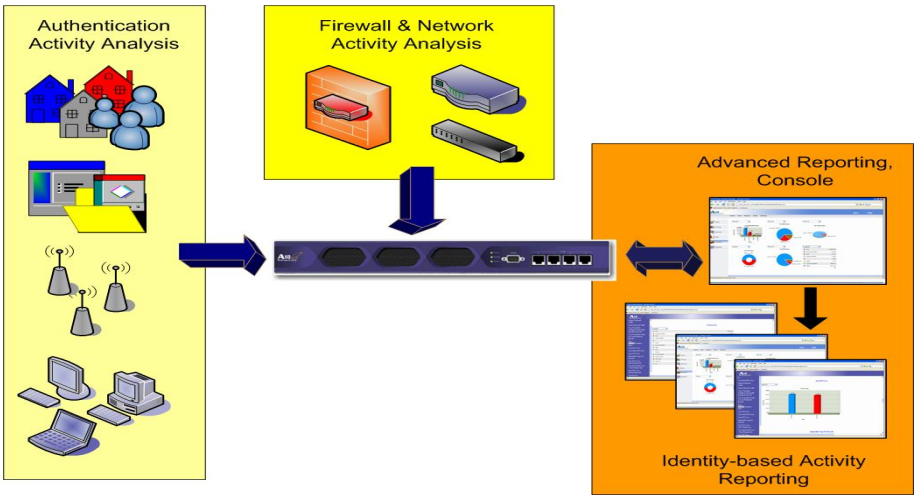


用戶自助式服務（Self-Help）

管理太多的帳戶與密碼對用戶與IT人員都是一個頭痛的問題，遵循強化的密碼規則、定期更新密碼、重設被遺忘的密碼、預告密碼即將過期、解開被鎖住的帳戶、更新用戶個人資料等周而復始繁瑣的工作往往造成IT人員沉重的負擔，但如果不即時處理，用戶無法使用IT資源，又會影響到用戶的生產力。IDsentrie™的用戶自助式服務幫助用戶透過Web介面即時自行處理以上的資料更新並自動與各目錄達成同步更新，同時IT人員也會收到詳細的更改報告，這樣便徹底解決了用戶與IT人員的頭痛問題，也強化了身份識別與網路連接管理。

基於身份的事件管理引擎（IEM）

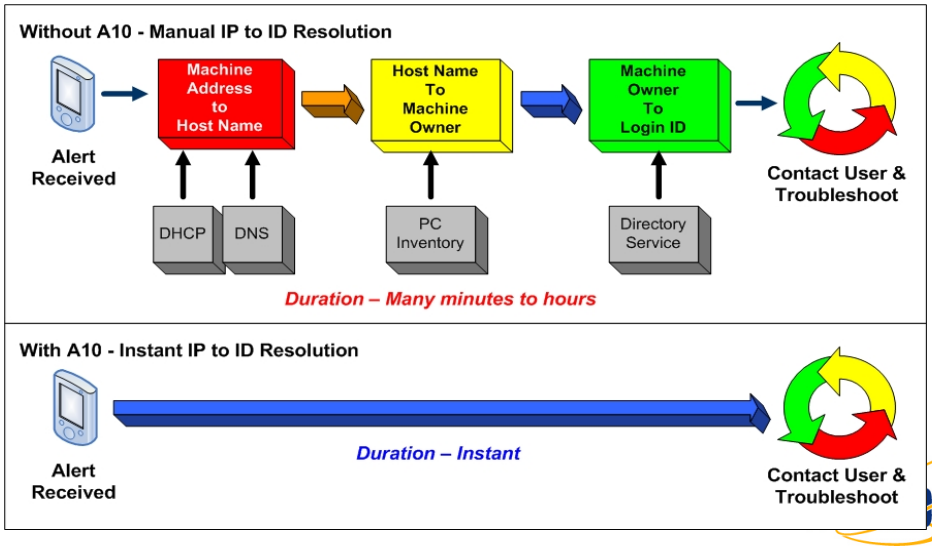
IDsentrie™的事件管理引擎通過對網路中的防火牆、IDS/IPS 等安全設備以及網路設備的日誌進行綜合分析，並與用戶身份和認證訊息進行相互關聯，能夠準確地追蹤網路資源的使用情況和重要的用戶行爲。可以基於用戶身份進行即時監視、查看以往的歷史記錄、提供基於身份的報表、日誌以及預警功能，使得用戶的網路行爲具有較深層次的可視性。網路行爲監視及事件管理能夠快速地指出某個用戶、在什麼時間、通過哪個防火牆做了哪些事情，這樣對快速解決問題和預防網路異常發揮了積極的作用。



IP-to-ID 即時身份解析服務（UIR）

解析身份訊息一直是管理公司網路與強化資訊安全的關鍵部分、每個 IT 人員都希望在發生重大安全或網路事件時能迅速正確找出用戶的真實身份以便有效保護網路與公司資源，但是當面對大量的日誌、告警時，傳統以人工的方式透過 MAC 及 IP 地址來查找用戶真實身份將會費時又費勁，徒然喪失有效解決問題的黃金時間，進而造成更大範圍的安全風險及更嚴重的損失。

IDsentrie™的IP-to-ID即時身份解析服務透過對網路中多重訊息的整合，如遠程接入認證訊息、無線接入認證訊息、各種目錄伺服器（AD、NT、eDirectory、LDAP、Sun ONE/iPlanet Directory、Linux、Solaris,…）中登入登出訊息、VPN登入登出訊息、及DHCP等等訊息，自動且及時提供IP到ID對應的身份訊息，絲毫沒有人力與時間的耗損。此外，IP-to-ID即時身份解析服務也提供基於開放的XML API介面，及CLI、GUI、jEdit等介面，可以對為數眾多的第三方設備提供即時ID請求與ID回應的代理服務。



高級報表（Reporting）

IDsentrie™系列的高級報表組件透過對RADIUS認證組件、統一身份管理引擎組件以及事件管理引擎組件之間的緊密結合，提供全面的日誌、報表和預警功能。高級報表組件爲企業在身份認證和基于身份的網路行爲分析管理方面提供了一個完整的視圖。

IT 人員可以爲他們的報表、圖形和預警功能進行客制化來簡化管理功能。

解決方案說明

IDsentrie™系列客戶案例，客戶需求重點如下：

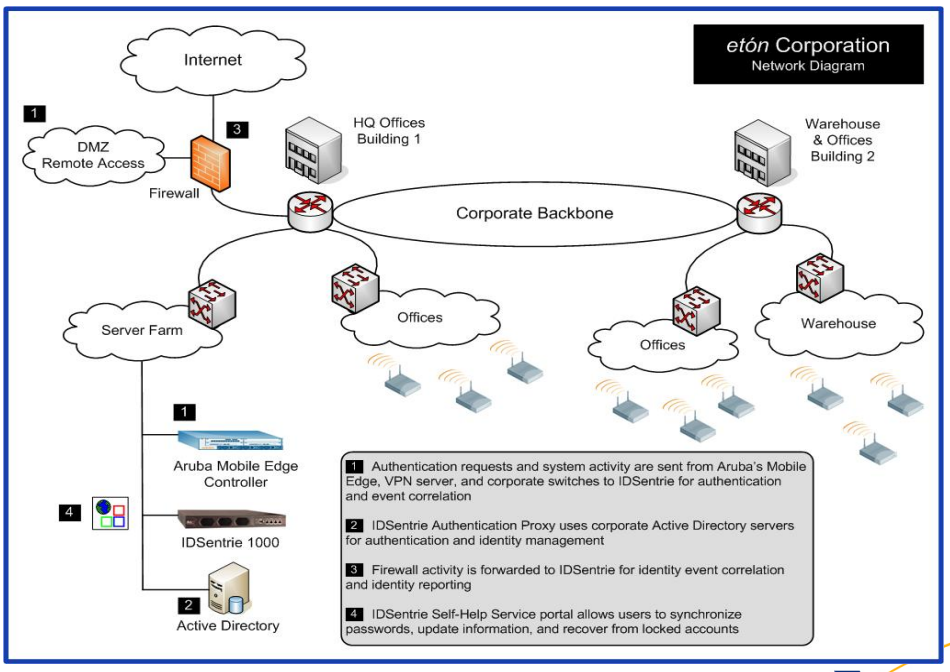
●無線網路接入認證

●認證代理服務沿用既有目錄的帳戶訊息

●基於身份的防火牆日誌、報表

●用戶自助式服務

說明：A10 **IDsentrie 1000 放在企業內部與公司內 AD 做相互認證，並結合其內部的無線網路管理系統，在認證時同時達到"安全的身份管理"的目的；並提供高級報表，及 MIS 管理日誌；針對使用者也提供簡易的用戶自助服務，用關鍵問題提示用戶答案，並同步給後端認證系統。**



IDsentrie™的主要的特點包括如下：

- 基於硬體平台的 IAM 完整解決方案
- 幫助客戶實現從 IP 網路向 ID 網路的自然遷移
- 四大功能組件使企業實現通過一個統一的硬體平台對網路與安全進行更加有效的管理
- 業界領先的高性能硬體 Radius 認證伺服器，支持每秒 6000 個認證請求
- 全面支援最新的認證協議：包括 Radius 認證、802.1x 認證、EAP、SecurID、證書、Authenticated DHCP 功能、Radius 認證代理及 LDAP 認證代理服務，設備內部資料儲存最大支援 20,000 筆帳戶資料
- 支援遠程撥接、VPN、Wireless AP、Wired LAN 等多種網路接入的認證
- 支援多廠家、多類型的網路安全設備和用戶身份的關聯管理
- 支援 Windows、Linux 以及 Sun、HP 伺服器的用戶登入認證
- 支援 Active Directory、Windows NT、LDAP v2，v3/OpenLDAP、Novell eDirectory、Sun ONE/iPlanet Directory Server、Solaris、Fedora Linux、Red Hat/FreeBSD/NetBSD、Kerberos、SecurID 等目錄、資料儲存及 Oracle、MS SQL、MySQL 等數據庫的用戶登入認證及統一帳戶管理功能
- 提供開放的 API 介面，為不同廠家、設備、及應用提供身份識別訊息
- 提供 IP-to-ID 解析服務並可透過 CLI、GUI、XML API 界面、解析器等工具以進行 IP 與用戶名的解析。
- 提供日誌（Syslog）解析服務，可自動將身份訊息（ID）與 IP Based 事件日誌及各種報表加以結合
- 提供用戶透過網頁自助重設密碼、更改密碼、更改個人資料等功能，並且所有更改動作均有記錄可供查核
- 靈活細緻的身份策略配置使連接管理更加完善
- 智能化網路安全報表爲企業管理階層提供全面的網路安全掌控
- 提供精準即時的網路可疑行爲預警
- 不可更改的用戶網路行爲記錄爲公司機密資料的保護提供了法律依據
- 支持多種不同的數據儲存格式，能夠快速的部署到現有的網路中
- 具有雙機熱備援功能，實施監控重要硬體和軟體的安全運行情況
- 採用用戶慣用的界面，降低了操作複雜性，使操作變得簡單、易用
- 簡化企業內部身份訊息的管理，提高企業工作效率，降低管理成本
- 為企業內部審計及遵循各種法規提供堅實有力的基礎（SOX, HIPPA,…）