

Cisco Secure Access Control Server Version 3.0 for Windows

產品概述

Internet與各種網路(公有、私有、有線、無線、LAN 與 extranet)的成長，使得如何對使用者的認證與網路存取進行控制、授權及稽核面臨更大的難題。為了應付愈來愈多以不同類型裝置與服務上網的網路使用者，Cisco Systems 推出可在 Windows 2000 與 NT 上執行的 Cisco Secure Access Control Server 3.0版(Cisco Secure ACS)。Cisco Secure ACS 是一部具有高擴充性與高效能的存取控制伺服器，能夠作為中央的「遠端存取撥接使用者服務」(Remote Access Dial-In User Service, RADIUS)或 TACACS+ 伺服器系統，並對利用網路存取公司資源的使用者進行身份認證、授權與帳戶稽核(Authentication、Authorization、Accounting, AAA)。

Cisco Secure ACS 能集中管理撥接存取伺服器、VPNs 與防火牆、voice-IP 解決方案、寬頻解決方案、內容網路與 Cisco 無線解決方案的存取控制與帳戶稽核。Cisco Secure ACS 3.0 版新增 IEEE 802.1X 使用者認證標準，可對 Cisco Catalyst® 交換器解決方案的 LAN 使用者進行身份認證。

目前企業可利用同一個存取控制架構(AAA)，以新版 Cisco Secure ACS 的 Extensible Authentication Protocol(EAP)模組，來管理乙太網路 LAN 客戶端或無線客戶端使用者的存取。有了 Cisco Secure ACS 3.0 版，網路管理者就能快速管理所有網路使用者的存取。此可改善網路管理者擴充與配置安全網路服務的整體能力，並藉著 Cisco Secure ACS 架構中的集中式控制、存取管理與帳戶稽核，而節省作業時間。

Cisco Secure ACS 3.0 版新增了一部功能強大的裝置指令政策引擎，用於 TACACS+ 的管理控制。裝置指令集符(device command sets, DCSs)的特色，是全新、精細地控制行政管理作業，並提供可重覆使用的政策，大幅提高於大量使用者群組與網路裝置群組間擴充管理權限的能力。

利用 Cisco Secure ACS，網路管理者就能控制：

- ★ 以有線或無線連線登入網路者；
- ★ 網路中各個使用者的權限；
- ★ 安全稽核與帳單系統記錄的帳戶資料；
- ★ 每位組態管理者能夠進行的存取與指令控制。



主要特色與優點

Cisco Secure ACS 新增的重要特色

- ★ *IEEE 802.1x*：LAN 使用者的存取控制—Cisco Secure ACS 3.0 版可支援 IEEE 802.1x 標準，藉著讓網路管理者控制欲存取 LAN 環境的使用者，為網路 LAN 端提供新的安全服務。802.1x 標準，是 IEEE 新提出的存取控制標準，用來管理埠級(port-level)的存取控制。其仰賴在 RADIUS 上執行的 EAP，可管理埠級(port-level)存取控制的使用者身份認證與授權。
- ★ *EAP 訊息摘要 5 (EAP Message Digest 5, EAP—MD5) 與 EAP 傳輸 LAN 服務(EAP-TLS)*：新的認證模式-EAP 是一種 Internet Engineering Task Force (IETF) RFC 標準，用於執行點對點協定(PPP)連線間不同的認證方法。EAP-MD5 是一種利用使用者名稱 / 密碼進行認證的方法，其結合了 MD5 雜湊方式以保障安全。EAP-TLS 則是一種可讓 Cisco 安全存取伺服器端與客戶端兩方使用 X.509 數位簽章(digital certificates)進行身份認證的方法，並可提供動態 session key 的協商。
- ★ *裝置指令集(Device Command Sets, DCS)*：一種功能強大、能夠管理 TACACS+ 的新方式—此種新的管理工具能提供集中式的 Cisco Secure ACS 圖形使用者介面(GUI)機制，並透過每一使用者、每一群組或每一網路裝置群組的對應關係來控制每一裝置的指令之授權。受到某些使用 Cisco Secure ACL 的大企業與服務供應商網路需求的驅使，DCSs 能作為一種將指令集群組並命名的方法，並可與使用者、使用者群組或裝置群組整合。DCSs 的主要優點，就是能將移除每部網路存取伺服器(NAS)的個別權限階級或指令限制。此一特色將大幅提高網路管理者設定授權限制時的可擴展性與管理能力。

- ★ *支援 Microsoft Challenge Authentication Protocol (MSCHAP) 2 版與新的密碼過期或更換*—目前 Cisco Secure ACS 能夠支援 MSCHAP 2 版的交換以及 MSCHAP 密碼變更服務，以供 Microsoft 撥接網路客戶端、Cisco VPN 客戶端和其它能夠支援 MSCHAP 2 版密碼變更服務的桌上型客戶端使用。此項新功能在使用者登入後，提醒或強迫使用者變更過期的密碼。
- ★ *每位使用者的存取控制清單*—此項新服務乃特別為 Cisco PIX™ 防火牆解決方案而建立，以使管理者能夠為 Cisco 存取控制伺服器圖形使用者介面中的使用者或使用者群組，定義各種長度的存取控制清單。
- ★ *NAS wildcarding*—此項新的 wildcarding 能夠為裝置、新增裝置群組以及 NAS 過濾器提供支援，使 Cisco 安全存取控制系統在新增裝置與管理時，能變得更容易。
- ★ *“Multi NAS”*—除了 wildcarding 之外，新的 Multi-NAS 功能能使管理者替同一群組的網路裝置訂定相同屬性，如：共享的 key、認證方式或登入 / 帳戶參數。其亦可使管理者提供多重 IP 位址或 IP 位址的範圍。
- ★ *為存取過濾器(access filters)命名*—此項新功能，能為存取過濾器命名，以使相同過濾器分派至多個裝置或裝置群組的作業，能夠更簡化且更容易。
- ★ *Multiple Lightweight Directory Access Protocol (LDAP) 查閱表與 LDAP 失敗接管功能*—有了此項功能，就能夠對多個不同的 LDAP 使用者查閱表進行設定；此外，能夠定義備份的 LDAP 目錄位置，以便在主要 LDAP 伺服器無法運作時，有備份的 LDAP 伺服器接管。



- ★ 使用者可擴充的 *vendor-specific attributes*(VSAs)—目前 Cisco Secure ACS 可透過 Web 圖形使用者介面，支援使用者定義的 outbound VSAs。
- ★ 為 *Broadband Service Manager*(BBSM)增加新的 VSA 支援—Cisco Secure ACS 3.0 版能為 Cisco BBSM 解決方案增加新的 VSA 支援。
- ★ 改良的使用者文件—Cisco Secure ACS 3.0 版提供了大幅改善與重新編排的線上使用者指南，以及改良的使用者文件。

Cisco Secure ACS 的優點

Cisco Secure ACS 是一部功能強大的存取控制伺服器，其具有許多高效能與具擴充性的特色，對於想要提升 WAN 或 LAN 連線功能的企業而言，是非常理想的產品：

- ★ 使用容易—Web-based 的使用者介面，能夠簡化並配送使用者資料、群組資料的組態設定以及 ACS 的組態設定。
- ★ 擴充性—Cisco Secure ACS 可支援配置有備用伺服器、遠端資料庫與使用者資料庫備份服務的大型網路環境。
- ★ 延展性—LDAP 認證轉送(authentication forwarding)功能，能夠支援主要目錄廠商如 Netscape、Novell 和 Microsoft 目錄中所儲存之使用者資料的認證。

- ★ 管理—對 Windows 2000 動態目錄(Active Directory)和 NT 資料庫的支援，能夠結合 Windows 使用者名稱 / 密碼的管理功能，並利用 Windows 效能監視器(Performance Monitor)即時瀏覽統計資料。
- ★ 管理者—每位 Cisco Secure 管理者有不同的存取層級，以及將網路裝置群組的能力 - 能使控制更容易且具有更大的彈性，能夠讓網路中所有裝置之安全政策的管理與改變更為容易。
- ★ 產品彈性—因為 Cisco Secure ACS 內建有支援 AAA 的 Cisco IOS 軟體，因此幾乎可與所有 Cisco 售出的 NAS 整合。(所使用的 Cisco IOS 的版本必須可支援 RADIUS 或 TACACS+。)
- ★ 協定彈性—Cisco Secure ACS 同時支援 TACACS+ 與 RADIUS，可作為 VPN，或是為網際網路通訊協定安全設定(IPSec)之發出端與終止端提供撥接以及 Point-to-Point Tunneling Protocol(PPTP)的彈性解決方案。
- ★ 整合性—其與 Cisco IOS 路由器和 VPN 解決方案密切結合，能提供多項功能，例如：Multichassis Multilink 點對點協定與 Cisco IOS 指令授權等。
- ★ 協力廠商支援—Cisco Secure ACS 能提供 token 伺服器的支援，包括：RSA SecurID, Passgo, Secure Computing, ActiveCard, Vasco, 與 CryptoCard。
- ★ 控制—Cisco Secure ACS 能夠動態限制每日的使用時間、網路的使用量、登入交談的人數以及每星期存取的天數等。



硬體與軟體需求

硬體需求

要安裝 Cisco Secure ACS，您的 Windows 2000 或 Windows NT 伺服器至少必須符合下列硬體需求：

- ★ 處理速度 550 MHz 或以上的 Pentium 處理器
- ★ 256 MB 的 RAM
- ★ 未使用的硬碟空間至少 250 MB；如果在同一部機器上執行資料庫，則需要更大的硬碟空間
- ★ 解析度最少 256 色，800 x 600 像素

軟體需求

您的 Windows 2000 或 Windows NT 伺服器至少必須符合下列軟體需求：

- ★ NAS 必須能執行 Cisco IOS 軟體 11.2 或更新版本，或使用可支援 TACACS+ 或 RADIUS 的協力廠商設備。

更多資訊

如欲了解更多有關 Cisco Secure ACS 3.0 版的資訊，包括使用者指南與 release notes，請至：<http://www.cisco.com/go/acs>。

如對產品功能或技術上有任何疑問，請 e-mail 至 ACS-MKT@cisco.com 給 ACS 的產品行銷部。

如對產品訂購、上市情形與支援合約等資訊有疑問，請 e-mail 至 ciscoworks@cisco.com 給產品行銷部。

CISCO SYSTEMS



台灣思科系統股份有限公司
台北市敦化南路二段333號 6樓B座
高雄市三多四路110號 19F-2
服務專線：(02)2455-2764
<http://www.cisco.com>

Cisco 專業代理商



數技股份有限公司
RUNCOMP INTERNATIONAL CORP.
總公司:114台北市瑞光路2號2F-1
台北: Tel:02-8791-1999 Fax:02-8791-1988
新竹: Tel:03-575-1706 Fax:03-575-1707
台中: Tel:04-2329-6559 Fax:04-2310-6770
高雄: Tel:07-556-9682 Fax:07-556-9680
<http://www.runcomp.com.tw>

經銷商