安全Web裝置版本更改

目錄

簡介

本檔案介紹不同版本Secure Web Appliance(SWA)中的主要變更和新增功能。

必要條件

需求

本文沒有特殊要求。

本文的縮寫為：

LD：有限部署。

GD:通用部署。

MD:維護部署

ED：早期部署。

HP:熱修補程式。

CLI:命令列介面。

GUI:圖形使用者介面

HTTP:超文本傳輸協定。

HTTPS:超文本傳輸協定安全。

ECDSA:橢圓曲線數位簽章演算法。

PID：進程識別符號。

CTR:思科威脅響應。

AMP:高級惡意軟體防護。

URL:統一資源定位器。

CDA:上下文目錄代理。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

更改每個版本的歷史記錄

版本	類型	行為變化	增強功能/新增功能
12.0.1-268	LD	— 從12.0版本開始，系統CPU和記憶體要求將發生變化。 — 預設情況下，TLSv1.3在裝置上啟用。 — 密碼「TLS_AES_256_GCM_SHA384」已新增到預設密碼清單中。	- Cisco AsyncOS 12.0版本為平台S680、S690和S695提供高效能(HP)的網路安全裝置。 — 在advanced proxyconfig主命令下新增新的子命令highperformance，以啟用和禁用高效能模式。 — 將SWA與思科威脅響應(CTR)門戶整合。 — 裝置支援TLSv1.3版本。 — 配置檔案備份功能從系統管理下的子選單「Log Subscriptions」移動到「Configuration File」。 — 裝置現在支援為HTTPS代理上傳ECDSA證書。 — 在diagnostic > proxy下新增了一個新的診斷CLI proxyscannermap子命令。顯示每個代理和相應的掃描程式進程之間的PID對映。 — 在CLI命令authcache下新增新的選項searchdetails。 — 在CLI命令reportingconfig下新增新的子命令CTROBSERVABLE，以啟用或禁用CTR基於可觀察的索引。

12.0.1-334	GD		— 在advancedproxyconfig主命令下新增新的子命令掃描器，以排除AMP引擎要掃描的MIME類型。
12.0.2-004	MD	— 使用TLS 1.2或更高版本將裝置連線到AMP檔案信譽伺服器。 - AMERICAS（舊版）cloud-sa.amp.sourcefire.com無法在裝置上配置。	— 在主CLI命令advancedproxyconfig > scanners > AMP中新增了新選項「Enter the number of concurrent scans to be supported by AMP」（輸入AMP支援的併發掃描數）。 在CLI主命令advancedproxyconfig > scanners中，您可以將長時間運行的掃描逐出的預設Unscannable判定更改為Timeout，反之亦然，從新的CLI子命令逐出。
12.02-012	MD		— 在裝置的Web使用者介面上觸發警報消息 當代理Malloc Memory超過90%的代理Malloc Memory限制時，會向配置為接收「Web Proxy」嚴重警報的所有「警報收件人」傳送電子郵件通知。 — 新的網路介面為監控報告和跟蹤Web服務提供了新外觀。
12.0.3-005	MD		
12.0.3-007	MD		— 新URL類別更新通知
12.0.4-002	MD		
12.0.5-011	MD	— 裝置管理Web使用者介面預設啟用TLSv1.2 — 預設情況下禁用會話恢復。	— 在CDA配置部分新增消息以指示CDA支援終止。
12.5.1-011	LD	-預設情況下，裝置上啟用思科成功網路功能。 — 這些日誌經過修改，包含更多詳細資訊： 現在，身份驗證失敗時，訪問日誌會顯示使用者名稱。	- Cisco AsyncOS 12.5版本為平台S680、S690和S695提供高效能(HP)網路安全裝置。這將提高當前高端裝置的流量效能。 — 現在，即使已在裝置上啟用以下功能，也可以升級到12.5版本並在型號（S680、S690、S695、S680F、S690F和S695F）上使用高效能模式：

		身份驗證框架日誌現在顯示以下失敗身份驗證協定的客戶端IP地址：NTLM、BASIC、SSO（透明）	• Web流量分流器 • 數量和時間配額 • 整體頻寬限制 - 現在可以通過建立IP欺騙配置檔案並將其新增到路由策略來配置Web代理IP欺騙。 - 現在，您可以為YouTube建立自定義URL類別，並在YouTube自定義類別上設定策略以實現安全訪問控制。 - 在新網路介面中，裝置有一個新頁面(Monitoring > System Status)以顯示裝置的當前狀態和配置。 - 思科成功網路(CSN)功能使思科能夠收集裝置的功能使用資訊遙測資料。 - 用於網路、日誌訂閱和其他配置的REST API。
12.5.1-035	GD	— 棄用TLS 1.0/1.1： 使用TLS 1.2或更高版本將裝置連線到AMP檔案信譽伺服器。AMERICAS（舊版）cloud-sa.amp.sourcefire.com已從AMP檔案信譽伺服器清單中刪除，因此無法在裝置上配置AMERICAS（舊版）cloud-sa.amp.sourcefire.com。	— 從AsyncOS 12.5.1-035及更高版本不支援配置身份驗證的快取大小（網路>身份驗證>身份驗證設定>憑據快取選項）。
12.5.1-043	GD		— 警報消息顯示在裝置的Web使用者介面上（「系統管理」>「警報」>「檢視頂級警報」）： • 當代理malloc記憶體超過90%的代理malloc記憶體限制時 • 當代理在malloc記憶體的100%上重新啟動時 在這兩種情況下，都會向配置為接收「Web Proxy」嚴重警報的所有「警報收件人」傳送電子郵件通知。
12.5.2-007	MD		— 新URL類別更新通知引入標語中。有關即

			將進行的URL類別更新的電子郵件通知也會傳送給使用者。
12.5.2-011	MD		
12.5.3-002	MD		
12.5.4-005	MD	— 在Cisco AsyncOS 12.5.4版本中，裝置管理Web使用者介面預設啟用TLSv1.2。 - 升級到Cisco AsyncOS 12.5.4版本後，預設情況下會禁用會話恢復。 — 在CDA配置部分新增消息以指示CDA支援終止	
12.5.4-011	MD-Refresh		
12.5.5-004	MD		-升級到Cisco AsyncOS 12.5後，首次執行networktuning命令時，系統會提示您重新啟動代理進程。
12.5.5-008	MD-Refresh		
12.5.6-008	MD		
14.0.1-014	LD	— 預設情況下，HTTP 2.0功能處於禁用狀態。要啟用此功能，請使用<HTTP2>命令。 — 適用於思科網路安全裝置的AsyncOS 14.0支援客戶端和伺服器中的TLSv1.3會話恢復。 — 修改這些證書的有效期： • HTTPS • ISE	— 思科網路安全裝置現在支援與Cisco SecureX整合。 — 您可以為HTTP請求配置自定義報頭配置檔案，也可以在報頭重寫配置檔案下建立多個報頭。 — 您現在可以為Active Directory配置基於報頭的身份驗證方案。客戶端和網路安全裝置將使用者視為經過身份驗證，並且不會再次提示輸入身份驗證或使用者憑據。當網路安全裝置充當上游裝置時，X驗證功能將發揮作用。

		• SAAS • 裝置證書 • 演示/管理證書 — 由於日誌訂閱中的日誌名和檔名無效，升級失敗時，裝置的CLI和GUI現在會顯示消息。 — 預設情況下，輪詢間隔設定為24小時。 — 升級到此版本後，如果Base DN(Base Distinguished Name)欄位(「網路」(Network)>「身份驗證」(Authentication)>「新增領域」(Add Realm))為空，則無法執行LDAP身份驗證的啟動測試。	- 裝置的系統狀態控制面板已增強： • Capacity頁籤 — 提供時間範圍、系統CPU和記憶體使用率、頻寬和RPS、按功能劃分的CPU使用率以及客戶端或伺服器連線的詳細資訊。 • Status頁籤下的Proxy Traffic Characteristics提供客戶端和伺服器連線的詳細資訊。 • 服務響應時間現在包含條形圖的更多詳細資訊，以及以前日期的圖例資料。 — 現在您可以檢索配置資訊，並在裝置的配置資料中執行更改（如修改當前資訊、新增新資訊或刪除條目），使用管理策略、訪問策略和繞過策略的REST API - Cisco AsyncOS 14.0版本支援HTTP 2.0以通過TLS進行Web請求和響應。HTTP 2.0支援需要基於TLS ALPN的協商，該協商僅從TLS 1.2版本開始。 在此版本中，以下功能不支援HTTPS 2.0: • Web流量分流器 • 外部DLP • 總頻寬和應用頻寬 — 引入新的CLI命令<HTTP2>以啟用或禁用HTTP 2.0配置。您無法通過裝置Web使用者介面啟用或禁用HTTP 2.0並限制HTTP 2.0的域。 — 不支援通過Cisco Secure Email和Web Manage配置HTTP 2.0 — 當您嘗試使用以下任何功能的預設證書時，CLI會顯示新的警告消息： • 裝置證書（在Web使用者介面中，導航到Network > Certificate Management > Appliance Certificate） • 憑據加密證書（在Web使用者介面中，導航到網路>身份驗證>編輯設定>高級部分）

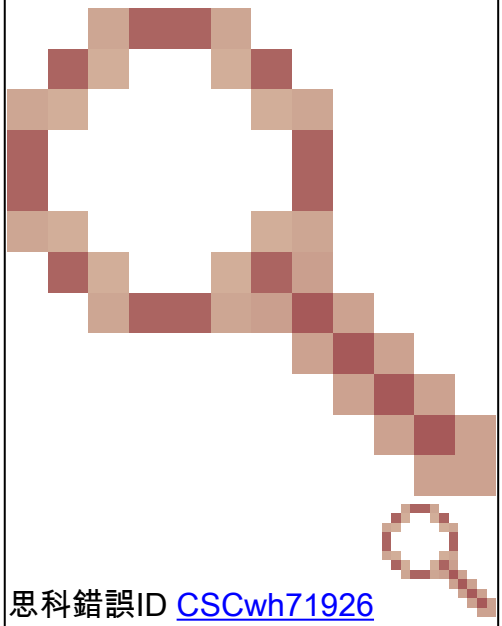
			• HTTPS管理UI證書（在命令列介面中使用certconfig > SETUP） — 在certconfig下新增了一個新的子命令OCSPVALIDATION_FOR_SERVER_CERT。使用此新子命令，可以為LDAP和更新伺服器證書啟用OCSP驗證。如果啟用了證書驗證，則當通訊中涉及的證書被吊銷時，您會收到警報。 — 新增了一個新的CLI命令gatheredconfig，以配置裝置和身份驗證伺服器之間的輪詢功能。 — 在裝置上配置智慧許可證功能時，現在可以在管理和資料介面之間選擇。
14.0.1-040	LD	— 當您啟用智慧軟體許可並在思科智慧軟體管理器中註冊網路安全裝置時，思科雲服務 (Network > Cloud Service Settings)通過思科雲服務門戶自動啟用和註冊安全Web裝置。 — 如果在裝置上註冊了智慧許可，則無法禁用或註銷思科雲服務。 — 如果您已將裝置註冊到思科智慧軟體管理器(Cisco Smart Software Manager)，且尚未配置思科雲服務(Cisco Cloud Services)，則在升級到AsyncOS 14.0.1-040後會自動啟用思科雲服務(Cisco Cloud Services)。預設情況下，該區域註冊為美洲，您可以根據需要修改該區域（歐洲和APJC）。 — 如果在裝置上註冊了智慧許可證，則無法禁用或註銷思科雲服務。	— 您可以在CLI中通過smartaccountinfo命令檢視在Cisco智慧軟體管理器門戶中建立的智慧帳戶的詳細資訊。 — 如果思科雲服務證書已過期或即將過期，則在升級到AsyncOS 14.0.1-040後，思科雲服務會自動續訂證書。 — 如果Cisco Cloud Services證書已過期，現在您可以在CLI中從cloudserviceconfig > fetchcertificate子命令從Cisco Talos Intelligence Services門戶下載新證書。 — 您可以使用思科雲服務門戶自動註冊網路安全裝置(CLI中的cloudserviceconfig > autoregister子命令) — 您可以在CLI中從updateconfig > clientcertificate子命令載入虛擬裝置和硬體裝置的證書。 — 新URL類別更新通知引入標語中。 還將向使用者傳送有關即將進行的URL類別更新的電子郵件通知。
14.0.1-053	GD		
14.0.1-503	HP		

14.0.2-012	MD	— 在Cisco AsyncOS 14.0.2版本中，在System Administrator > SSL Configuration下，Appliance Management Web User Interface預設啟用TLSv1.2。 — 預設情況下禁用會話恢復。	— 在CDA配置部分新增消息以指示CDA支援終止。 — 現在，您可以從Test Interface下拉選單中選擇Data或Management interface for Smart License Registration。
14.0.3-014	MD	— 升級到Cisco AsyncOS 14.0後，首次執行networktuning命令時，系統會提示您重新啟動代理進程。	
14.0.3-502	HP	— 當Secure Web Appliance在高效能模式下運行時，堆限制耗盡會禁用高延遲並接受處理程式。這會導致連線數量減少。	
14.0.4-005	MD		
14.5.0-498	LD	— 產品重新命名： • 面向終端的AMP、高級惡意軟體防護和AMP已更改為 安全端點 • 執行緒網格（檔案分析）已更改為Malware Analytics — 錯誤分類請求通過HTTPS傳送，因此您不會收到安全警報通知。 - Samba版本已升級到4.11.15版。 — 裝置管理Web使用者介面在System Administrator > SSL Configuration下預設啟用TLSv1.2。 — 在AsyncOS 14.5的新安裝中，預設情況下，HTTPS Proxy頁中的Expired and Mismatched Hostname certificate configurations值將選擇為Drop，而不是Monitor。	— 安全網路裝置現在可以驗證從DNS伺服器收到的DNS響應是否支援加密簽名。 — 安全Web裝置將客戶端啟動的併發連線數限製為已配置的值。 — 在AsyncOS版本14.5中，思科網路安全裝置已重新命名為思科安全網路裝置 — 當客戶端Web瀏覽器上顯示EUN頁時，解密策略組中的訪問日誌決策標籤會附加有EUN（終端使用者通知）。 — 克隆策略功能允許您複製或克隆策略的配置並建立新策略。 — 可以通過在配額配置檔案中配置頻寬值並對映訪問策略URL類別或整體Web活動配額中的配額配置檔案來管理流量頻寬。 - REST API，用於配置管理策略、解密策略、路由策略、IP欺騙策略、防惡意軟體和信譽、身份驗證領域、思科智慧軟體許可證、思科保護傘無縫ID、身份服務和系統設定。

			— 您可以將ISE-SXP部署與思科安全Web裝置整合以實現被動身份驗證。這允許您獲取所有已定義的對映，包括通過SXP發佈的SGT到IP地址對映。 — 通過思科Umbrella無縫ID功能，裝置可在成功身份驗證後將使用者標識資訊傳遞到Cisco Umbrella安全網路網關(SWG)。 — 在CDA配置部分新增消息以指示CDA支援終止。 — 現在，您可以從Test Interface下拉選單中選擇Data或Management interface for Smart License Registration。 — 升級到Cisco AsyncOS 14.5後，首次執行networktuning命令時，系統會提示您重新啟動代理進程。
14.5.0-537	GD		— 這些在Secure Web Appliance中具有克隆選項的策略也可由Cisco Secure Email and Web Manager(SMA)管理： • 訪問策略 • 標識配置檔案 • 解密策略 • 路由策略
14.5.1-008	MD		
14.5.1-016	MD		
14.6.0-108	LD		- AsyncOS 14.6通過思科安全網路裝置(SWA)為Cisco Umbrella提供支援。Umbrella和安全網路裝置的整合方便了從Umbrella到安全網路裝置的通用網路策略的部署。
15.0.0-322	LD	- FreeBSD版本已升級到FreeBSD 13.0。 - Cisco SSL版本1.0.2到Cisco SSL版本1.1.1。	— 對智慧軟體許可功能進行了以下增強： • 許可證保留 • 裝置Led轉換 — 使用智慧許可證註冊安全Web裝置後，當前所有有效的傳統許

		- AVC、WBRSD、DCA和Beaker等Talos引擎已升級。 — 已升級Webroot和McAfee等掃描程式引擎。	可證將通過Device Led Conversion(DLC)過程自動轉換為智慧許可證。這些轉換的許可證將在CSSM門戶的虛擬帳戶中更新。 — 可以通過在配額配置檔案中配置頻寬值並對映解密策略和訪問策略中的配額配置檔案、URL類別或總的Web活動配額來管理流量頻寬。 — 克隆策略功能允許您複製或克隆策略的配置並建立新策略。 — 應用發現與控制(ADC)引擎： 可接受的使用策略元件，用於檢查web流量，以便更深入地瞭解和控制用於應用程式的web流量。 在AsyncOS 15.0中，可以使用AVC或ADC引擎來監控Web流量。預設情況下，AVC處於啟用狀態。ADC引擎支援高效能模式。 — 用於ADC配置的REST API — 管理員可以選擇配置除預設使用者名稱v3get以外的自定義SNMPv3使用者名稱。 — 自定義報頭的最大長度為16k。 — 用於選擇安全隧道介面和遠端訪問連線的選項。
15.0.0-335	GD	- Device Led Conversion — 使用智慧許可註冊Secure Web Appliance後，所有當前有效的經典許可證將通過Device Led Conversion(DLC)過程自動轉換為智慧許可證。這些轉換的許可證將在CSSM門戶的虛擬帳戶中更新。 — 預設情況下，AVC已啟用。 - Cisco SSL版本1.0.2到Cisco SSL版本1.1.1 - Talos引擎（例如AVC、WBRSD、DCA和Beaker）已升級	— 許可證保留 — 您可以為安全網路裝置中啟用的功能保留許可證，而無需連線到思科智慧軟體管理器(CSSM)門戶。這主要適用於在高度安全的網路環境中部署Secure Web Appliance而不與Internet或外部裝置通訊的使用者。 -可以通過在配額配置檔案中配置頻寬值並在解密策略和訪問策略URL類別或總體Web活動配額中對映配額配置檔案來管理流量頻寬。 -克隆策略功能允許您複製或克隆策略的配置並建立新策略。 — 支援應用發現和控制(ADC)引擎，這是一個

		。 -已升級Webroot和McAfee等掃描程式引擎。 - FreeBSD 13.0僅與Cisco SSL版本1.1.1相容。 只有與Cisco SSH相容的密碼、mac和kex演算法才能支援與FreeBSD 13.0的SSH連線。 -作為AsyncOS15.0 GD版本的一部分，Secure Web Appliance中的DCA功能被禁用。在升級到此版本後，您可以通過導航到Security Services>Acceptable Use Controls並選中DCA覈取方塊來啟用它。 — 多代理SWA(S690、S695、S1000V)不支援對代理Malloc記憶體的SNMP OID執行SNMPWALK/SNMPGET操作。	可接受的使用策略元件，用於檢查Web流量，以更深入地瞭解和控制用於應用的Web流量。 現在，您可以使用AVC或ADC引擎來監控Web流量。 - ADC引擎支援高效能模式。 — 您現在可以在具有REST API的裝置的訪問策略配置資料中檢索配置資訊，並執行任何更改（如修改當前資訊、新增新資訊或刪除條目）。 -Admin可以選擇配置除預設使用者名稱v3get以外的自定義SNMPv3使用者名稱。 - 自定義報頭對Web請求的最大長度為16k。 - 用於選擇安全隧道介面和遠端訪問連線的選項
15.0.0-364	HP	已修復以下缺陷： 思科錯誤ID CSCvz26149 思科錯誤ID CSCwf78874 思科錯誤ID CSCwf84371 思科錯誤ID CSCwh31573 思科錯誤ID CSCwh37834 思科錯誤ID CSCwh41379 思科錯誤ID CSCwh48523	

		 思科錯誤ID CSCwh71926	
15.1.0-287	LD	— 在AsyncOS 15.1及更高版本中，必須提供智慧軟體許可證。 - Cisco Umbrella與Cisco Secure Web Appliance的整合方便了從Umbrella到Secure Web Appliance的常見Web策略的部署。此外，您還可以通過Umbrella控制面板和檢視日誌來配置策略。	

開源元件

以下是在SWA中使用的開源元件更改的清單：

版本	11.8.X	12.0.X	12.5.X	14.0.X	14.5.X	14.6.X	15.0.X
freebsd	10.4	10.4	10.4	11.2	11.2	11.2	13.0

相關資訊

- 思科網路安全裝置AsyncOS 12.0版本說明 — 思科
- 思科網路安全裝置AsyncOS 12.5版本說明 — 思科
- 思科網路安全裝置AsyncOS 14.0版本說明 — 思科
- 思科安全網路裝置AsyncOS 14.5版本說明 — 思科
- 內容安全的版本術語是什麼？(cisco.com)
- 思科安全電子郵件和網路虛擬裝置安裝指南

- 技術支援與文件 - Cisco Systems
- 思科安全網路裝置AsyncOS 15.1版本說明 — 思科
- 思科安全網路裝置AsyncOS 15.0 Hot Patch 1發行說明 — 思科

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。