Versionsänderungen der sicheren Webanwendung

Inhalt

Einleitung

In diesem Dokument werden die wichtigsten Änderungen und hinzugefügten Funktionen in den verschiedenen Versionen der Secure Web Appliance (SWA) beschrieben.

Voraussetzungen

Anforderungen

Für diesen Artikel gibt es keine besonderen Anforderungen.

Abkürzungen, die in diesem Artikel verwendet werden:

LD: Eingeschränkte Bereitstellung.

GD: Allgemeine Bereitstellung.

MD: Wartungsbereitstellung

ED: Frühzeitige Bereitstellung.

HP: Hot Patch.

CLI: Command Line Interface (Befehlszeilenschnittstelle)

GUI: Grafische Benutzeroberfläche

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure

ECDSA: Elliptic Curve Digital Signature Algorithm.

PID: Prozesskennung.

CTR: Cisco Threat Response

AMP: Advanced Malware Protection

URL: Uniform Resource Locator

CDA: Kontextverzeichnis-Agent.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Änderungshistorie pro Version

Version	Typ	Verhaltensänderungen	Verbesserungen/zusätzliche Funktionen
12.0.1-268	Niederländisch	- Die CPU- und Speicheranforderungen des Systems wurden ab Version 12.0 geändert. - Standardmäßig ist TLSv1.3 auf der Appliance aktiviert. - Die Chiffre "TLS_AES_256_GCM_SHA384" wird der Liste der Standardchiffren hinzugefügt.	- Cisco AsyncOS 12.0 umfasst die Web Security Appliance mit High Performance (HP) für die Plattformen S680, S690 und S695. - Ein neuer Unterbefehl **high performance** wird unter dem Befehl main **advanced proxyconfig** hinzugefügt, um den High Performance-Modus zu aktivieren und zu deaktivieren. - Integration der SWA in das Cisco Threat Response (CTR)-Portal - Die Appliance unterstützt die TLSv1.3-Version. - Die Sicherungsfunktion der Konfigurationsdatei wird unter "**Systemverwaltung**" aus dem Untermenü "**Protokoll-Subscriptions**" in "**Konfigurationsdatei"** verschoben. - Die Appliance unterstützt jetzt den Upload des **ECDSA**-Zertifikats für den **HTTPS**-Proxy. - Ein neuer Diagnose-**CLI proxyscannermap**-Unterbefehl wird unter **Diagnose** > **Proxy** hinzugefügt. Tto zeigt die **PID**-Zuordnung zwischen den einzelnen Proxys und dem entsprechenden Scannerprozess an. - Neue **Suchdetails für** Optionen werden unter dem **CLI**-Befehl **authcache**

			hinzugefügt. - Der neue Unterbefehl **CTROBSERVABLE** wird unter dem **CLI-**Befehl **reportingconfig** hinzugefügt, um die **CTR-**basierte Indizierung zu aktivieren oder zu deaktivieren.
12.0.1-334	GD		- Ein neuer Unterbefehlsscanner wird unter dem Befehl main **advanced proxyconfig** hinzugefügt, um die von der **AMP-**Engine zu scannenden MIME-Typen auszuschließen.
12.0.2-004	MD	- Verwenden Sie TLS 1.2 oder höher, um die Appliance mit dem AMP-Dateireputations-Server zu verbinden. - AMERICAS (Legacy) cloud-sa.amp.sourcefire.com kann nicht auf der Appliance konfiguriert werden.	- Eine neue Option "Geben Sie die Anzahl der gleichzeitigen Scans ein, die von AMP unterstützt werden sollen" wird im Haupt-**CLI-**Befehl **advanced proxyconfig** > **scanners** > **AMP** hinzugefügt. Sie können das Standard-Verdict "Unscannable" der Entfernung von lang laufenden Scans in "Timeout" und umgekehrt ändern, indem Sie im Haupt-**CLI-**Befehl "**advanced proxyconfig** > **scanners"** die **Entfernung** von neuen CLI-Unterbefehlen ändern.
12.02-012	MD		- Warnmeldungen werden auf der Web-Benutzeroberfläche der Appliance ausgelöst. Wenn der Proxy-**Malloc-Speicher** 90 % des Proxy-Malloc-Speichers überschreitet und eine E-Mail-Benachrichtigung an alle Alert-Empfänger gesendet wird, die für den Empfang wichtiger Web Proxy-Warnungen konfiguriert sind. - Die neue Web-Oberfläche bietet ein neues Aussehen für **Monitoring-**Berichte und **Tracking-**Web-Services.
12.0.3-005	MD		
12.0.3-007	MD		- Aktualisierungsbenachrichtigung für neue **URL**-Kategorien
12.0.4-002	MD		

12.0.5-011	MD	- TLSv1.2 ist standardmäßig für die Web-Benutzeroberfläche der Appliance-Verwaltung aktiviert. - **Die Sitzungswiederaufnahme** ist standardmäßig deaktiviert.	- Es wird eine Nachricht hinzugefügt, die das Ende der Unterstützung für CDA im CDA-Konfigurationsabschnitt anzeigt.
12.5.1-011	Niederländisch	- Standardmäßig ist die Cisco Success Network-Funktion auf der Appliance aktiviert. - Diese Protokolle werden geändert, um weitere Details zu enthalten: Die Zugriffsprotokolle zeigen jetzt den Benutzernamen an, wenn die Authentifizierung fehlschlägt. Die Authentifizierungs-Framework-Protokolle zeigen jetzt die Client-IP-Adresse für die folgenden fehlgeschlagenen Authentifizierungsprotokolle an: NTLM, BASIC, SSO (Transparent)	- Cisco AsyncOS 12.5 umfasst die Web Security Appliance mit High Performance (HP) für die Plattformen S680, S690 und S695. Dies erhöht die Datenverkehrsleistung der aktuellen High-End-Appliances. - Sie können jetzt ein Upgrade auf die Version 12.5 durchführen und den Hochleistungsmodus für die Modelle (S680, S690, S695, S680F, S690F und S695F) nutzen, selbst wenn Sie die folgenden Funktionen auf Ihrem Gerät aktiviert haben: • Anzapfen des Webverkehrs • Volumen- und Zeitkontingente • Allgemeine Bandbreitenlimits - Sie können jetzt Webproxy-IP-Spoofing konfigurieren, indem Sie ein IP-Spoofing-Profil erstellen und es den Routing-Richtlinien hinzufügen. - Sie können jetzt eine benutzerdefinierte URL-Kategorie für YouTube erstellen und Richtlinien für die sichere Zugriffskontrolle in der benutzerdefinierten YouTube-Kategorie festlegen. - In der neuen Webschnittstelle hat die Appliance eine neue Seite (Überwachung > Systemstatus), um den aktuellen Status und die Konfiguration der Appliance anzuzeigen. - Die CSN-Funktion (Cisco Success Network) ermöglicht Cisco die Erfassung von Telemetriedaten zur Funktionsnutzung der Appliance. - REST-API für Netzwerk, Protokoll-Subscription und andere Konfigurationen.
12.5.1-035	GD	- Herabsetzung von TLS 1.0/1.1: Verwenden Sie TLS 1.2 oder höher, um die Appliance mit	- Die Konfiguration der Cachegröße für die Authentifizierung (Netzwerk > Authentifizierung > Authentifizierungseinstellungen > Cache-

		dem AMP-Dateireputations-Server zu verbinden. AMERICAS (Legacy) **cloud-sa.amp.sourcefire.com** wird aus der Liste der AMP-Dateireputations-Server entfernt, sodass AMERICAS (Legacy) **cloud-sa.amp.sourcefire.com** auf der Appliance nicht konfiguriert werden kann.	Optionen für Anmeldeinformationen) wird von AsyncOS 12.5.1-035 und höheren Versionen nicht unterstützt.
12.5.1-043	GD		- Die Warnmeldungen werden auf der Web-Benutzeroberfläche der Appliance angezeigt (Systemverwaltung > Warnmeldungen > Häufigste Warnmeldungen anzeigen): • Wenn der Proxy-Malloc-Speicher 90 % des Proxy-Malloc-Speicherlimits überschreitet. • wenn der Proxy auf 100 % des Mallock-Speichers neu gestartet wird. In beiden Fällen wird eine E-Mail-Benachrichtigung an alle Alert-Empfänger gesendet, die so konfiguriert sind, dass sie kritische Web Proxy-Warnungen empfangen.
12.5.2-007	MD		- Eine neue Benachrichtigung zur Aktualisierung der URL-Kategorien wird in das Banner eingefügt. Eine E-Mail-Benachrichtigung über bevorstehende Updates der URL-Kategorie wird ebenfalls an die Benutzer gesendet.
12.5.2-011	MD		
12.5.3-002	MD		
12.5.4-005	MD	- Ab Version Cisco AsyncOS 12.5.4 ist TLSv1.2 standardmäßig für die Web-Benutzeroberfläche der Appliance-Verwaltung aktiviert. - Nach einem Upgrade auf Cisco AsyncOS 12.5.4 ist die Sitzungswiederaufnahme	

		standardmäßig deaktiviert. - Die Meldung wird hinzugefügt, um das Ende der Unterstützung für CDA im CDA-Konfigurationsabschnitt anzugeben.	
12.5.4-011	MD-Aktualisierung		
12.5.5-004	MD		- Nach einem Upgrade auf Cisco AsyncOS 12.5 erhalten Sie eine Aufforderung, den Proxy-Prozess neu zu starten, wenn Sie den Befehl **zur Netzwerkoptimierung** zum ersten Mal ausführen.
12.5.5-008	MD-Aktualisierung		
12.5.6-008	MD		
14.0.1-014	Niederländisch	- Standardmäßig ist die HTTP 2.0-Funktion deaktiviert. Verwenden Sie den Befehl <HTTP2>, um diese Funktion zu aktivieren. - AsyncOS 14.0 für Cisco Web Security Appliance unterstützt die TLSv1.3-Sitzungswiederaufnahme auf Client und Server. - Die Gültigkeitsdauer dieser Bescheinigungen wird wie folgt geändert: • HTTPS • ISE • SAAS • Appliance-Zertifikate • Demo-/Verwaltungszertifikat - Die CLI und die GUI der Appliance zeigen jetzt eine Meldung an, wenn ein Upgrade aufgrund eines ungültigen	- Die Cisco Web Security Appliance unterstützt jetzt die Integration mit Cisco SecureX. - Sie können benutzerdefinierte Header-Profile für HTTP-Anforderungen konfigurieren und mehrere Header unter einem Header-Umschreibprofil erstellen. - Sie können jetzt das Header Based Authentication-Schema für ein Active Directory konfigurieren. Der Client und die Websicherheits-Appliance betrachten den Benutzer als authentifiziert und fragen nicht erneut nach Authentifizierung oder Benutzeranmeldeinformationen. Die X-Authenticated-Funktion funktioniert, wenn die Web Security Appliance als Upstream-Gerät agiert. - Das Systemstatus-Dashboard der Appliance wurde verbessert: • Registerkarte "Kapazität": Eine Registerkarte, die Details zu

		Protokollnamens und Dateinamens in den Protokollabonnements fehlschlägt. - Standardmäßig ist das Abfrageintervall auf 24 Stunden festgelegt. - Nach dem Upgrade auf diese Version können Sie den Start-Test für die LDAP-Authentifizierung nicht durchführen, wenn das Feld Basis-DN (Basis-Distinguished Name) (Netzwerk > Authentifizierung > Bereich hinzufügen) leer ist.	Zeitbereich, System-CPU- und Speicherauslastung, Bandbreite und RPS, CPU-Auslastung nach Funktion und Client- oder Server-Verbindungen enthält. • Die Eigenschaften des Proxy-Datenverkehrs auf der Registerkarte Status enthalten Details zu Client- und Serververbindungen. • Die Service-Reaktionszeit umfasst jetzt weitere Details in Balkendiagrammen sowie Legendendaten für frühere Datumsangaben. - Sie können nun Konfigurationsinformationen abrufen und Änderungen (z. B. das Ändern aktueller Informationen, das Hinzufügen neuer Informationen oder das Löschen eines Eintrags) in den Konfigurationsdaten der Appliance vornehmen. Verwenden Sie REST-APIs für Verwaltungsrichtlinien, Zugriffsrichtlinien und Umgehungsrichtlinien. - Cisco AsyncOS 14.0 unterstützt HTTP 2.0 für Webanfragen und -antworten über TLS. Für die Unterstützung von HTTP 2.0 ist eine TLS-ALPN-basierte Aushandlung erforderlich, die erst ab der Version TLS 1.2 verfügbar ist. In dieser Version wird HTTPS 2.0 für folgende Funktionen nicht unterstützt: • Anzapfen des Webverkehrs • Externer DLP • Gesamtbandbreite und Anwendungsbandbreite - Ein neuer CLI-Befehl <HTTP2> wird eingeführt, um HTTP 2.0-Konfigurationen zu aktivieren oder zu deaktivieren. Sie können HTTP 2.0 nicht aktivieren oder deaktivieren und die Domäne für HTTP 2.0 nicht über die Web-Benutzeroberfläche der Appliance einschränken. - Die Konfiguration von HTTP 2.0 wird von Cisco Secure Email und Web Manage nicht unterstützt.

			- Die CLI zeigt die neue Warnmeldung an, wenn Sie versuchen, das Standardzertifikat einer der folgenden Funktionen zu verwenden: • Appliance-Zertifikat (Navigieren Sie in der Web-Benutzeroberfläche zu Netzwerk > Zertifikatsverwaltung > Appliance-Zertifikat) • Zertifikat für die Verschlüsselung der Anmeldeinformationen (Navigieren Sie auf der Webbenutzeroberfläche zu Netzwerk > Authentifizierung > Einstellungen bearbeiten > Erweitert) • HTTPS-Management-UI-Zertifikat (Verwenden Sie in der Befehlszeilenschnittstelle certconfig > SETUP) - Der neue Unterbefehl OCSPVALIDATION_FOR_SERVER_CERT wird unter **certconfig** hinzugefügt. Mit diesem neuen Unterbefehl können Sie die OCSP-Validierung für LDAP- und Updater-Serverzertifikate aktivieren. Wenn die Zertifikatsvalidierung aktiviert ist, können Sie eine Warnung erhalten, wenn die an der Kommunikation beteiligten Zertifikate widerrufen werden. - Der neue CLI-Befehl **gacererdconfig** wird hinzugefügt, um die Polling-Funktion zwischen der Appliance und dem Authentifizierungsserver zu konfigurieren. - Sie können jetzt zwischen Management und Datenschnittstelle wählen, während Sie die Smart-Lizenzfunktion auf der Appliance konfigurieren.
14.0.1-040	Niederländisch	- Wenn Sie die Lizenzierung intelligenter Software aktivieren und Ihre Web Security Appliance beim Cisco Smart Software Manager registrieren, den Cisco Cloud Services (Netzwerk > Cloud-Serviceeinstellungen) aktiviert und registriert Ihre sichere Web-Appliance automatisch über das Cisco Cloud Services-Portal.	- Sie können die Details des Smart Accounts, der im Cisco Smart Software Manager-Portal erstellt wurde, über den Befehl **smartaccountinfo** in der CLI anzeigen. - Wenn das Cisco Cloud Services-Zertifikat abgelaufen ist oder bald abläuft, erneuert der Cisco Cloud Service das Zertifikat nach dem Upgrade auf AsyncOS 14.0.1-040 automatisch. - Wenn das Cisco Cloud Services-Zertifikat abgelaufen ist, können Sie jetzt ein neues

		- Sie können den Cisco Cloud Service nicht deaktivieren oder die Registrierung aufheben, wenn Smart Licensing auf Ihrer Appliance registriert ist. - Wenn Sie Ihre Appliances bereits beim Cisco Smart Software Manager registriert und Cisco Cloud Services nicht konfiguriert haben, werden Cisco Cloud Services nach dem Upgrade auf AsyncOS 14.0.1-040 automatisch aktiviert. Standardmäßig ist die Region als Nord- und Südamerika registriert, und Sie können die Region (Europa und APJC) nach Bedarf ändern. - Sie können den Cisco Cloud-Service nicht deaktivieren oder die Registrierung aufheben, wenn die Smart-Lizenz auf Ihrer Appliance registriert ist.	Zertifikat vom Cisco Talos Intelligence Services-Portal aus dem Unterbefehl **cloudserviceconfig** > **fetchcertificate** in der CLI herunterladen. - Sie können die Web Security Appliance automatisch im Cisco Cloud Service-Portal registrieren (Unterbefehl **cloudserviceconfig** > **autoregister** in der CLI) - Sie können das Zertifikat für die virtuelle Appliance und die Hardware-Appliances über den Unterbefehl **updateconfig** > **clientcertificate** in die CLI laden. - Eine neue Benachrichtigung zur Aktualisierung der URL-Kategorien wird in das Banner eingefügt. Außerdem erhalten die Benutzer eine E-Mail-Benachrichtigung über bevorstehende Updates der URL-Kategorie.
14.0.1-053	GD		
14.0.1-503	HP		
14.0.2-012	MD	- In Cisco AsyncOS 14.0.2 ist TLSv1.2 unter Systemadministrator > SSL-Konfiguration standardmäßig für die Webbenutzeroberfläche der Appliance-Verwaltung aktiviert. - Die Sitzungswiederaufnahme ist standardmäßig deaktiviert.	- Es wird eine Nachricht hinzugefügt, die das Ende der Unterstützung für CDA im CDA-Konfigurationsabschnitt anzeigt. - Sie können jetzt in der Dropdown-Liste "Test Interface" (Testschnittstelle) zwischen der Daten- oder der Verwaltungsschnittstelle für die Smart License-Registrierung wählen.
14.0.3-014	MD	- Nach einem Upgrade auf Cisco AsyncOS 14.0 erhalten Sie eine Aufforderung, den Proxy-Prozess neu zu starten, wenn Sie zum ersten Mal den Befehl **zur Netzwerkoptimierung** ausführen.	
14.0.3-502	HP	- Wenn die sichere Web-	

		Appliance im Hochleistungsmodus betrieben wird, deaktiviert die Erschöpfung der Heapbegrenzung die hohe Latenz und akzeptiert Handler. Dies führt zu einer geringeren Anzahl von Verbindungen.	
14.0.4-005	MD		
14.5.0-498	Niederländisch	- Produkt-Rebranding: • AMP für Endgeräte, Advanced Malware Protection und AMP wurden geändert in **Sichere Endgeräte** • Thread Grid (Dateianalyse) geändert zu **Malwareanalysen** - Die Anforderung für eine falsche Klassifizierung wird über HTTPS gesendet, sodass Sie keine Sicherheitswarnungen erhalten. - Die Samba-Version wurde auf Version 4.11.15 aktualisiert. - TLSv1.2 ist standardmäßig für die Web-Benutzeroberfläche der Appliance-Verwaltung unter Systemadministrator > SSL-Konfiguration aktiviert. - Bei einer Neuinstallation von AsyncOS 14.5 wird der Wert für die Zertifikatskonfigurationen für abgelaufene und nicht übereinstimmende Hostnamen auf der Seite "HTTPS-Proxy" standardmäßig anstelle von "**Monitor"** als "**Drop"** ausgewählt.	- Die sichere Web-Appliance kann jetzt überprüfen, ob die vom DNS-Server empfangene DNS-Antwort kryptografische Signaturen unterstützt. - Die sichere Web-Appliance beschränkt die Anzahl der gleichzeitigen Verbindungen, die vom Client initiiert wurden, auf einen konfigurierten Wert. - Mit AsyncOS Version 14.5 wurde die Cisco Web Security Appliance unter dem Namen Cisco Secure Web Appliance - Der Zugriffsprotokoll-Entscheidungstag in der Gruppe "Entschlüsselungsrichtlinie" wird mit EUN (Endbenutzer-Benachrichtigung) angehängt, wenn die EUN-Seite im Webbrowser des Clients angezeigt wird. - Mit der Funktion zum Klonen von Richtlinien können Sie die Konfigurationen einer Richtlinie kopieren oder klonen und eine neue Richtlinie erstellen. - Sie können die Datenverkehrsbandbreite verwalten, indem Sie den Bandbreitenwert im Kontingentprofil konfigurieren und das Kontingentprofil in der URL-Kategorie der Zugriffsrichtlinie oder dem Gesamtkontingent für Webaktivität zuordnen. - REST-API zur Konfiguration von Managementrichtlinien, Entschlüsselungsrichtlinien, Routing-Richtlinien, IP-Spoofing-Richtlinien, Anti-Malware und Reputation, Authentifizierungsbereichen, Cisco Smart Software-Lizenz, Cisco Umbrella Seamless ID, Identitätsdiensten und System-Setup. - Sie können die ISE-SXP-Bereitstellung für

			die passive Authentifizierung in die Cisco Secure Web Appliance integrieren. Auf diese Weise können Sie alle definierten Zuordnungen abrufen, einschließlich der SGT-IP-Adresszuordnungen, die über SXP veröffentlicht werden. - Mit der Funktion für nahtlose Cisco Umbrella-ID kann die Appliance die Benutzeridentifizierungsinformationen nach erfolgreicher Authentifizierung an das Cisco Umbrella Secure Web Gateway (SWG) weitergeben. - Es wird eine Nachricht hinzugefügt, die das Ende der Unterstützung für CDA im CDA-Konfigurationsabschnitt anzeigt. - Sie können jetzt in der Dropdown-Liste "Test Interface" (Testschnittstelle) zwischen der Daten- oder der Verwaltungsschnittstelle für die Smart License-Registrierung wählen. - Nach einem Upgrade auf Cisco AsyncOS 14.5 erhalten Sie eine Aufforderung, den Proxy-Prozess neu zu starten, wenn Sie zum ersten Mal den Befehl **zur Netzwerkoptimierung** ausführen.
14.5.0-537	GD		- Diese Richtlinien mit Klonoption in Secure Web Appliance können auch von Cisco Secure Email und Web Manager (SMA) verwaltet werden: • Zugriffsrichtlinie • Identifizierungsprofil • Entschlüsselungsrichtlinie • Routingrichtlinie
14.5.1-008	MD		
14.5.1-016	MD		
14.6.0-108	Niederländisch		- AsyncOS 14.6 unterstützt Cisco Umbrella mit Cisco Secure Web Appliance (SWA). Die Integration von Umbrella und Secure Web Appliance vereinfacht die Bereitstellung gemeinsamer Webrichtlinien von Umbrella bis hin zu Secure Web Appliance.

15.0.0-322	Niederländisch	- Die FreeBSD-Version wurde auf FreeBSD 13.0 aktualisiert. - Cisco SSL-Version 1.0.2 in Cisco SSL-Version 1.1.1 - Talos-Engines wie AVC, WBRSD, DCA und Beaker wurden aktualisiert. - Scanner-Engines wie Webroot und McAfee wurden aktualisiert.	- Folgende Verbesserungen wurden an der Smart Software-Lizenzierungsfunktion vorgenommen: • Lizenzreservierung • Device Led Conversion: Nach der Registrierung der Secure Web Appliance mit Smart License werden alle aktuellen gültigen klassischen Lizenzen automatisch mithilfe des DLC-Prozesses (Device Led Conversion) in Smart-Lizenzen umgewandelt. Diese umgewandelten Lizenzen werden im Virtual Account des CSSM-Portals aktualisiert. - Sie können die Datenverkehrsbandbreite verwalten, indem Sie den Bandbreitenwert im Kontingentprofil konfigurieren und das Kontingentprofil in der Entschlüsselungsrichtlinie und Zugriffsrichtlinie, der URL-Kategorie oder dem Gesamtkontingent für Web-Aktivitäten zuordnen. - Mit der Funktion zum Klonen von Richtlinien können Sie die Konfigurationen einer Richtlinie kopieren oder klonen und eine neue Richtlinie erstellen. - Application Discovery and Control (ADC)-Engine: Eine Komponente für akzeptable Nutzungsrichtlinien, die den Web-Datenverkehr überprüft, um ein besseres Verständnis und eine bessere Kontrolle des für Anwendungen verwendeten Web-Datenverkehrs zu erhalten. Mit AsyncOS 15.0 können Sie entweder die AVC- oder die ADC-Engine zur Überwachung des Web-Datenverkehrs verwenden. AVC ist standardmäßig aktiviert. Die ADC-Engine unterstützt den Hochleistungsmodus. - REST-API für ADC-Konfiguration - Admin kann einen anderen benutzerdefinierten SNMPv3-Benutzernamen als den Standardbenutzernamen v3get konfigurieren.

			- Die maximale Länge des benutzerdefinierten Headers beträgt 16k. - Option zur Auswahl der sicheren Tunnelschnittstelle und der Remote-Zugriffsverbindung
15.0.0-335	GD	- Device Led Conversion: Nach der Registrierung der Secure Web Appliance mit Smart Licensing werden alle aktuellen gültigen klassischen Lizenzen automatisch mithilfe des DLC-Prozesses (Device Led Conversion) in Smart Lizenzen umgewandelt. Diese umgewandelten Lizenzen werden im Virtual Account des CSSM-Portals aktualisiert. - AVC ist standardmäßig aktiviert. - Cisco SSL Version 1.0.2 zu Cisco SSL Version 1.1.1 - Talos-Engines wie AVC, WBRSD, DCA und Beaker wurden aktualisiert. - Scanner-Engines wie Webroot und McAfee wurden aktualisiert. - FreeBSD 13.0 ist nur mit Cisco SSL Version 1.1.1 kompatibel. Nur SSH-kompatible Verschlüsselungs-, MAC- und Kex-Algorithmen von Cisco können für SSH-Verbindungen mit FreeBSD 13.0 unterstützt werden. - Die DCA-Funktion in der sicheren Web-Appliance ist als Teil von AsyncOS15.0 GD deaktiviert.Sie können sie nach dem Upgrade auf diese Version aktivieren, indem Sie zu Sicherheitsdienste> Kontrollen für akzeptable Nutzung navigieren und das Kontrollkästchen **DCA** aktivieren.	- Lizenzreservierung - Sie können Lizenzen für die in Secure Web Appliance aktivierten Funktionen reservieren, ohne eine Verbindung zum Cisco Smart Software Manager (CSSM)-Portal herzustellen. Dies ist vor allem für Benutzer von Vorteil, die Secure Web Appliance in einer hochgradig sicheren Netzwerkumgebung ohne Kommunikation mit dem Internet oder externen Geräten bereitstellen. - Sie können die Datenverkehrsbandbreite verwalten, indem Sie den Bandbreitenwert im Kontingentprofil konfigurieren und das Kontingentprofil in der Entschlüsselungsrichtlinie und der URL-Kategorie der Zugriffsrichtlinie oder dem Gesamtkontingent für Webaktivität zuordnen. - Mit der Funktion zum Klonen von Richtlinien können Sie die Konfigurationen einer Richtlinie kopieren oder klonen und eine neue Richtlinie erstellen. - Unterstützt die ADC-Engine (Application Discovery and Control), eine Komponente für Richtlinien zur akzeptablen Nutzung, die den Web-Datenverkehr überprüft, um ein besseres Verständnis und eine bessere Kontrolle des für Anwendungen verwendeten Web-Datenverkehrs zu erhalten. können Sie jetzt entweder die AVC- oder die ADC-Engine zur Überwachung des Web-Datenverkehrs verwenden. - Die ADC-Engine unterstützt den Hochleistungsmodus. - Sie können nun Konfigurationsinformationen abrufen und Änderungen (z. B. aktuelle Informationen ändern, neue Informationen hinzufügen oder einen Eintrag löschen) an den Konfigurationsdaten der Zugriffsrichtlinie der Appliance mit REST-APIs vornehmen.

		- Die SNMPWALK-/SNMPGET-Vorgänge für SNMP-OIDs für Proxy-Mallock-Speicher werden von den Multi-Prox-SWAs (S690, S695, S1000V) nicht unterstützt.	-Admin kann einen anderen benutzerdefinierten SNMPv3-Benutzernamen als den Standardbenutzernamen **v3get** konfigurieren. - Die maximale Länge der benutzerdefinierten Header für Webanfragen beträgt 16.000. - Option zur Auswahl einer sicheren Tunnelschnittstelle und Remote-Zugriffsverbindung

Open Source-Komponenten

Nachfolgend finden Sie eine Liste der Änderungen an Open Source-Komponenten, die in SWA verwendet werden:

Version	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

Zugehörige Informationen

- Versionshinweise für AsyncOS 12.0 für Cisco Web Security Appliances - Cisco
- Versionshinweise für AsyncOS 12.5 für Cisco Web Security Appliances - Cisco
- Versionshinweise für AsyncOS 14.0 für Cisco Web Security Appliances - Cisco
- Versionshinweise für AsyncOS 14.5 für Cisco Secure Web Appliance - Cisco
- Wie lautet die Versionsterminologie für Content-Sicherheit? (cisco.com)
- Installationsleitfaden für die Cisco Secure Email und Web Virtual Appliance
- **Technischer Support und Dokumentation für Cisco Systeme**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.