Configurazione di Secure Web Appliance per consentire l'accesso guest

Sommario

Introduzione

In questo documento viene descritto come consentire agli utenti che non hanno installato il certificato di decrittografia di accedere a Internet tramite Secure Web Appliance (SWA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- SWA fisico o virtuale installato.
- Licenza attivata o installata.
- Installazione guidata completata.
- Accesso amministrativo all'interfaccia grafica (GUI) SWA.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica dello scenario

Questo articolo descrive uno scenario di controllo dell'accesso alla rete all'interno della subnet Wi-Fi 10.10.10.0/24. L'ambiente è costituito da due gruppi di utenti distinti che richiedono regole di protezione e di accesso diverse:

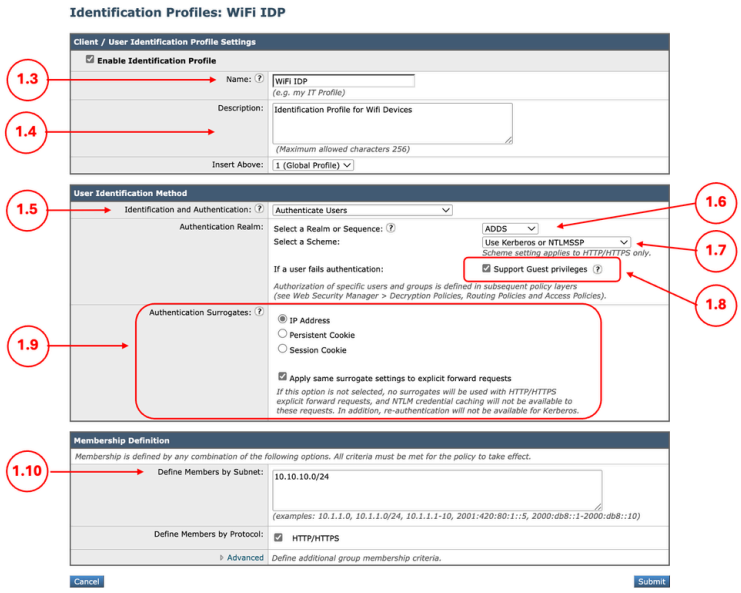
- Dispositivi gestiti: Notebook aziendali completamente autenticati e con il certificato di decrittografia SWA installato. Questi dispositivi sono affidabili e sono in genere soggetti alle policy di accesso aziendali standard.
- Dispositivi non gestiti/guest: Notebook personali e dispositivi mobili non autenticati e privi del certificato di decrittografia SWA.

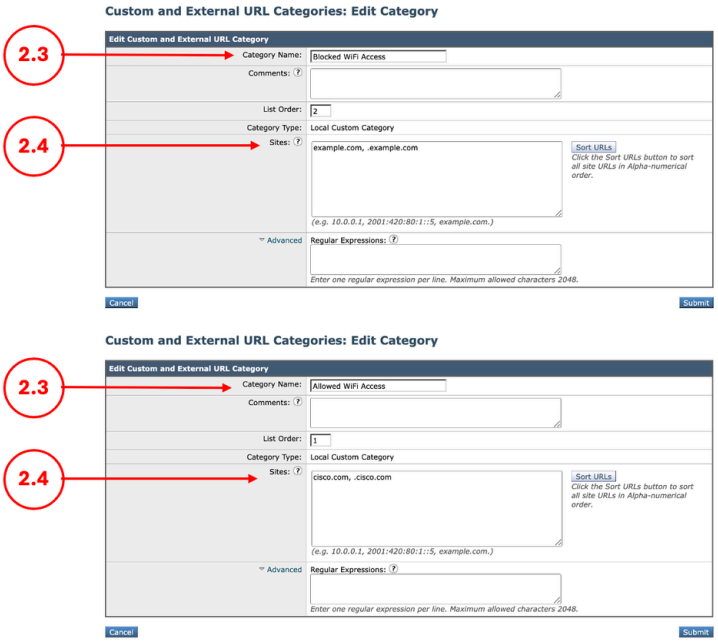
Obiettivo:
L'obiettivo dell'azienda è implementare policy di accesso al Web restrittive per i dispositivi non gestiti, limitando la connettività a un sottoinsieme specifico di URL consentiti e garantendo al contempo la sicurezza delle risorse aziendali.

Nota: Poiché il certificato di decrittografia non è considerato attendibile sui dispositivi non gestiti, non è possibile decrittografare il traffico HTTPS e l'azione deve essere impostata in modo da consentirne la trasmissione.

Procedura di configurazione

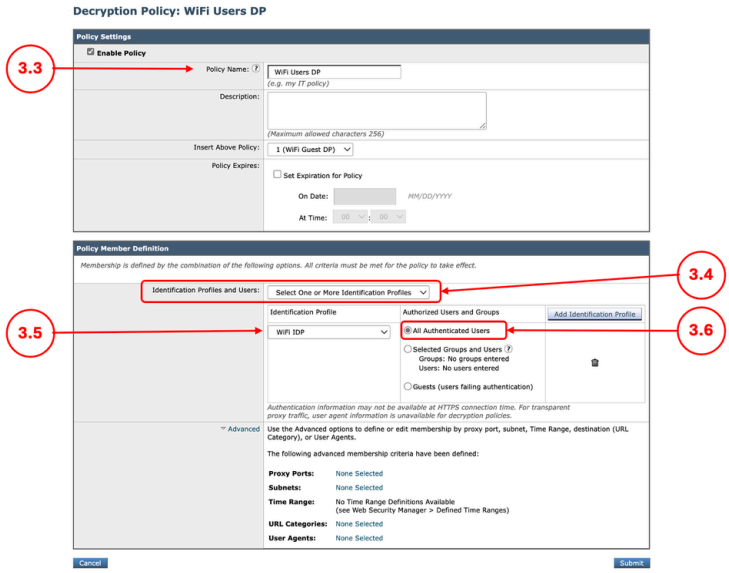
Passaggio 1. Creare il profilo di identificazione.	Passaggio 1.1. Dalla GUI SWA, passare a Web Security Manager e selezionare Identification Profile (Profilo di identificazione). Passaggio 1.2. Fare clic su Aggiungi profilo di identificazione. Passaggio 1.3. Definire un nome per il profilo. Passaggio 1.4. (Facoltativo) Definire la descrizione. Passaggio 1.5. Scegliere Autentica utenti in Identificazione e autenticazione. Passaggio 1.6. Scegliere il realm di Active Directory da Selezionare un realm o una sequenza.

	Passaggio 1.7. Da Selezionare uno schema, selezionare i protocolli di autenticazione desiderati. Suggerimento: Non scegliere Autenticazione di base nell'elenco Selezionare uno schema. Passaggio 1.8. Selezionare la casella di controllo Privilegi Guest di supporto. Passaggio 1.9. (Facoltativo) A seconda del progetto, è possibile abilitare il surrogato abilitando Applica le stesse impostazioni del surrogato alle richieste di inoltro esplicite. Attenzione: Poiché non è possibile decrittografare il traffico, nella distribuzione trasparente non selezionare Cookie persistente o Cookie di sessione. Passaggio 1.10. Definire la subnet di indirizzi IP in, Definire i membri in base alla subnet. Passaggio 1.11. Sottomettere e confermare le modifiche.  Immagine - Definizione del profilo di identificazione
Passaggio 2. (Facoltativo) Creazione di categorie di URL personalizzati per gli URL consentiti	Passaggio 2.1.Dalla GUI, passare a Web Security Manager e sceglierеCategorie URL personalizzate ed esterne.

e bloccati	Passaggio 2.2.Fare clic su Aggiungi categoria per creare una nuova categoria di URL personalizzati. Passaggio 2.3.Inserire il nome della nuova categoria. Passaggio 2.4.Definire il dominio e/o i sottodomini dei siti Web a cui si desidera bloccare l'accesso. Passaggio 2.5.Inviare le modifiche. Passaggio 2.6. Per creare una categoria URL per il sito Web a cui si desidera consentire l'accesso, attenersi alla stessa procedura.  Immagine - Definisci categoria URL personalizzata
Passaggio 3. Creazione dei criteri di decrittografia per i dispositivi gestiti	Passaggio 3.1. Dalla GUI, passare a Web Security Manager e selezionare Decryption Policies (Criteri di decrittografia) Passaggio 3.2. Fare clic su Aggiungi criterio. Passaggio 3.3.EnterName per il nuovo criterio. Passaggio 3.4. Scegliere Seleziona uno o più profili di identificazione dal menu a discesa Profili di identificazione e utenti. Passaggio 3.5.Selezionare il profilo di identificazione creato nel passaggio 1.

Passaggio 3.6. Selezionare Tutti gli utenti autenticati.

Passaggio 3.7.Fare clic su Sottometti.



Crea criterio di decrittografia per dispositivi gestiti

Passaggio 3.8. Nella pagina Criteri di decrittografia, fare clic sul collegamento dal filtro URL per il nuovo criterio.

Passaggio 3.9. (Facoltativo) È possibile aggiungere una categoria di URL personalizzati facendo clic su Seleziona categorie personalizzate e scegliendo Includi nei criteri davanti ai nomi delle categorie

Passaggio 3.10. Configurare l'azione per ciascun filtro personalizzato ed esterno delle categorie di URL e per ciascun filtro predefinito delle categorie di URL.

Passaggio 3.11. Fare clic su Invia

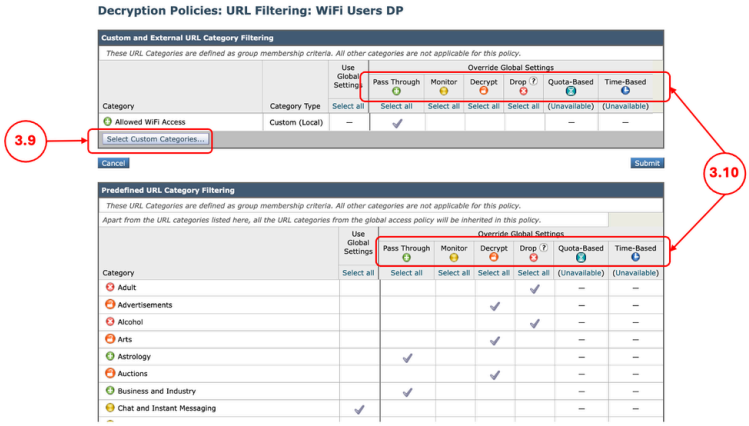
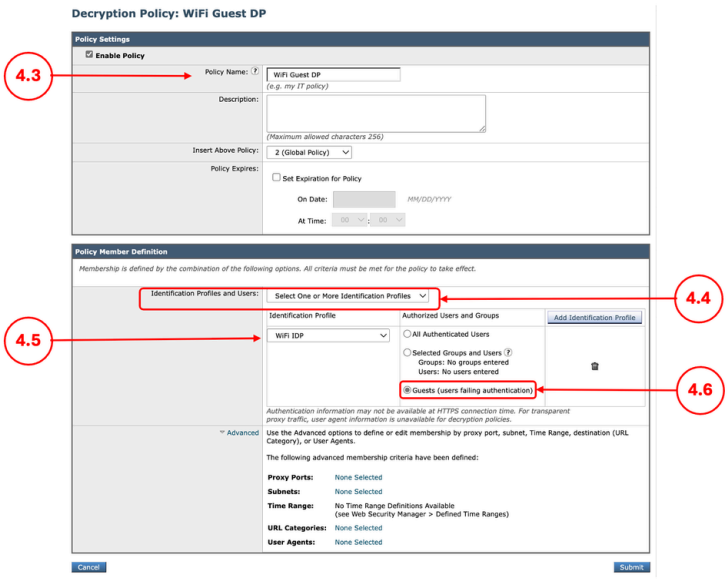
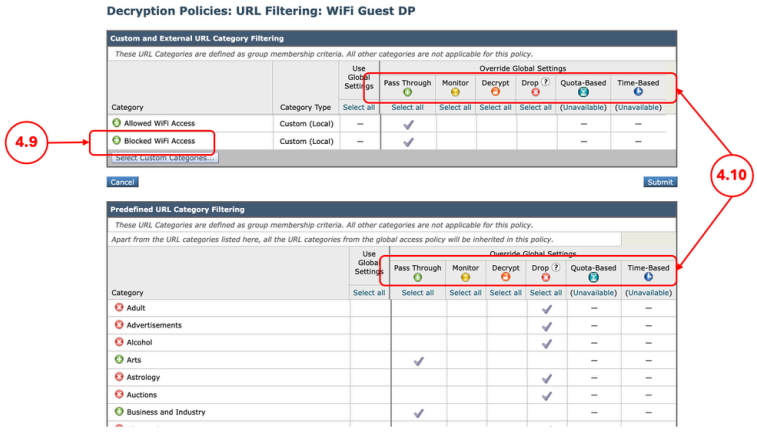


Immagine - Configura azione per criterio di decrittografia

Passaggio 4. Creazione dei criteri di decrittografia per i dispositivi non gestiti	Passaggio 4.1. Dalla GUI, passare a Web Security Manager e selezionare Decryption Policies (Criteri di decrittografia) Passaggio 4.2. Fare clic su Aggiungi criterio. Passaggio 4.3.EnterName per il nuovo criterio. Passaggio 4.4. Scegliere Seleziona uno o più profili di identificazione dal menu a discesa Profili di identificazione e utenti. Passaggio 4.5.Selezionare il profilo di identificazione creato nel passaggio 1. Passaggio 4.6. Selezionare Guests (errori di autenticazione degli utenti). Passaggio 4.7.Fare clic su Sottometti.  Crea criterio di decrittografia per dispositivi non gestiti Passaggio 4.8. Nella pagina Criteri di decrittografia, fare clic sul collegamento dal filtro URL per il nuovo criterio. Passaggio 4.9. (Facoltativo) È possibile aggiungere una categoria di URL personalizzati facendo clic su Seleziona categorie personalizzate e scegliendo Includi nei criteri davanti ai nomi delle categorie Passaggio 4.10. Configurare l'azione per ciascun filtro personalizzato ed esterno delle categorie di URL e per ciascun filtro predefinito delle categorie di URL.

	Nota: Non utilizzare Decrypt come azione, poiché il certificato di decrittografia SWA non è attendibile sui dispositivi non gestiti.  Immagine - Azione di decrittografia per dispositivi non gestiti Passaggio 4.11. Scorrere verso il basso la sezione URL non classificati e scegliere l'azione appropriata.  Immagine - URL non classificati Suggerimento: Per motivi di sicurezza, è consigliabile impostare l'azione su Elimina, nel caso in cui un URL richieda l'accesso, è possibile aggiungerlo nella Categoria URL personalizzato assegnata al criterio. Passaggio 4.12. Fare clic su Submit
Passaggio 5. Creazione dei criteri di accesso per i dispositivi gestiti	Passaggio 5.1. Dalla GUI, passare a Web Security Manager e scegliere Access Policies (Policy di accesso) Passaggio 5.2. Fare clic su Aggiungi criterio. Passaggio 5.3.EnterName per il nuovo criterio. Passaggio 5.4. Scegliere Seleziona uno o più profili di identificazione dal menu a discesa Profili di identificazione e utenti.

Passaggio 5.5.Selezionare il profilo di identificazione creato nel passaggio 1.

Passaggio 5.6. Selezionare Tutti gli utenti autenticati.

Passaggio 5.7.Fare clic su Sottometti.

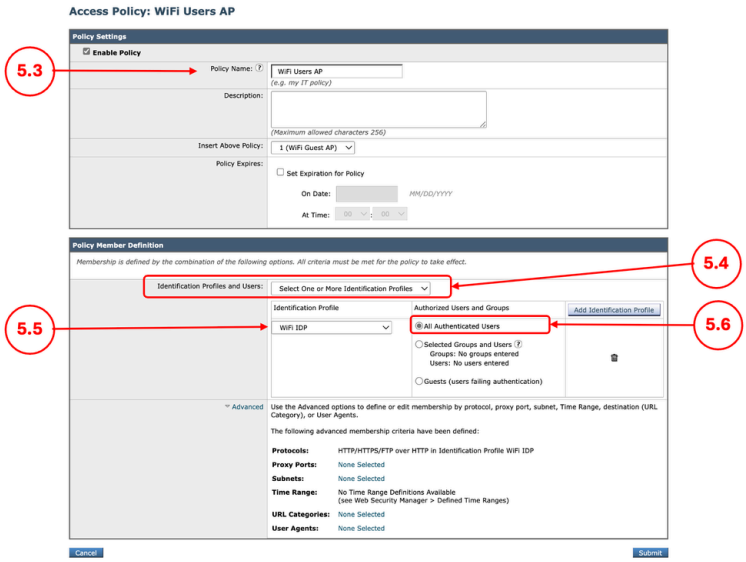


Immagine - Criteri di accesso per dispositivi gestiti

Passaggio 5.8. Nella pagina Criteri di accesso, fare clic sul collegamento dal filtro URL per il nuovo criterio.

Passaggio 5.9. (Facoltativo) È possibile aggiungere una categoria di URL personalizzati facendo clic su Seleziona categorie personalizzate e scegliendo Includi nei criteri davanti ai nomi delle categorie

Passaggio 5.10. Configurare l'azione per ciascun filtro personalizzato ed esterno delle categorie di URL e per ciascun filtro predefinito delle categorie di URL.

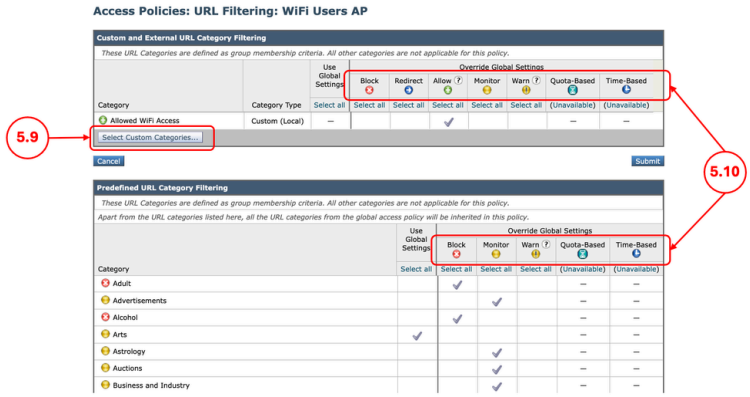
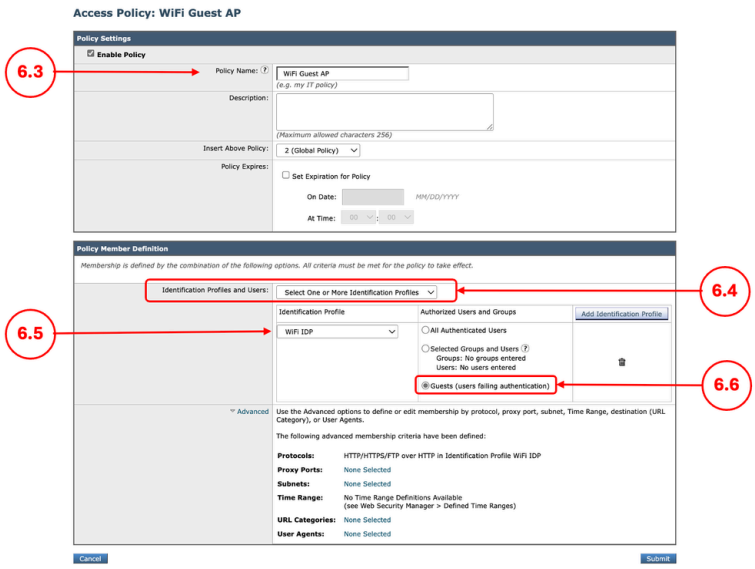
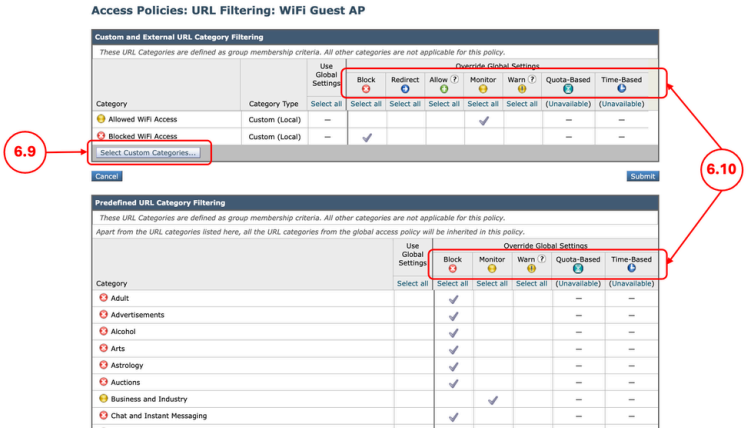
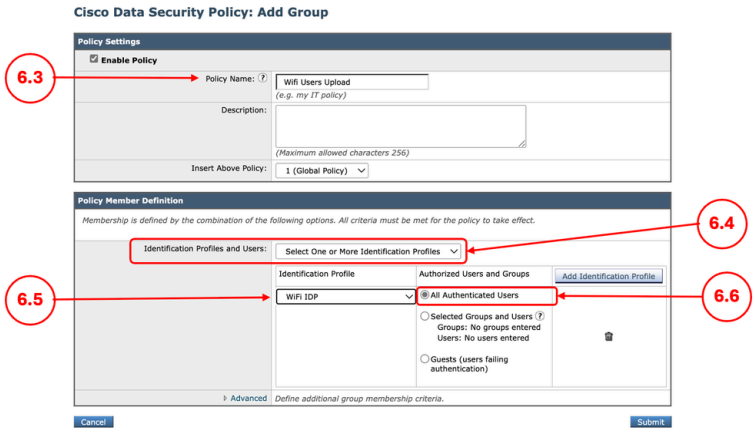
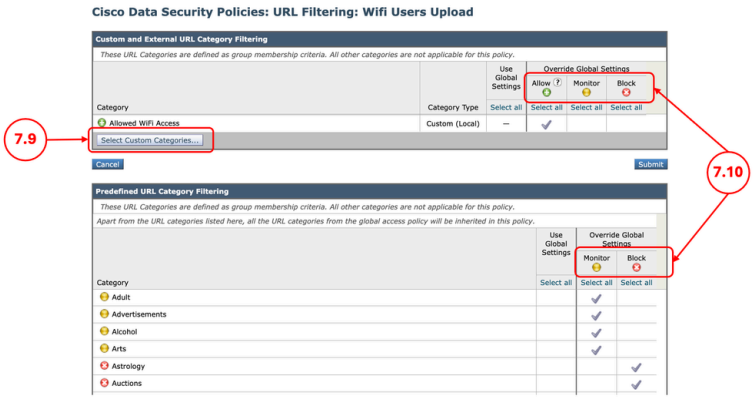


Immagine - Filtro URL criteri di accesso per dispositivi gestiti

	Passaggio 5.11. Fare clic su Submit (Invia).
Passaggio 6. Creazione dei criteri di accesso per i dispositivi non gestiti	Passaggio 6.1. Dalla GUI, passare a Web Security Manager e scegliere Access Policies (Policy di accesso) Passaggio 6.2. Fare clic su Aggiungi criterio. Passaggio 6.3.EnterName per il nuovo criterio. Passaggio 6.4. Scegliere Seleziona uno o più profili di identificazione dal menu a discesa Profili di identificazione e utenti. Passaggio 6.5.Selezionare il profilo di identificazione creato nel passaggio 1. Passaggio 6.6. Selezionare Guests (errori di autenticazione degli utenti). Passaggio 6.7.Fare clic su Sottometti.  Immagine - Criteri di accesso per dispositivi non gestiti Passaggio 6.8. Nella pagina Criteri di accesso, fare clic sul collegamento dal filtro URL per il nuovo criterio. Passaggio 6.9. (Facoltativo) È possibile aggiungere una categoria di URL personalizzati facendo clic su Seleziona categorie personalizzate e scegliendo Includi nei criteri davanti ai nomi delle categorie

	Passaggio 6.10. Configurare l'azione per ciascun filtro personalizzato ed esterno delle categorie di URL e per ciascun filtro predefinito delle categorie di URL.  Immagine - Filtro URL criteri di accesso per dispositivi non gestiti Passaggio 6.11. Scorrere verso il basso la sezione URL non classificati e scegliere l'azione appropriata.  Immagine - URL non classificati nei criteri di accesso Suggerimento: Per motivi di sicurezza, è consigliabile impostare l'azione su Blocca, nel caso in cui un URL richieda l'accesso, è possibile aggiungerlo nella Categoria URL personalizzato assegnata al criterio. Passaggio 6.12. Fare clic su Submit (Invia)
Passaggio 7. (Facoltativo) Creazione di criteri di sicurezza dei dati Cisco per dispositivi gestiti Nota: Se non si desidera filtrare il traffico di caricamento per i dispositivi gestiti, è possibile ignorare questo passaggio.	Passaggio 7.1. Dalla GUI, passare a Web Security Manager e scegliere Cisco Data Security. Passaggio 7.2. Fare clic su Aggiungi criterio. Passaggio 7.3.EnterName per il nuovo criterio. Passaggio 7.4. Scegliere Seleziona uno o più profili di identificazione dal menu a discesa Profili di identificazione e utenti. Passaggio 7.5.Selezionare il profilo di identificazione creato nel passaggio 1.

	Passaggio 7.6. Selezionare Tutti gli utenti autenticati. Passaggio 7.7.Fare clic su Sottometti.  Immagine - Criterio di sicurezza dei dati Cisco per dispositivi gestiti Passaggio 7.8. Nella pagina Criteri di sicurezza dei dati Cisco, fare clic sul collegamento dal filtro URL per il nuovo criterio. Passaggio 7.9. (Facoltativo) È possibile aggiungere una categoria di URL personalizzati facendo clic su Seleziona categorie personalizzate e scegliendo Includi nei criteri davanti ai nomi delle categorie Passaggio 7.10. Configurare l'azione per ciascun filtro personalizzato ed esterno delle categorie di URL e per il filtro predefinito delle categorie di URL.  Immagine - Azione di caricamento per dispositivi gestiti Passaggio 7.11. Fare clic su Sottometti.
Passaggio 8. (Facoltativo) Creazione di criteri di sicurezza dei	Passaggio 8.1. Dalla GUI, passare a Web Security Manager e scegliere Cisco Data Security.

dati Cisco per dispositivi non gestiti

Nota: Se non si desidera filtrare il traffico di caricamento per i dispositivi non gestiti, è possibile ignorare questo passaggio.

Passaggio 8.2. Fare clic su Aggiungi criterio.

Passaggio 8.3.EnterName per il nuovo criterio.

Passaggio 8.4. Scegliere Seleziona uno o più profili di identificazione dal menu a discesa Profili di identificazione e utenti.

Passaggio 8.5.Selezionare il profilo di identificazione creato nel passaggio 1.

Passaggio 8.6. Selezionare Tutti gli utenti autenticati.

Passaggio 8.7.Fare clic su Sottometti.

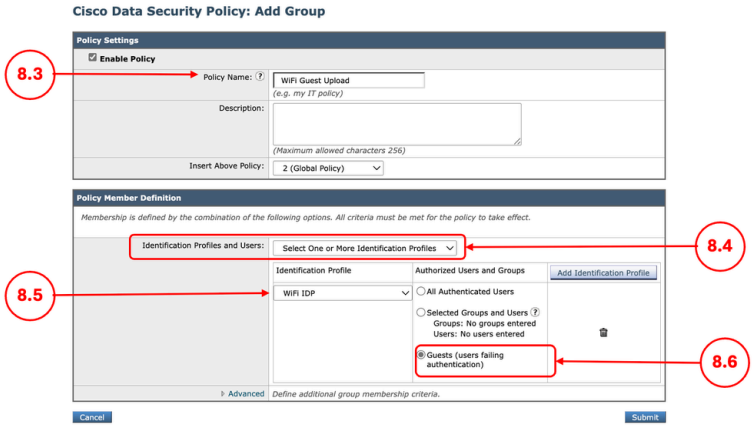
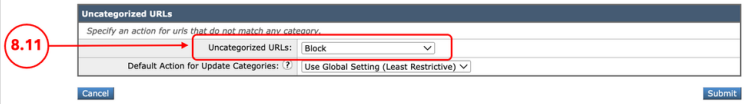


Immagine - Criterio di sicurezza dei dati Cisco per dispositivi non gestiti

Passaggio 8.8. Nella pagina Criteri di sicurezza dei dati Cisco, fare clic sul collegamento dal filtro URL per il nuovo criterio.

Passaggio 8.9. (Facoltativo) È possibile aggiungere una categoria di URL personalizzati facendo clic su Seleziona categorie personalizzate e scegliendo Includi nei criteri davanti ai nomi delle categorie

Passaggio 8.10. Configurare l'azione per ciascun filtro personalizzato ed esterno delle categorie di URL e per ciascun filtro predefinito delle categorie di URL.

	 Immagine - Azione di caricamento per dispositivi non gestiti Passaggio 8.11. Scorrere verso il basso la sezione URL non classificati e scegliere l'azione appropriata.  Immagine - Azione di caricamento per URL non classificati Suggerimento: Per motivi di sicurezza, è consigliabile impostare l'azione su Blocca, nel caso in cui un URL richieda l'accesso, è possibile aggiungerlo nella Categoria URL personalizzato assegnata al criterio. Passaggio 8.12. Fare clic su Submit (Invia)
Passaggio 9. Salvataggio delle modifiche	Passaggio 9.1. Eseguire il commit delle modifiche

Informazioni correlate

- Guida per l'utente di AsyncOS 15.0 for Cisco Secure Web Appliance - LD (installazione limitata) - Risoluzione dei problemi...
- Blocca download file eseguibile in SWA
- Blocca il traffico di caricamento in Secure Web Appliance
- Blocca il traffico in Secure Web Appliance
- Ignora autenticazione in Secure Web Appliance
- Configura restrizione tenant Microsoft O365 in SWA
- Configura installazione iniziale di Secure Web Appliance
- Ignora traffico aggiornamenti Microsoft in Secure Web Appliance

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).