Aviser les utilisateurs finaux des actions du proxy

Cette rubrique contient les sections suivantes :

Survol des notifications envoyées à l'utilisateur final

Vous pouvez configurer les types de notifications suivants pour les utilisateurs finaux :

Option	Description	Informations complémentaires
Page End-user acknowledgement (Accusé de réception de l'utilisateur final)	Informe les utilisateurs finaux que leur activité Web est filtrée et surveillée. Une page d'accusé de réception de l'utilisateur final s'affiche lorsqu'un utilisateur accède à un navigateur pour la première fois après un certain temps.	page End-User Acknowledgment (Accusé de réception à destination de l'utilisateur final), on page 3
Pages End-User Notification (Notification d'utilisateur final)	Page présentée aux utilisateurs finaux lorsque l'accès à une page particulière est bloqué, en fonction du motif du blocage.	Pages End-User Notification (Notification d'utilisateur final) , on page 7

Option	Description	Informations complémentaires
Page End-user URL filtering warning (Avertissement concernant le filtrage d'URL de l'utilisateur final)	Avertit les utilisateurs finaux qu'un site auquel ils accèdent ne respecte pas les politiques d'utilisation acceptable de votre organisation et leur permet de continuer s'ils le choisissent.	Configuration de la page d'avertissement du filtrage des URL de l'utilisateur final, on page 11
FTP notification messages (Messages de notification FTP)	Indique aux utilisateurs finaux le motif du blocage d'une transaction FTP native.	Configuration des messages de notification FTP, on page 12.
Page Time and Volume Quotas Expiry Warning (Avertissement d'expiration des quotas de volume et de temps)	Avertit les utilisateurs finaux lorsque leur accès est bloqué parce qu'ils ont atteint la limite de volume de données ou de temps configurée.	Configurez ces paramètres dans la page d'avertissement d'expiration des quotas de temps et de volume, section Security Services > End User Notification (Services de sécurité > Notification de l'utilisateur final). Voir aussi Plages de temps et quotas.

Configuration des paramètres généraux pour les pages de notification

Indiquez les langues d'affichage et le logo des pages de notification. Les restrictions sont décrites dans la présente procédure.

Étape 1 Sélectionnez **Security Services > End-User Notification** (Services de sécurité > Notification de l'utilisateur final).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Dans la section des paramètres généraux, sélectionnez la langue que le proxy Web doit utiliser lors de l'affichage des pages de notification.

- Le paramètre de langue HTTP s'applique à toutes les pages de notification HTTP (accusé de réception, utilisateur final sur la boîte, utilisateur final personnalisé et avertissement de filtrage d'URL de l'utilisateur final).
- La langue du FTP s'applique à tous les messages de notification FTP.

Étape 4 Choisissez d'utiliser ou non un logo sur chaque page de notification. Vous pouvez indiquer le logo Cisco ou tout fichier graphique référencé dans l'URL que vous saisissez dans le champ Use Custom Logo (Utiliser un logo personnalisé).

Ce paramètre s'applique à toutes les pages de notification HTTP desservies sur IPv4. AsyncOS ne prend pas en charge les images sur IPv6.

Étape 5 Envoyez et validez les modifications.

What to do next

Thèmes connexes

- Mises en garde concernant les URL et les logos dans les pages de notification , on page 13

page End-User Acknowledgment (Accusé de réception à destination de l'utilisateur final)

Vous pouvez configurer Secure Web Appliance pour informer les utilisateurs qu'il filtre et surveille leur activité Web. Une fois ce paramètre configuré, l'appliance affiche une page d'accusé de réception de l'utilisateur final pour chaque utilisateur accédant au Web à l'aide de HTTP ou HTTPS. Elle affiche la page d'accusé de réception de l'utilisateur final la première fois qu'un utilisateur tente d'accéder à un site Web ou après un intervalle de temps configuré.

Le proxy Web suit les utilisateurs par nom d'utilisateur si l'authentification a rendu un nom d'utilisateur disponible. Si aucun nom d'utilisateur n'est disponible, vous pouvez choisir votre mode de suivi, par adresse IP ou par témoin de session de navigateur Web.

Note Les transactions FTP natives sont exclues de la page d'accusé de réception de l'utilisateur final.

- Accès aux sites HTTPS et FTP avec la page End-User Acknowledgment (Accusé de réception à destination de l'utilisateur final), on page 3
- À propos de la page End-user Acknowledgment (Accusé de réception de l'utilisateur final), on page 4
- Configuration de la page End-User Acknowledgment (Accusé de réception à destination de l'utilisateur final), on page 4

Accès aux sites HTTPS et FTP avec la page End-User Acknowledgment (Accusé de réception à destination de l'utilisateur final)

La page d'accusé de réception de l'utilisateur final fonctionne, car elle affiche une page HTML à l'utilisateur final qui l'oblige à cliquer sur un contrat de politique d'utilisation acceptable. Une fois que les utilisateurs ont cliqué sur le lien, le proxy Web redirige les clients vers le site Web initialement demandé. Il conserve une trace du moment où les utilisateurs ont accepté la page d'accusé de réception de l'utilisateur final à l'aide d'un remplaçant (par adresse IP ou témoin de session de navigateur Web) si aucun nom d'utilisateur n'est disponible pour l'utilisateur.

- **HTTPS.** Le proxy Web vérifie si l'utilisateur a accusé réception de la page de confirmation de l'utilisateur final à l'aide d'un témoin, mais il ne peut pas obtenir le témoin s'il ne déchiffre pas la transaction. Vous pouvez choisir de contourner (interconnexion) ou d'abandonner les requêtes HTTPS lorsque la page de confirmation de l'utilisateur final est activée et suit les utilisateurs à l'aide de témoins de session. Pour ce faire, utilisez la commande advancedproxyconfig > EUN de l'interface de ligne de commande et choisissez la commande bypass (contourner) pour « Action à exécuter pour les requêtes HTTPS avec EUA basé sur la session (« bypass » ou « drop ») ».
- **FTP sur HTTP.** Les navigateurs Web n'envoient jamais de témoins pour les transactions FTP sur HTTP, de sorte que le proxy Web ne peut pas obtenir de témoin. Pour contourner ce problème, vous pouvez

dispenser les transactions FTP sur HTTP d'exiger la page d'accusé de réception de l'utilisateur final. Pour ce faire, créez une catégorie d'URL personnalisée en utilisant l'expression régulière « ftp:// » comme expression régulière (sans les guillemets) et définissez une politique d'identité qui exonère les utilisateurs de la page de confirmation de l'utilisateur final pour cette catégorie d'URL personnalisée.

À propos de la page End-user Acknowledgment (Accusé de réception de l'utilisateur final)

- Lorsqu'un utilisateur est suivi par son adresse IP, l'appliance utilise la valeur la plus courte pour l'intervalle de temps maximal et le délai d'inactivité maximal de l'adresse IP pour déterminer quand afficher à nouveau la page d'accusé de réception de l'utilisateur final.
- Lorsqu'un utilisateur est suivi à l'aide d'un témoin de session, le proxy Web affiche à nouveau la page d'accusé de réception de l'utilisateur final si l'utilisateur ferme puis rouvre son navigateur Web ou ouvre un deuxième navigateur Web.
- L'utilisation d'un témoin de session pour suivre les utilisateurs lorsque le client accède à des sites HTTPS ou à des serveurs FTP au moyen de FTP sur HTTP ne fonctionne pas.
- Lorsque l'appliance est déployée en mode de transfert explicite et qu'un utilisateur accède à un site HTTPS, la page d'accusé de réception de l'utilisateur final n'inclut que le nom de domaine dans le lien qui redirige l'utilisateur vers l'URL demandée à l'origine. Si l'URL demandée à l'origine contient du texte après le nom de domaine, ce texte est tronqué.
- Lorsque la page d'accusé de réception de l'utilisateur final s'affiche, l'entrée du journal d'accès pour cette transaction indique OTHER (AUTRE) comme balise de décision ACL. En effet, l'URL demandée à l'origine a été bloquée et la page d'accusé de réception de l'utilisateur final a été affichée à la place de l'utilisateur.

Configuration de la page End-User Acknowledgment (Accusé de réception à destination de l'utilisateur final)

Before you begin

- Pour configurer la langue d'affichage et personnaliser le logo affiché, consultez Configuration des paramètres généraux pour les pages de notification, on page 2.
- Si vous souhaitez personnaliser le message affiché aux utilisateurs finaux, consultez Messages personnalisés sur les pages de notification, on page 12. Si vous avez besoin d'options de personnalisation supplémentaires qui ne sont pas disponibles dans la zone Custom Message (Message personnalisé), consultez Modification directe des fichiers HTML de la page de notification , on page 14.

Vous pouvez activer et configurer la page d'accusé de réception de l'utilisateur final dans l'interface Web ou l'interface de ligne de commande. Lorsque vous configurez la page d'accusé de réception de l'utilisateur final dans l'interface Web, vous pouvez inclure un message personnalisé qui s'affiche sur chaque page.

Dans l'interface de ligne de commande, utilisez `advancedproxyconfig` > `eun`.

Étape 1 Choisissez **Security Services > End-User Notification** (Services de sécurité > Notification de l'utilisateur final).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Cochez le champ « **Require end-user to click through acknowledgment page** » (Exiger de l'utilisateur final qu'il fasse un clic sur la page d'accusé de réception).

Étape 4 Saisissez des options :

Paramètres	Description
Time Between Acknowledgements (Délai entre les accusés de réception)	L'intervalle entre les accusés de réception détermine la fréquence à laquelle le proxy Web affiche la page d'accusé de réception de l'utilisateur final pour chaque utilisateur. Ce paramètre s'applique aux utilisateurs suivis par nom d'utilisateur et utilisateurs par adresse IP ou témoin de session. Vous pouvez indiquer n'importe quelle valeur comprise entre 30 et 2 678 400 secondes (un mois). La valeur par défaut est un jour (86 400 secondes). Lorsque la durée entre les accusés de réception change et est validée, le proxy Web utilise la nouvelle valeur même pour les utilisateurs qui ont déjà accusé réception du proxy Web.
Inactivity Timeout (Délai d'inactivité maximum)	Le délai d'inactivité détermine combien de temps un utilisateur suivi et reconnu par son adresse IP ou son témoin de session (utilisateurs non authentifiés uniquement) peut être inactif avant que l'utilisateur ne soit plus considéré comme ayant accepté la politique d'utilisation acceptable. Vous pouvez indiquer n'importe quelle valeur comprise entre 30 et 2 678 400 secondes (un mois). La valeur par défaut est de 4 heures (14 400 secondes).

Paramètres	Description
Surrogate Type (Type de substitution)	Détermine la méthode que le proxy Web utilise pour suivre l'utilisateur : • **Adresse IP.** Le proxy Web permet à l'utilisateur de cette adresse IP d'utiliser n'importe quel navigateur Web ou processus HTTP autre qu'un navigateur pour accéder au Web une fois que l'utilisateur a cliqué sur le lien de la page d'accusé de réception de l'utilisateur final. Le suivi de l'utilisateur par adresse IP permet à l'utilisateur d'accéder au Web jusqu'à ce que le proxy Web affiche une nouvelle page d'accusé de réception pour l'utilisateur final en raison de l'inactivité ou de l'intervalle de temps configuré pour les nouveaux accusés de réception. Contrairement au suivi par témoin de session, le suivi par adresse IP permet à l'utilisateur d'ouvrir plusieurs applications de navigateur Web sans avoir à accepter l'accusé de réception de l'utilisateur final, à moins que l'intervalle configuré n'ait expiré. **Note** Lorsque l'adresse IP est configurée et que l'utilisateur est authentifié, le proxy Web suit les utilisateurs par nom d'utilisateur plutôt que par adresse IP. • **Témoin de session.** Le serveur proxy Web envoie un témoin au navigateur Web de l'utilisateur lorsque l'utilisateur cliquez sur le lien de la page d'accusé de réception de l'utilisateur final et utilise le témoin pour suivre sa session. Les utilisateurs peuvent continuer à accéder au Web à l'aide de leur navigateur Web jusqu'à ce que la valeur du Délai entre les accusés de réception expire, ils ont été inactifs plus longtemps que le temps alloué ou ils ferment leur navigateur Web. Si l'utilisateur utilise une application cliente HTTP sans navigateur, il doit être en mesure de cliquer sur le lien sur la page d'accusé de réception de l'utilisateur final pour accéder à Web. Si l'utilisateur ouvre une deuxième application de navigateur Web, l'utilisateur doit exécuter à nouveau le processus d'accusé de réception de l'utilisateur final pour que le proxy Web envoie un témoin de session au deuxième navigateur Web. **Note** L'utilisation d'un témoin de session pour suivre les utilisateurs lorsque le client accède à des sites HTTPS ou à des serveurs FTP au moyen de FTP sur HTTP n'est pas prise en charge.
Custom message (Message personnalisé)	Personnalisez le texte qui s'affiche sur chaque page de confirmation de l'utilisateur final. Vous pouvez inclure des balises HTML simples pour mettre en forme le texte. **Note** Vous ne pouvez inclure un message personnalisé que lorsque vous configurez la page d'accusé de réception de l'utilisateur final dans l'interface Web, plutôt que dans l'interface de ligne de commande. Voir aussi Messages personnalisés sur les pages de notification, on page 12.

Étape 5 (Facultatif) Cliquez sur **Preview Acknowledgment Page Customization** (Survol de la personnalisation de la page d'accusé de réception) pour afficher la page d'accusé de réception actuelle de l'utilisateur final dans une fenêtre de navigateur distincte.

Note Si les fichiers HTML de notification ont été modifiés, cette fonctionnalité d'aperçu n'est pas disponible.

Étape 6 Envoyez et validez les modifications.

Pages End-User Notification (Notification d'utilisateur final)

Lorsqu'une politique empêche un utilisateur d'accéder à un site Web, vous pouvez configurer l'appliance pour qu'elle informe l'utilisateur des raisons pour lesquelles elle a bloqué la demande d'URL. Pour y parvenir, vous avez plusieurs possibilités :

Destinataire	Voir
Affichage des pages prédéfinies et personnalisables qui sont hébergées sur Secure Web Appliance.	Configuration des pages On-Box End-User Notification (Notification d'utilisateur final intégré), on page 7
Redirection de l'utilisateur vers les pages de notification HTTP à l'utilisateur final à une URL spécifique.	Pages Off-Box End-User Notification (Notification d'utilisateur final off-box) , on page 8

Configuration des pages On-Box End-User Notification (Notification d'utilisateur final intégré)

Before you begin

- Pour configurer la langue d'affichage et personnaliser le logo affiché, consultez Configuration des paramètres généraux pour les pages de notification, on page 2.
- Si vous souhaitez personnaliser le message affiché à l'aide des notifications intégrées, consultez les rubriques sous Messages personnalisés sur les pages de notification, on page 12. Si vous avez besoin d'options de personnalisation supplémentaires qui ne sont pas disponibles dans la zone Custom Message (Message personnalisé), consultez Modification directe des fichiers HTML de la page de notification , on page 14.

Les pages intégrées sont des pages de notification prédéfinies et personnalisables qui se trouvent sur l'appliance.

Étape 1 **Security Services > End-User Notification** (Services de sécurité > Notification de l'utilisateur final).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Dans le champ Notification Type (Type de notification), choisissez **Use On Box End User Notification** (Utiliser la notification de l'utilisateur final/intégrée).

Étape 4 Configurez les paramètres de la page de notification de l'utilisateur final/intégrée.

Paramètres	Description
Custom Message (Message personnalisé)	Incluez tout texte supplémentaire requis sur chaque page de notification. Lorsque vous saisissez un message personnalisé, AsyncOS place le message avant la dernière phrase sur la page de notification contenant les coordonnées.

Paramètres	Description
Contact Information (Coordonnées)	Personnaliser les coordonnées indiquées sur chaque page de notification. AsyncOS affiche la phrase de coordonnées comme dernière phrase d'une page, avant de fournir les codes de notification que les utilisateurs peuvent communiquer à l'administrateur réseau.
End-User Misclassification Reporting (Rapports sur les erreurs de classification de l'utilisateur final)	Si elle est activée, à partir d'AsyncOS 14.5, la demande de classification incorrecte est envoyée sur HTTPS. Vous ne recevrez aucune notification d'alerte de sécurité. Lorsque cette option est activée, les utilisateurs peuvent signaler à Cisco des URL mal classées. Un bouton supplémentaire s'affiche sur les pages On-Box End-User Notification (Notification d'utilisateur final intégré) pour les sites bloqués en raison d'une suspicion de logiciel ou de filtres d'URL malveillants. Ce bouton permet à l'utilisateur de signaler tout doute d'erreur de classification de la page. Il ne s'affiche pas pour les pages bloquées en raison d'autres paramètres de politique. **Note** • Vous devez activer la participation au réseau SenderBase. Consultez la section Activation de la participation au réseau Cisco SensorBase pour plus d'informations. • Vous devez avoir un compte Cisco valide associé au(x) numéro(s) de série de votre/vos appliances. • Le signalement des URL mal classées ne fonctionne pas sur les Secure Web Appliance virtuels.

Étape 5 (Facultatif) Cliquez sur le lien **Preview Notification Page Customization** (Survol de la personnalisation de la page de notification) pour afficher la page de notification de l'utilisateur final actuelle dans une fenêtre de navigateur distincte.

Note Si les fichiers HTML de notification ont été modifiés, cette fonctionnalité d'aperçu n'est pas disponible.

Étape 6 Envoyez et validez les modifications.

Pages Off-Box End-User Notification (Notification d'utilisateur final off-box)

Le proxy Web peut être configuré pour rediriger toutes les pages de notification HTTP à l'utilisateur final vers une URL spécifique que vous spécifiez.

Affichage de la page off-box correcte en fonction du motif du blocage de l'accès

Par défaut, AsyncOS redirige tous les sites Web bloqués vers l'URL, quelle que soit la raison pour laquelle il a bloqué la page d'origine. Cependant, AsyncOS transmet également des paramètres sous forme de chaîne de requête ajoutée à l'URL de redirection afin que vous puissiez vous assurer que l'utilisateur voit une page

unique expliquant la raison du blocage. Pour plus d'informations sur les paramètres inclus, consultez Paramètres de la page off-box des notifications envoyées à l'utilisateur final, on page 9.

Lorsque vous souhaitez que l'utilisateur affiche une page différente pour chaque raison d'un site Web bloqué, créez un script CGI sur le serveur Web qui peut analyser la chaîne de requête dans l'URL de redirection. Le serveur peut ensuite effectuer une deuxième redirection vers une page appropriée.

Critères d'URL pour les pages de notification off-box

- Vous pouvez utiliser n'importe quelle URL HTTP ou HTTPS.
- L'URL peut préciser un numéro de port précis.
- L'URL ne peut pas avoir d'arguments après le point d'interrogation.
- L'URL doit contenir un nom d'hôte bien formé.

Par exemple, si vous avez saisi l'URL suivante dans le champ Rediriger vers l'URL personnalisée :

```
http://www.example.com/eun.policy.html
```

Et vous avez l'entrée de journal des accès suivante :

```
1182468145.492 1 172.17.0.8 TCP_DENIED/403 3146 GET http://www.espn.com/index.html HTTP/1.1
 - NONE/- - BLOCK_WEBCAT-DefaultGroup-DefaultGroup-NONE-NONE-DefaultRouting
<IW_sprt,-,-,-,-,-,-,-,-,-,-,-,-,-,IW_sprt,-> -
```

Ensuite, AsyncOS crée l'URL redirigée suivante :

```
http://www.example.com/eun.policy.html?Time=21/Jun/
2007:23:22:25%20%2B0000&ID=0000000004&Client_IP=172.17.0.8&User=-
&Site=www.espn.com&URI=index.html&Status_Code=403&Decision_Tag=
BLOCK_WEBCAT-DefaultGroup-DefaultGroup-NONE-NONE-DefaultRouting
&URL_Cat=Sports%20and%20Recreation&WBRS=-&DVS_Verdict=-&
DVS_ThreatName=-&Reauth_URL=-
```

Paramètres de la page off-box des notifications envoyées à l'utilisateur final

AsyncOS transmet les paramètres au serveur Web en tant que paramètres d'URL standard dans la demande HTTP GET. Il utilise le format suivant :

```
<notification_page_url>?param1=value1&param2=value2
```

Le tableau décrit les paramètres qu'AsyncOS inclut dans la chaîne de requête.

Nom du paramètre	Description
Time (Durée)	Date et heure de la transaction.
ID (Identifiant)	ID de transaction.
Client_IP	Adresse IP du client.
User (Utilisateur)	Nom d'utilisateur du client ayant fait la demande, si celui-ci est disponible.
Site	Nom d'hôte de la destination dans la demande HTTP.
URI	Chemin d'accès URL spécifié dans la demande HTTP.

Nom du paramètre	Description
Status_Code	Code d'état HTTP de la demande.
Decision_Tag	Balise de décision ACL telle que définie dans l'entrée du journal d'accès qui indique comment le moteur DVS a géré la transaction.
URL_Cat	Catégorie d'URL attribuée par le moteur de filtrage d'URL à la demande de transaction. **Remarque :** AsyncOS pour le Web envoie le nom complet des catégories d'URL prédéfinies et définies par l'utilisateur. Il effectue l'encodage de l'URL sur le nom de la catégorie, de sorte que les espaces sont écrits comme « %20 ».
WBRS	Score WBRS que les filtres de réputation Web ont attribué à l'URL dans la demande.
DVS_Verdict	Catégorie de programme malveillant que le moteur DVS affecte à la transaction.
DVS_ThreatName	Nom du programme malveillant trouvé par le moteur DVS.
Reauth_URL	URL sur laquelle les utilisateurs peuvent cliquer pour s'authentifier à nouveau si l'utilisateur est bloqué sur un site Web en raison d'une politique de filtrage d'URL restrictive. Utilisez ce paramètre lorsque le paramètre d'authentification global « Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction » (Activer l'invite de réauthentification si l'utilisateur final est bloqué par la catégorie d'URL ou la restriction de session utilisateur) est activé et que l'utilisateur est bloqué sur un site Web en raison d'une catégorie d'URL bloquée. Pour utiliser ce paramètre, assurez-vous que le script CGI effectue les étapes suivantes : 1. Obtient la valeur du paramètre `Reauth_Url`. 2. Décode la valeur par URL-decode. 3. Décode la valeur par Base64 et obtient l'URL de réauthentification réelle. 4. Incluez l'URL décodée sur la page de notification de l'utilisateur final d'une manière ou d'une autre, sous la forme d'un lien ou d'un bouton, ainsi que des instructions à l'intention des utilisateurs pour les informer qu'ils peuvent cliquer sur le lien et saisir de nouveaux identifiants d'authentification qui permettent un accès amélioré.

Note AsyncOS inclut toujours tous les paramètres dans chaque URL redirigée. Si aucune valeur n'existe pour un paramètre particulier, AsyncOS transmet un tiret (-).

Redirection des pages End-User Notification (Notification d'utilisateur final) vers une URL personnalisée (off-box)

Étape 1 **Security Services > End-User Notification** (Services de sécurité > Notification de l'utilisateur final).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Dans la section **End-User Notification Pages** (Pages de notification d'utilisateur final), choisissez **Redirect to Custom URL** (Rediriger vers une URL personnalisée).

Étape 4 Dans le champ **Notification Page URL** (URL de la page de notification), saisissez l'URL vers laquelle vous souhaitez rediriger les sites Web bloqués.

Étape 5 (Facultatif) Cliquez sur **Preview Custom URL** (Survol du lien URL personnalisée).

Étape 6 Envoyez et validez les modifications.

Configuration de la page d'avertissement du filtrage des URL de l'utilisateur final

Before you begin

- Si vous souhaitez personnaliser le message affiché à l'aide des notifications intégrées, consultez les rubriques sous Messages personnalisés sur les pages de notification, on page 12. Si vous avez besoin d'options de personnalisation supplémentaires qui ne sont pas disponibles dans la zone Custom Message (Message personnalisé), consultez Modification directe des fichiers HTML de la page de notification , on page 14.

Une page d'avertissement concernant le filtrage d'URL destinée à l'utilisateur final s'affiche lorsqu'un utilisateur accède pour la première fois à un site Web dans une catégorie d'URL particulière après un certain laps de temps. Vous pouvez également configurer la page d'avertissement lorsqu'un utilisateur accède au contenu pour adultes lorsque la fonction d'évaluation du contenu du site est activée.

Étape 1 **Security Services > End-User Notification** (Services de sécurité > Notification de l'utilisateur final).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Faites défiler la liste jusqu'à la section d'avertissement concernant le filtrage des URL de l'utilisateur final.

Étape 4 Dans le champ Time Understanding (intervalle entre les avertissements), saisissez l'intervalle de temps utilisé par le proxy Web entre l'affichage de la page d'avertissement de filtrage des URL de l'utilisateur final pour chaque catégorie d'URL par utilisateur.

Vous pouvez indiquer n'importe quelle valeur comprise entre 30 et 2 678 400 secondes (un mois). La valeur par défaut est 1 heure (3 600 secondes). Vous pouvez entrer la valeur en secondes, minutes ou jours. Utilisez « s » pour les secondes, « m » pour les minutes et « d » pour les jours.

Étape 5 Dans le champ Message personnalisé, saisissez le texte que vous souhaitez voir apparaître sur chaque page d'avertissement de filtrage d'URL d'utilisateur final.

Étape 6 (Facultatif) Cliquez sur **Preview URL Category Warning Page Customization** (Survol de la personnalisation de la page d'avertissement de catégorie d'URL) pour afficher la page d'avertissement actuelle relative au filtrage des URL de l'utilisateur final dans une fenêtre de navigateur distincte.

Note Si les fichiers HTML de notification ont été modifiés, cette fonctionnalité d'aperçu n'est pas disponible.

Étape 7 Envoyez et validez les modifications.

Configuration des messages de notification FTP

Before you begin

Si vous souhaitez personnaliser le message affiché à l'aide des notifications intégrées, consultez les rubriques sous Messages personnalisés sur les pages de notification, on page 12. Si vous avez besoin d'options de personnalisation supplémentaires qui ne sont pas disponibles dans la zone Custom Message (Message personnalisé), consultez Modification directe des fichiers HTML de la page de notification , on page 14.

Le proxy FTP affiche un message de notification prédéfini et personnalisable aux clients FTP natifs lorsqu'il ne peut pas établir de connexion avec le serveur FTP pour une raison, comme une erreur d'authentification par le proxy FTP ou une mauvaise réputation pour le nom de domaine du serveur. La notification est spécifique à la raison du blocage de la connexion.

Étape 1 **Security Services > End-User Notification** (Services de sécurité > Notification de l'utilisateur final).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Faites défiler la liste jusqu'à la section FTP natif.

Étape 4 Dans le champ **Language** (Langue), sélectionnez la langue à utiliser lors de l'affichage des messages de notification FTP natifs.

Étape 5 Dans le champ **Custom Message** (Message personnalisé), saisissez le texte que vous souhaitez afficher dans chaque message de notification FTP natif.

Étape 6 Envoyez et validez les modifications.

Messages personnalisés sur les pages de notification

Les sections suivantes s'appliquent au texte saisi dans la zone « Custom Message » (Message personnalisé) pour tout type de notification configuré dans la page Edit End User Notification (Modifier la notification de l'utilisateur final).

- Balises HTML prises en charge dans les messages personnalisés sur les pages de notification, on page 12
- Mises en garde concernant les URL et les logos dans les pages de notification , on page 13

Balises HTML prises en charge dans les messages personnalisés sur les pages de notification

Vous pouvez utiliser des balises HTML pour mettre en forme le texte de n'importe quelle notification sur la page Modifier la notification de l'utilisateur final (Edit End User Notification) qui propose une zone « Custom Message » (Message personnalisé). Les balises doivent être en minuscules et respecter la syntaxe HTML standard (balises fermantes, etc.)

Vous pouvez utiliser les balises HTML suivantes.

- <a>
-

-
- <big></big>
-
- <code></code>
-
-
- <small></small>
-

Par exemple, vous pouvez mettre du texte en italique :

```
Please acknowledge the following statements <i>before</i> accessing the Internet.
```

La balise vous permet d'utiliser n'importe quel style CSS pour mettre en forme le texte. Par exemple, vous pouvez afficher du texte en rouge :

```
 <span style="color: red">Warning:</span> You must acknowledge the following statements
<i>before</i> accessing the Internet.
```

Note Si vous avez besoin de plus de flexibilité ou si vous souhaitez ajouter du code JavaScript à vos pages de notification, vous devez modifier directement les fichiers de notification HTML. Le code JavaScript saisi dans la zone de message personnalisé pour les notifications dans l'interface utilisateur Web sera supprimé. Consultez Modification directe des fichiers HTML de la page de notification , on page 14.

Mises en garde concernant les URL et les logos dans les pages de notification

Cette section s'applique si vous effectuez l'une des personnalisations suivantes :

- Saisissez du texte dans la zone « Custom Message » (Message personnalisé) pour toute notification sur la page Edit End User Notification (Modifier la notification de l'utilisateur final).
- Modifier directement les fichiers HTML pour les notifications sur la boîte
- Utiliser un logo personnalisé

Toutes les combinaisons de chemins d'URL et de noms de domaine dans les liens intégrés dans un texte personnalisé et le logo personnalisé sont dispensés des éléments suivants pour les notifications sur la boîte :

- Authentification de l'utilisateur
- Accusé de réception de l'utilisateur final
- Toutes les analyses, comme l'analyse des programmes malveillants et l'évaluation de la réputation de sites Web

Par exemple, si les URL suivantes sont intégrées dans du texte personnalisé :

```
http://www.exemple.com/index.html
```

```
http://www.monentreprise.com/logo.jpg
```

Ensuite, toutes les URL suivantes seront également traitées comme dispensées de toute analyse :

```
http://www.exemple.com/index.html
```

```
http://www.monentreprise.com/logo.jpg
```

`http://www.exemple.com/logo.jpg`

`http://www.monentreprise.com/index.html`

Également, lorsqu'une URL intégrée est de la forme `<protocol>://<domain-name>/<directory path>/` Alors tous les sous-fichiers et sous-répertoires de ce chemin de répertoire sur l'hôte seront également exclus des tâches d'analyse.

Par exemple, si l'URL suivante est intégrée : `http://www.exemple.com/gallery2/`, les URL telles que `http://www.exemple.com/gallery2/main.PH` seront également traitées comme dispensées.

Cela vous permet de créer une page plus élaborée avec du contenu intégré tant que le contenu intégré est relatif à l'URL initiale. Cependant, vous devez également faire preuve de prudence lorsque vous décidez des chemins à inclure en tant que liens et logos personnalisés.

Modification directe des fichiers HTML de la page de notification

Chaque page de notification est stockée sur Secure Web Appliance au format HTML. Si vous avez besoin de plus de personnalisation que ne le permet la zone « Custom Message » (Message personnalisé) de l'interface Web, vous pouvez modifier directement ces fichiers HTML. Par exemple, vous pouvez inclure du code JavaScript standard ou modifier l'aspect général de chaque page.

Les renseignements dans les sections suivantes s'appliquent à tout type de fichier HTML de notification à l'utilisateur final sur l'appliance, y compris les pages d'accusé de réception de l'utilisateur final.

- Exigences relatives à la modification directe des fichiers HTML de notification , on page 14
- Modification directe des fichiers HTML de la page de notification , on page 14
- Utilisation de variables dans les fichiers HTML de notification , on page 15
- Variables de personnalisation des fichiers HTML de notification , on page 16

Exigences relatives à la modification directe des fichiers HTML de notification

- Chaque fichier d'échange de notification doit être un fichier HTML valide. Pour obtenir la liste des balises HTML que vous pouvez inclure, consultez Balises HTML prises en charge dans les messages personnalisés sur les pages de notification, on page 12.
- Les noms des fichiers d'échange de notifications doivent correspondre exactement aux noms des fichiers livrés avec Secure Web Appliance.

  Si le répertoire `configuration\eun` ne contient pas de fichier en particulier avec le nom requis, l'appliance affiche la page de notification standard de l'utilisateur final sur l'ordinateur.
- N'incluez aucun lien vers les URL dans les fichiers HTML. Tout lien inclus dans les pages de notification est soumis aux règles de contrôle d'accès définies dans les politiques d'accès et les utilisateurs peuvent se retrouver dans une boucle récursive.
- Testez vos fichiers HTML dans des navigateurs clients pris en charge pour vous assurer qu'ils se comportent comme prévu, en particulier s'ils comprennent du code JavaScript.

- Pour que vos pages personnalisées prennent effet, vous devez activer les fichiers personnalisés à l'aide de la commande d'interface de ligne de commande `advancedproxyconfig > EUN > Refresh EUN Pages`.

Modification directe des fichiers HTML de notification

Before you begin

- Prenez connaissance des exigences dans Exigences relatives à la modification directe des fichiers HTML de notification , on page 14.
- Consultez Variables de personnalisation des fichiers HTML de notification , on page 16 et Utilisation de variables dans les fichiers HTML de notification , on page 15.

Étape 1 Utilisez un client FTP pour vous connecter à Secure Web Appliance.

Étape 2 Accédez au répertoire `configuration\eun`.

Étape 3 Téléchargez les fichiers de répertoire de langue correspondant aux pages de notification que vous souhaitez modifier.

Étape 4 Sur votre ordinateur local, utilisez un éditeur de texte ou un éditeur HTML pour modifier les fichiers HTML.

Étape 5 Utilisez le client FTP pour charger les fichiers HTML personnalisés dans le répertoire à partir duquel vous les avez téléchargés à l'étape 3.

Étape 6 Ouvrez un client SSH et connectez-vous à Secure Web Appliance.

Étape 7 Exécutez la commande de l'interface de ligne de commande `advancedproxyconfig > EUN`.

Étape 8 Tapez **2** pour utiliser les pages de notification de l'utilisateur final personnalisées.

Étape 9 Si l'option de pages de notification de l'utilisateur final personnalisées est actuellement activée lorsque vous mettez à jour les fichiers HTML, saisissez **1** pour actualiser les pages de notification de l'utilisateur final personnalisées.

Si vous ne le faites pas, les nouveaux fichiers ne prendront effet qu'au redémarrage du proxy Web.

Étape 10 Validez vos modifications.

Étape 11 Fermez le client SSH.

Utilisation de variables dans les fichiers HTML de notification

Lorsque vous modifiez des fichiers HTML de notification, vous pouvez inclure des variables conditionnelles pour créer des instructions « if-then » pour effectuer différentes actions en fonction de l'état actuel.

Le tableau décrit les différents formats de variable conditionnelle.

Format de variable conditionnelle	Description
%?*V*	Cette variable conditionnelle évalue à TRUE si la sortie de la variable %*V* n'est pas vide.
%!*V*	Représente la condition suivante : `else` Utilisez cette condition avec la variable conditionnelle %?*V*.

Format de variable conditionnelle	Description
%#*V*	Représente la condition suivante : `endif` Utilisez cette condition avec la variable conditionnelle %?*V*.

Par exemple, le texte suivant est du code HTML qui utilise %R comme variable conditionnelle pour vérifier si la réauthentification est offerte, et %r comme variable normale pour fournir l'URL de réauthentification.

```
%?R
<div align="left">
  <form name="ReauthInput" action="%r" method="GET">
    <input name="Reauth" type="button" OnClick="document.location='%r'" id="Reauth"
value="Login as different user...">
  </form>
</div>
%#R
```

Toute variable incluse dans Variables de personnalisation des fichiers HTML de notification , on page 16 peut être utilisée comme variable conditionnelle. Cependant, les meilleures variables à utiliser dans les instructions conditionnelles sont celles qui sont liées à la *demande du client* plutôt qu'à la réponse du serveur, et les variables qui peuvent ou non avoir la valeur TRUE au lieu des variables qui donnent toujours la valeur TRUE.

Variables de personnalisation des fichiers HTML de notification

Vous pouvez utiliser des variables dans les fichiers HTML de notification pour afficher des informations précises à l'utilisateur. Vous pouvez également convertir chaque variable en variable conditionnelle pour créer des instructions « if-then ». Pour en savoir plus, consultez Utilisation de variables dans les fichiers HTML de notification , on page 15.

Variable	Description	Toujours évaluée sur TRUE si elle est utilisée comme variable conditionnelle
%a	Domaine d'authentification pour FTP	Non
%A	Adresse ARP	Oui
%b	Nom de l'agent utilisateur	Non
%B	Motif du blocage, par exemple BLOCK-SRC ou BLOCK-TYPE	Non
%c	Personne-ressource dans la page d'erreur	Oui
%C	Ensemble complet - Témoin : ligne d'en-tête ou chaîne vide	Non
%d	Adresse IP du client	Oui
%D	Nom d'utilisateur	Non
%e	Adresse de messagerie de la page d'erreur	Oui

Variable	Description	Toujours évaluée sur TRUE si elle est utilisée comme variable conditionnelle
%E	URL du logo de la page d'erreur	Non
%f	Section de commentaires de l'utilisateur	Non
%F	URL pour les commentaires de l'utilisateur	Non
%g	Nom de la catégorie Web, si disponible	Oui
%G	Taille de fichier maximale (Mo)	Non
%h	Nom d'hôte du proxy	Oui
%H	Nom de serveur de l'URL	Oui
%i	Identifiant de transaction sous forme de nombre hexadécimal	Oui
%I	Management IP Address (adresse IP de gestion)	Oui
%j	Texte personnalisé de la page d'avertissement de catégorie d'URL	Non
%k	Lien de redirection vers la page d'accusé de réception de l'utilisateur final et la page d'avertissement du filtrage des URL de l'utilisateur final	Non
%K	Type de fichier de réponse	Non
%l	WWW-Authenticate : ligne d'en-tête	Non
%L	Proxy-Authenticate : ligne d'en-tête	Non
%M	La méthode de la demande, par exemple « GET » ou « POST »	Oui
%n	Nom de la catégorie de programmes malveillants, si disponible	Non
%N	Nom du programme malveillant, s'il est disponible	Non
%o	Type de menace pour la réputation Web, s'il est disponible	Non
%O	Motif de la menace pour la réputation Web, le cas échéant	Non
%p	Chaîne pour l'en-tête HTTP Proxy-Connection	Oui
%P	Protocole	Oui
%q	Nom du groupe de politiques d'identité	Oui
%Q	Nom du groupe de politiques pour les politiques autres que celles d'identité	Oui
%r	URL de redirection	Non

Variable	Description	Toujours évaluée sur TRUE si elle est utilisée comme variable conditionnelle
%R	Réauthentification proposée. Cette variable génère une chaîne vide lorsqu'elle est fausse et un espace lorsqu'elle est vraie, il n'est donc pas utile de l'utiliser seule. Utilisez-la plutôt comme variable de condition.	Non
%S	La signature du proxy	Non, toujours la valeur FALSE
%t	Horodatage en secondes Unix plus millisecondes	Oui
%T	La date	Oui
%u	La partie URI de l'URL (l'URL sans le nom du serveur)	Oui
%U	L'URL complète de la demande	Oui
%v	Version du protocole HTTP	Oui
%W	Port de gestion WebUI	Oui
%X	Code de blocage étendu Il s'agit d'une valeur base64 de 16 octets qui code la plupart des informations de réputation Web et de protection contre les programmes malveillants enregistrées dans le journal des accès, telles que la balise de décision ACL et le score WBRS.	Oui
%Y	Chaîne de texte personnalisée de l'administrateur, si définie, vide sinon	Non
%y	Texte personnalisé de la page d'accusé de réception de l'utilisateur final	Oui
%z	Niveau de réputation Web	Oui
%Z	Métadonnées DLP	Oui
%%	Imprime le symbole de pourcentage (%) dans la page de notification	s.o.

Types de pages de notification

Par défaut, le proxy Web affiche une page de notification indiquant aux utilisateurs qu'ils ont été bloqués et la raison du blocage.

La plupart des pages de notification affichent un ensemble de codes différent qui peut aider les administrateurs ou l'assistance client de Cisco à résoudre tout problème potentiel. Certains codes sont réservés à un usage interne chez Cisco. Les différents codes qui peuvent s'afficher dans les pages de notification sont identiques aux variables que vous pouvez inclure dans les pages de notification personnalisées, comme indiqué dans Variables de personnalisation des fichiers HTML de notification , on page 16.

Le tableau décrit les différentes pages de notification que les utilisateurs peuvent rencontrer.

Nom de fichier et Titre de la notification	Description des notifications	Texte de la notification
ERR_ACCEPTED Commentaires acceptés, merci	Page de notification qui s'affiche après que les utilisateurs ont utilisé l'option « Report Misclassification » (Signaler une erreur de classification).	Le rapport de classification incorrecte a été envoyé. Nous vous remercions de vos commentaires.
ERR_ADAPTIVE_SECURITY Politique : générale	Bloque la page qui s'affiche lorsque l'utilisateur est bloqué en raison de la fonctionnalité d'analyse adaptative.	En fonction des politiques de sécurité de votre entreprise, le site Web <*URL* > a été bloqué, car son contenu a été considéré comme un risque pour la sécurité.
ERR_ADULT_CONTENT Politique : accusé de réception	Page d'avertissement qui s'affiche lorsque l'utilisateur final accède à une page classée comme contenu pour adultes. Les utilisateurs peuvent cliquer sur un lien d'accusé de réception pour continuer vers le site initialement demandé.	Vous essayez de visiter une page Web dont le contenu est classé comme explicite ou réservé aux adultes. En cliquant sur le lien ci-dessous, vous reconnaissez avoir lu et accepté les politiques de l'organisation qui régissent l'utilisation d'Internet pour ce type de contenu. Les données concernant votre comportement de navigation peuvent être surveillées et enregistrées. Il vous sera régulièrement demandé de confirmer cette déclaration pour continuer à accéder à ce type de page Web. Cliquez ici pour accepter cette déclaration et accéder à Internet.
ERR_AVC Politique : contrôles des applications	Page de blocage qui s'affiche lorsque l'utilisateur est bloqué en raison du moteur de visibilité et de contrôle des applications.	Selon les politiques d'accès de votre organisation, l'accès à l'application %1 de type %2 a été bloqué.
ERR_BAD_REQUEST Demande incorrecte	Page d'erreur résultant d'une demande de transaction non valide.	Le système ne peut pas traiter cette demande. Un navigateur non standard a peut-être généré une requête HTTP non valide. Si vous utilisez un navigateur standard, réessayez la demande.
ERR_BLOCK_DEST Politique : destination	Page de blocage qui s'affiche lorsque l'utilisateur tente d'accéder à une adresse de site Web bloquée.	Selon les politiques d'accès de votre organisation, l'accès au site Web <*URL* > a été bloqué.

Nom de fichier et Titre de la notification	Description des notifications	Texte de la notification
ERR_BROWSER Sécurité : navigateur	Page de blocage qui s'affiche lorsque la demande de transaction émane d'une application qui a été identifiée comme menacée par un programme malveillant ou un logiciel espion.	Selon les politiques d'accès de votre organisation, les demandes de votre ordinateur ont été bloquées, car il a été déterminé qu'il s'agit d'une menace pour le réseau de l'organisation. Votre navigateur a peut-être été compromis par un programme malveillant ou un logiciel espion identifié comme « [*nom du programme malveillant*] ». Veuillez communiquer avec <*contact name* > <*email address* > et indiquez les codes présentés ci-dessous. Si vous utilisez un navigateur non standard et pensez qu'il a été mal classé, utilisez le bouton ci-dessous pour signaler cette erreur de classification.
ERR_BROWSER_CUSTOM Politique : navigateur	Page de blocage qui s'affiche lorsque la demande de transaction provient d'un agent utilisateur bloqué.	Selon les politiques d'accès de votre organisation, les demandes de votre navigateur ont été bloquées. Ce navigateur « <*browser type* > » n'est pas autorisé en raison de risques pour la sécurité potentiels.
ERR_CERT_INVALID Certificat non valide	Page de blocage qui s'affiche lorsque le site HTTPS demandé utilise un certificat non valide.	Une session sécurisée n'a pas pu être établie, car le site <*hostname* > a fourni un certificat non valide.
ERR_CONTINUE_ UNACKNOWLEDGED Politique : accusé de réception	Page d'avertissement qui s'affiche lorsque l'utilisateur demande un site qui fait partie d'une catégorie d'URL personnalisée à laquelle l'action avertir est affectée. Les utilisateurs peuvent cliquer sur un lien d'accusé de réception pour continuer vers le site initialement demandé.	Vous essayez de consulter une page Web qui appartient à la catégorie d'URL <*URL category* >. En cliquant sur le lien ci-dessous, vous reconnaissez avoir lu et accepté les politiques de l'organisation qui régissent l'utilisation d'Internet pour ce type de contenu. Les données concernant votre comportement de navigation peuvent être surveillées et enregistrées. Il vous sera régulièrement demandé de confirmer cette déclaration pour continuer à accéder à ce type de page Web. Cliquez ici pour accepter cette déclaration et accéder à Internet.

Nom de fichier et Titre de la notification	Description des notifications	Texte de la notification
ERR_DNS_FAIL Échec du DNS	Page d'erreur qui s'affiche lorsque l'URL demandée contient un nom de domaine non valide.	La résolution du nom d'hôte (recherche DNS) pour ce nom d'hôte <*hostname* > a échoué. L'adresse Internet est peut-être mal épelée ou obsolète, l'hôte <*hostname* > peut être temporairement indisponible ou le serveur DNS peut ne pas répondre. Veuillez vérifier l'orthographe de l'adresse Internet saisie. Si elle est correcte, essayez d'exécuter cette demande plus tard.
ERR_EXPECTATION_ FAILED Échec de l'attente	Page d'erreur qui s'affiche lorsque la demande de transaction déclenche la réponse HTTP 417 « Expectation Failed » (Échec de l'attente).	Le système ne peut pas traiter la demande pour ce site| Un navigateur non standard a peut-être généré une requête HTTP non valide. Si vous utilisez un navigateur standard, réessayez la demande.
ERR_FILE_SIZE Politique : taille du fichier	Page de blocage qui s'affiche lorsque le fichier demandé est plus volumineux que la taille de fichier maximale autorisée.	Selon les politiques d'accès de votre organisation, l'accès à ce site Web ou <*URL* > de téléchargement a été bloqué, car la taille du téléchargement dépasse la limite autorisée.
ERR_FILE_TYPE Politique : type de fichier	Page de blocage qui s'affiche lorsque le fichier demandé est de type bloqué.	Selon les politiques d'accès de votre organisation, l'accès à ce site Web ou <*URL* > de téléchargement a été bloqué, car le type de fichier « <*file type* > » n'est pas autorisé.
ERR_FILTER_FAILURE Échec du filtre	Page d'erreur qui s'affiche lorsque le moteur de filtrage d'URL est temporairement incapable de fournir une réponse de filtrage d'URL et que l'option « action par défaut pour le service inaccessible » est définie sur Block (Bloquer).	La demande de la page <*URL* > a été refusée, car un serveur interne est actuellement inaccessible ou surchargé. Veuillez réessayer la demande plus tard.
ERR_FOUND Trouvé	Page de redirection interne pour certaines erreurs.	La page <*URL* > est redirigée vers <*redirected URL* >.

Nom de fichier et Titre de la notification	Description des notifications	Texte de la notification
ERR_FTP_ABORTED FTP abandonné	Page d'erreur qui s'affiche lorsque la demande de transaction FTP sur HTTP déclenche la réponse HTTP 416 « Requested Plage Not Satisfiable » (Plage demandée impossible à satisfaire).	La demande pour le fichier <*URL* > n'a pas réussi. Le serveur FTP <*hostname* > a mis fin à la connexion de manière inattendue. Veuillez réessayer la demande plus tard.
ERR_FTP_AUTH_ REQUIRED Autorisation FTP requise	Page d'erreur qui s'affiche lorsque la demande de transaction FTP sur HTTP déclenche la réponse FTP 530 « Not Logded In » (Pas connecté).	L'authentification est requise par le serveur FTP <*hostname* >. Un identifiant d'utilisateur et une phrase secrète valides doivent être saisis lorsque vous y êtes invité. Dans certains cas, le serveur FTP peut limiter le nombre de connexions anonymes. Si vous vous connectez habituellement à ce serveur en tant qu'utilisateur anonyme, veuillez réessayer plus tard.
ERR_FTP_CONNECTION_ FAILED Échec de connexion FTP	Page d'erreur qui s'affiche lorsque la demande de transaction FTP sur HTTP déclenche la réponse FTP 425 « Can't open data connection » (Impossible d'ouvrir la connexion de données).	Le système ne peut pas communiquer avec le serveur FTP <*hostname* >. Le serveur FTP est peut-être hors service de façon temporaire ou permanente, ou peut être inaccessible en raison de problèmes de réseau. Veuillez vérifier l'orthographe de l'adresse saisie. Si elle est correcte, essayez d'exécuter cette demande plus tard.
ERR_FTP_FORBIDDEN FTP interdit	Page d'erreur qui s'affiche lorsque la demande de transaction FTP sur HTTP concerne un objet auquel l'utilisateur n'est pas autorisé à accéder.	L'accès a été refusé par le serveur FTP <*hostname* >. Votre ID utilisateur n'a pas l'autorisation d'accéder à ce document.
ERR_FTP_NOT_FOUND FTP introuvable	Page d'erreur qui s'affiche lorsque la demande de transaction FTP sur HTTP concerne un objet qui n'existe pas sur le serveur.	Le fichier <*URL* > est introuvable. L'adresse est incorrecte ou obsolète.

Nom de fichier et Titre de la notification	Description des notifications	Texte de la notification
ERR_FTP_SERVER_ERR Erreur du serveur FTP	Page d'erreur qui s'affiche pour les transactions FTP sur HTTP qui tentent d'accéder à un serveur qui ne prend pas en charge FTP. Le serveur renvoie généralement la réponse HTTP 501 « Not Implemented » (Non mis en œuvre).	Le système ne peut pas communiquer avec le serveur FTP <*hostname* >. Le serveur FTP peut être en panne de façon temporaire ou permanente, ou peut ne pas fournir ce service. Veuillez confirmer qu'il s'agit d'une adresse valide. Si elle est correcte, essayez d'exécuter cette demande plus tard.
ERR_FTP_SERVICE_ UNAVAIL Service FTP non disponible	Page d'erreur qui s'affiche pour les transactions FTP sur HTTP qui tentent d'accéder à un serveur FTP qui n'est pas disponible.	Le système ne peut pas communiquer avec le serveur FTP <*hostname* >. Le serveur FTP est peut-être occupé, en panne permanente ou ne fournit pas ce service. Veuillez confirmer qu'il s'agit d'une adresse valide. Si elle est correcte, essayez d'exécuter cette demande plus tard.
ERR_GATEWAY_TIMEOUT Expiration de la passerelle	Page d'erreur qui s'affiche lorsque le serveur demandé n'a pas reçu de réponse en temps opportun.	Le système ne peut pas communiquer avec le serveur externe <*hostname* >. Le serveur Internet est peut-être occupé, en panne permanente ou inaccessible en raison de problèmes de réseau. Veuillez vérifier l'orthographe de l'adresse Internet saisie. Si elle est correcte, essayez d'exécuter cette demande plus tard.
ERR_IDS_ACCESS_ FORBIDDEN Accès IDS interdit	Page de blocage qui s'affiche lorsque l'utilisateur tente de charger un fichier bloqué en raison d'une politique de sécurité des données Cisco configurée.	Votre demande de téléchargement a été bloquée en fonction des politiques de transfert de données de votre organisation. Détails des fichiers : <*file details* >
ERR_INTERNAL_ERROR Erreur interne	Page d'erreur qui s'affiche en cas d'erreur interne.	Erreur de système interne lors du traitement de la demande pour la page <*URL* >. Veuillez réessayer cette demande. Si ce problème persiste, veuillez communiquer avec <*contact name* > <*email address* > et lui communiquer le code indiqué ci-dessous.

Nom de fichier et Titre de la notification	Description des notifications	Texte de la notification
ERR_MALWARE_SPECIFIC Sécurité : programme malveillant détecté	Page de blocage qui s'affiche lorsqu'un programme malveillant est détecté lors du téléchargement d'un fichier.	Selon les politiques d'accès de votre entreprise, ce site Web <*URL* > a été bloqué, car il a été considéré comme une menace pour votre ordinateur ou le réseau de l'entreprise. Un programme malveillant <*nom* du programme malveillant> dans la catégorie <*catégorie du programme malveillant* > a été détecté sur ce site.
ERR_MALWARE_SPECIFIC_OUTGOING Sécurité : programme malveillant détecté	Page de blocage qui s'affiche lorsqu'un programme malveillant est détecté lors du chargement d'un fichier.	Conformément à la politique de votre organisation, le téléchargement du fichier vers l'URL (<*URL* >) a été bloqué, car il a été détecté que le fichier contenait des logiciels malveillants susceptibles de nuire à la sécurité du réseau du destinataire. Nom du programme malveillant : <*malware name* > Catégorie du programme malveillant : <*malware category* >
ERR_NATIVE_FTP_DENIED	Message de blocage affiché dans les clients FTP natifs lorsque la transaction FTP native est bloquée.	530 Connexion refusée
ERR_NO_MORE_FORWARDS Plus de transferts	Page d'erreur qui s'affiche lorsque l'appliance a détecté une boucle vers l'avant entre le proxy Web et un autre serveur proxy du réseau. Le proxy Web interrompt la boucle et affiche ce message pour le client.	La demande pour la page <*URL* > a échoué. Il se peut que l'adresse du serveur <*hostname* > ne soit pas valide ou vous devrez peut-être préciser un numéro de port pour accéder à ce serveur.
ERR_POLICY Politique : générale	Page de blocage qui s'affiche lorsque la demande est bloquée par un paramètre de politique.	Selon les politiques d'accès de votre organisation, l'accès au site Web <*URL* > a été bloqué.
ERR_PROTOCOL Politique : protocole	Page de blocage qui s'affiche lorsque la demande est bloquée en fonction du protocole utilisé.	Selon les politiques d'accès de votre organisation, cette demande a été bloquée, car le protocole de transfert de données « <*protocol type* > » n'est pas autorisé.

Nom de fichier et Titre de la notification	Description des notifications	Texte de la notification
ERR_PROXY_AUTH_REQUIRED Autorisation du proxy requise.	Page de notification qui s'affiche lorsque les utilisateurs doivent saisir leurs informations d'authentification pour continuer. Ceci est utilisé pour les demandes de transaction explicites.	Une authentification est requise pour accéder à Internet à l'aide de ce système. Un identifiant d'utilisateur et une phrase secrète valides doivent être saisis lorsque vous y êtes invité.
ERR_PROXY_PREVENT_MULTIPLE_LOGIN Déjà connecté à partir d'un autre appareil	Page de blocage qui s'affiche quand un utilisateur tente d'accéder au Web en utilisant le même nom d'utilisateur que celui qui est déjà authentifié auprès du proxy Web sur un autre appareil. Cette fonctionnalité est utilisée lorsque l'option d'authentification globale User Session Restrictions (Restrictions des sessions utilisateur) est activée.	Selon les politiques de votre organisation, la demande d'accès à Internet a été refusée, car cet identifiant d'utilisateur dispose d'une session active à partir d'une autre adresse IP. Si vous souhaitez vous connecter sous un nom d'utilisateur différent, cliquez sur le bouton ci-dessous et entrez un nom d'utilisateur et une phrase secrète différents.
ERR_PROXY_REDIRECT Rediriger	Page de redirection.	Cette demande est en cours de redirection. Si cette page n'est pas automatiquement redirigée, cliquez ici pour continuer.
ERR_PROXY_UNACKNOWLEDGED Politique : accusé de réception	Page de confirmation de l'utilisateur final. Pour en savoir plus, consultez Pages End-User Notification (Notification d'utilisateur final) , on page 7.	Veuillez accepter les déclarations suivantes avant d'accéder à Internet. Vos transactions Web seront automatiquement surveillées et traitées pour détecter le contenu dangereux et appliquer les politiques de l'entreprise. En cliquant sur le lien ci-dessous, vous reconnaissez cette supervision et acceptez que des données concernant les sites que vous visitez puissent être enregistrées. Il vous sera régulièrement demandé d'accepter la présence du système de supervision. Vous êtes responsable du respect des politiques de l'entreprise en matière d'accès à Internet. Cliquez ici pour accepter cette déclaration et accéder à Internet.

Nom de fichier et Titre de la notification	Description des notifications	Texte de la notification
ERR_PROXY_ UNLICENSED Proxy sans licence	Page de blocage qui s'affiche lorsqu'il n'y a pas de clé de licence valide pour le proxy Web Secure Web Appliance.	L'accès à Internet n'est pas disponible sans une licence appropriée du périphérique de sécurité. Veuillez communiquer avec <*contact name* > <*email address* > et lui indiquer le code présenté ci-dessous. **Note** Pour accéder à l'interface de gestion du périphérique de sécurité, entrez l'adresse IP configurée avec port.
ERR_RANGE_NOT_ SATISFIABLE Plage impossible à satisfaire	Page d'erreur qui s'affiche lorsque la plage d'octets demandée ne peut pas être traitée par le serveur Web.	Le système ne peut pas traiter cette demande. Un navigateur non standard a peut-être généré une requête HTTP non valide. Si vous utilisez un navigateur standard, réessayez la demande.
ERR_REDIRECT_ PERMANENT Redirection permanente	Page de redirection interne.	La page <*URL* > est redirigée vers <*redirected URL* >.
ERR_REDIRECT_REPEAT_ REQUEST Rediriger	Page de redirection interne.	Veuillez renouveler votre demande.
ERR_SAAS_AUTHENTICATION Politique : accès refusé	Page de notification qui s'affiche lorsque les utilisateurs doivent saisir leurs informations d'authentification pour continuer. Ceci est utilisé pour accéder aux applications.	Selon la politique de votre organisation, la demande d'accès à <*URL*> a été redirigée vers une page où vous devez saisir les coordonnées de connexion. Vous serez autorisé à accéder à l'application si l'authentification réussit et si vous disposez des privilèges appropriés.
ERR_SAAS_AUTHORIZATION Politique : accès refusé	Page de blocage qui s'affiche lorsque les utilisateurs tentent d'accéder à une application à laquelle ils n'ont pas accès.	Selon la politique de votre organisation, l'accès à l'application <*URL* > est bloqué, car vous n'êtes pas un utilisateur autorisé. Si vous souhaitez vous connecter sous un autre nom d'utilisateur, entrez un nom d'utilisateur et une phrase secrète différents pour l'utilisateur autorisé à accéder à cette application.

Nom de fichier et Titre de la notification	Description des notifications	Texte de la notification
ERR_SAML_PROCESSING Politique : accès refusé	Page d'erreur qui s'affiche lorsqu'un processus interne échoue en tentant de traiter l'URL de connexion unique pour accéder à une application.	La demande d'accès de <*nom d'utilisateur* > n'a pas été retenue, car des erreurs ont été trouvées au cours du processus de la demande de connexion unique.
ERR_SERVER_NAME_EXPANSION Extension du nom du serveur	Page de redirection interne qui développe automatiquement l'URL et redirige les utilisateurs vers l'URL mise à jour.	Le nom du serveur <*hostname* > semble être une abréviation et est redirigé vers <*redirected URL* >.
ERR_URI_TOO_LONG URI trop long	Page de blocage qui s'affiche lorsque la longueur de l'URL est trop longue.	L'URL demandée était trop longue et n'a pas pu être traitée. Il peut s'agir d'une attaque contre votre réseau. Veuillez communiquer avec <*contact name* > <*email address* > et lui indiquer le code présenté ci-dessous.
ERR_WBRS Sécurité : risque lié aux programmes malveillants	Page de blocage qui s'affiche lorsque les filtres de réputation Web bloquent le site en raison d'un faible score de réputation Web.	Selon les politiques d'accès de votre entreprise, ce site Web <*URL* > a été bloqué, car les filtres de réputation Web ont déterminé qu'il constitue une menace pour votre ordinateur ou le réseau de l'entreprise. Ce site Web a été associé à des programmes malveillants et espions. Type de menace : %o Motif de la menace : %O
ERR_WEBCAT Politique : filtrage d'URL	Page de blocage qui s'affiche lorsque les utilisateurs tentent d'accéder à un site Web dans une catégorie d'URL bloquée.	Selon les politiques d'accès de votre organisation, l'accès à ce site Web <*URL* > a été bloqué, car la catégorie Web « <*category type* > » n'est pas autorisée.
ERR_WWW_AUTH_REQUIRED Autorisation WWW requise.	Page de notification qui s'affiche lorsque le serveur demandé demande aux utilisateurs de saisir leurs informations d'authentification pour continuer.	Une authentification est requise pour accéder au site Web <*hostname* > demandé. Un identifiant d'utilisateur et une phrase secrète valides doivent être saisis lorsque vous y êtes invité.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.