CHAPTER 8

Web セキュリティ アプライアンスの管理

この章は、次の項で構成されています。

Web セキュリティ アプライアンスの管理の概要

AsyncOS for Security Management を使用すると、地理的に離れたネットワークにわたって、均一の Web セキュリティ ポリシーおよびカスタム URL カテゴリを適用できます。Web セキュリティ アプライアンスの設定は、Security Management アプライアンスの GUI から直接編集および公開できます。

Web セキュリティ アプライアンスの管理プロセスは次のとおりです。

ステップ 1 **Web セキュリティ アプライアンス。**AsyncOS 7.1 for Web にアップグレードします。『*Cisco IronPort AsyncOS 7.0 for Web User Guide*』または『*Cisco IronPort AsyncOS 7.1 for Web User Guide*』を参照してください。

ステップ 2 **Web セキュリティ アプライアンス。**ネットワーキング、認可、およびセキュリティ サービスを設定します。『*Cisco IronPort AsyncOS 7.1 for Web User Guide*』を参照してください。

「Configuration Master の使用に関する重要事項」（P.8-3）の設定要件を満たすようにしてください。

ステップ 3　**Web セキュリティ アプライアンス。**ポリシーの設定とテストを行います。『*Cisco IronPort AsyncOS 7.1 for Web User Guide*』を参照してください。

ステップ 4　**（任意）Web セキュリティ アプライアンス。**希望どおりの設定になったら、Web セキュリティ アプライアンスからコンフィギュレーション ファイルをダウンロードします。（このファイルを使用すると、Security Management アプライアンスの Configuration Master の設定を迅速化できます）。『*Cisco IronPort AsyncOS 7.1 for Web User Guide*』を参照してください。

コンフィギュレーション ファイルと Configuration Master のバージョンの互換性については、「表 2-5（WSA のある導入環境のみ）Configuration Master の互換性」（P.2-36）を参照してください。

ステップ 5　**Security Management アプライアンス。**Cisco IronPort 中央集中型コンフィギュレーション マネージャをイネーブルにします。「Security Management アプライアンスでのサービスのイネーブル化」（P.3-3）を参照してください。

ステップ 6　**Security Management アプライアンス。**Web セキュリティ アプライアンスを Security Management アプライアンスに追加します。「管理対象アプライアンスの追加」（P.3-11）を参照してください。

ステップ 7　**Security Management アプライアンス。**[Security Services] の設定を編集して、Web セキュリティ アプライアンスに現在設定されている状態に合わせます。「セキュリティ サービスの設定の編集」（P.8-4）を参照してください。

ステップ 8　**Security Management アプライアンス。**Configuration Master を初期化します。「Configuration Master の初期化」（P.8-8）を参照してください。

ステップ 9　**Security Management アプライアンス。**Web セキュリティ アプライアンスを Configuration Master に関連付けます。「Web セキュリティ アプライアンスと Configuration Master の関連付け」（P.8-8）を参照してください。

ステップ 10　**Security Management アプライアンス。**ポリシー、カスタム URL カテゴリ、Web プロキシ バイパス リストを Configuration Master にインポートするか、手動で設定します。「Configuration Master の設定」（P.8-10）を参照してください。

ステップ 11　**Security Management アプライアンス。**必要に応じて、Security Management アプライアンスのバックアップ、復元、アップグレードを行います。「Security Management アプライアンスのバックアップ」（P.12-8）を参照してください。

ステップ 12　**Security Management アプライアンス。**設定を Web セキュリティ アプライアンスに公開します。「Web セキュリティ アプライアンスへの設定の公開」（P.8-14）を参照してください。

Configuration Master の操作

Configuration Master を使用すると、特定の設定（特に、Web セキュリティ アプライアンスの [Web Security Manager] メニューの下の設定）を Web セキュリティ アプライアンスに公開できます。

AsyncOS for Security Management では、複数の Configuration Master が提供されるため、各種の機能を含むさまざまなバージョンの AsyncOS for Web Security を Web セキュリティ アプライアンスが実行している、異種の導入環境を集中管理することができます。

Security Management アプライアンスの GUI の [Web] セクション内にあるそれぞれの Configuration Master には、特定バージョンの AsyncOS for Web Security の設定が格納されています。

Configuration Master を設定するためのオプションについては、「Configuration Master の設定」（P.8-10）を参照してください。

Configuration Master の使用に関する重要事項

（注）　複数の Web セキュリティ アプライアンスがある場合は、それぞれの Web セキュリティ アプライアンスをチェックし、同名のレルムの設定が同一の場合を除いて、[Network] > [Authentication] のすべてのレルム名がアプライアンス間で一意になっていることを確認します。

（注）　Security Management アプライアンスは、互換性のある AsyncOS のバージョンを実行する Web セキュリティ アプライアンスにのみ Configuration Master を公開できます（たとえば、Web セキュリティ アプライアンスが AsyncOS 6.3 を実行している場合、それを Configuration Master 6.3 に割り当てます）。「管理対象アプライアンスの追加」（P.3-11）を参照してください。

セキュリティ サービスの設定の編集

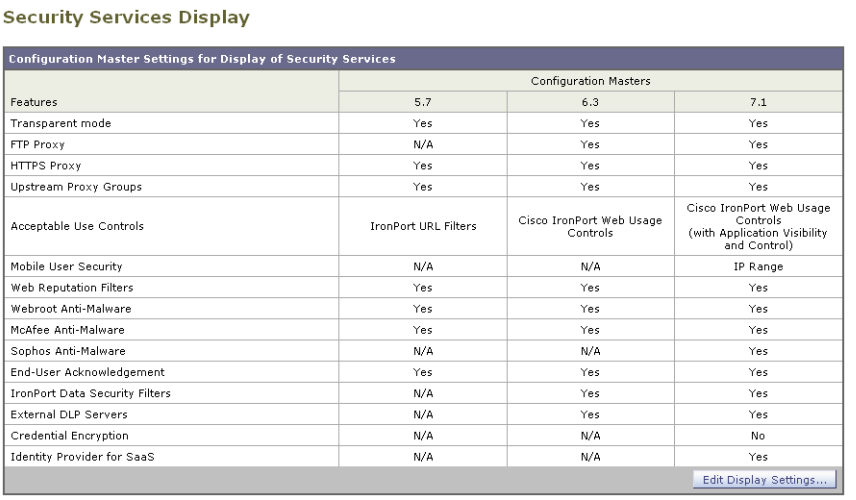
Configuration Master の使用を開始する前に、セキュリティ サービスの設定を編集して、Web セキュリティ アプライアンスの設定を反映するよう Configuration Master の表示をカスタマイズします。これらの設定により、Security Management アプライアンスでの設定に適切な機能を使用できるようになります。

デフォルトでは、[Web] > [Utilities] > [Security Services Display] ページに、すべての Configuration Master の設定が表示されます。機能に対して [N/A] とある場合、その機能は、そのバージョンの AsyncOS for Web Security で使用できないことを示します。

[Security Services Display] ページで選択されていない機能は、それらの機能が、Web セキュリティ アプライアンスでイネーブルにされていても、Configuration Master を使用して設定することはできません。

警告　**Configuration Master の設定を管理対象の Web セキュリティ アプライアンスに対して適切に公開するには、Configuration Master のセキュリティ サービスの設定が、Web セキュリティ アプライアンスでの設定と一致している必要があります。Configuration Master のセキュリティ サービスの設定を変更しても、Web セキュリティ アプライアンスの設定が自動的に変更されることはありません。Configuration Master の公開を行う前に、[Web] > [Utilities] > [Web Appliance Status] ページをチェックして、セキュリティ サービスの設定と Web セキュリティ アプライアンスでの設定の間に不一致がないか調べることをお勧めします（「Web セキュリティ アプライアンスのステータスの表示」（P.8-23）を参照）。不一致に気づいた場合は、セキュリティ サービスの設定（「セキュリティ サービスの設定の編集」（P.8-4）を参照）、または Web セキュリティ アプライアンスでの設定のいずれかを変更する必要があります。**

図 8-1　[Security Services Display] ページ



Security Services Display

Configuration Master Settings for Display of Security Services

Features	Configuration Masters		
	5.7	6.3	7.1
Transparent mode	Yes	Yes	Yes
FTP Proxy	N/A	Yes	Yes
HTTPS Proxy	Yes	Yes	Yes
Upstream Proxy Groups	Yes	Yes	Yes
Acceptable Use Controls	IronPort URL Filters	Cisco IronPort Web Usage Controls	Cisco IronPort Web Usage Controls (with Application Visibility and Control)
Mobile User Security	N/A	N/A	IP Range
Web Reputation Filters	Yes	Yes	Yes
Webroot Anti-Malware	Yes	Yes	Yes
McAfee Anti-Malware	Yes	Yes	Yes
Sophos Anti-Malware	N/A	N/A	Yes
End-User Acknowledgement	Yes	Yes	Yes
IronPort Data Security Filters	N/A	Yes	Yes
External DLP Servers	N/A	Yes	Yes
Credential Encryption	N/A	N/A	No
Identity Provider for SaaS	N/A	N/A	Yes

Edit Display Settings...

セキュリティ サービスの設定を編集するには、次の手順を実行します。

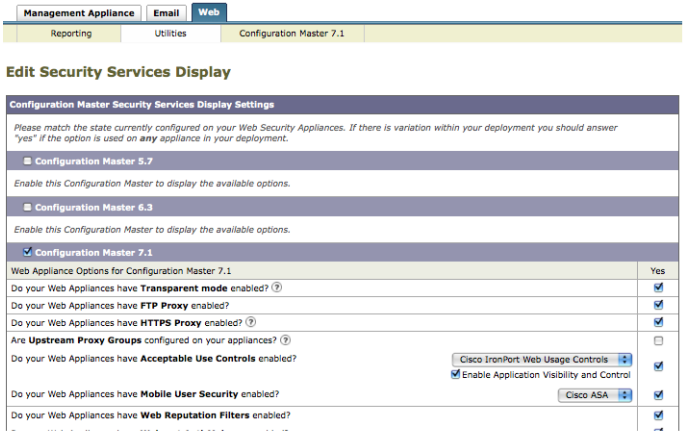
ステップ 1　Security Management アプライアンスで、[Web] > [Utilities] > [Security Services Display] を選択します。

ステップ 2　[Edit Settings] をクリックします。

[Edit Security Services Display] ページが表示され、Configuration Master に表示される機能がリストされます。

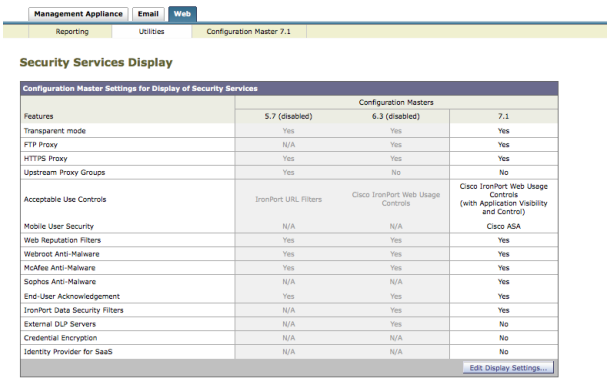
（注）　Web Proxy は機能としてリストされていません。Web Proxy は Web セキュリティ アプライアンスの管理対象ポリシー タイプのいずれかを実行するために、イネーブルになっていると見なされるからです。Web Proxy がディセーブルの場合は、Web セキュリティ アプライアンスに公開されるすべてのポリシーが無視されます。

ステップ 3　（任意）Configuration Master のいずれかを使用しない場合は、それを非表示にするために、[Edit Security Services Display] ページで対応する Configuration Master のチェックボックスをオフにします。



（注） Configuration Master を非表示にすると、それに対するすべての参照が、対応する [Configuration Master] タブを含む GUI から削除されます。Configuration Master を使用する保留中の公開ジョブは削除され、非表示のすべての Configuration Master に割り当てられている Web セキュリティ アプライアンスが、未割り当てとして再分類されます。少なくとも 1 つの Configuration Master をイネーブルにする必要があります。

たとえば、Configuration Master 5.7 および 6.3 がディセーブルにされている [Security Services Display] ページは、次のようになります。



ステップ 4　機能が Web セキュリティ アプライアンスでイネーブルにされているかどうかを反映するため、[Yes] チェックボックスをオンまたはオフにします。導入環境内で設定が一定でない場合は、導入された*いずれか*のアプライアンスで機能がイネーブルにされていれば、このチェックボックスを選択します。

機能は次のとおりです。

- トランスペアレント プロキシ モード。フォワード モードを使用した場合、プロキシ バイパス機能は使用できなくなります。
- FTP プロキシ。*Configuration Master 6.3 および 7.1 のみ。*
- HTTPS プロキシ。HTTPS プロキシは、復号ポリシーを実行するためにイネーブルにする必要があります。
- アップストリーム プロキシ グループ。ルーティング ポリシーを使用する場合は、Web セキュリティ アプライアンスでアップストリーム プロキシ グループが使用できるようになっている必要があります。
- 許容範囲内の使用制御。使用するサービスとして、Cisco IronPort URL Filters または Cisco IronPort Web Usage Controls を選択します。
- Web レピュテーション フィルタ。
- Webroot アンチマルウェア。
- McAfee アンチマルウェア。
- エンド ユーザ承認。
- Cisco IronPort データ セキュリティ フィルタ。*Configuration Master 6.3 および 7.1 のみ。*
- 外部 DLP サーバ。*Configuration Master 6.3 および 7.1 のみ。*

ステップ 5　[Submit] をクリックします。セキュリティ サービスの設定に加えた変更が、Web セキュリティ アプライアンスで設定されたポリシーに影響する場合、GUI に特定の警告メッセージが表示されます。変更を送信することが確実な場合は、[Continue] をクリックします。

ステップ 6　[Security Services Display] ページで、選択した各オプションの横に [Yes] と表示されることを確認します。

ステップ 7　[Submit] をクリックし、[Commit] をクリックして変更を確定します。

Configuration Master の初期化

ステップ 1　メイン Security Management アプライアンスで、[Web] > [Utilities] > [Configuration Masters] を選択します。

[Configuration Master] ページが表示されます。

ステップ 2　[Options] カラムの [Initialize] をクリックします。

ステップ 3　[Configuration Master] ページで次の操作を実行します。

- 以前のリリースに対する既存の Configuration Master があり、その同じ設定を新しい Configuration Master に使用するか、その設定で開始する場合は、[Copy Configuration Master] を選択します。

  Configuration Master のバージョンの互換性については、「表 2-5（WSA のある導入環境のみ）Configuration Master の互換性」（P.2-36）を参照してください。
- そうでない場合は、[Use default settings] を選択します。

ステップ 4　[Initialize] をクリックします。

これで Configuration Master が使用可能な状態になります。

Web セキュリティ アプライアンスと Configuration Master の関連付け

集中管理するそれぞれの Web セキュリティ アプライアンスについて、ポリシー設定を、そのアプライアンスの AsyncOS バージョンと一致する Configuration Master に関連付ける必要があります。たとえば、Web セキュリティ アプライアンスが AsyncOS 6.3 for Web を実行中の場合は、それを Configuration Master 6.3 に関連付ける必要があります。これは、Web セキュリティ アプライアンスを Security Management アプライアンスに追加するとき（「管理対象アプライアンスの追加」（P.3-11）を参照）、または [Web] > [Utilities] > [Configuration Masters] ページで行うことができます。

このリリースでは、5.7、6.3、7.1 の 3 つの Configuration Master が使用可能です。

（注）　Web セキュリティ アプライアンスを Configuration Master に関連付けても、新しい設定がアプライアンスに自動的に公開されることはありません。設定は、手動でアプライアンスに公開する必要があります。「Web セキュリティ アプライアンスへの設定の公開」（P.8-14）を参照してください。

アプリケーションを Configuration Master に関連付けるには、次の手順を実行します。

ステップ 1　メイン Security Management アプライアンスで、[Web] > [Utilities] > [Configuration Masters] を選択します。

[Configuration Master] ページが表示されます。

ステップ 2　[Edit Appliance Assignment List] をクリックして、[Configuration Master Assignments] ページを表示します。

ステップ 3　関連付けるアプライアンスの行でクリックし、[Masters] カラムにチェックマークを入れます。

（注）　Configuration Master が非表示の場合、ページにその Configuration Master のカラムは表示されません。非表示の Configuration Master をイネーブルにするには、[Web] > [Utilities] > [Security Services Display] に移動します。「セキュリティ サービスの設定の編集」（P.8-4）を参照してください。

ステップ 4　[Submit] をクリックし、[Commit] をクリックして変更を確定します。

（注）　Configuration Master のアップグレード方法、またはアプライアンスに関連付ける方法の例については、「例 5：既存の Security Management アプライアンスでの新しい Configuration Master へのアップグレード」（P.D-16）を参照してください。

Configuration Master の設定

Configuration Master を設定するには、次のようにいくつかの方法があります。

- 以前のリリースからのアップグレードの場合：以前の既存の Configuration Master を新しい Configuration Master のバージョンにコピーまたはインポートします。
- Web セキュリティ アプライアンスをすでに設定してあり、同じ設定を複数の Web セキュリティ アプライアンスに使用する場合：すでに設定済みの Web セキュリティ アプライアンスからコンフィギュレーション ファイルをインポートします。

  「Configuration Master への既存の Web セキュリティ アプライアンス設定の取り込み」（P.8-10）を参照してください。
- ポリシー、URL カテゴリ、バイパス設定を Web セキュリティ アプライアンスでまだ設定していない場合は、該当する Configuration Master を Security Management アプライアンスで設定します。

  詳細については、「Configuration Master を使用した Web セキュリティ機能の設定について」（P.8-12）を参照してください。

（注） Configuration Master に加えた変更は、編集した設定を公開するまで、その Configuration Master に割り当てられた Web セキュリティ アプライアンスに適用されません。「Web セキュリティ アプライアンスへの設定の公開」（P.8-14）を参照してください。

Configuration Master への既存の Web セキュリティ アプライアンス設定の取り込み

すでに実際に設定があり、それを Web セキュリティ アプライアンスの 1 つから使用する場合には、コンフィギュレーション ファイルを Security Management アプライアンスにインポートして、Configuration Master にデフォルトのポリシー設定を作成できます。Configuration Master は、同じバージョンの Web セキュリティ アプライアンスからのコンフィギュレーション ファイルを受け入れます。

たとえば、Configuration Master に XML ファイルをロードする場合、そのファイルは、Configuration Master 自体と同じバージョンからのものにする必要があります。つまり、6.3 の Configuration Master に取り込むことができるのは、6.3 マシンからのファイルのみです。また、7.1 の Configuration Master に取り込むことができるのは、7.1 マシンからのファイルのみです。

コンフィギュレーション ファイルと Configuration Master のバージョンの互換性については、「表 2-5（WSA のある導入環境のみ）Configuration Master の互換性」（P.2-36）を参照してください。

警告　**管理対象の Web セキュリティ アプライアンスに設定をすでに公開してある場合でも、互換性のある Web コンフィギュレーション ファイルを何回でもインポートすることができます。ただし、コンフィギュレーション ファイルを Configuration Master にインポートすると、選択した Configuration Master に関連付けられている設定が上書きされることに注意してください。また、[Security Services Display] ページのセキュリティ サービスの設定は、インポートしたファイルと一致するよう設定されます。**

Configuration Master に Web コンフィギュレーション ファイルを取り込むには、次の手順を実行します。

ステップ 1　Web セキュリティ アプライアンスからコンフィギュレーション ファイルを保存します。

ステップ 2　メイン Security Management アプライアンスで、[Web] > [Utilities] > [Configuration Masters] を選択します。

ステップ 3　[Options] カラムで、[Import Configuration] を選択します。

[Import Web Configuration] ページが表示されます。この例では、Configuration Master 7.1 が選択されています。

ステップ 4　[Select Configuration] ドロップダウン リストから、[Web Configuration File] を選択します。

図 8-2　[Import Web Configuration] ページ

ステップ 5　[New Master Defaults] セクションで、[Browse] をクリックし、Web セキュリティ アプライアンスから有効なコンフィギュレーション ファイルを選択します。

ステップ 6　[Import File] をクリックします。

ステップ 7　[Import] をクリックしてインポート プロセスに進むか、[Cancel] をクリックします。

Configuration Master を使用した Web セキュリティ機能の設定について

Web セキュリティ アプライアンスの機能を Security Management アプライアンスの GUI で直接設定して、その設定変更を、Configuration Master に割り当てられている Web セキュリティ アプライアンスに公開することができます。

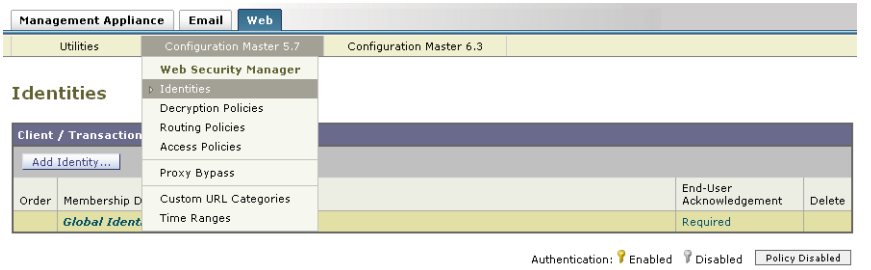
Security Management アプライアンスの GUI の [Web] セクション内にあるそれぞれの Configuration Master には、特定バージョンの AsyncOS for Web Security の設定が格納されています。このリリースの AsyncOS for Security Management には、AsyncOS 5.7 for Web Security、AsyncOS 6.3 for Web Security、および AsyncOS 7.1 for Web Security をサポートしている Configuration Master が含まれています。

Configuration Master 5.7 の使用

Configuration Master 5.7 を使用すると、ID、復号化ポリシー、ルーティング ポリシー、アクセス ポリシー、および時間ベースのポリシーを設定したり、Web プロキシをバイパスしたり、カスタム URL カテゴリを作成したりできます。

これらの機能を Configuration Master で設定する方法は、Web セキュリティ アプライアンスで設定する方法と同じです。『*Cisco IronPort AsyncOS for Web User Guide*』を参照してください。

図 8-3　Configuration Master 5.7

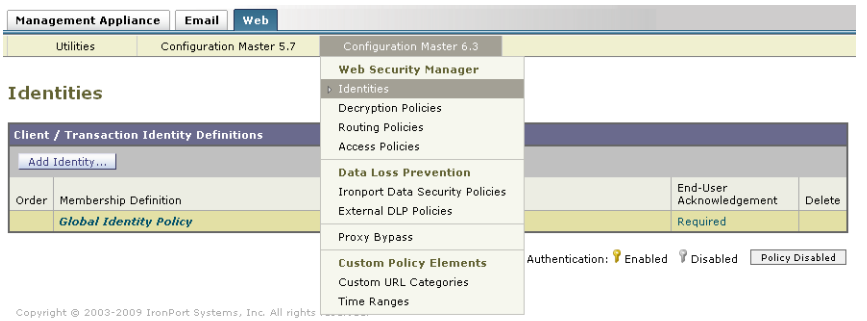


Configuration Master 6.3 の使用

Configuration Master 6.3 を使用すると、ID、復号化ポリシー、ルーティング ポリシー、アクセス ポリシー、時間ベースのポリシー、Cisco IronPort データ セキュリティ ポリシー、および外部 DLP ポリシーを設定したり、Web プロキシをバイパスしたり、カスタム URL カテゴリを作成したりできます。

これらの機能を Configuration Master で設定する方法は、Web セキュリティ アプライアンスで設定する方法と同じです。『*Cisco IronPort AsyncOS for Web User Guide*』を参照してください。

図 8-4　Configuration Master 6.3



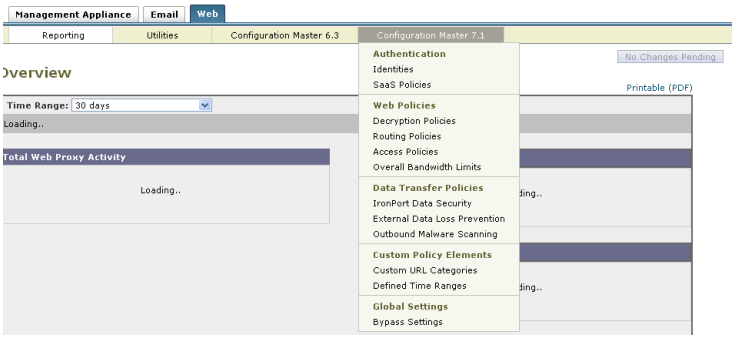
Configuration Master 7.1 の使用

Security Management アプライアンスで、Configuration Master 7.1 がサポートされるようになりました。Configuration Master 7.1 を使用すると、認証 ID、SaaS ポリシーを設定したり、復号化ポリシー、ルーティング ポリシー、アクセ

ス ポリシー、定義済みの時間範囲、および全体的な帯域幅制限を含む Web ポリシーを定義したりできます。また、この Configuration Master には、AVC、Sophos、クレデンシャル暗号化、Mobile User Security（MUS）も含まれています。さらに、Cisco IronPort データ セキュリティ ポリシーや外部 DLP ポリシーを定義したり、Web プロキシをバイパスしたり、外部 URL ポリシーを含むカスタム URL カテゴリを作成することもできます。

これらの機能を Configuration Master で設定する方法は、Web セキュリティ アプライアンスで設定する方法と同じです。『*Cisco IronPort AsyncOS for Web User Guide*』を参照してください。

図 8-5　Configuration Master 7.1



Web セキュリティ アプライアンスへの設定の公開

AsyncOS for Security Management には、2 種類の設定公開方法があります。どちらのタイプも Configuration Master の GUI で同じページから開始し、両方のタイプを何回でも実行できますが、それぞれのタイプで結果は異なるものになります。

Configuration Master の公開

Configuration Master で設定を編集した後で、その設定を、Configuration Master に関連付けられている Web セキュリティ アプライアンスへ公開できます。

Configuration Master を使用して編集できるのは、ポリシー（アクセス、復号化、SaaS、L4 Traffic Manager、ルーティングおよび ID を含む）、プロキシ バイパス リスト、発信マルウェア スキャン、時間範囲、ポリシー タグ、URL タグ、カスタム URL カテゴリ、FTP プロキシ（Configuration Master 6.3 および 7.1 のみ）、Cisco IronPort データ セキュリティ フィルタ（Configuration Master 6.3 および 7.1 のみ）、および外部 DLP サーバ（Configuration Master 6.3 および 7.1 のみ）という Web セキュリティ アプライアンスの設定変数のみです。

Configuration Master を使用して他の設定変数（たとえば、ユーザ、アラート、およびログ サブスクリプション）を編集することはできません。

Configuration Master を公開すると、その Configuration Master に関連付けられている Web セキュリティ アプライアンスで、既存のポリシー情報が上書きされます。

（注） Security Management アプライアンスから、RSA サーバ用に設定されていない複数の Web セキュリティ アプライアンスに、外部 DLP ポリシーを公開しても問題ありません。公開しようとすると、Security Management アプライアンスから、次の公開ステータス警告が送信されます。「**The Security Services display settings configured for Configuration Master 7.1 do not currently reflect the state of one or more Security Services on Web Appliances associated with this publish request.The affected appliances are: "[***WSA Appliance Name***]".This may indicate a misconfiguration of the Security Services display settings for this particular Configuration Master.Go to the Web Appliance Status page for each appliance provides a detailed view to troubleshooting this issue.Do you want to continue publishing the configuration now?**」

公開を続行した場合、RSA サーバ用に設定されていない Web セキュリティ アプライアンスは、外部 DLP ポリシーを受信しますが、これらのポリシーはディセーブルにされます。外部 DLP サーバが設定されていない場合、Web セキュリティ アプライアンスの [External DLP] ページには公開されたポリシーが表示されません。

「Configuration Master の公開」（P.8-16）を参照してください。Configuration Master の詳細については、「Configuration Master の操作」（P.8-3）を参照してください。

拡張ファイル公開

拡張ファイル公開は、Configuration Master の公開とは完全に独立しています。また、[Configuration Master Publish] セクションにリストされている設定のいずれにも影響を与えません。さらに、ネットワーク/インターフェイス設定、DNS、SNTPD、WCCP、アップストリーム プロキシ グループ、証明書、プロキシ モード、時間設定、L4TM 設定、認証リダイレクト ホスト名にも影響を与えません。

拡張ファイル公開を使用して、互換性のある XML コンフィギュレーション ファイルを、ローカル ファイル システムから管理対象の Web セキュリティ アプライアンスにプッシュします。

拡張ファイル公開は、ポリシー以外の設定変数のみ（たとえば、ユーザ、アラート、ログ サブスクリプション）を上書きします。拡張ファイル公開を使用して、管理対象の Web セキュリティ アプライアンスでポリシー情報を変更することはできません。つまり、Configuration Master の公開によって設定を変更できる場合、拡張ファイル公開を使用してその変更を行うことはできません。

「拡張ファイル公開の使用」（P.8-20）を参照してください。

（注） 公開タイプが Web セキュリティ アプライアンスでのネットワーク設定に影響することもありません。ネットワーク設定は、管理対象の Web セキュリティ アプライアンスで直接設定する必要があります。『*Cisco IronPort AsyncOS for Web User Guide*』を参照してください。

Configuration Master の公開

（注） 6.3 を実行中のアプライアンスを、5.7 の Configuration Master に割り当てることができます。バージョンは同一である必要はありませんが、アプライアンスのバージョンよりも新しい Configuration Master に、そのアプライアンスを割り当てることはできません。

警告 **Configuration Master の設定を管理対象の Web セキュリティ アプライアンスに対して適切に公開するには、Configuration Master の許容範囲内の使用制御が、Web セキュリティ アプライアンスの設定と一致している必要があります。Configuration Master のこれらの設定を変更しても、Web セキュリ**

ティ アプライアンスの設定が自動的に変更されることはありません。Configuration Master の公開を行う前に、[Web] > [Utilities] > [Web Appliance Status] ページをチェックして、許容範囲内の使用の設定と Web セキュリティ アプライアンスでの設定の間に不一致がないか調べることをお勧めします（「Web セキュリティ アプライアンスのステータスの表示」（P.8-23）を参照）。それらが一致しない場合、公開は失敗します。その他のすべての不一致では、それらのポリシーが使用不可になり、その詳細は [Publish History] ページで確認できます。不一致に気づいた場合は、許容範囲内の使用制御の設定（「セキュリティ サービスの設定の編集」（P.8-4）を参照）か、Web セキュリティ アプライアンスでの設定かのいずれかを変更する必要があります。

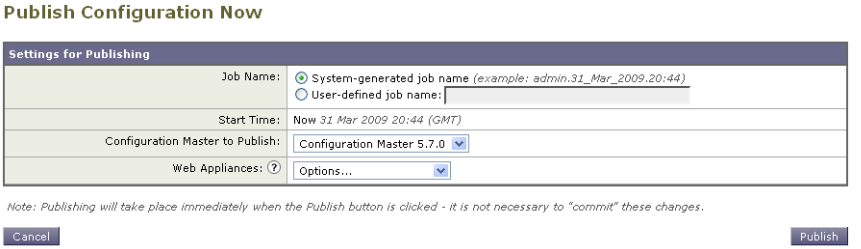
Configuration Master を Web セキュリティ アプライアンスに今すぐ公開するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Web] > [Utilities] > [Publish to Web Appliances] を選択します。

ステップ 2　[Publish Configuration Now] をクリックします。

[Publish Configuration Now] ページが表示されます。

図 8-6　[Publish Configuration Now] ページ



ステップ 3　デフォルトでは [System-generated job name] が選択されています。あるいは、ユーザ定義のジョブ名（80 文字以下）を入力します。

ステップ 4　公開する Configuration Master を選択します。

あるいは、拡張ファイル公開を実行する場合は、[Advanced file options] を選択します。「拡張ファイル公開の使用」（P.8-20）を参照してください。

ステップ 5　Configuration Master の公開先となる Web セキュリティ アプライアンスを選択します。Configuration Master に割り当てられているすべてのアプライアンスに設定を公開するには、[All assigned appliances] を選択します。

または

Configuration Master に割り当てられているアプライアンスのリストを表示するには、[Select appliances in list] を選択します。設定の公開先となるアプライアンスを選択します。

ステップ 6　[Publish] をクリックします。[Publish in Progress] ページが表示されます。赤いの経過表示バーとテキストは、公開中にエラーが発生したことを示しています。別のジョブが現在公開中の場合、要求は前のジョブが完了すると実行されます。

（注）　進行中のジョブの詳細は、[Web] > [Utilities] > [Publish to Web Appliances] ページにも表示されます。[Publish in Progress] にアクセスするには、[Check Progress] をクリックします。

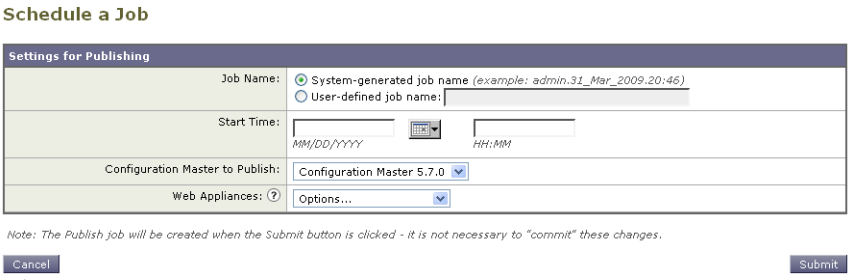
Configuration Master を後で Web セキュリティ アプライアンスに公開するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Web] > [Utilities] > [Publish to Web Appliances] を選択します。

ステップ 2　[Schedule a Job] をクリックします。

[Schedule a Job] ページが表示されます。

図 8-7　[Schedule a Job] ページ



ステップ 3　デフォルトでは [System-generated job name] が選択されています。あるいは、ユーザ定義のジョブ名（80 文字以下）を入力します。

ステップ 4　Configuration Master を公開する日時を入力します。

ステップ 5　公開する Configuration Master を選択します。

あるいは、拡張ファイル公開を実行する場合は、[Advanced file options] を選択します。「拡張ファイル公開の使用」（P.8-20）を参照してください。

ステップ 6　Configuration Master の公開先となる Web セキュリティ アプライアンスを選択します。Configuration Master に割り当てられているすべてのアプライアンスに設定を公開するには、[All assigned appliances] を選択します。

または

Configuration Master に割り当てられているアプライアンスのリストを表示するには、[Select appliances in list] を選択します。設定の公開先となるアプライアンスを選択します。

ステップ 7　[Submit] をクリックします。

ステップ 8　スケジュールされているジョブのリストは、[Web] > [Utilities] > [Publish to Web Appliances] ページに表示されます。スケジュールされているジョブを編集するには、そのジョブの名前をクリックします。保留中のジョブをキャンセルするには、対応するごみ箱アイコンをクリックして、ジョブの削除を確認します。

publishconfig コマンドの使用

Security Management アプライアンスでは、次の CLI コマンドを使用して Configuration Master の変更を公開できます。

publishconfig config_master [--*job_name*] [--*host_list* | *host_ip*]

ここで、**config_master** は 5.7、6.3、または 7.1 のいずれかです。このキーワードは必須です。*job_name* オプションは省略可能で、指定しなかった場合は生成されます。

host_list オプションは、公開する Web セキュリティ アプライアンスのホスト名または IP アドレスのリストで、指定しなかった場合は Configuration Master に割り当てられているすべてのホストに公開されます。*host_ip* オプションには、カンマで区切って複数のホスト IP アドレスを指定できます。

publishconfig コマンドが成功したことを確認するには、**smad_logs** ファイルを調べます。[Web] > [Utilities] > [Web Appliance Status] を選択することで、Security Management アプライアンスの GUI から公開履歴が成功だったことを確認することもできます。このページから、公開履歴の詳細を調べる Web アプライアンスを選択します。また、[Web] > [Utilities] > [Publish] > [Publish History] により、[Publish History] ページに進むことができます。

拡張ファイル公開の使用

拡張ファイル公開を実行するには、次のいずれかを選択します。

- 「拡張ファイル公開：[Publish Configuration Now]」（P.8-20）
- 「拡張ファイル公開：[Publish Later]」（P.8-21）

拡張ファイル公開：[Publish Configuration Now]

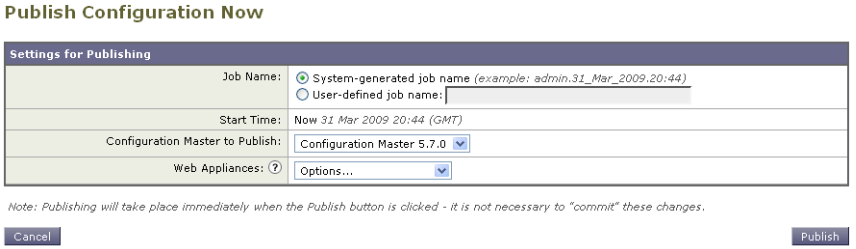
拡張ファイル公開の [Publish Configuration Now] を実行するには、次の手順に従います。

ステップ 1　メイン Security Management アプライアンスのウィンドウで、[Web] > [Utilities] > [Publish to Web Appliances] を選択します。

ステップ 2　[Publish Configuration Now] をクリックします。

[Publish Configuration Now] ページが表示されます。

図 8-8　[Publish Configuration Now] ページ



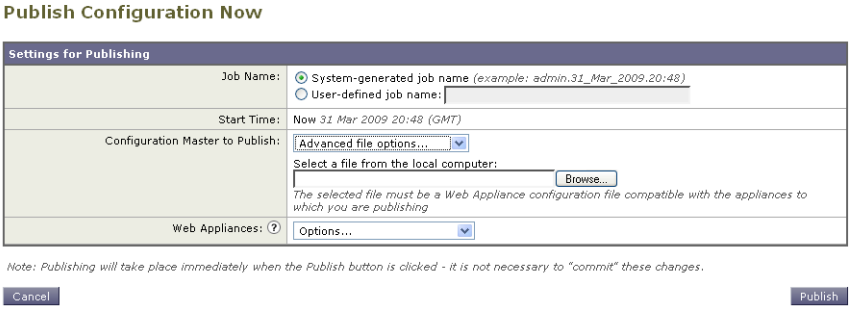
ステップ 3　デフォルトでは [System-generated job name] が選択されています。あるいは、ユーザ定義のジョブ名（80 文字以下）を入力します。

ステップ 4　[Advanced file options] を選択します。

ステップ 5　[Browse] をクリックし、公開するファイルを選択します。

[Publish Configuration Now] ページが表示されます。

図 8-9　[Publish Configuration Now] ページ



ステップ 6　[Web Appliances] ドロップダウン リストから、[Select appliances in list] または [All assigned to Master] を選択して、コンフィギュレーション ファイルの公開先となるアプライアンスを選択します。

ステップ 7　[Publish] をクリックします。

拡張ファイル公開：[Publish Later]

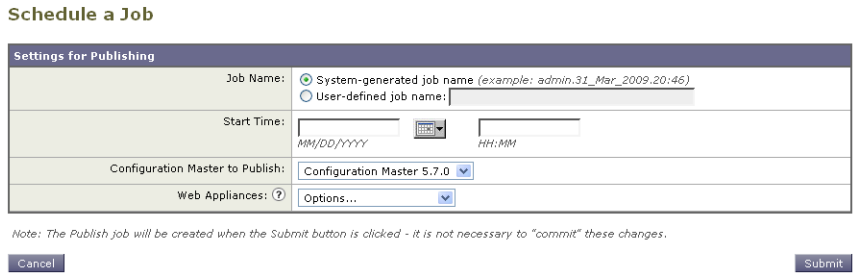
拡張ファイル公開の [Publish Later] を実行するには、次の手順に従います。

ステップ 1　Security Management アプライアンスで、[Web] > [Utilities] > [Publish to Web Appliances] を選択します。

ステップ 2　[Schedule a Job] をクリックします。

[Schedule a Job] ページが表示されます。

図 8-10　[Schedule a Job] ページ

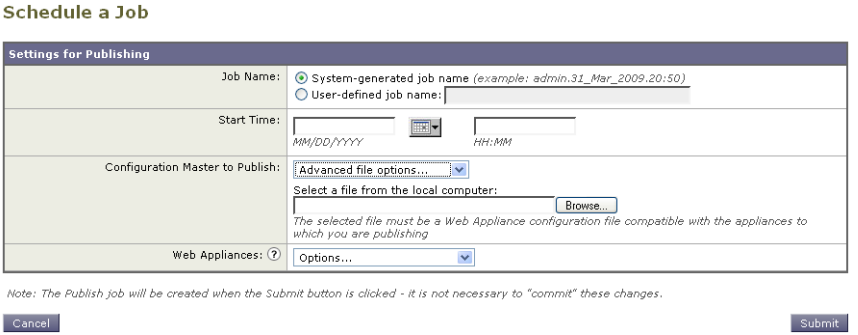


ステップ 3　デフォルトでは [System-generated job name] が選択されています。あるいは、ユーザ定義のジョブ名（80 文字以下）を入力します。

ステップ 4　設定を公開する日時を入力します。

ステップ 5　[Advanced file options] を選択して [Browse] をクリックし、公開するファイルを選択します。

図 8-11　[Schedule a Job] ページ : [Advanced File Options]



ステップ 6　[Web Appliances] ドロップダウン リストから、[Select appliances in list] または [All assigned to Master] を選択して、コンフィギュレーション ファイルの公開先となるアプライアンスを選択します。

ステップ 7　[Publish] をクリックします。

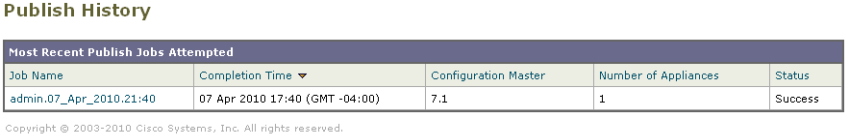
公開履歴の表示

公開履歴を表示すると、公開中に発生した可能性のあるエラーのチェックに役立ちます。

公開履歴を表示するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Web] > [Utilities] > [Publish History] を選択します。

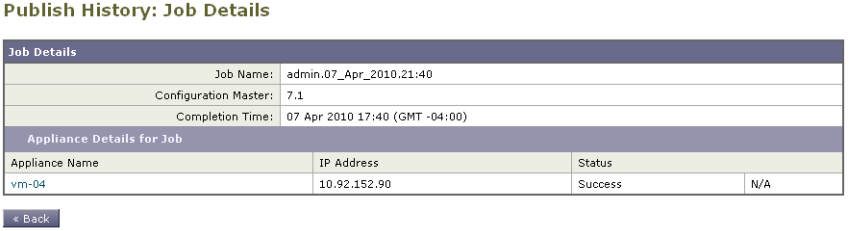
[Publish History] ページが表示されます。



[Publish History] ページには、試行された最近のすべての公開ジョブがリストされます。カラム情報には、ジョブ名、ジョブ完了時刻、使用された Configuration Master（または、拡張ファイル公開を実行した場合は XML コンフィギュレーション ファイルの名前）、ジョブの公開先にしたアプライアンスの数、およびステータス（[Success] または [Failure]）があります。

特定のジョブに関してさらに詳細を表示するには、[Job Name] カラムで特定のジョブ名のハイパーテキスト リンクをクリックします。

[Publish History: Job Details] ページが表示されます。



[Publish History: Job Details] ページでは、アプライアンス名をクリックすることにより、[Web] > [Utilities] > [Web Appliance Status] ページを表示して、ジョブの特定のアプライアンスに関する追加の詳細を表示できます。ジョブの特定のアプライアンスに関するステータスの詳細を表示することもでき、対応する [Details] リンクをクリックして [Web Appliance Publish Details] ページに詳細を表示します。

Web セキュリティ アプライアンスのステータスの表示

AsyncOS には、2 つの Web セキュリティ アプライアンス ステータス レポートがあります。1 つは Security Management アプライアンスに接続された Web セキュリティ アプライアンスの概略サマリーを示すもので、もう 1 つは接続され

た各 Web セキュリティ アプライアンスのステータスの詳細ビューです。ステータス情報としては、接続されている Web セキュリティ アプライアンスに関する一般情報、それらの公開された設定、公開履歴などがあります。

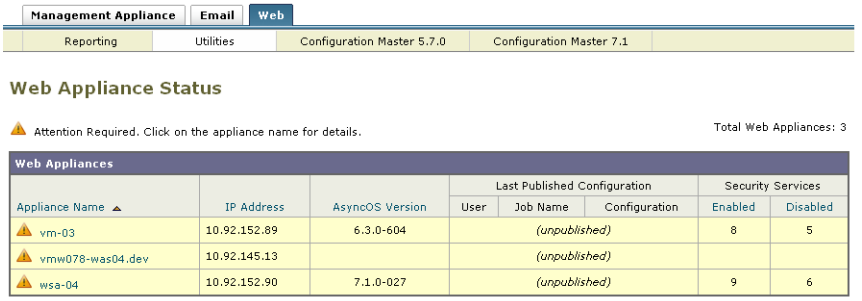
（注）　Security Management アプライアンスに追加するすべての Web アプライアンスは、[Web] > [Utilities] > [Web Appliance Status] ページにエントリが表示されます。ただし、表示可能なデータがあるのは、集中管理をサポートするマシンのみです。管理がサポートされるバージョンは、6.0 を除く、5.7 以降のすべてのバージョンの Web セキュリティ アプライアンスです。したがって、5.7、6.3、または 7.1 を実行中のすべてのアプライアンスはデータが表示されます。6.0 バージョンでは、使用可能な情報がないことを示すエラー メッセージが表示されます。

Web セキュリティ アプライアンスのステータスを表示するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Web] > [Utilities] > [Web Appliances Status] を選択します。

[Web Appliances Status] ページが表示されます。

図 8-12　[Web Appliances Status] ページ



[Web Appliance Status] ページには、接続されている Web セキュリティ アプライアンスのリストが、アプライアンス名、IP アドレス、AsyncOS バージョン、最後に公開された設定情報（ユーザ、ジョブ名、コンフィギュレーション バージョン）、使用可能または使用不可にされているセキュリティ サービスの数、お

よび接続しているアプライアンスの総数（最大 150）とともに表示されます。警告アイコンは、接続されたアプライアンスの 1 つに注意が必要なことを示しています。

（注）　Web セキュリティ アプライアンスで発生した最新の設定変更が [Web Appliance Status] ページに反映されるまでに、数分かかることがあります。データをすぐに更新するには、[Refresh Data] リンクをクリックします。ページのタイム スタンプは、データが最後にリフレッシュされた時刻を示しています。

Web セキュリティ アプライアンスのステータスに関する詳細を表示するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Web] > [Utilities] > [Web Appliances Status] を選択します。

ステップ 2　表示するアプライアンスの名前をクリックします。

詳細には次の情報が含まれます。

- システム ステータス情報（稼動時間、アプライアンスのモデルおよびシリアル番号、AsyncOS バージョン、ビルドの日付、AsyncOS インストールの日時、ホスト名）
- 設定公開履歴（公開日時、ジョブ名、コンフィギュレーション バージョン、公開の結果、ユーザ）
- Web セキュリティ機能（機能説明、設定のサマリー、セキュリティ サービスの設定、機能キーのステータス）
- プロキシ設定（アップストリーム プロキシとプロキシの HTTP ポート）
- 認証サービス（認証レルムの名前/プロトコル/サーバ、認証シーケンスでのレルムの名前と順序、認証失敗時にトラフィックをブロックするか許可するか）

ステップ 3　詳細を更新するには、たとえば、新しいアプライアンスを追加した場合、またはアプライアンスの情報がまだ使用できないことを示すメッセージが表示された場合には、[Refresh Data] リンクをクリックします。ページのタイム スタンプは、データが最後にリフレッシュされた時刻を示しています。

特定の Web セキュリティ アプライアンスに関するきめ細かな詳細を確認するには、[Web Appliance] カラムのハイパーテキスト リンクをクリックします。次のページが表示されます。

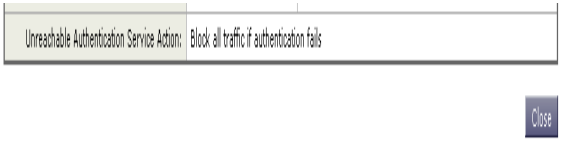


図 8-13　[Web Appliance Status Details] ページ

Appliance Status: vmw095-wsa11.sma (vmw095-wsa11.sma)

Data Refreshed: 06 Aug 2010 21:55 (GMT +03:00) — Refresh Data

Appliance Status

System

Uptime:	8 hours, 53 mins, 52 secs Up since: 06 Aug 2010 13:01 (GMT +03:00)
Model:	S10
Serial Number:	000C29BEA7DC-vmware
AsyncOS Version:	7.1.0-265 for Web
Build Date:	2010-08-05
AsyncOS Install Date/Time:	2010-08-06 13:27:57
Configured Time Zone:	Europe/Kiev
Host Name:	vmw095-wsa11.sma

Centralized Configuration Manager

Configuration Publish History:	Publish Date/Time	Job Name	Configuration Version	Result	User
	06 Aug 2010 14:56 (GMT +03:00)	**admin.06_Aug_2010.14:55**	**7.1 (current)**	**Success**	**admin**

*The last successful configuration published appears in **bold**.*
For a complete list of appliances in each publishing event, go to Web > Utilities > Publish History

Centralized Reporting

Status:	Connected and transferred data
Last Data Transfer Attempt:	06 Aug 2010 21:54 (GMT +03:00)

Security Services

Description	Services: Web Appliance Service	Services: Is Service Displayed on Management Appliance?	Feature Keys: Status	Feature Keys: Time Remaining	Feature Keys: Expiration Date
IronPort Web Proxy & DVS(TM) Engine	Enabled	N/A	Active	29 days	Sun 05 Sep 2010 13:13:23 (GMT +03:00)
IronPort L4 Traffic Monitor	Enabled	N/A	Active	29 days	Sun 05 Sep 2010 13:13:23 (GMT +03:00)
Proxy Mode	Transparent	N/A			
FTP Proxy	Enabled	Yes			
IronPort HTTPS Proxy	Enabled	Yes	Active	29 days	Sun 05 Sep 2010 13:14:45 (GMT +03:00)
Upstream Proxy Groups	Configured	Yes (Routing Policies)			
Mobile User Security	IP Range	Yes (IP Range)	Active	29 days	Sun 05 Sep 2010 13:16:03 (GMT +03:00)
IronPort URL Filtering	Disabled	N/A	Active	30 days	Sun 05 Sep 2010 21:55:24 (GMT +03:00)
Cisco IronPort Web Usage Controls	Enabled	N/A	Active	29 days	Sun 05 Sep 2010 13:13:23 (GMT +03:00)
Application Visibility and Control	Enabled	N/A			
Cisco IronPort Centralized Web Reporting	Enabled	N/A			
IronPort Web Reputation Filters	Enabled	Yes	Active	29 days	Sun 05 Sep 2010 13:13:23 (GMT +03:00)
Webroot Anti-Malware	Enabled	Yes	Active	29 days	Sun 05 Sep 2010 13:13:23 (GMT +03:00)
McAfee Anti-Malware	Enabled	Yes	Active	29 days	Sun 05 Sep 2010 13:13:23 (GMT +03:00)
Sophos Antivirus	Enabled	Yes	Active	29 days	Sun 05 Sep 2010 13:13:23 (GMT +03:00)
End-User Acknowledgement	Enabled	Yes			
IronPort Data Security Filters	Enabled	Yes			
External DLP Servers	Configured	Yes			
Credential Encryption	Disabled	No			
Identity Provider for SaaS	Configured	Yes			

Acceptable Use Controls Engine Updates

Update Type	Web Appliance Version	Management Appliance Version
Web Categorization Categories List	1280964334	1280964334
Application Visibility and Control Data	1278707745	1278707745

Mobile User Security Settings

IP Range:	1.1.1.1-20

Proxy Settings

	Group	Proxies
Upstream Proxies:	upstream_group	127.10.1.1:31281
HTTP Ports to Proxy:	80, 3128	

Authentication Service

	Name	Protocol	Servers	Support Novell eDirectory
Authentication Realms:	sma19.sma	LDAP	sma19.sma:636	Yes
	w2k3.qa	NTLM	w2k3.qa	N/A

Authentication Sequences:	Name	Order of Realms
	sequence1	NTLMSSP: w2k3.qa Basic: sma19.sma, w2k3.qa
	All Realms	NTLMSSP: w2k3.qa Basic: sma19.sma, w2k3.qa

（注） Web セキュリティ アプライアンスの Acceptable Use Control Engine の各種バージョンが、Security Management アプライアンスのバージョンと一致しない場合は、警告メッセージが表示されます。そのサービスが Web セキュリティ アプライアンスでディセーブルになっているか、そこに存在しない場合は、[N/A] と表示されます。