M86 Secure Web Gateway

Hybrid Deployment Guide

Release 10.2 Manual Version 1

M86 Secure Web Gateway

Hybrid Deployment Guide

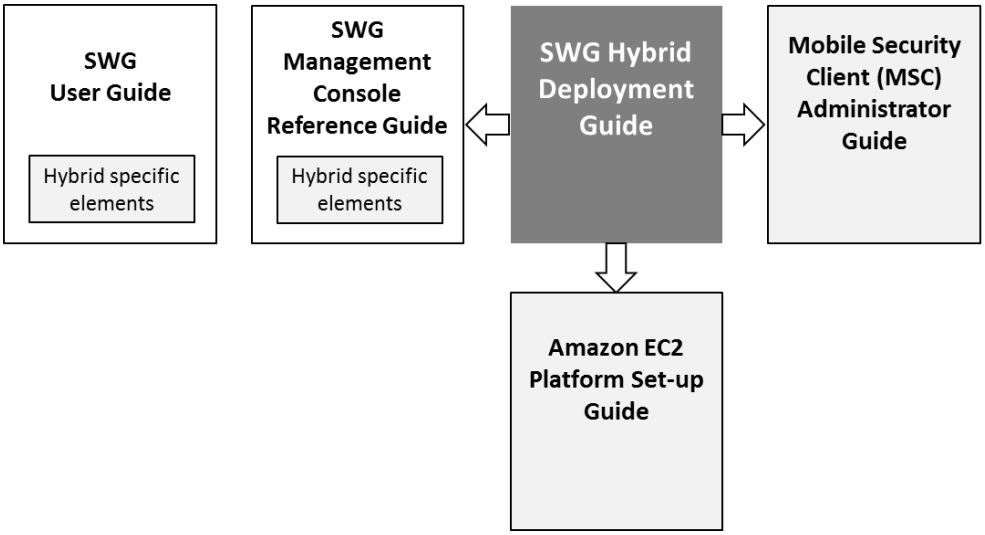
8845 Irvine Center Drive, Irvine, CA 92618, United States

Contents

1 Start Here

1.1 What is the purpose of this Guide?

This guide will help SWG Administrators to set-up and configure an M86 Security SWG Hybrid deployment. As well as providing essential background and insight, it supplements and coordinates use of the standard SWG product documentation.



The Hybrid Deployment Guide assumes that you have a working knowledge of the M86 Security SWG product and an existing functioning SWG Policy Server and on-premise Scanning Server.

1.2 Top Tips!

Three key items in this guide that should help simplify a deployment:

- Get a 50,000 foot view of the four step Hybrid Deployment process in **section 3**.
- Simplify planning by reading Deployment Decisions & Preparation **section 4**.
- SWG Policy Server Configuration workflow summarised in **section 6.1**.

1.3 Deployment Guide Conventions

The following icons are used throughout this user guide:

***NOTE**: The "note" icon is followed by italicized text providing additional information about the current topic.*

***TIP**: The "tip" icon is followed by italicized text giving you hints on how to execute a task more efficiently.*

***WARNING**: The "warning" icon is followed by italicized text cautioning you about making entries in the application, executing certain processes or procedures, or the outcome of specified actions.*

***IMPORTANT**: The "important" icon is followed by italicized text informing you about important information or procedures to follow.*

1.4 Terminology

The following terms are used throughout this user guide:

Cloud Load Balancer	A load balancer that is either deployed by a customer on the Amazon EC2 platform or by M86 Security on the M86 SWS-Hybrid platform.
EC2	Amazon Elastic Computer Cloud (Amazon EC2). http://aws.amazon.com/ec2/ is a web service that provides resizable compute capacity in the cloud. It is used as a platform for the M86 Security SWG Cloud Scanner.
Cloud Proxy	Used to refer to both Cloud Scanners and Cloud Load Balancers.
Cloud Scanner	An SWG scanning server type designed to support mobile/roaming workers whilst being deployed in cloud based infrastructure such as Amazon EC2, M86 SWS-Hybrid or in an organization's own private cloud infrastructure.
Elastic IP Address	Amazon EC2 Elastic IP addresses are static IP addresses designed for dynamic cloud computing. An Elastic IP address is associated with your EC2 account and then used against a specific Cloud Scanner Instance or Cloud Load Balancer instance.
Mac OS X	Apple Macintosh ("Mac") operating system.
MSC	M86 Security Mobile Security Client software installed on the user's Personal Computer (Windows or Mac OS X) to redirect web traffic to available SWG Cloud Scanners. Mobile Security Client; works with both SWG and WFR products.
PAC file	A Proxy Auto-Configuration (PAC) file defines how web browsers and other user agents can automatically choose the appropriate proxy server (access method) for fetching a given URL. A PAC file contains a Java Script function "FindProxyForURL(url, host)".
PC	Personal computer; refers to both MS Windows and Apple Mac based systems.
Mobile/remote user/computer	A laptop, home office desktop or otherwise non-static computer.
Region	A geographic region in which Cloud Scanners can be located.
SWG	M86 Secure Web Gateway product.
SWG Scanner or Scanning Server	An M86 Security SWG Scanner server installed in the corporate network.
SWG Policy Server	An M86 Security SWG Policy Server installed in the corporate network.

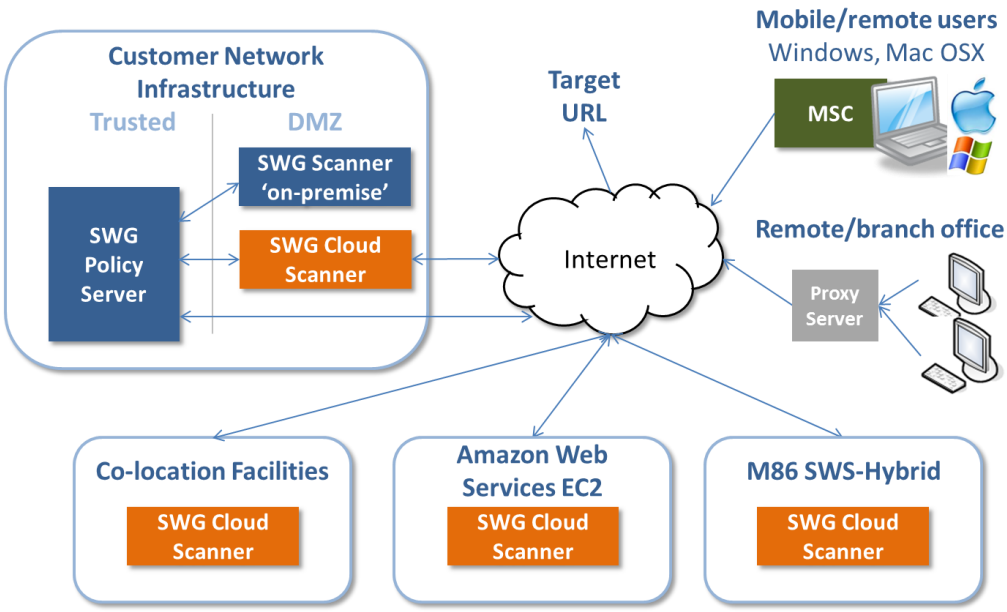
1.5 Introduction - What is a Hybrid Deployment?

Hybrid deployment is a feature of the M86 SWG product that extends web filtering/security to Windows and Mac Personal Computer(PC)[1] users when they are off-premise, i.e. connecting to the internet from hotels, airports, internet cafes, working from home or even working from remote offices. Hybrid deployment can also be used to secure remote offices that have a local web proxy.

For mobile/roaming users the Hybrid involves installing a piece of client software on the PC, the **M86 Mobile Security Client** (MSC), and setting up one or more dedicated **SWG Cloud Scanners** that the client can authenticate with and securely route its web traffic through. Remote/branch offices can be secured using the MSC on each PC or by using a local proxy server linked to a Cloud Scanner.

[1] Note: For details of support for smartphones and tablets please see the "Mobile Device Support Technical Brief".

The Cloud Scanner systems can be deployed within the customer's own data centers, in co-location facilities, in Amazon Web Services EC2 or using M86 Secure Web Service Hybrid as shown in the diagram below.



The aim is to position them as close to the mobile/remote user community as possible to ensure low latency connections and therefore a good web browsing experience. A typical deployment might include a Cloud Scanner at head office to cover home workers or visitors to the area and one in each main geographical area of operation, e.g. Europe, APAC, US East and US West coast to cover travelling users and remote/branch offices.

As a mobile user moves to different locations, they will automatically use the most appropriate available Cloud Scanner that gives them best performance (lowest latency), e.g. if they are on-premise and an on-premise gateway is available they will use that, if they are on a business trip abroad then a scanner that gives the lowest latency will be used.

PCs connected using these scenarios are fully integrated into the policy enforcement, management and reporting provided by the M86 SWG product no matter where they are working from.

1.6 Why use an SWG Hybrid Deployment?

In summary a Hybrid deployment of SWG can protect mobile/roaming and remote/branch office Personal Computer users:

- with the same command, control and reporting infrastructure as on-premise users
- while applying the same AUP and reporting as on-premise users
- allowing web gateways to be placed close to where the users are (ensuring low latency)
- by reaching geographic locations that would otherwise be impractical
- without backhauling web traffic to the HQ
- with multiple cloud scanner platform options: hardware appliance, virtual appliance, Amazon EC2, M86 SWS-Hybrid.

Mobile/remote users are supported as a seamless extension of the existing SWG implementation.

2 Deployment Scenarios

Hybrid deployments of SWG allow mobile/roaming users and remote/branch offices to be protected by using SWG Cloud Scanners and the Mobile Security Client software.

Cloud Scanners are virtualized SWG Scanning Servers that are configured to support connections only from user computers running the M86 Mobile Security Client, or specifically defined proxy servers for example in remote/branch offices. Cloud Scanners can be run on a choice of four different platforms depending on the target environment and management needs.

The **Mobile Security Client** (MSC) is software that is installed on the computer endpoint and re-directs web traffic to the appropriate Cloud Scanner. The MSC enables identification, authentication and privacy of traffic between itself and the cloud scanner(s).

The **SWG Policy Server** is, as with normal on-premise Scanning Server deployments, the central point of administration and control.

First we will look at the MSC end-point deployment, then the Cloud Scanner deployments. MSC and Cloud Scanner deployments can be mixed to produce the most appropriate web security solution.

2.1 End Point Deployment

The most common use cases are:

1. Mobile/roaming workers using Mobile Security Client (MSC)
2. Branch office with PCs using MSC
3. Branch office with local proxy server

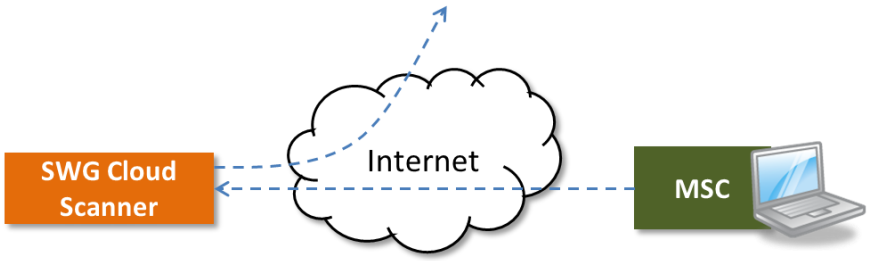
2.1.1 Mobile/Roaming Workers using Mobile Security Client (MSC)

Mobile/roaming workers have the MSC software installed on their PC (Windows or Mac). When the user is travelling and connects to the Internet from an external (non-company) network, e.g. hotel, airport, home office etc. the client will understand this and will attempt to route web traffic to the nearest available Cloud Scanner defined it its configuration.

Direct connection

No proxy and open firewall (or no firewall) between the client and the ISP, e.g. working from home using broadband or Dial-up over 3G.

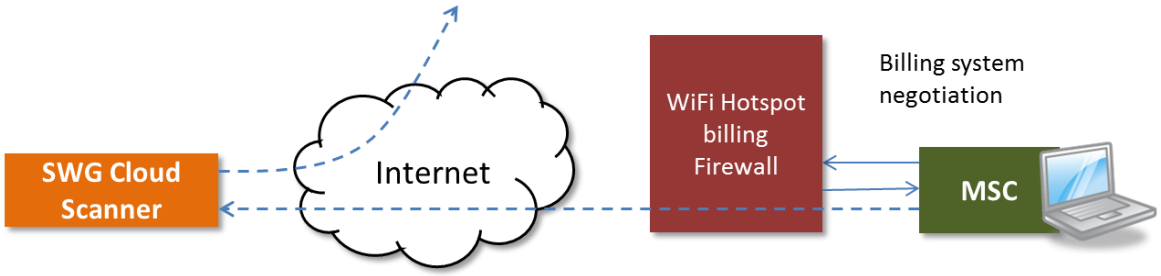
Traffic Flow: The MSC re-directs Web requests from the PC browser to the Cloud Scanner proxy where the security policy is applied.



WiFi Hotspot

WiFi hotspots in locations such as airports cafes and hotels often use front end billing/registration systems that must be negotiated before receiving an internet connection. The MSC is able to deal with these scenarios automatically.

Traffic Flow: The MSC first tries to reach the configured Cloud Scanner, on failing to do this it falls back to direct connection on port 80 which is intercepted by the Billing System firewall. Once the billing system has been negotiated by the user, the hotspot firewall opens up and the MSC is able to see the Cloud Scanner and automatically begins to re-direct web traffic to it so that security policy can be applied.



On-premise (headquarters)

When the mobile/roaming user returns to the office (i.e. on-premise) and connects from the secure zone of the company network, the MSC can detect this and will attempt to use the on-premise security solution; local SWG Scanning Server, local web proxy or transparent mode SWG according to configuration previously set. Alternatively the configuration can be set, via the SWG Policy Server, to allow the MSC to continue as though it were off-premise.

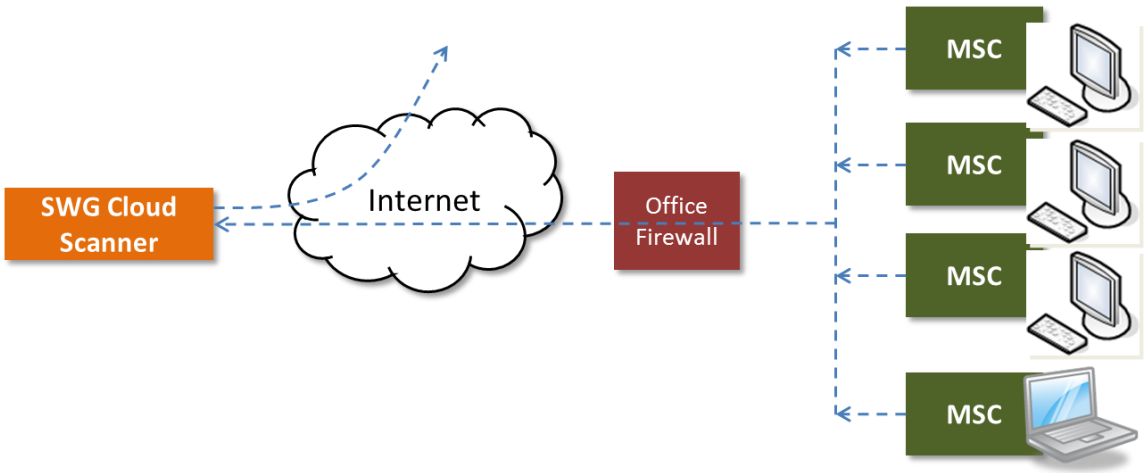
2.1.2 Remote/Branch Office with PCs Using MSC

All PCs can be installed with the MSC and web traffic can be routed via the nearest Cloud Scanner in the same way as for the roaming user. Roaming users who visit the office will continue to operate as though they were roaming.

This is a good solution for offices where:

- geographic location makes deployment and support of local equipment difficult
- where a VPN connection back to the headquarters is not available
- connecting back to the headquarters would introduce too much latency
- there is no desire to backhaul web traffic to the corporate HQ

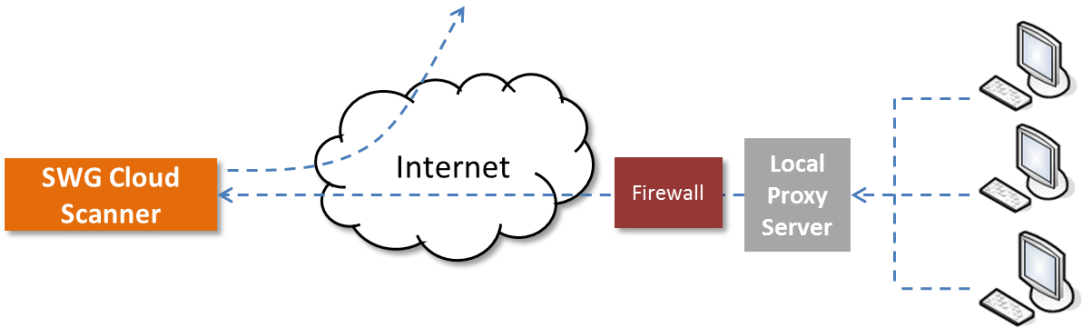
Traffic Flow: The MSC on each PC re-directs web traffic directly to the Cloud Scanner where the security policy is applied.



Remote/Branch Office with Local Proxy Server

In remote/branch offices where there is already a local proxy server, e.g. Microsoft ISS, it is not necessary for all PCs to run the MSC.

Traffic Flow: Each PC is configured to pass its web traffic to the local proxy server. The proxy server is configured to forward this traffic to the Cloud Scanner where security policy is applied.



This topology has the advantage of ease of set-up and maintenance since the PCs do not need software to be installed, however there are some caveats:

- HTTP traffic from the proxy server to the Cloud Scanner is *not* encrypted.
- There may be a reduction in the level of identification information available making policy application and reporting less granular.
- The proxy may not be able to fail-over to another Cloud Scanner (in another Region) in the event of the first failing. This situation can be mitigated by the use of multiple Cloud Scanners and a Cloud Load Balancer in the same Region (see Cloud Scanner Deployment section below).
- Access to the Cloud Scanner by local proxy servers must be restricted to specific customer IP addresses or the security of the implementation is compromised.

If required the proxy server scenario can be combined with PCs running MSC, for example where mobile/roaming workers come into a branch office to work for the day.

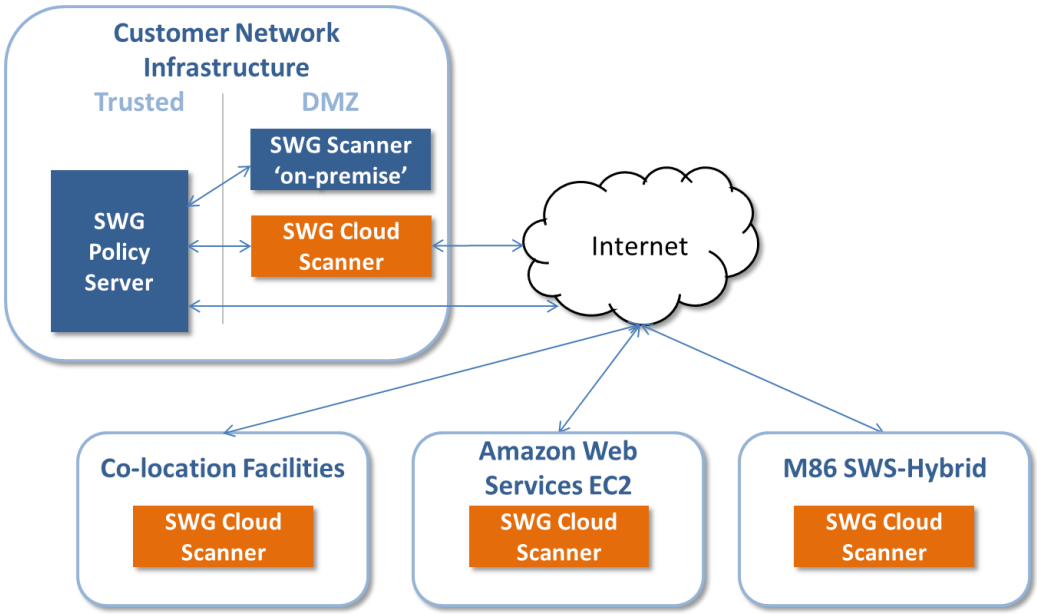
2.2 Cloud Scanner Deployment

Cloud Scanners can be deployed using four different platforms to match the customer's network environment. In general the aim is to locate Cloud Scanners close to where the mobile/roaming users and remote/branch offices are in order to minimize latency thereby providing the best browsing experience.

1. M86 Hardware Appliance
2. M86 Virtual Appliance
3. Amazon Web Services EC2
4. M86 Secure Web Service Hybrid (SWS-Hybrid)

Cloud Scanners are controlled by and interact with the SWG Policy Server in the same manner regardless of which platform they are deployed on.

Each of the cloud scanner platform options are represented in the illustration below (an on-premise SWG Scanner and SWG Policy Server are shown for context):



2.2.1 Customer Network Infrastructure (Private Cloud)

In this topology the Cloud Scanner is deployed on a DMZ on the customer's network infrastructure. This is a typical use case to support mobile/roaming users and remote/branch offices in the same country as the Cloud Scanner. This type of deployment typically has high speed network connectivity between the Cloud Scanner and the SWG Policy Server. This is sometimes termed a **Private Cloud** configuration.

2.2.2 Co-location Facility

Sometimes is it not possible to deploy a Cloud Scanner where it is needed; either the customer does not have a data center nearby or the other platform options, Amazon EC2 and M86 SWS-Hybrid, do not cover that area. In this situation a Co-location Facility deployment is recommended. The Cloud Scanner is implemented in a Co-location data center in the required location using customer owned/hired hardware (either M86 Hardware Appliance or M86 Virtual Appliance platforms). This is similar to the Customer Network Infrastructure deployment, but located instead in a business partner's data center.

2.2.3 Amazon Web Services EC2

An alternative to a Co-location Facility deployment is to use the Amazon Web Services EC2 cloud service. Special M86 SWG Cloud Scanner AMIs (Amazon Machine Images) are provided which can be used to create Cloud Scanner instances. This option takes away the effort of procuring, deploying, operating, maintaining the underlying Cloud Scanner hardware platform and network connectivity. The customer will need to learn to use the Amazon EC2 environment however.

Cloud Scanners can be placed in the following geographic Regions:

- APAC (Tokyo)
- APAC (Singapore)
- Europe (Eire)
- South America (Sao Paulo)
- US East (North Virginia)
- US West (California)
- US West (Oregon)

Please note: this option is *not* available for SWG Policy Servers.

2.2.4 M86 Secure Web Service Hybrid (SWS-Hybrid)

SWS-Hybrid is for customers who require a completely hands-off approach to the Cloud Scanner platform. M86 take care of the platform set-up and maintenance using an IaaS provider such as Amazon. The customer can now focus on SWG policy management. The same geographic regions are covered as for the Amazon EC2 Cloud Scanner platform covered above.

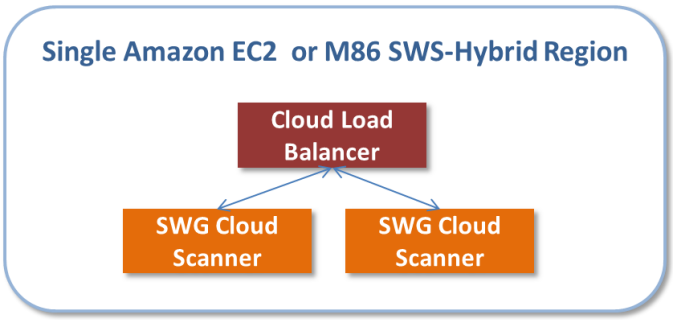
An SWS-Hybrid Cloud Scanner can often be implemented in as little as a day or two making it ideal for fast deployment and where the logistics of deployment are difficult, e.g. foreign countries.

Please note: this option is *not* available for SWG Policy Servers.

2.2.5 Multi-Scanner and Load Balancer deployment

In the on-premise and co-location scenarios the same load balancer methods as for the normal on-premise SWG Scanning Servers are used.

With Amazon EC2 and M86 SWS-Hybrid deployment platforms, if more than one Cloud Scanner is needed in a single geographic Region to increase user capacity then a special Cloud Load Balancer instance is used.



IMPORTANT: A *Region is typically split into Availability Zones which can enble geographic reslience.*

*Availability Zones are *not* currenlty supported by the M86 SWS-Hybrid platform.*

For the Amazon EC2 platforms be aware that placing Cloud Scanners in more than one Availability Zone in the same Region and linking them with a Load Balancer will lead to increased Amazon EC2 data transfers charges. For further details consult the Amazon EC2 Platform Set-up Guide (Using Amazon EC2 as a platform for SWG Cloud Scanners).

2.3 Combining End Point and Cloud Scanner Deployments

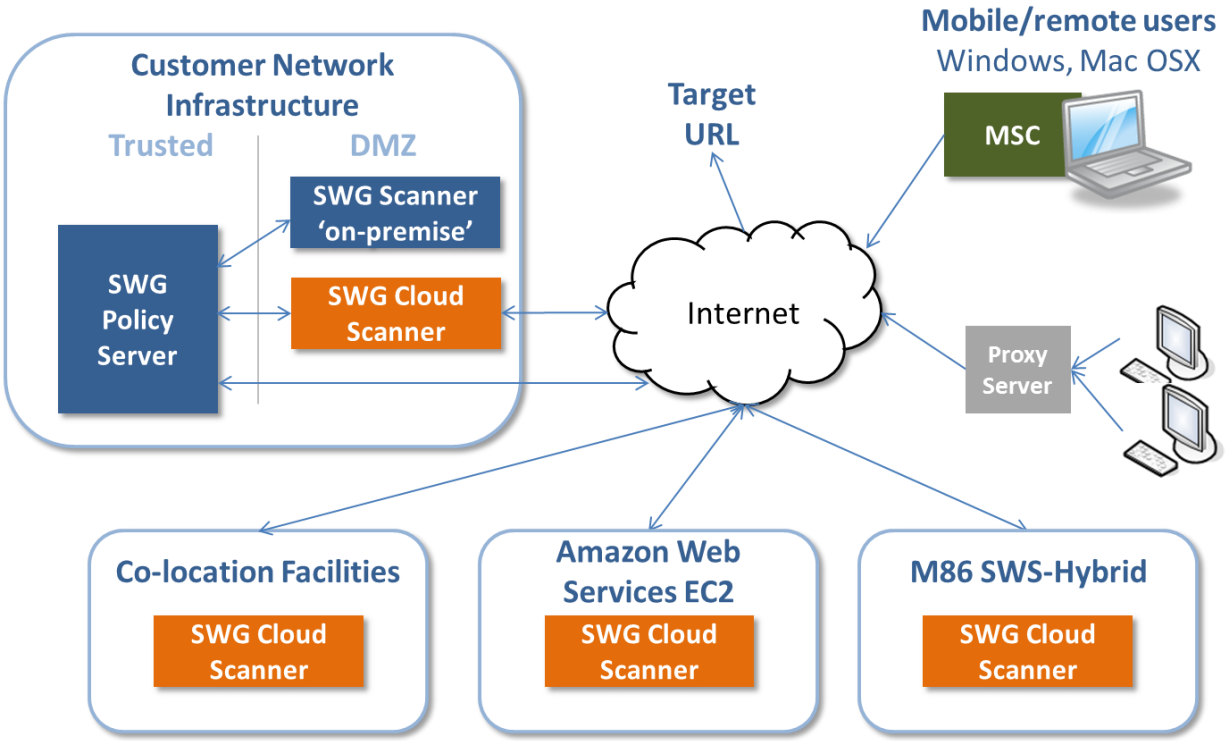
The SWG Hybrid solution is very flexible:

- All end point deployments can be used with all Cloud Scanner deployments.
- Endpoint deployments can be mixed within an implementation.
- Cloud Scanner deployments can be mixed in the following manner:

	Co. Network Infrastructure		Co-Location Facility		Amazon EC2	M86 SWS-Hybrid
	Hardware Appliance	Virtual Appliance	Hardware Appliance	Virtual Appliance	IaaS	Service
Scenario 1	✓	✓	✓	✓	✓	×
Scenario 2	✓	✓	✓	✓	×	✓

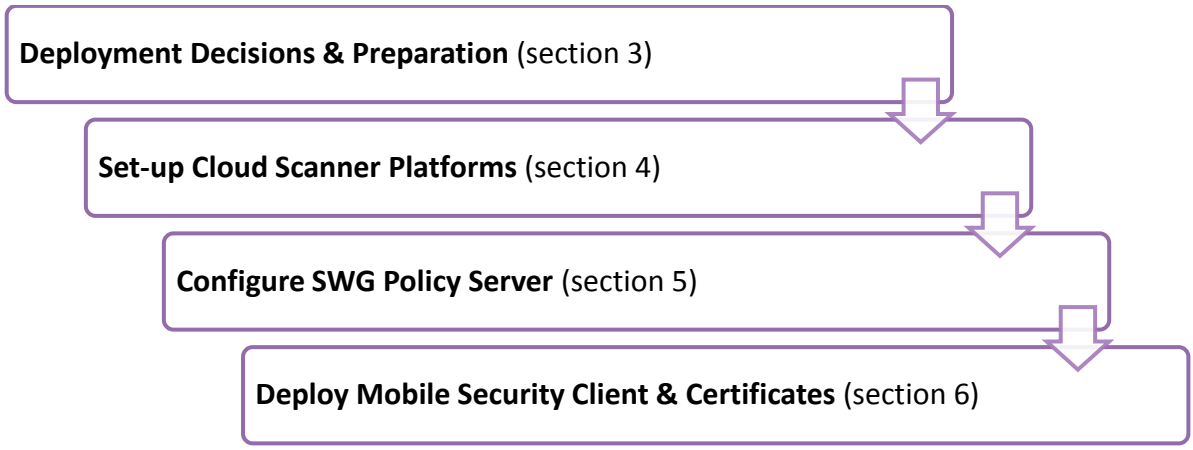
Note: Mixing Amazon EC2 (customer managed) and M86 SWS-Hybrid within a deployment is *not* permitted dues to support complexities.

Each of the cloud scanner platform and end point options (excluding Cloud Load Balancers) are represented in the diagram below:



3 How to implement SWG Hybrid (four steps)

Follow the four steps below to set-up an SWG Hybrid deployment, but first ensure that there is a functioning SWG implementation, including Policy Server and on-premise Scanner, already in place.



NOTE: Although these steps are laid out sequentially for ease of reading, in practice there will be some level of recursion.

4 Deployment Decisions & Preparation

Before a Hybrid deployment is attempted a number of decisions need to be made to determine:

1. Cloud Scanner platform types
2. Cloud Scanner platform sizing and Load Balancers
3. Certificate management method choice: PKI Mode or Internal Certification Mode?
4. Client types to be used: MS Windows and/or Mac OSX?
5. Client deployment method choice: email or external system?
6. PAC File deployment/management method – from SWG Policy Server or manual?

Each of these decision areas are explored below.

4.1 Cloud Scanner platform types

Cloud Scanners are virtualised SWG Scanning Servers that are configured to support connections only from user computers running the M86 Mobile Security Client, or specifically defined proxy servers for example in remote/branch offices. Cloud Scanners can be run on a choice of four different platforms depending on the target environment and management needs. The platform choice will impact the set-up process that need to be used later, however the SWG Policy Server Configuration does not change.

Here is a summary of the platform types and their application and restrictions on combinations.

	SWG Cloud Scanner Platform Options			
Customer Requirement	**Hardware Appliance**	**Virtual Appliance**	**EC2**	**SWS-Hybrid**
Policy of using IBM hardware	✓			
Use own or partner datacenters	✓	✓		
Consolidating systems in a VMware environment		✓		
Want hardware platform flexibility inc. Cloud		✓	✓	✓
Reach hard to manage remote locations			✓	✓
Don't want to backhaul mobile pc/mac user traffic			✓	✓
Hands-off' SWG Cloud Scanner platform				✓

***IMPORTANT**: There are some restrictions in terms of which platforms can be combined in an implementation. See section 2.3, **Combining End Point and Cloud Scanner Deployments** above for details.*

4.1.1 Cloud Scanner Platform Set-up Responsibilities

Secure Web Service-Hybrid cloud scanner platforms are set-up exclusively by M86. All other cloud scanner platforms are the customer's responsibility, though of course assistance can be provided via Professional Services. This is illustrated by the table below.

		SWG Cloud Scanner Platform Options			
Component	**Activity**	**Hardware Appliance**	**Virtual Appliance**	**EC2**	**SWS-Hybrid**
M86 SWG Config & Operation	SWG Commissioning On-going SWG configuration & maintenance On-going SWG operations & monitoring	Customer*	Customer*	Customer*	Customer*
M86 SWG Product Platform	SWG Cloud Scanner software upgrades IaaS configuration IaaS fee payment management IaaS supplier liaison/escalation	Customer*	Customer*	Customer*	M86
Infrastructure	Virtualisation & operating system provision Hardware infrastructure provision Networking infrastructure & bandwidth provision	Customer*	Customer*	Amazon Web Services	M86 (via IaaS provider)

* M86 can assist via Professional Services.

4.1.2 What functionality does each Cloud Scanner Platform support?

Not all SWG features make sense or can be used on a Cloud Scanner. This may be due to the need for high speed network connections, the impact on bandwidth costs when moving traffic around or simply that the function is not implemented. The following table summarizes feature support as of SWG 10.2:

SWG v10.2 Cloud Scanner Feature Support by Platform Type

Updated 2012-03-02

Features		IBM Appliance & Virtual Appliance	EC2	M86 SWS-Hybrid
Scanning	Authentication	✓	✓	✓
	Cache	✓	✓	✓
	FTP native	×	×	×
	FTP (over HTTP)	Incoming only	Incoming only	Incoming only
	HTTP	✓	✓	✓
	HTTPS (SSL)	✓	✓	✓
	ICAP Client	✓[1]	×	×
	ICAP Server	×	×	×
	General	✓	✓	✓
	WCCP	✓[1]	×	×
	Transparent proxy mode	×	×	×
URL List	M86	✓	✓	✓
	IBM	×[2]	×[2]	×[2]
	Websense	×	×	×
Anti-Virus	Kaspersky	✓	✓	✓
	Sophos	✓	✓	✓
	McAfee	Not available	Not available	Not available

[1] Latency and bandwidth costs make this unsuitable except for Private Cloud.

[2] The IBM list is only available if previously in use by the customer and specifically requested and then approved by M86.

Key: ✓ = Supported × = not supported

4.2 Cloud Scanner Platform Sizing & Load Balancers

4.2.1 What size Cloud Scanner Platforms do I need?

Your M86 Security Sales Representative will be able to assist with sizing calculations for each platform type. When using M86 Secure Web Service Hybrid (SWS-H) this is all taken care of for you.

4.2.2 Are cloud based Load Balancers needed?

For Amazon EC2 and M86 SWS-H platforms, if more than one Cloud Scanner is needed in single geographic Region (e.g. Europe) then a cloud based Load Balancer will be required. For M86 SWS-H platforms this will be taken care of for you. For Amazon EC2 platforms (where the customer uses their own Amazon EC2 account) please consult the SWG Sizing Calculator for guidance on platform capacity and the need for Load Balancers.

***IMPORTANT**: If more than four Cloud Scanners are required in a single geographic Region (EC2 or SWS-Hybrid), please contact M86 Security for assistance.*

4.3 Certificate management method choice: PKI Mode or Internal Certification Mode?

One of the most important decisions that impact the Hybrid set-up and operation process is choice of client certificate management approach. Every end user of the Mobile Security Client requires a digital certificate (client certificate) in order to be able to authenticate and identify with the SWG Cloud Scanners. SWG supports two approaches to this: either an external PKI system is used or the SWG Policy Server is used as an internal Certificate Authority. The following summarizes the available options and their implications.

Certificate Distributions Options

	Creation	Distribution	Management
PKI Mode	PKI System	PKI System	PKI System
Internal Mode	SWG Policy Server is the Certificate Authority (CA)	SWG Email (attachment) or Export to AD/G.P.O	SWG Policy Server

AD = Active Directory, G.P.O = Group Policy Objects or similar.

4.3.1 PKI Mode (External PKI System)

If a PKI (Public Key Infrastructure) system is employed, certificate distribution will be taken care of completely outside of the SWG solution. Subsequent certificate management is also performed via the customer's PKI system. This choice of certificate management is global so far as the Hybrid configuration is concerned and will change the configuration screens available in the Cloud Configuration section of the SWG policy Server.

4.3.2 Internal Certification Mode (Internal Certificate Authority)

When the Policy Server acts as the Certificate Authority (CA) it is also used as the certificate distribution point. Control over certificate validity (block, revoke, allow etc.) is then maintained on the SWG Policy Server.

Two distribution choices are available depending on the size of the deployment:

- Internal Email Distribution

  For smaller implementations and proof of concept (POC) projects the internal (SWG Policy Server) distribution mechanism can used to email certificates to each end user. When new users are added, certificates can optionally be automatically be emailed to the end user.

  Default email templates are provided however you may wish to consider tailoring these for your organization's particular needs.

  When using Internal Certification Mode, a password can be applied to the certificate installation process. Without the password the user cannot install the certificate. The password is defined as part of the client configuration step (see section 6.3.5 Client Enforcement Settings - Client Configuration Tab below) and distributed manually by the administrator to the target end users.

- Export to Directory System (Active Directory)

  For larger deployments certificates can be exported from the Policy Server management screens and then uploaded into a directory system such as MS Active Directory using an upload utility program. Subsequently MS GPO is used to deliver the certificates to individual end users when they login to their domain. A utility script and instructions are provided (see Appendix A).

4.4 Client types to be used: MS Windows and/or Mac OSX?

If both Windows and Mac clients are to be used then consider that:

- Different code binary files are used for the Mobile Security Client on Windows and Mac.
- Different code distribution mechanisms may be required (e.g. GPO for Windows, Casper suite for MAC).

- You may need to edit the default client deployment email templates.

4.5 Client deployment method choice: email or external system?

The Mobile Security Client software is included as an individual executable file as part of the SWG product installation package. Updates to the client are provided as part of an overall SWG product version release, maintenance release or hotfix. In SWG v10.2 onward client code versions are de-coupled from the main product in which case it may be supplied separately as an update package as well as part of an overall SWG release.

Client Deployment Options

	Create Installer	Initial installation	Update
PKI Mode	SWG Policy Server	G.P.O	Automatic (from SWG Policy Server)
Internal Mode	SWG Policy Server	SWG Email (link) or G.P.O	Automatic (from SWG Policy Server)

G.P.O = Group Policy Objects or similar.

4.5.1 Client Deployment

Initial deployment of the MSC client software can be managed in two ways:

- Internal distribution (Internal Certification Mode Only)

  The client can be distributed by using the built-in email feature of the Policy Server and then manually installed by the end user. A customizable email contains a download link and instructions for installing the MSC. The download location is chosen by the Administrator and can be placed on an internal shared directory or in a web server requiring user/password or FTP server or even sent by email. This method is good for small/medium size and proof of concept deployments.

- External software management system (e.g. G.P.O)

  In a Microsoft environment an external software management system, such as Microsoft Group Policy Objects, can be used to deploy the MSC. The administrator makes the MSC install package available to the GPO system and end user systems are installed at domain login time. A silent install option is also available.

  In a Mac OSX environment the equivalent software distribution system, Casper Suite or even Apple Remote Desktop Management could be used. Alternatively the client code could be built into a master image of the client machines.

4.5.2 On-going Client Software Updates

Once installed the MSC client code (binary) is updated automatically[2] from the Cloud Scanner (via the Policy Server). The new client package is made available on the Policy Server via the Administrator. The MSC checks once per hour for code updates and if a newer version is available it will automatically download and execute it.

Client configuration updates are also checked for once per hour. If the configuration version is the same or more recent than that on the client then a fresh copy is downloaded and applied; this is all transparent to the end user.

[2] Applies to SWG version 10.2 and MSC v2.0 onwards.

4.5.3 Client Installation & Initial Configuration

The MSC installation process implements the various MSC components and sets an initial default configuration as defined on the SWG Policy Server. Installation is performed under Administrator privileges.

System settings are automatically adjusted to use "proxy auto configuration script" and the URL location of the MSC PAC (Proxy Auto Configuration) file is set. Browsers and other applications that use the system setting will automatically use the PAC file. Other supported browser types will have their network settings adjusted directly by the MSC to point to the same PAC file. This setting of network configuration happens both at MSC install and periodically (approximately every fifteen seconds) whilst the MSC is running to help mitigate tampering.

4.6 PAC file deployment method: manual or from SWG Policy Server?

The Mobile Security Client uses a Proxy Auto Configuration (PAC) file. The SWG Policy Server automatically generates and maintains the PAC file based on the Cloud Configuration entered. There are two ways to manage the PAC file:

4.6.1 Automatic PAC File Management

The administrator can choose to distribute and update the PAC file automatically via the SWG Policy server.

The Mobile Security Client will periodically check for updated PAC file. Switch this function on by navigating to the Configuration – Cloud Configuration – Client Configuration tab and clicking the "Enforce PAC file usage via the Mobile Security Client" option.

4.6.2 Customer Managed PAC File

If the PAC file needs to be customized in some way or is needed for a chained proxy deployment (remote/branch office) it is possible for the customer to take control of the distribution. The PAC file can be downloaded from the SWG Policy Sever (Client Provisioning Tab) by the administrator and placed on an accessible file share from which the roaming users (Mobile Security Clients) can in turn access it. Configuration updates and enforcement of the PAC file and client browser connection settings are then performed by the customer as part of their end point management system, e.g. Group Policy Objects.

5 Set-up Cloud Scanner Platforms

Cloud Scanner platforms should be set-up before attempting to configure the SWG Policy Server. The set-up of each Cloud Scanner platform type requires a different approach, instructions can be found as follows:

***IMPORTANT**: Before continuing please ensure that you have read section 4: Deployment Decisions & Preparation.*

5.1 M86 SWG Hardware Appliance

For instructions on how to set-up an M86 SWG Hardware Appliance, see the following references:

1. Build the SWG scanner platform: SWG Set-up Guide.
2. Covert the platform to an SWG Cloud Scanner: SWG User Guide Procedure: Defining a Private Cloud Scanner

5.2 M86 SWG Virtual Appliance

For instructions on how to set-up an M86 SWG Virtual Appliance, see the following references:

1. Build the SWG scanner platform: SWG Set-up Guide.
2. Covert the platform to an SWG Cloud Scanner: SWG User Guide Procedure: Defining a Private Cloud Scanner

5.3 M86 Secure Web Services Hybrid (SWS-H)

Set-up of the M86 SWS-Hybrid platform is performed exclusively by M86 Security staff – please ask for assistance.

5.4 Amazon Web Services EC2 Platform Set-up

Refer to the M86 document: “Amazon EC2 Platform Set-up Guide (Using Amazon EC2 as a platform for SWG Cloud Scanners)”.

6 Configure SWG Policy Sever

6.1 Work Flow for Configuring the SWG Policy Server for Hybrid Deployment

The recommended sequence of steps needed to configure the SWG Policy Server with a hybrid deployment, i.e. using Cloud Scanners and Mobile Security Client, are detailed below. The main steps (what) are on the left of the table, the SWG Management Console screen needed (how) is then listed followed by the activities undertaken (why). Each step is detailed in the following sections.

IMPORTANT: . *In this deployment guide we focus on the essential configuration details and provide additional background to help provide a better understanding of the overall process of SWG Hybrid Deployment. More detailed procedures for using each of the SWG Management Console screens are available in the "SWG Management Console Reference Guide".*

Table: SWG Policy Server Configuration Work Flow			
	Deployment Step (What)	**SWG Management Console Screen (How)**	**Explanation (Why)**
General Set-up			
	Mail Server	**Mail Server Screen** (Administration – System Settings)	Configure email servers settings to ensure that the SWG can send client provisioning emails. This step may already have been completed in existing SWG implementations.
	Cloud Scanners Definition and Connection	**M86 Devices Screen**	Define and connect the previously built SWG Cloud Scanners to the SWG.
Cloud Configuration			
	Choose Certificate Management Mode	**Cloud Configuration** (Administration – Cloud – Configuration)	Choose **Internal Certification Mode** (SWG Policy Servers acts as Certificate Authority), or **PKI Mode** (client certificates are managed by an external PKI system). Note: Available Cloud Configuration screens will vary according to the choice made.
	Cloud Configuration (Internal Certification Mode)		
	Internal Certification Mode Certificate Management	**CA Management Tab** (Administration – Cloud – Configuration)	Determine the Certificate Authority as Internal or External. If internal generate certificates.
	Network and URL exclusions	**Bypass Tab** (Administration – Cloud – Configuration)	Define those addresses that should be excluded (bypassed) from scanning and for which the user will connect directly to the Internet.
	On-premise settings	**Proxies (On-premise) Tab** (Administration – Cloud – Configuration)	Configure On-premise Proxies and define how to determine when the client is on premise vs. off premise.
	Communications ports	**Proxies (Cloud) Tab** (Administration – Cloud – Configuration)	Configure Cloud Scanners (Proxies) communications port numbers.
	Client enforcement settings	**Client Configuration Tab**	Client enforcement options and PAC file

Table: SWG Policy Server Configuration Work Flow			
	Deployment Step (What)	**SWG Management Console Screen (How)**	**Explanation (Why)**
		(Administration – Cloud – Configuration)	management options. Uninstall warning message text definition.
	Client provisioning settings	**Provisioning Tab** (Administration – Cloud – Configuration)	Define where to find client installers. PAC file download option for manual PAC file management. Mobile Security Client installer downloads for Windows and Mac OSX.
	Email template configuration	**Email Template Screen** (Administration – Cloud)	Customize the text of the client and/or client certificate provisioning emails.
	Cloud Configuration (PKI Mode)		
	Where the configuration tabs are the same as for Internal mode use this guide, otherwise please refer to the SWG Management Console Reference Guide Chapter 5, Cloud, "MSC Cloud Configuration in PKI Mode"	Choosing PKI mode causes changes to the available configuration screens. CRL handling - for PKI Mode only. Bypass - same as Internal Certification Mode. Proxies (On-premise) Tab - same as Internal Certification Mode. Proxies (Cloud) Tab - same as Internal Certification Mode. Provisioning – different for PKI Mode. Client Configuration – different for PKI Mode. Email Template Screen – not needed in PKI Mode.	
User Management			
	Cloud Users and Groups	**Users/User Groups Screen** (Users)	Define Users and User Groups (including LDAP) that will use the Cloud Scanners (Proxies).
	Client certificates management (Internal Certification Mode)	**Cloud User Certificate Management** (Users)	On-going management of client certificates (i.e. issue, revoke, export etc.) when the SWG is working in Internal CA mode.

6.2 General Set-up

6.2.1 Mail Server

***NOTE**: This may step have already been completed in existing SWG deployments.*

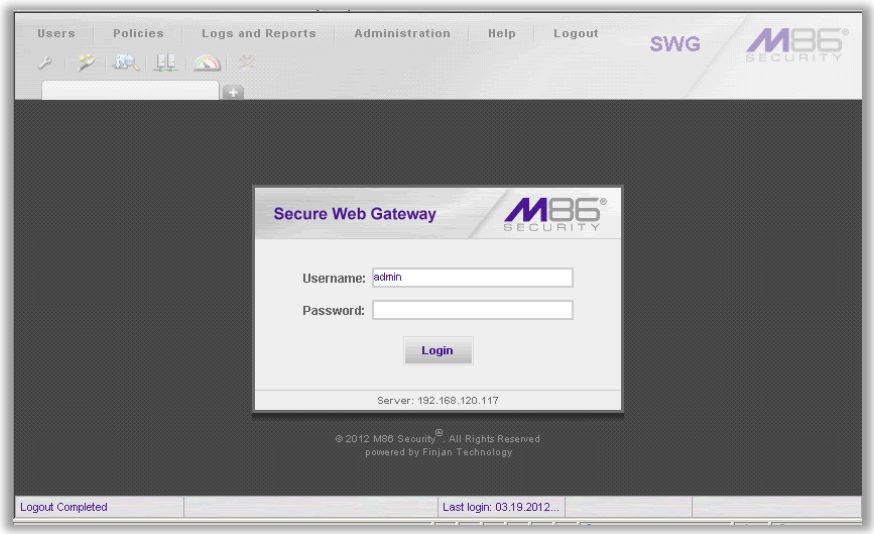
This is a necessary and important step when using **Internal Certification Mode.** Email is used to distribute Client Installation packages, client certificates and other Cloud related notification emails.

Refer to the SWG Management Condole Reference Guide "Mail Server" section for details on how enter the configuration.

6.2.2 Cloud Scanner Definition and Connection

Login to the SWG Policy Sever

1. Navigate to the Secure Web Gateway Management Console and login.



To link a Cloud Scanner to the Policy Server:

1. Navigate in the Management Console to **Administration – System Settings - M86 Devices**.
2. Right-click **Devices** and **Add Device**.
3. **Select Cloud Scanning Server** in the Type dropdown menu.
4. In the **Device IP** field, enter **Cloud Scanner IP**.

***WARNING**: If using Amazon EC2 instances or M86 SWS-Hybrid Cloud Scanner platforms it is **highly recommended** that the Amazon EC2 **Elastic IP Address** is used. If a Load Balancer is also being used in EC2, then it **must** have an Elastic IP address.*

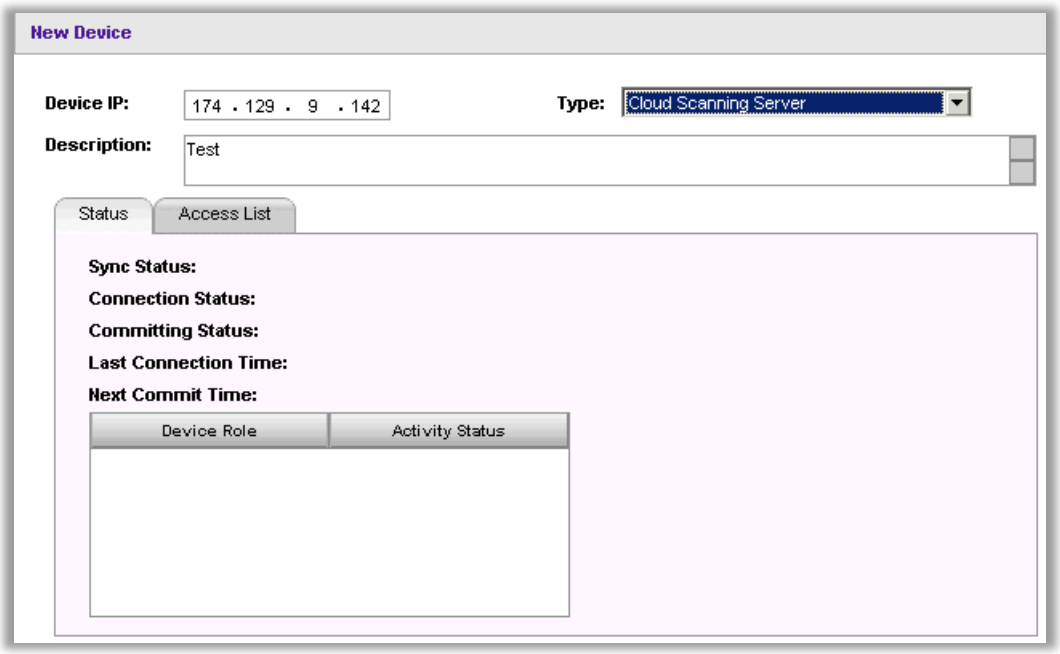


Figure: Example of connecting a Cloud Scanner instance to the SWG Policy Server.

5. Repeat steps 1 to 4 for each new Cloud Scanner.
6. Click **Save**. Click  to commit changes.
7. **Wait** for policy distribution to complete.

***NOTE**: The initial connection time depends on the speed of the link between the SWG Policy Server and the Cloud Scanners. Around 30-40 minutes is typical.*

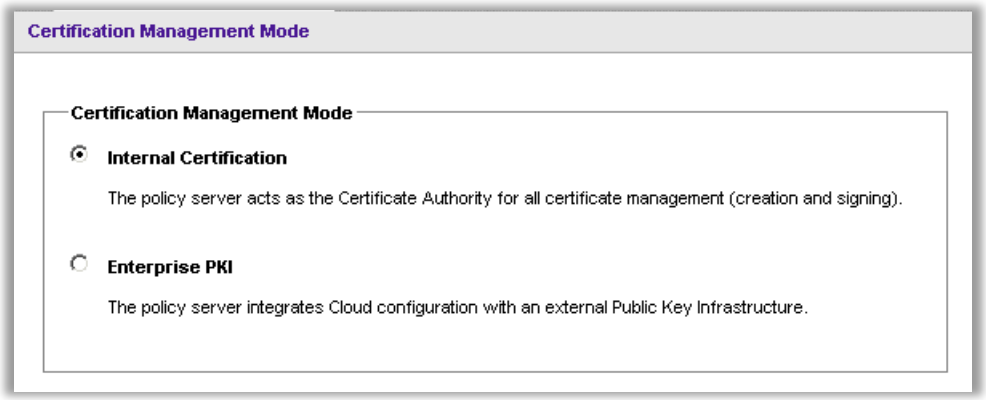
***TIP**: It is not possible to directly determine the scanner status during this period other than checking the sync indicator on the M86 Devices screen. However, in the system logs viewer it is possible to see when synchronization with a certain scanner started and ended.*

6.2.3 Choose Certificate Management Mode

***IMPORTANT**: The work flow sequence changes depending on whether an external PKI (Public Key Infrastructure) system is being users to manage client certificates (**PKI Mode**) or the SWG Policy Server is to be used as the certificate authority (**Internal Certification Mode**). See the "Deployment Preparation and Decisions" section above for a more detailed explanation.*

To set the Certificate Management Mode

1. Navigate to **Administration – Cloud – Configuration.**
2. From the bottom of any of the **Cloud Configuration** tabs select the **Change Certification Management Mode** button.
3. Select either the **Internal Certification** or **Enterprise KPI** option.
4. Click **Save**.



6.3 Cloud Configuration - Internal Certification Mode

6.3.1 Internal Certification Mode Certificate Management (CA Management Tab)

The CA Management screen defines the Certificate Authority required for the creation and signing of all the certificates used in the Cloud environment (server certificates, mobile worker certificates).

For detailed instruction please see the **SWG Management Console Reference Guide section 5, Cloud - CA Management Tab (and CA Generation Options)**.

For details of the methods available for Client Certificates export and distribution, see Section 7.2 **Certificate Deployment** in this guide.

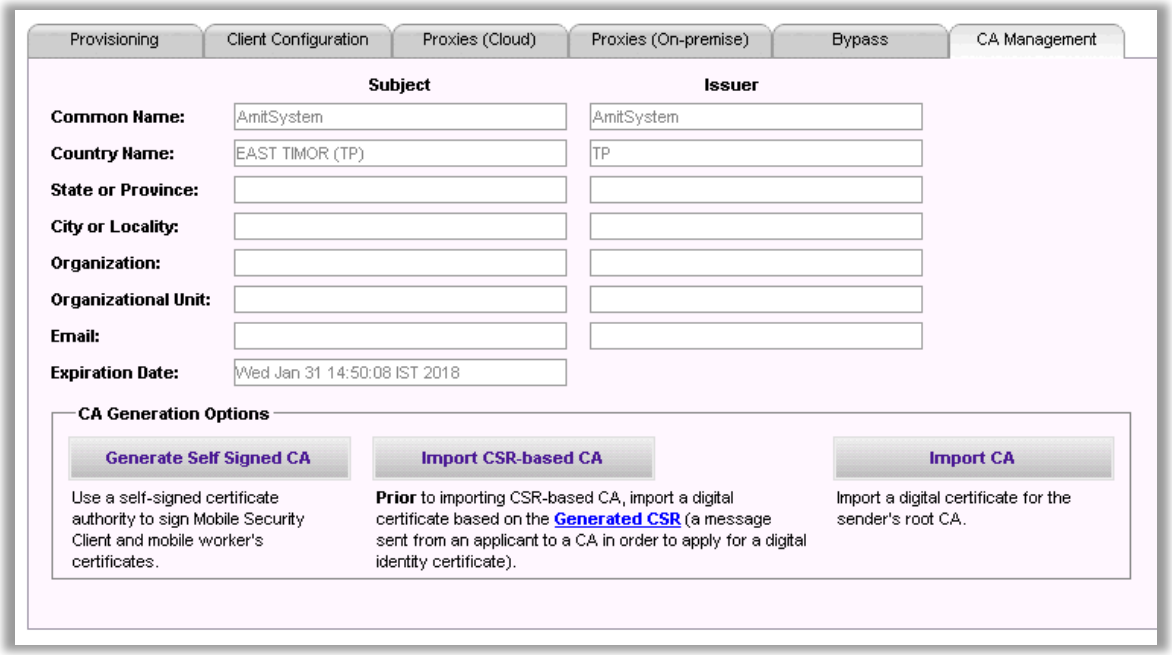


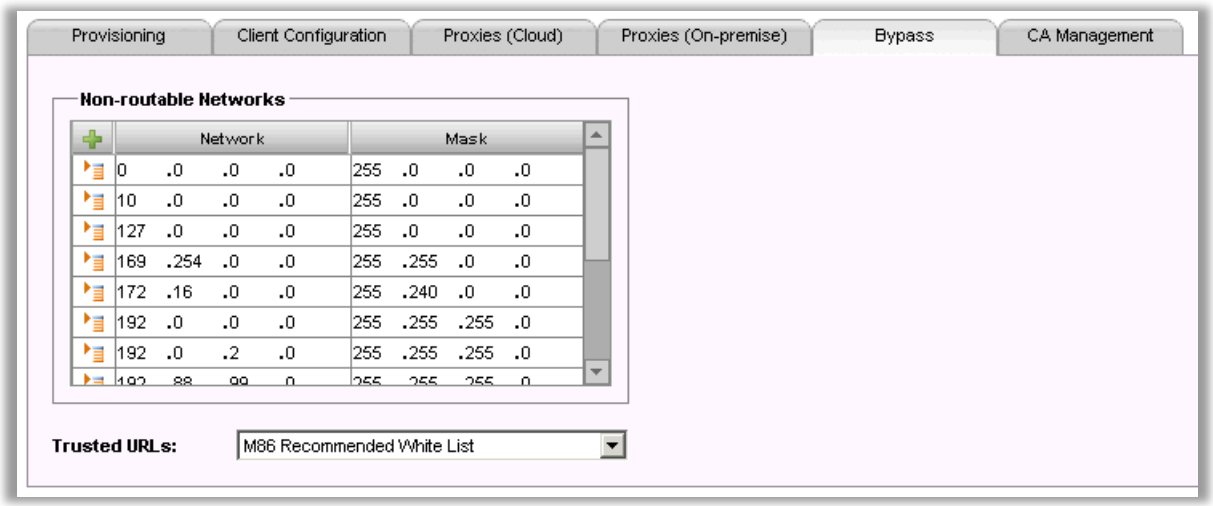
Figure: Sample CA Management Tab

6.3.2 Network and URL Exclusions - Bypass Tab

The **Bypass** tab is used to define those addresses that should be excluded (bypassed) from scanning and for which the user will connect directly to the Internet. The tab includes the following fields:

Non-Routable Networks: This table shows all networks or domains (IPs) to bypass while using Mobile Security Client with Cloud proxy or on-premise proxy.

Trusted URLs: Choose URLs that you want the Cloud proxy to bypass. Allow the organization to bypass certain URLs that the administrator deems safe (for example, Microsoft update etc.).



6.3.3 On-premise Settings - Proxies (On-premise) Tab

TIP**: SWG Management Console Reference Guide location: Chapter 5, Cloud Configuration in Internal Certification Mode, **Proxies (On-premise) Tab

The Proxies (on-premise) tab has two functions:

- To define web proxies that exist within the customer network and are to be used when a mobile user is working 'on-premise'.
- To define when a mobile user is on-premise and when they are off premise. This is achieved by defining a **Corporate Hostname** that can only be resolved to the defined **Internal Hostname IP** address when the user is 'on-premise'. The Mobile Security Client will use this information to connect either to an on-premise proxy or a Cloud Proxy (i.e. Cloud Scanner).

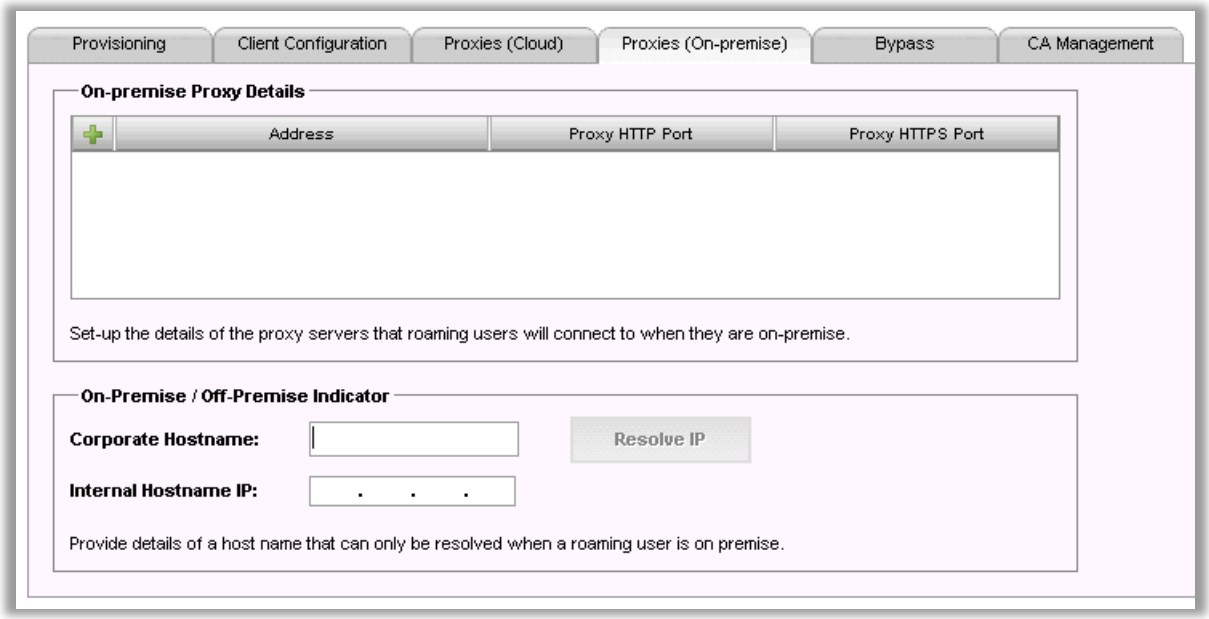


Figure: Proxies (On-premise) Tab

***NOTE**: The PAC file generated by the SWG Policy Sever will include instructions to use the local proxy, if resolvable, as it recognizes you are within the local network. If the corporate hostname is not resolvable to the configured IP, it will use the nearest defined Cloud Scanner (proxy) available.*

Enter On-Premise Proxy Details

1. Add the on-premise proxy details. There are two scenarios to consider depending on the SWG deployment type:

   Transparent Mode (implicit Proxy): If a transparent mode deployment has been used for the on-premise proxy, i.e. no proxy details used at the PC end, then do **not** add any **on-premise proxy details**.

   Implicit proxy: If the on-premise proxy (or load balancer) is used by pointing to it explicitly from the PC then add the IP address, HTTP and HTTPS ports for each one.

2. Repeat step 1 for each on-premise proxy.

To enter On-Premise/Off Premise Indicator details:

***NOTE**: This is effectively a indicator that allows the Mobile Security Client to determine whether it is on or off-premise.*

1. Enter the **Corporate Hostname** to be used as the on/off premise indicator.
2. Enter the **Internal hostname IP** that the **Corporate Hostname** will resolve to, or click the **Resolve IP** button.
3. Test the on/off premise indicator by selecting the **Resolve IP** button.

***IMPORTANT:** The administrator must ensure that the **Corporate Hostname is resolvable with the supplied Internal Hostname IP only when on-premise**. When the user is outside of the corporate network the corporate hostname should *not* be resolvable.*

6.3.4 Communications Ports - Proxies (Cloud) Tab

NOTE**: The term **Cloud Proxy** is used in this section. **Cloud Proxy** can be used refer to both **Cloud Scanner** and **Cloud Load Balancer.

TIP**: SWG Management Console Reference Guide location: Chapter 5, Cloud Configuration in Internal Certification Mode, **Proxies (Cloud) Tab

6.3.4.1 Port Numbering Considerations

IMPORTANT:

One very important aspect of the Hybrid that **must** be understood before attempting an implementation is IP port numbering. In SWG version 10.2 the configuration of IP port numbers has been greatly simplified by providing default values (port numbering scheme), validating all port numbers to look for potential clashes and more logical screen design/layouts. The three key things to remember about IP port numbers:

1. Communications between Mobile Security Client and Cloud Scanners are always on the same ports designated “Server Side” IP ports. There will be up to three ports, one for HTTP, one for HTTPS (if used) and a Control Port. These ports must be open on intermediate firewalls.

2. The Mobile Security Client software identifies different Cloud Scanners (e.g. one in Europe and one in the US West Coast) by internally mapping different IP port numbers to each; these “Local Client” port numbers are *not* used for communications to the scanners however.

3. Do not confuse protocol types and port numbers, normal defaults do not apply here. All communication from the Mobile Security Client to Cloud proxy is encrypted. So even when the client system is communicating using HTTP that traffic will be wrapped in HTTPS when travelling between the client and the Cloud Proxy. So port 443 is used by default to carry end user HTTP traffic, and port 993 has been chosen as the default for carrying end user HTTPS traffic.

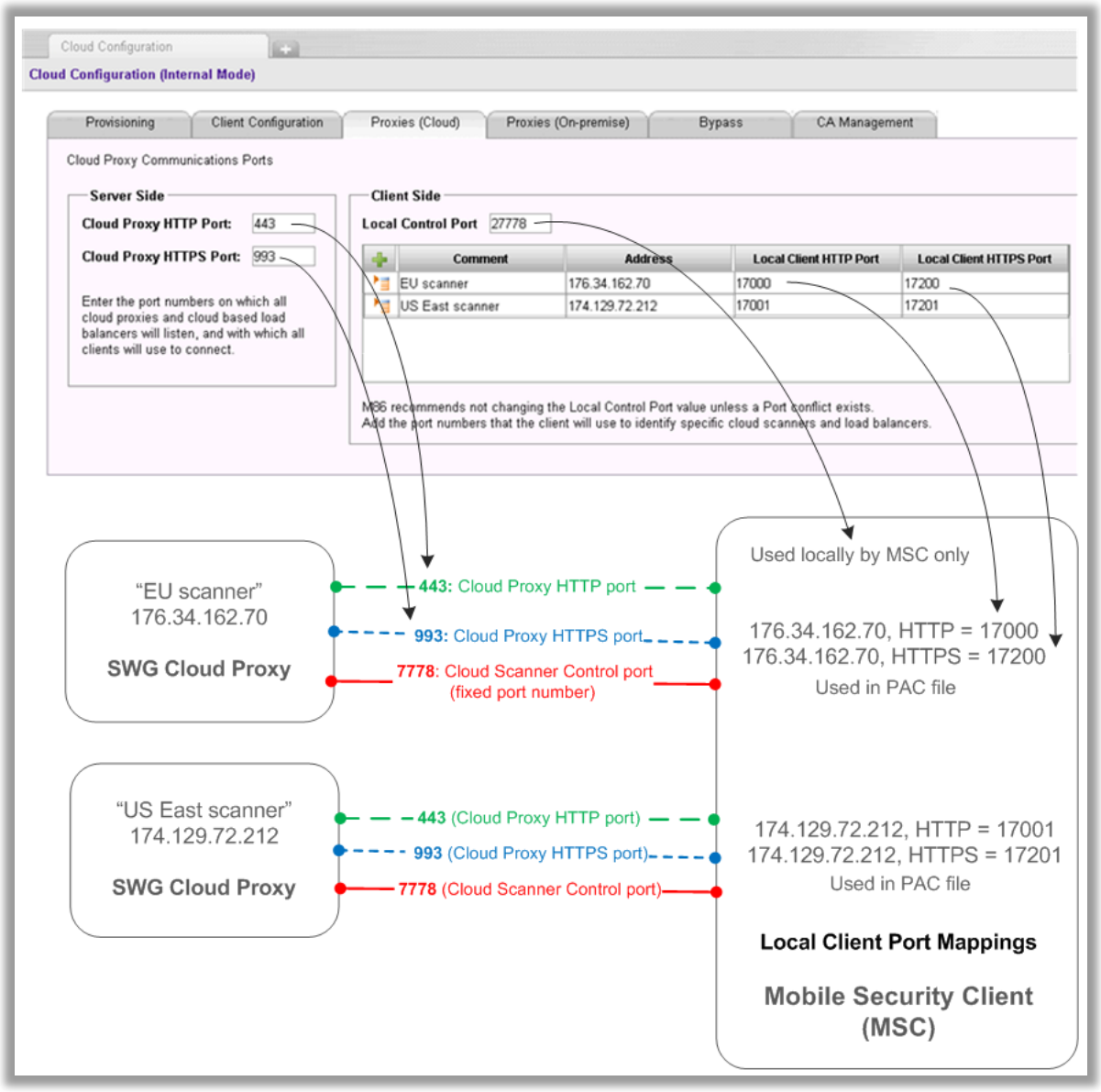
4. Please note that where an SWG Cloud Scanner is *not* configured to process HTTPS (perhaps the HTTPS option has not been purchased); the MSC will re-direct its HTTPS traffic over the same port as HTTP to the Cloud Scanner. The HTTPS traffic will be forwarded but not scanned.

6.3.4.2 Cloud Proxy Communications Port Settings

***NOTE**: the term “Cloud Proxy” equates to “Cloud Scanner” or “Cloud Load Balancer”.*

The following diagram illustrates how the port numbers in the SWG Policy Server Cloud Proxy configuration screen are used in an implementation. The scenario is that we have two Cloud Scanners in different geographic regions (Europe and the USA) and a personal computer (Windows or Mac OSX) with the Mobile Security Client installed.

***IMPORTANT**: The order in which the Cloud Proxies are defined determines the default sequence in which they are selected during initial startup of the Mobile Security Client (MSC). In the example below, the **EU scanner** would be the default Cloud Scanner. Once latency measurements have been made by the MSC, the Cloud Scanner exhibiting the lowest latency will be used. See the Mobile Security Client (MSC) Administrator Guide for further details.*



Default Cloud Proxy Ports are chosen to be opportunistic. They make use of commonly open port numbers in most firewall implementations, thus reducing the amount of work required to modify the network infrastructure and also to increase the chance of being able to communicate from, for example, an airport WiFi Hotspot.

TIP: See "**Port Numbering Best Practice**" in the Appendix B for further details.

6.3.5 Client Enforcement Settings - Client Configuration Tab

The **Client Configuration** tab allows you to define how use of the client software is enforced.

- **Prevent user from disabling client**: Enabling this checkbox ensures that the user cannot disable the agent in the browser, thereby allowing surfing through an M86 agent only.

NOTE: *This option only takes effect in conjunction with the **Prevent user from disabling Mobile Security Client** option set against the user groups (see section 6.5.1 Cloud Users and Groups (Internal Certification Mode)), i.e. switch the capability on in the Client Provisioning Tab, but apply it to specific users in the User /User Groups tab.*

- **Enforce PAC file usage via the Secure Web Service Agent**: This is key to correct operation of the client. Enabling this checkbox assures that the PAC file being used is an M86 PAC file, automatically generated, maintained and distributed to the Mobile Security Client. Administrators should keep this box unchecked if a proprietary PAC file is used. See also section 6.3.6.3 Download PAC File.

- **Enable Client Uninstall Warning Text**: When enabled, a warning message can be presented to the user if they attempt to uninstall the Mobile Security Client. The idea is to make the user fully aware of what they are attempting to do whilst linking this to the fact that they may contravening their employees acceptable use policy which will have a set of consequences. A default message is provided, however this can be customised as required. The default text is as follows:

> IMPORTANT WARNING!
>
> By uninstalling the Mobile Security Client you may be contravening your employer's Acceptable Use Policy.
>
> Please consider carefully whether you have the appropriate authority to take this action.

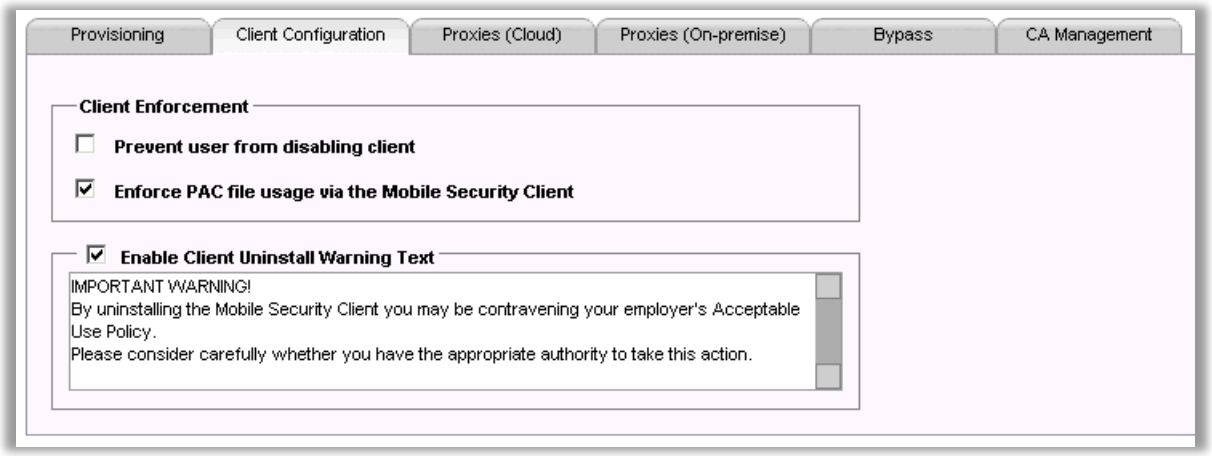


Figure: Client Configuration Tab

6.3.6 Client Provisioning Settings - Provisioning Tab

For details of fields on this screen, please see the SWG User Reference “Bypass Tab” section.

Please read this section in combination with the main “Client Software Provisioning” section below.

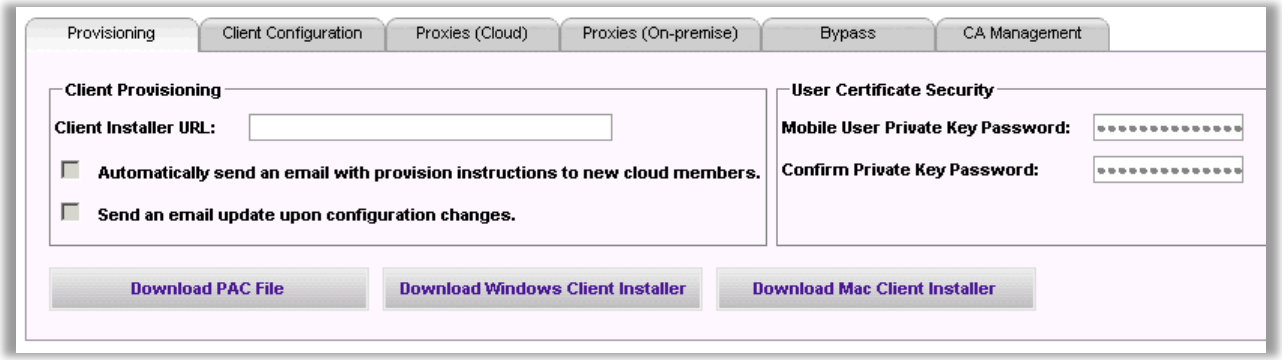


Figure: Provisioning Tab

6.3.6.1 User Certificate Security

The "Mobile User Private Key Password" is required by the end users to open their client certificates. Distribution of the password is performed manually by the administrator.

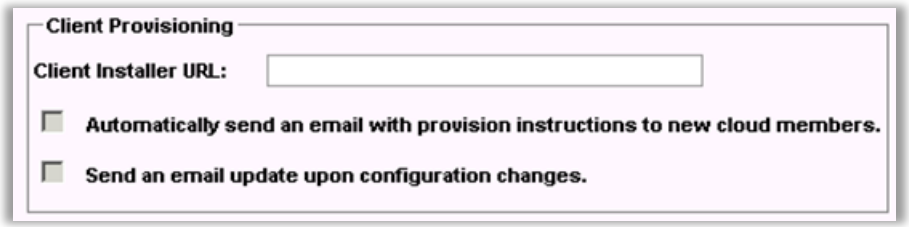
6.3.6.2 Provisioning by Email Settings

A mobile user can be self-provisioned using a **Provisioning email** (see section 6.3.7 Email Template below). This screen allows you to configure the Policy Server to automatically send a provisioning email to target cloud users with a link to the agent installation location either with or without a user certificate. The user must have local administrative rights on their PC to do this. This option is suitable for the integration phase or for small rollout / proof of concept deployment of up to a few hundred users.

***NOTE**: You can also choose to use the Policy Server to automatically or manually send the target user an email with the client certificate, and optionally the client installation instructions.*

***NOTE**: Emails will only be sent after configuration, after a new certificate is issued, and after changes have been committed.*

- Enabling the **Automatically send an email with provision instructions to new Cloud members checkbox** ensures that update emails are sent to users. Each time a new user receives new Cloud certification or a configuration change has occurred, an update email is sent.
- Enabling the **Send an email update upon configuration changes** is for existing users if changes have been made in the configuration



***NOTE**: Before downloading Client Installation packages or the PAC file the following should be configured. It will only be possible to download the Client installer if all of the esential configuration items have been addressed.*

- *At least one Cloud Scanner defined*
- *Proxies (Cloud)*
- *Proxies (On-premise) optional*
- *Client Provisioning*
- *Bypass optional*
- *CA Management tab information/configurations must be completed. All download buttons are disabled until all relevant information is input and committed successfully.*

We don't need the Mail Server to be configured, nor should we have Cloud Users or Groups. We do must have CA Management, Proxies (Cloud) and Provisioning tabs configured correctly, as well as at least one Cloud Scanner before installers and PAC file are available for download.

6.3.6.3 Download PAC File

The Proxy Auto Configuration (PAC) file defines how browsers can automatically choose the appropriate proxy server for retrieving a given URL. PAC files contain a "FindProxyForURL(url, host)" function that returns a string with one or more access method specifications. These specifications cause the user to use a particular proxy server or to connect directly.

There is no need to download the PAC file unless you intend to management it manually or have an agentless implementation (e.g. no Mobile Security clients, only remote/branch offices with web proxies chained to the Cloud Scanners.)

- **Automatic PAC File Management**

  The SWG Policy Server automatically generates and maintains a PAC file based on the Cloud Configuration entered. This can be automatically updated and distributed to PCs running the Mobile Security Client. Switch this function on by navigating to the **Configuration – Cloud Configuration – Client Configuration** tab and clicking the "**Enforce PAC file usage via the Mobile Security Client**" option; see section 6.3.5 Client Enforcement Settings - Client Configuration Tab for further details.

- **Customer Managed PAC File**

  Alternatively the PAC file can be managed manually to allow for customization. In this case download the PAC file whenever configuration changes are made and re-apply any customization before re-distribution. Customers using a proprietary PAC file **must** ensure that the local host proxy within the PAC file belongs to M86. Configuration updates and **enforcement** of the browser connection settings are then performed by the customer as part of their end point management system, e.g. Group Policy Objects.

To download PAC file for Customization or Inspection

1. Navigate in the Management Console to **Administration – Cloud Configuration- Provisioning** tab.
2. Click the **Download PAC file** button and Save.

***IMPORTANT**: It is the customer's responsibility to distribute a customized PAC file to its remote workers so that this is used in preference and also to enforce its use. The M86 PAC file is always included in the Client Installation Package and will be enforced only if explicitly configured to do so.*

6.3.6.4 Client Installation Packages

- **Using only one Client type (i.e. Windows or Mac)**

  In the **Client Installer URL** enter the location from which the user should download the Client installer package. This is the full URL including the client installer filename. The URL is used in the provisioning email templates.

- **Using both Windows and Mac clients in the same deployment**

When using both Windows and Mac clients, the **Client Installer URL** must point to a folder where both installers are listed. The end user then must choose the correct installer for their operating system. Be sure to make it clear in the email template which client is for Windows and which is for Mac.

To download the client installer code press the appropriate download buttons and save the file to a shared location as defined in the **Client Installer URL** definition above.

Windows and Mac clients can be distinguished by the file extension, e.g.:

- Windows: MobileSecurityClient-2.0.0.13-installer**.exe**
- Mac: MobileSecurityClient-2.0.0.13-installer**.mpkg.gz**

Rename main part of the filename as required to prevent end user confusion.

6.3.7 Email Template Configuration (Email Templates Screen)

The Secure Web Gateway provides a series of default email templates to automatically provision Cloud users via email. The templates can be customized as required, for example when using more than one client type.

To setup the provisioning email:

1. See the **SWG Management Console Reference Guide** section **Email Template**.

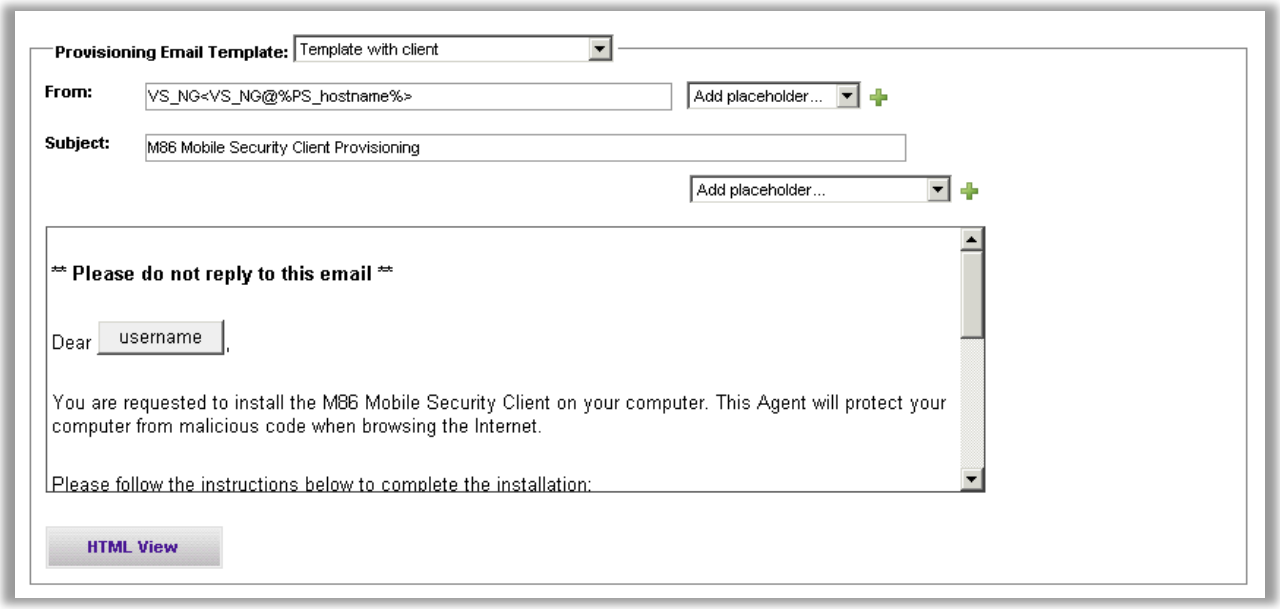


Figure: Example Email Template

6.4 Cloud Configuration in PKI Mode

When PKI Mode is used for certificate management the screen Cloud Configuration screens and associated tasks change:

- Proxies (Cloud) Tab - same as Internal Certification Mode.
- Proxies (On-premise) Tab - same as Internal Certification Mode.
- Bypass - same as Internal Certification Mode.

- CRL handling - for PKI Mode only.
- Provisioning – different for PKI Mode.
- Client Configuration – different for PKI Mode.
- Email template – not needed in PKI Mode.

A detailed treatment of the PKI mode configuration is being constructed for this Hybrid Deployment Guide. For now please refer to the **SWG Management Console Reference Guide Chapter 5, Cloud, and "MSC Cloud Configuration in PKI Mode"** for further details.

***NOTE**: Managing groups of mobile users in PKI Mode is performed by the administrator on the organizations PKI systems (assigning certificates only to mobile users). All that is required in the SWG Management Console is to import those user groups so that the SWG will be able to identify them and assign them a security policy.*

6.5 User Management

6.5.1 Cloud Users and Groups (Internal Certification Mode)

NOTE: This section is relevant to cloud implementation only in **Internal Certification Mode** as we can detect new users in Cloud groups and assign them certificates and send a provisioning email. In **PKI Mode** this has no bearing on the abovementioned.

User Groups can be created locally on the SWG or imported from LDAP. Using LDAP is recommended since it makes it possible for changes in, for example, Active Directory group membership to be reflected automatically in the SWG, i.e. new joiners to an organization will automatically be added, and leavers will be removed.

The key Cloud related parameters which you will need to configure are:

- Enable **Issue Mobile Security Client Certificates to new Group members** to automate certificate distribution.
- Enable **Prevent user from disabling Mobile Security Client** if you wish to prevent the users in this group from being able to temporarily disable the client software. This function is typically for trusted users.

6.5.1.1 User Defined User Groups

To modify User Defined User Groups settings for Cloud navigate to **Users – Users / User Groups** then click the particular group node.

For details of how to configure user groups and LDAP refer for the **SWG User Reference section 2, User Groups and User Defined User Groups**. Screen

6.5.1.2 LDAP Groups

To modify LDAP group settings for Cloud navigate to **Users - Authentication Directories - LDAP Groups** the click the particular LDAP Group node.

For details of how to configure Directory Groups for Cloud Users refer to the **SWG User Reference section 2, LDAP Groups** (Fields of the LDAP Group Details Screen).

6.5.2 Client Certificate Management (Internal Certification Mode)

See section 7.2.2 Internal Certification Mode – Internal Email Distribution of Certificates below.

7 Deploy Mobile Security Client & Certificates

This section is provided to help steer the Administrator through the activities of MSC and Certificate deployment.

7.1 Client Deployment

Options for deployment of the Mobile Security Client software are discussed in section 4.5 “Client deployment method choice: email or external system?” above.

7.1.1 Internal Certification Mode email distribution of Client

To configure the SWG to deploy the MSC by SWG ‘internal’ email delivered link direct to the end user, consult section **6.3.6 Client Provisioning Settings - Provisioning Tab**.

***NOTE**: Using Internal Certification Mode email distribution method also assumes that the client certificates will also be delivered by email from the SWG Policy Server.*

7.1.2 Active Directory/Group Policy Object Based Deployment of Client

To deploy the MSC using an external software distribution mechanism such as MS Active Directory and Group Policy Objects you will need to:

1. Download the client installers required (see section 6.3.6.4 Client Installation Packages above).
2. Follow the AD/GPO instructions in **Appendix A - AD MSC Installer Distribution**, below.

7.2 Certificate Deployment

Options for Certificate management are discussed in section **4.3 Certificate management method choice: PKI Mode or Internal Certification Mode?** above. Depending on your choice of certificate management method use the appropriate section below.

7.2.1 PKI Mode (External PKI System)

To configure for PKI mode see the Workflow Table in section **6.1 Work Flow for Configuring the SWG Policy Server for Hybrid Deployment** above.

7.2.2 Internal Certification Mode – Internal Email Distribution of Certificates

The following sections are provided as a quick reference. For more detailed instructions on issuing Client Certificates by groups, domains and individual users please see the **Users** chapter of the **SWG Management Console Reference Guide**.

7.2.2.1 Issue Certificate to Users and Groups Automatically

To issue Cloud certificates to Users and Groups

1. Navigate to the **Users – Users/User Groups** menu.
2. Enable the **Issue Mobile Security Client Cloud Certificate to new group members** checkbox.

***NOTE**: This section relies on previously configured domain users. For more information on domain users and local users, refer to the SWG User Reference Guide on Adding Domain Users.*

Client certificates will then automatically be issued to new group members.

7.2.2.2 *Issue Certificates to Domain Users Automatically*

To issue Cloud certificates for domain users:

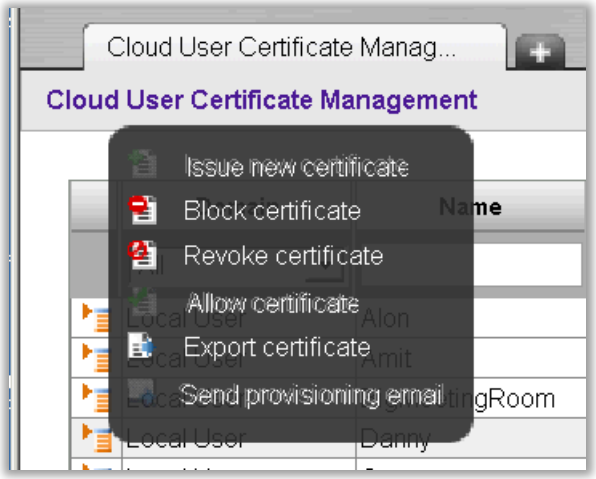
1. Navigate to **Users - Authentication Directory - LDAP**.
2. Right-click the LDAP directory and select the required LDAP group.
3. Click **Edit** and then enable the checkbox in the screen.

Client certificates will then automatically be issued to new group members.

7.2.2.3 *Issue Certificates to Individual Users Manually*

Issue Cloud certificates per User:

1. Navigate to **Users – Cloud User Certificate Management**.
2. Select the particular cloud user for whom a certificate is to be issued.
3. Click the  icon, then select **Issue New certificate**.



A client certificate will be sent via email to the selected user.

7.2.3 Issue Certificates via Active Directory Distribution

The following steps are needed:

Export all client certificates from SWG for use in Active Directory.

1. Login to the SWG Management Console and navigate to **Users – Cloud User Certificate Management**.
2. **Click** the **Export All Certificates** button.
3. **Save** the export file.

The export file will contain all valid client certificates arranged in a zipped directory structure organized by folders representing the user groups (defined in the Users – User Group screen). Use this file as input to the Active Directory / Group Policy Object distribution process.

Import the client certificate files into the Active Directory.

1. See **Appendix A – AD Certificate Distribution** below.

Appendix A – Active Directory Distribution

AD Certificate Distribution

M86-Security provides a solution for the distribution of the **Client Certificates** (p12) via the organizations Active Directory Group Policy Objects (GPO). The solution is a silent installation and distribution of digital certificates as a unique identifier for end-users of the M86 SWG Hybrid deployment with Cloud Scanners.

Upon user login to the domain, on a station in which the Mobile Security Client is already installed, the user will receive the unique key and certificate via the domain's GPO. It should be noted that this solution will be applied at the user's login (not when unlocked) and when the policy is refreshed (based on the set defaults of the organization). The Solution will test whether the certificate is needed, and if so, the certificate will be installed for the user.

Preparation

Obtain the script files

1. Download and install a file archive manager, such as 7-zip (www.7-zip.org).
2. Define a dedicated file folder in the system where cloud user certificates are to be placed (for example: CertsDir).
3. Extract the cloud user certificates, as downloaded from the SWG Policy Server GUI [insert exact screen name and documentation reference], into CertsDir. **Ensure the certificate name format is as follows: <username>.p12**
4. Extract both "**ChangePermissions**.bat" and "**Install.vbs**" script files to the CertsDir (obtain M86 SWS-AD Integration.zip file or create the scripts from the details provided in section **0 Active Directory Integration Scripts** below).
5. Run the **ChangePermissions**.bat file (The file should be run under Administrator privileges).

***NOTE**: The .bat file changes the permissions on the certificates (.p12) files and allows each user to access only the certificate file that belongs uniquely to that user.*

Edit the script variables according to the enterprise-specific environment:

1. Right-click the file **Install.vbs** and select **Edit**.
2. In the selected text, change the values for the following:

   SERVER – The server from which the cloud users obtain their certificates.

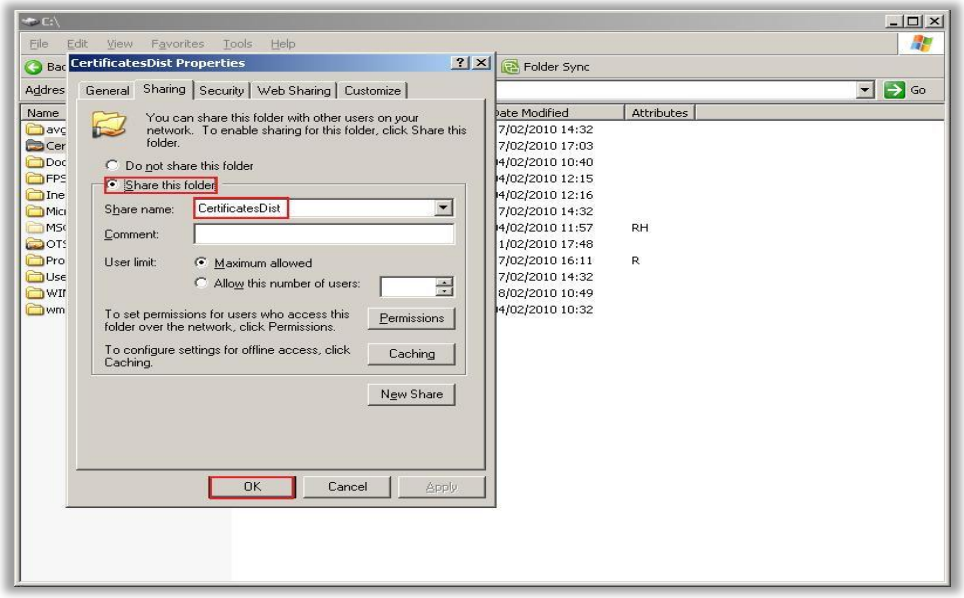
***NOTE**: "The server" pertains to the Domain Controller IP/name and not the Policy Server name.*

   PASSWORD – The cloud user's certificate password as defined in the Policy Server GUI during initial policy server configurations.

3. Save the file and exit.

Server Actions

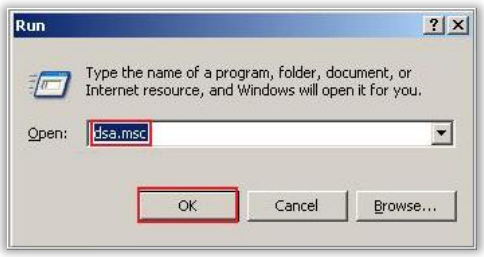
1. Create a folder titled "CertificatesDist". This folder can be created anywhere in the file system of the operating system.
2. Right-click the "CertificatesDist" folder and select **Sharing and Security**.
3. Enable the **Share this folder** radio button and set the share name as **CertificatesDist**.



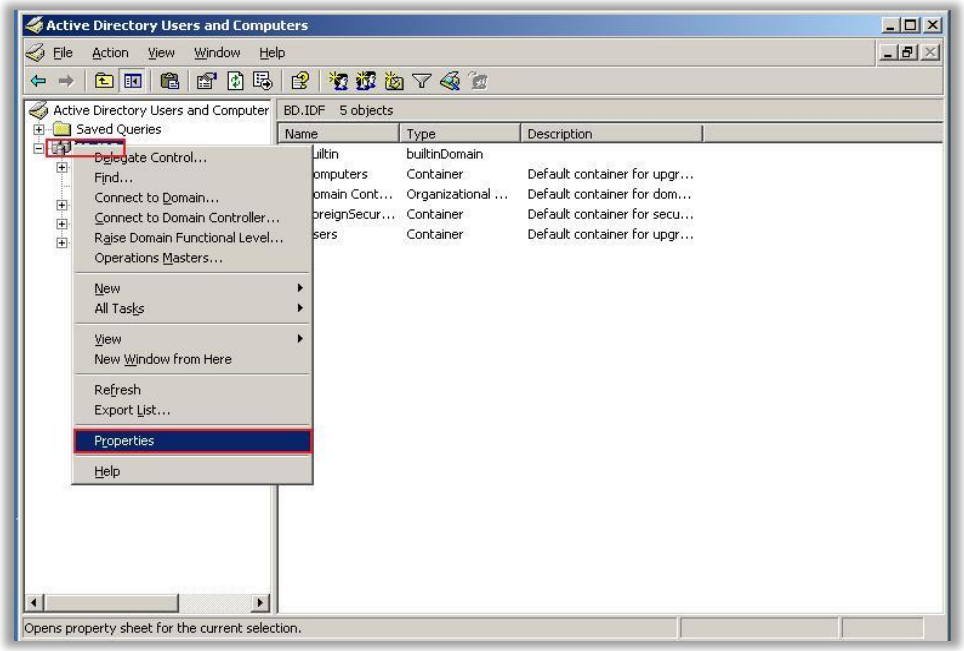
4. Move all the files previously created in the Preparation section above, as well as the certificate files, to the "CertificatesDist" folder.

Active Directory Actions

1. Open the Active Directory Users and Computers Management Screen.
2. Navigate to the **Start** menu, select **Run**.
3. Enter line: **dsa.msc** and click **OK**.

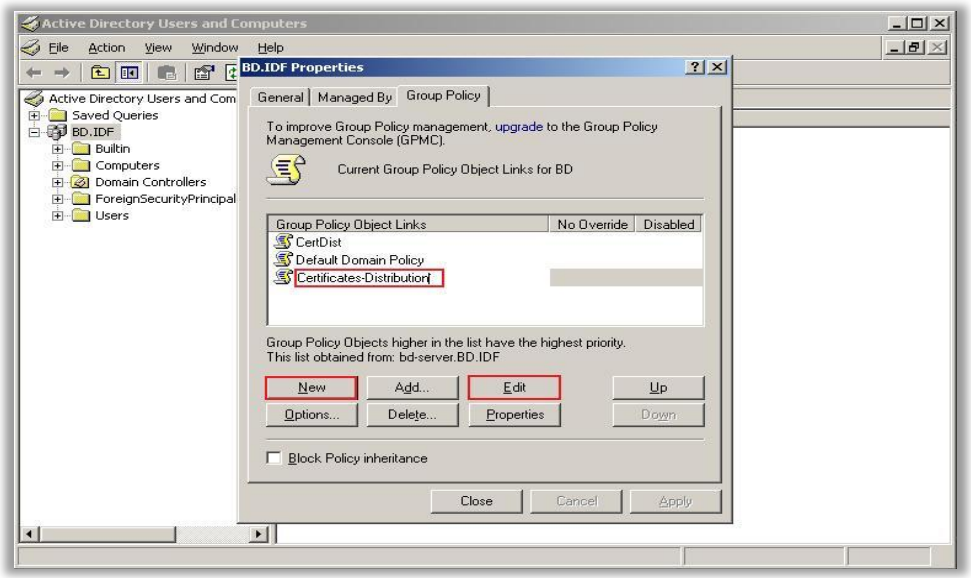


The Active Directory Users and Computers screen will open:

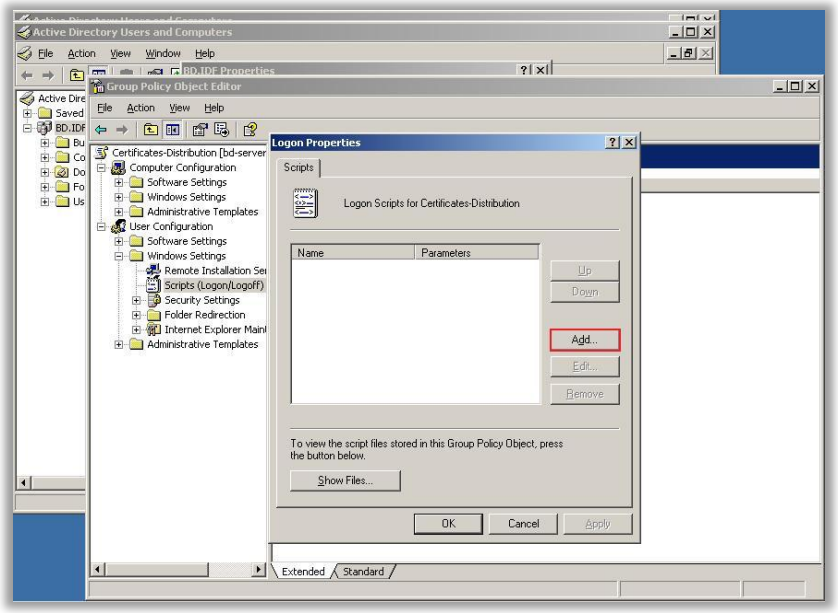


4. In the left tree pane, select the **Domain**, right-click and choose **properties**.
5. In the **Domain Properties** window, in the **Group Policy** tab, create the required Group Policy Object:

   a. Click **New**.
   b. Change the name of the Group Policy Object as required. For example: **Certificates-Distribution**.
   c. Click **Edit**.

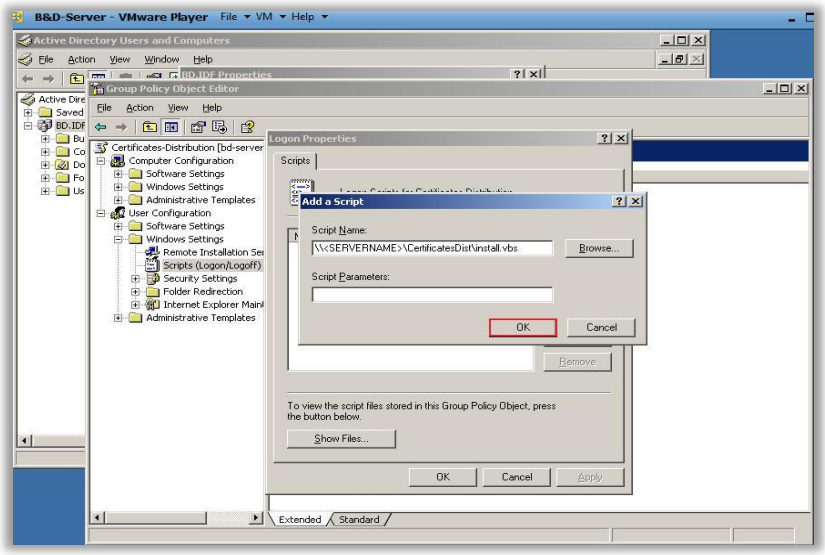


   d. In the open **Group Policy Object Editor** window, navigate to **Windows Settings**.
   e. Select Scripts (Logon /Logoff) and double-click Logon.
   f. Click **Add**.



g. Under **Script Name**, register the full path of the share folder where the script **Install.vbs** is saved, and click **OK**. The path should be, for example, \\<SERVERNAME>\CertificatesDist\install.vbs

WARNING! *Do not choose the path via Browse! Enter the path manually.*



h. In the window **Logon Properties** click **OK**.

i. Close the **Group Policy Object Editor** window.

6. In the **Properties** window (Domain), click **Close**.
7. Close Active Directory Users and Computers.
8. Click **Start**, select **Run**, and enter “gpupdate /force” in the text box.
9. Click **OK**.

Active Directory Integration Scripts

M86SWS-AD-Integration.zip

Obtain the Active Directory integration utility scripts from the M86 Knowledge Base/Support web site, or create the required scripts based on the text below:

Change Permissions (Windows Batch File)

```
dir /b *.p12 > p12s.txt
for /f %%a IN (p12s.txt) do Echo Y| cacls %%~na.p12 /t /c /g %%~na:F
del p12s.txt
```

Install (VBScript Script File)

```
Dim PASSWORD, SERVER, USER, TEMPDIR, PROGDIR
PASSWORD = "12345"
SERVER = "192.168.90.64"
USER = CreateObject("WScript.Shell").ExpandEnvironmentStrings("%username%")
TEMPDIR = CreateObject("WScript.Shell").ExpandEnvironmentStrings("%Temp%")
PROGDIR = CreateObject("WScript.Shell").ExpandEnvironmentStrings("%ProgramFiles%")

set FSO = CreateObject("Scripting.FileSystemObject")
If FSO.FileExists( PROGDIR & "\Finjan\FCS Agent\fcsagent.exe") Then
        If  FSO.FileExists("\\" & SERVER & "\CertificatesDist" & "\" & USER & ".p12") Then
                Dim objFSO, WSHNetwork
                Const OverWriteExisting = True
                Set objFSO = Createobject("Scripting.FileSystemObject")
                wsLocation = TEMPDIR & "\"
                objFSO.CopyFile "\\" & SERVER & "\CertificatesDist" & "\" & USER & ".p12",
wsLocation, OverWriteExisting

                strProgramPath = PROGDIR & "\Finjan\FCS Agent\CertificateImporter.exe"
                set objShell = createobject("Wscript.Shell")
                objShell.Run Chr(34) & strProgramPath & Chr(34) & " " & wsLocation & USER &
".p12" & " " & PASSWORD, 1, true

                Set aFile = fso.GetFile(TEMPDIR & "\" & USER & ".p12")
                aFile.Delete
        End If
End If
```


AD MSC Installer Distribution

M86-Security provides a solution for the distribution of the **Mobile Security Client** via the organizations Active Directory Group Policy Objects (GPO). The solution is a silent installation of the Mobile Security Client for end-users of the M86 SWG Hybrid deployment with Cloud Scanners.

To install the Agent, an administrator must log into the work station/PC. This is required as the agent must be installed with administrator privileges.

Preparation

Obtain the script files

1. Download and install any file archive manager, such as 7-zip (www.7-zip.com).
2. Define a dedicated file folder in the system where MSC installer is to be placed (for example: MSCInstallerDir).
3. Download the MSC installer from the SWG Policy Server GUI [insert exact screen name and documentation reference], into MSCInstallerDir. **Installer name can be changed!!**
4. Extract the "**installAgent.vbs**" script file to the MSCInstallerDir (obtain M86 SWS-AD Integration.zip file or create the script from the details provided in section **0 Active Directory Integration Scripts** below.

Edit the script variables according to the enterprise-specific environment:

5. Right-click the file **InstallAgent.vbs** and select **Edit**.
6. In the selected text, change the values for the following:

   SERVER – The server from which the cloud users obtain their certificates.

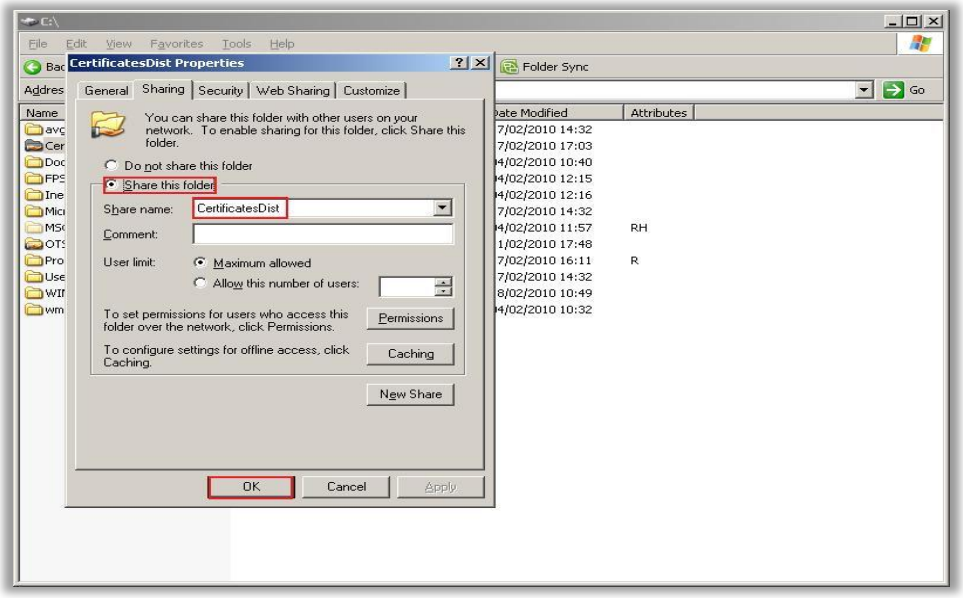
***NOTE**: The "server" pertains to the Domain Controller IP/name and not the Policy Server name.*

   INSTALLER – The Secure Web Service Agent installer file name. The installer is downloaded from the Policy Server GUI (see 6.3.6.4 Client Installation Packages above).

7. Save the file and exit.

Server Actions

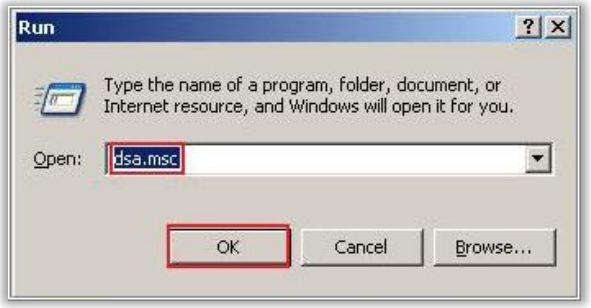
1. Create a folder titled "ClientDist". This folder can be created anywhere in the file system of the operating system.
2. Right-click the "ClientDist" folder and select **Sharing and Security**.
3. Enable the **Share this folder** radio button and set the share name as ClientDist.



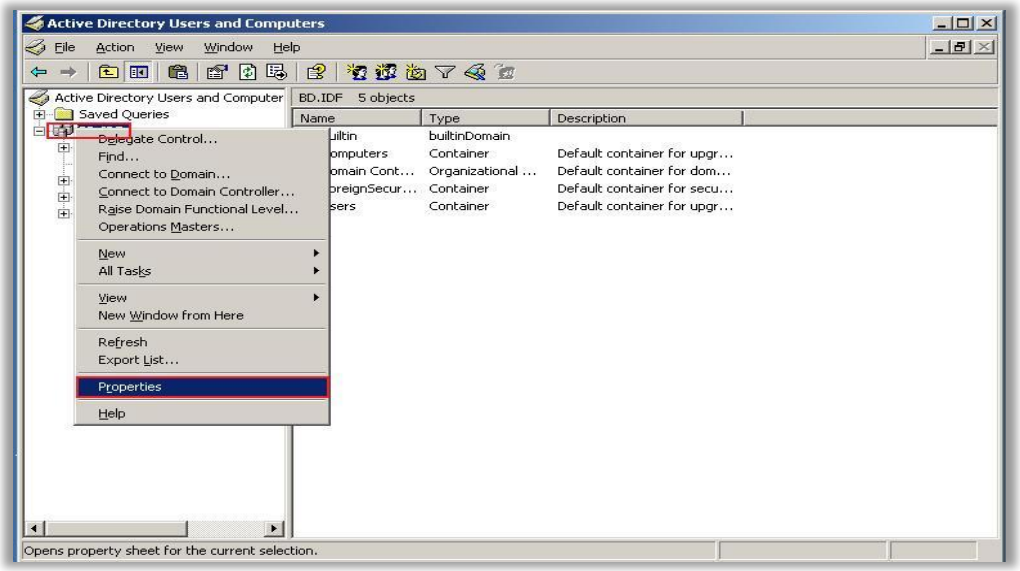
4. Move all the files previously created in the Preparation section above, as well as the MSC installer, to the "ClientDist" folder.

Active Directory Actions

1. Open the Active Directory Users and Computers Management Screen.
2. Navigate to the **Start** menu, select **Run**.
3. Enter line: **dsa.msc** and click **OK**.



The Active Directory Users and Computers screen will open:

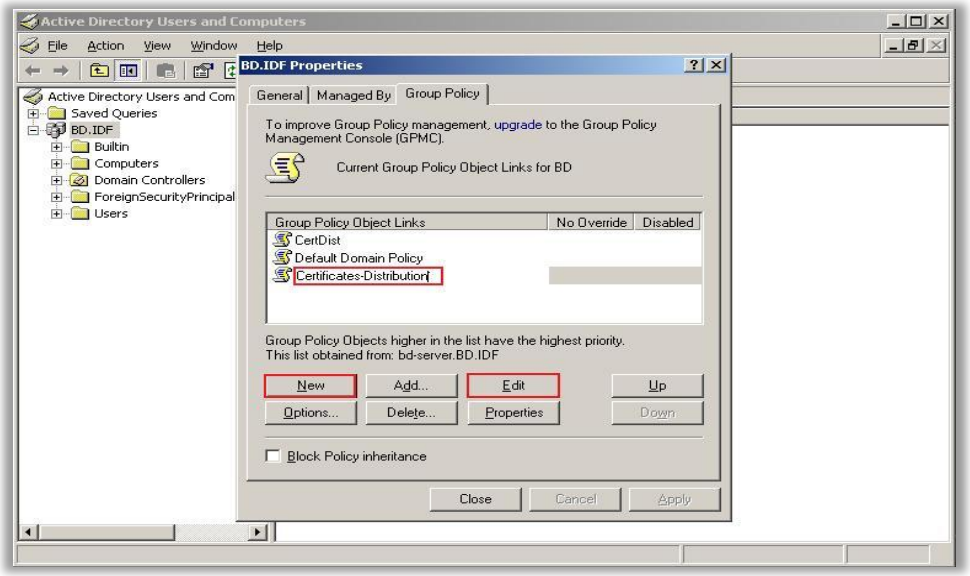


4. In the left tree pane, select the **Domain**, right-click and choose **properties**.
5. In the **Domain Properties** window, in the **Group Policy** tab, create the required Group Policy Object:

a. Click **New**.

b. Change the name of the Group Policy Object as required. For example: **MSC-Distribution**.

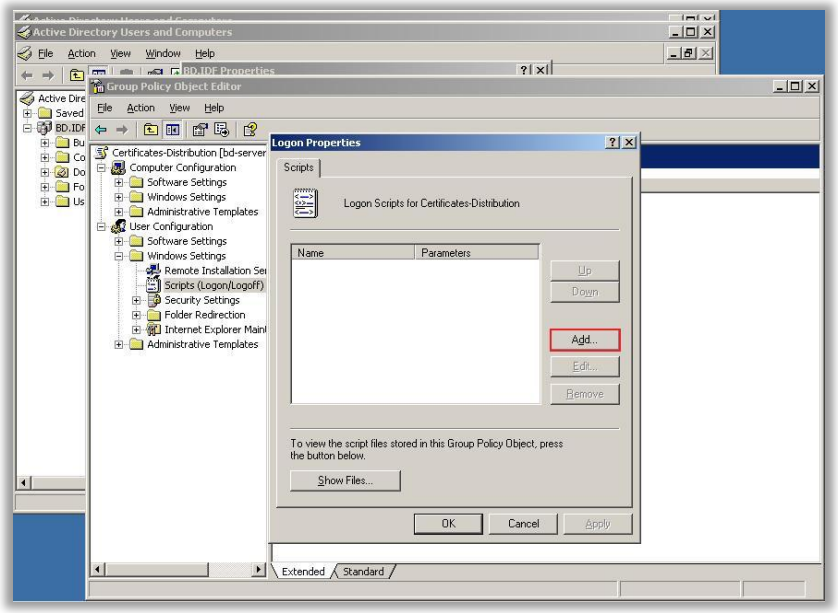
c. Click **Edit**.



d. In the open **Group Policy Object Editor** window, navigate to **Windows Settings**.

e. Select Scripts (Logon /Logoff) and double-click Logon.

f. Click **Add**.



g. Under Script Name, enter the full path of the share folder where the script **InstallAgent.vbs** is saved and click **OK**.

WARNING! *Do not choose the path via Browse! Enter the path manually.*

h. In the windows **Logon Properties** click **OK**.

i. Close the **Group Policy Object Editor** window.

6. In the **Properties** window (Domain), click **Close**.
7. Close Active Directory Users and Computers.
8. Click **Start** , select **Run**, and enter “gpupdate /force” in the text box.
9. Click **OK**.

Active Directory Integration Scripts

M86SWS-AD-Integration.zip

To obtain the Active Directory integration utility scripts, either speak to M86 Security Technical Support or create the required scripts based on the text below.

Obtain the Active Directory integration utility scripts from the M86 Knowledge Base/Support web site or create the required scripts based on the text below

installAgent (VBScript Script File)

```
Dim SERVER, INSTALLER, USER, TEMPDIR, PROGDIR
SERVER = "192.168.90.64"
INSTALLER = "SWSA.exe"
USER = CreateObject("WScript.Shell").ExpandEnvironmentStrings("%username%")
TEMPDIR = CreateObject("WScript.Shell").ExpandEnvironmentStrings("%Temp%")
PROGDIR = CreateObject("WScript.Shell").ExpandEnvironmentStrings("%ProgramFiles%")
```



```
set FSO = CreateObject("Scripting.FileSystemObject")
If FSO.FileExists(PROGDIR  & "\Finjan\fcs agent\fcsagent.conf") Then
	wscript.quit
End If

If StrComp(USER, "administrator", vbTextCompare) = 0 Then
	Dim objFSO
	Set objFSO = CreateObject("Scripting.FileSystemObject")
	objFSO.CopyFile "\\" & SERVER & "\CertificatesDist\" & INSTALLER, TEMPDIR & "\", True
	strProgramPath = TEMPDIR & "\" & INSTALLER
	set objShell = createobject("Wscript.Shell")
	objShell.Run strProgramPath & " /S"
End If
```


Appendix B – Port Numbering Best Practice

All Cloud configuration port numbers are customisable by the administrator; however the defaults have been chosen to give best results in most situations.

TIPS:

Windows PCs and Mac PCs are no different when it comes to port configuration.

An Amazon EC2 Cloud Scanner looks the same to the SWG Policy Server as an M86 Security SWS-Hybrid Cloud Scanner.

In order to make the configuration self-documenting we suggest that the comment field "Cloud Instance Identifier) is used to identify the type and location of the Cloud Scanner device. This can also be linked to the Amazon EC2 Instance name.

In the example configuration data below, both HTTP and HTTPS are being used, also the "IP Address" - is the IP address of the Cloud Scanner or Load Balancer.

CONTROL PORT	27778		
SERVER SIDE			
Cloud Proxy HTTP Port	443		
Cloud Proxy HTTPS Port	993		
CLIENT SIDE		**Local Client**	
Comment	**IP Address**	**HTTP Port**	**HTTPS Port**
Cloud Scanner 1 (e.g. USA)	n.n.n.a	17000	17200
Cloud Scanner 2 (e.g. Europe)	n.n.n.b	17001	17201
Cloud scanner x	n.n.n.c	1700x	1720x

Appendix C – Useful Links

PAC file resource: http://findproxyforurl.com/iphone_proxy_pac.html

Amazon EC2 FAQs: http://aws.amazon.com/ec2/faqs/

M86 Security SWG Documentation: http://www.m86security.com/support/Secure-Web-Gateway/Documentation.asp

---

About M86 Security

M86 Security is the global authority in malware prevention and content security. The company's appliance, software, and Software as a Service (SaaS) solutions for Web and email security protect more than 25,000 customers and 26 million users worldwide. M86 products use patented real-time code analysis and behavior-based malware detection technologies as well as threat intelligence from M86 Security Labs to protect networks against new and advanced threats, secure confidential information, and ensure regulatory compliance. The company is based in Irvine, California with international headquarters in London and development centers in California, Israel, and New Zealand. For more information about M86 Security, please visit www.m86security.com.

