

QUICK START GUIDE

# ActiveTrust Cloud

Custom redirect destinations

Integration with Proxy, Security Web Gateway, Blackhole, Honeypot

April 2018

# Contents

- Overview ..... 3
- Prerequisites ..... 3
- Architecture ..... 3
- Redirect options ..... 4
  - Default Redirect Page ..... 4
  - Custom IP/Domain redirect ..... 5
- Policies ..... 6
- References ..... 6

## Overview

Infoblox ActiveTrust Cloud blocks DNS based data exfiltration, stops malware communications with command-and-control servers, and automatically prevents access to content that are not in compliance with defined policies. The solution provides these benefits using automated, high-quality threat intelligence feeds, behavioral analytics, and machine learning to catch even zero-day threats. Delivered as a service, ActiveTrust Cloud is easy to use, deploy, and maintain without dedicated IT resources and it protects devices everywhere—on the enterprise network, roaming, or in remote office/branch offices.

ActiveTrust Cloud also offers unified policy management, reporting, and threat analytics across the entire spectrum.

You can integrate ActiveTrust Cloud with 3rd party proxy, secure web gateway, blackhole, honeypot and sinkhole solutions as well as create your own redirect site.

The document contains an overview of how you can apply multiple redirect actions and integrate ActiveTrust Cloud with McAfee Web Gateway solution, on-premise or in the cloud.

This document covers configuration on the Infoblox ActiveTrust Cloud portal and doesn't cover any configuration required on McAfee Web Gateway. Please refer to the relevant documentation provided by McAfee for any Web Gateway related configuration.

## Prerequisites

ActiveTrust Cloud subscription and relevant 3rd party software licenses or subscriptions.

## Architecture

DNS is a core network protocol which can be used as an additional protection layer to mitigate malware, stop data exfiltration and redirect traffic for further analysis.

### Packet flow

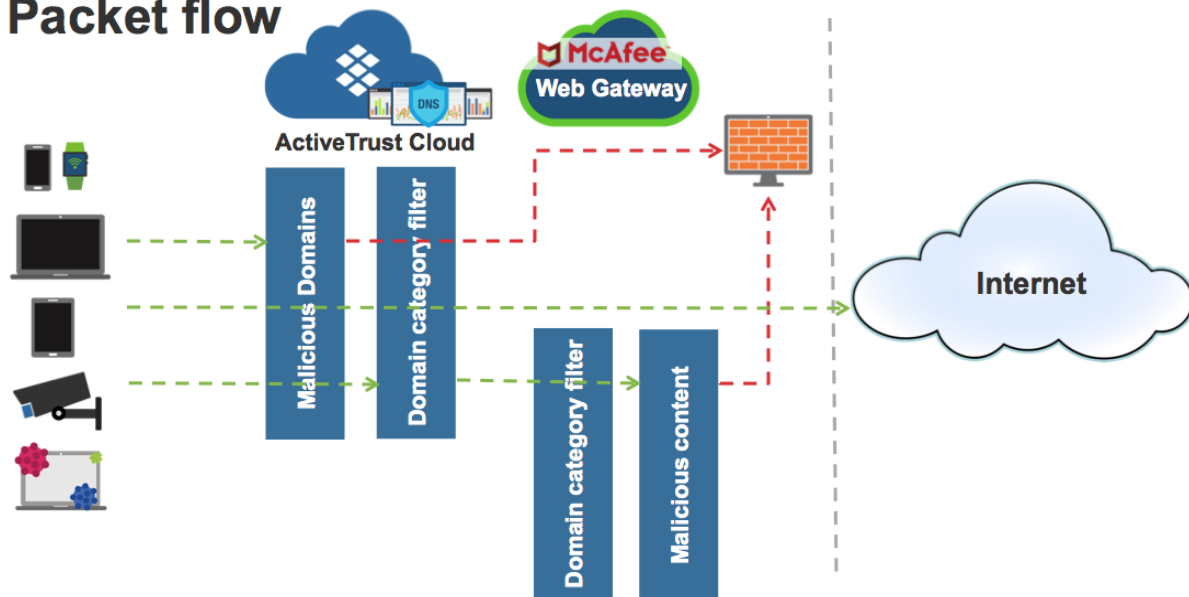


Figure 1. Traffic analysis flow

Based on your security policies there could be multiple deployment scenarios, depending on whether end clients are able to directly resolve domain names, and which threats and domain categories should be immediately blocked and which ones should be redirected to a 3rd party software for additional analysis.

McAfee Web Gateway can be installed on-premises or used as a service in the Cloud. All possible configurations are supported, including McAfee Web Proxy Client, which can be installed on roaming clients and work in conjunction with ActiveTrust Endpoint.

## Redirect options

ActiveTrust Cloud provides you multiple options on how to handle incoming DNS requests based on security policies or a domain categorization. The policy actions include: Allow, Log, Block, and Redirect. Multiple redirect destinations can be configured per policy depending on a domain category and/or a malicious destination list/custom list.

The default redirect destination is: "Redirect - Infoblox". Other custom redirect destinations must be created before using in a policy.

To configure redirect actions, navigate to "**Manage**" → "**Redirect Page**".

The screenshot shows the 'Define Redirect Page' configuration interface. The left sidebar contains navigation options: Networks, ActiveTrust Endpoints, DNS Forwarding Proxy, Custom Lists, Security Policies, Category Filters, Redirect Page (selected), and Bypass Internal Domains/IP Addresses. The main content area is titled 'Define Redirect Page' and includes a descriptive paragraph: 'When blocking users from accessing domains, you can redirect those users to a predefined page. Using the form below, you can set a redirect page of your own or you can customize the Infoblox redirect page.' Below this, there are two sections: 'Infoblox Redirect' and 'Custom IP/Domain Redirect'. The 'Infoblox Redirect' section features a dropdown menu with 'Use Default Redirect' selected, and a preview of the 'ACCESS DENIED' page. The 'Custom IP/Domain Redirect' section has a search bar and a table with the following data:

	Name	IP/Domain
<input type="checkbox"/>	MWG HQ	10.60.32.205
<input type="checkbox"/>	MWG Cloud	c1[REDACTED]9.saasprotection.com
<input type="checkbox"/>	Custom Block Page	block.example.com

Figure 2. McAfee Web Gateway on-prem, McAfee Web Gateway in the Cloud and custom redirect portal configured

## Default Redirect Page

The default redirect page is hosted in ActiveTrust Cloud and provides basic functionality to notify users about blocked requests. The redirect page is available via HTTP/HTTPS only. Other protocols are not supported. You can modify the default redirect page by providing a custom message in HTML format.

To update the content of the default redirect page:

- Navigate to "**Manage**" → "**Redirect Page**".
- Under "**Infoblox Redirect**" click on "**Use Default Redirect**" and select "**Use Custom Message**".
- Type or paste a custom message into "**HTML**" textbox. You can use HTML markup to include images, links, highlight text etc.

## Custom IP/Domain redirect

The "Custom IP/Domain redirect" option can be used to display a custom redirect page with additional contextual information and actions. It can also be used to specify integration points with different solutions like proxy servers, secure web gateways, sinkholes, honeypots, blackholes etc. These 3rd party solutions must be managed by the customer. It is the customer's responsibility to keep the destination IP-addresses and domains up to date. Currently, ActiveTrust Cloud supports up to 5 custom redirect destinations.

**Note:** There are no differences or dependencies on 3rd party software in terms of configuration on the ActiveTrust Cloud portal. You should register an IP-address or a domain name used by any 3rd party solution.

To add a custom redirect destination:

- Navigate to "**Manage**" → "**Redirect Page**".
- Click on the "**Custom IP/Domain Redirect**" label.
- Click "+".
- Fill "**Name**" and "**IP/Domain**" fields with appropriate values.
- Click "**Save**".

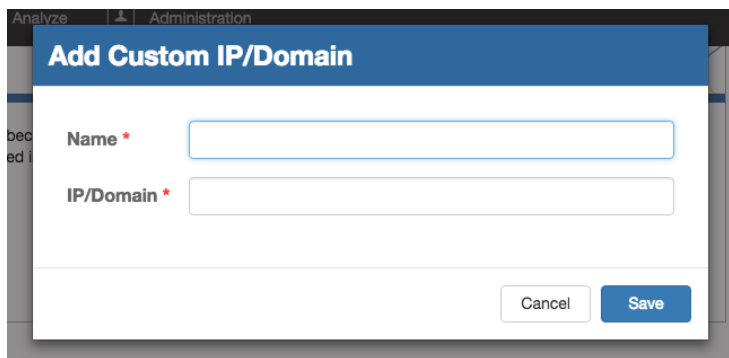


Figure 3. Add an IP/ domain window

Proxy servers and secure web gateways guarantee support for HTTP/HTTPs protocols. Because DNS redirects all traffic to a different destination, please check with your proxy server or security web gateway vendor about other supported protocols and estimate your risks if you will redirect traffic to these solutions using DNS, especially if you are implementing DNS filtering based on domain categories.

**Check that your proxy/web gateway supports all required protocols and complies with your security policy, if traffic should be redirected for further analysis via DNS. Some applications (e.g. mail service) can be affected by applied security policies. You can whitelist domains if required.**

## Policies

A security policy is a set of rules and actions that you define to balance access and security, to mitigate threats. When you configure a security policy, you define a scope and policy actions for each threat intelligence list, optional custom lists and category filters. In addition to the default actions (Allow, Log, Block, Redirect - Infoblox) you can specify a custom redirect action.

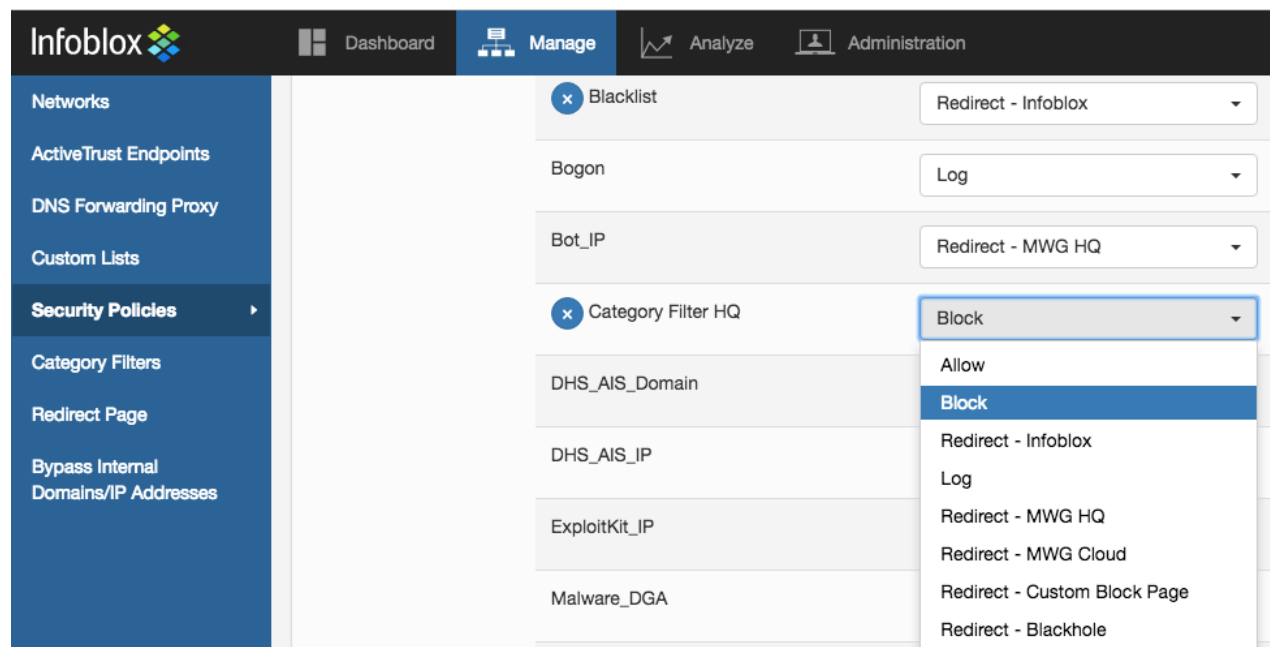


Figure 4. Policy configuration window

**To avoid service disruption the following are recommended as best practices:**

- Set all new threat feeds in the Log only mode
- Set category filtering in the Log only mode
- Carefully review the results after a few days or weeks

**Domains which should not be blocked or redirected for analysis must be whitelisted before applying Block or Redirect actions.**

## References

1. ActiveTrust Cloud Administrator guide (<http://help.csp.infoblox.com/infoblox-activetrustcloud-home/>)