Passive Identity Management Administrator Guide, Release 1.2

First Published: April 17, 2012
Last Modified: April 27, 2016

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number:
CONTENTS

Preface

Overview v
Prerequisites v
Limitations vi

CHAPTER 1

Configure PIM 1

Overview 1
Configure Portal 1
Configure Desktop 2
  Configure Firewall 2
  Configure Browser 2
Logon Script 2
PIM Command-Line Arguments 3
Upgrading from a Previous Version 4

CHAPTER 2

Deploy PIM 5

Overview 5
Verify Granularity 5
  Malware Scanning Service 5
  Web Filtering Service 5
Known Issues and Workarounds 6
Preface

- Overview, page v
- Prerequisites, page v
- Limitations, page vi

Overview

Passive Identity Management (PIM) has been developed to provide user-level granularity for Cisco Cloud Web Security (CWS).

PIM provides an alternate solution for large organizations which would previously have had to install and maintain multiple proxies within their environments to obtain this level of granularity. Alternatively, PIM may also be used for simple installation by smaller organizations.

PIM is a small Microsoft Windows application, typically executed using a sign-in script to obtain user or group information. This information is passed out-of-band using an HTTPS request and a user identifier is embedded in the browser user-agent request header for all subsequent requests.

Typically, PIM is hosted on a network location accessible by the client machine. Cisco recommends using a Domain Controller for this purpose so that PIM is visible across the domain to all users.

Customer HTTP and HTTPS traffic is forwarded directly to the 'in-the-cloud' scanning infrastructure using a proxy setting or proxy-auto config (PAC) file. No customer proxies are required. A unique identifier string is encrypted and added to the HTTP header. However, it is meaningless to any person or system except the CWS proxies. There is no performance overhead or increased packet size because PIM sends user and group data once only at the time of registration. HTTP headers contain only the short identifier.

As with standard deployments, customer IP addresses are registered with Cisco to allow access to the scanning infrastructure.

This guide assists you during rollout by explaining how to configure the solution across your infrastructure.

Prerequisites

For information on supported operating systems and web browsers, see the Passive Identity Management release notes.
Integration is available for Active Directory only.

PIM has the following prerequisites:

- Requires access to the CWS proxies on port 8080 on the client machine.
- Must be able to send out-of-band requests from the client to the CWS proxies. Ensure that:
  - PIM.exe is added as an exception to personal firewalls.
  - Corporate firewalls and gateway devices allow communication to the CWS proxies on port 8080.
  - Antivirus software allows PIM.exe to write to the Windows registry.

Limitations

PIM has the following limitations:

- PIM enables granularity only and does not perform any authentication or hotspot management or provide any tamper resistance. Where these are required, use Anywhere Plus instead.
- User and group information can be obtained only using the gpresult API (Active Directory). PIM does not integrate with LDAP or other authentication methods. Only cached groups on the domain will be used for lookups.
- HTTP traffic that bypasses the browser will not provide User granularity.
- PIM may cause some specific site exceptions to function incorrectly.
- PIM may cause some specific HTTPS sites to function incorrectly.
CHAPTER 1

Configure PIM

• Overview, page 1
• Configure Portal, page 1
• Configure Desktop, page 2
• Logon Script, page 2
• PIM Command-Line Arguments, page 3
• Upgrading from a Previous Version, page 4

Overview

This chapter explains how to configure the Passive Identity Management (PIM) solution end-to-end. If you are using Firefox as your primary web browser, you must still configure Internet Explorer because PIM relies on its proxy engine.

Configure Portal

Every time PIM runs, it collects all relevant information for the user from your organization’s Active Directory and sends it to the CWS proxies. If changes are made, they will not be sent until the next time PIM runs (by default the next time the user signs in).

No specific portal configuration is required. However, the portal can be configured to verify deployment. See Deploy PIM, on page 5.

Caution

Many users lock their screens or hibernate their computers at the end of the day. This can prevent the logon script from running regularly. Cisco recommends silently pushing the logon script to all users as a daily scheduled task.
Configure Desktop

The following sections explain how to configure your desktop computers.

Configure Firewall

Make sure your desktop security agents, such as personal firewalls, are PIM aware. Depending on your vendor, you may need to perform the following tasks:

- Allow the PIM.exe program file access to the Internet.
- Allow the firewall to accept a changed User Agent string.

Configure Browser

If you have already provisioned Internet Explorer to send traffic directly to Cisco's scanning infrastructure, you do not need to make any further changes to the browser settings.

If you are configuring the services for the first time, Cisco recommends the use of group policy objects (GPOs) to set the proxies within Internet Explorer and deploy the logon script.

Alternatively you can configure your browsers using a web-hosted PAC file on your local network. For example, in Internet Explorer, this can be configured in the Local Area Network (LAN) Settings dialog box.

PIM supports the Web Proxy Autodiscovery Protocol (WPAD) or PAC files hosted on a local computer or Windows network share only when using the /proxy command-line argument.

Note

Add the following lines to your PAC file to send PIM requests using your primary proxy:

```python
if (shExpMatch(host,"ds.scansafe.net")) return "PROXY proxy<#>.scansafe.net:8080";
```

Logon Script

The easiest way to deploy PIM is by using a logon script. PIM makes changes to the browser configuration which allow identification details to be sent to the 'in-the-cloud' infrastructure.

The following logon script can be used to deploy PIM. This script assumes that all user permissions are set correctly within the Active Directory network.

- Set up a logon script option for the user's organizational unit (OU).
- Create a command script (.cmd file) with the following content:

  ```
  \<server name>\<path>\pim.exe
  ```
Cisco recommends using a domain controller as the host server. The server should be visible across the domain.

## PIM Command-Line Arguments

The PIM program file accepts the following command-line arguments:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>/Cleanup</td>
<td>Removes the changes applied previously. After a system restart, the browser will no longer send the internal user data within the request header.</td>
</tr>
<tr>
<td>/Groups=&lt;comma separated list&gt;</td>
<td>Enables PIM to send the group information out-of-band for groups included in the list. It is necessary to use quote marks for group names containing spaces. This includes support for groups in multiple domains. You can use an asterisk (*) as a wildcard at the start, end, or both start and end of a group to match multiple groups. For example, <em>example</em> would match all group names containing the string 'example'.</td>
</tr>
<tr>
<td>/IP</td>
<td>Enables PIM to send the internal IP in headers by appending the base64 encoded value of the IP to the end of the user agent.</td>
</tr>
<tr>
<td>/KeyType=&lt;number&gt;</td>
<td>KeyType determines whether user sessions are persistent (2) or if a new session is created each time a user connects (1). Although the default is 1, this should be set to 2 unless otherwise directed by customer support.</td>
</tr>
<tr>
<td>/Proxy</td>
<td>Enables you to specify the primary CWS proxy to which an out-of-band request is sent. This setting is not used with Internet Explorer.</td>
</tr>
<tr>
<td>/Verbose</td>
<td>Provided for debugging purposes, this argument displays the username, group, and proxy. It also informs you if Firefox is not installed and if the post has succeeded.</td>
</tr>
</tbody>
</table>

Often a user may belong to more than one group in your organization's AD tree. When PIM runs using the logon script, it should be configured to register users only with groups that are relevant for applying browsing policy. This simplifies policy configuration in Cisco ScanCenter.
Here is an example:

```
PIM /Groups="WinNT://Test1\TET, WinNT://Test1\MPE" /Proxy=128.128.128.128:80 /Verbose
```

The example provided configures PIM to send the following information:

- User name
- Groups `WinNT://Test1\TET` and `WinNT://Test1\MPE` are included if the logged on user is a member

### Upgrading from a Previous Version

The `Cleanup` command-line argument is version-specific. Therefore, perform this action with the installed version of PIM before upgrading. The following command script (.cmd file) can be modified and used with Group Policy Objects to roll out a new version.

```
\pimserver\PIM1.2.0.1\PIM /Cleanup
\pimserver\PIM1.2.0.2\PIM /Groups="WinNT://netbios\security grouplist"
```

When all users have been upgraded, the first line of the command script can be commented out.
Deploy PIM

• Overview, page 5
• Verify Granularity, page 5
• Known Issues and Workarounds, page 6

Overview

This chapter will guide you through a test deployment. The supported deployment methods are:

• Logon script
• PAC file hosted on web server
• PAC file hosted locally
• Scheduled task

Verify Granularity

When you have deployed PIM, verify that user and group information is being passed to CWS.

Malware Scanning Service

If you have purchased the malware scanning service:

• Open your browser, and go to http://eicar.org/anti_virus_test_file.htm.
• Ensure that when you generate a block, you download the file using HTTP and not HTTPS.

Web Filtering Service

Alternatively, if you have purchased the web filtering service only, set up a policy in Cisco ScanCenter to block a specific category, for example banking.
From the PIM-enabled computer, attempt to browse to a site blocked within the category you chose. In both cases, a block page should be displayed in your browser.

Sign in to Cisco ScanCenter and generate a report for the relevant service (antivirus or web filtering) to identify the block record.

When PIM is configured correctly, the block includes username and group details.

To confirm that group information has been sent, in Cisco ScanCenter, navigate to Admin > Management > Groups. New groups are automatically added.

Known Issues and Workarounds

- A small number of identified sites use the User-Agent (UA) header as part of a session key. The PIM UA key is removed for all HTTP traffic passing through the CWS proxy, but this cannot be achieved with HTTPS as the stream is encrypted. If a site has mixed HTTPS/HTTP content, and uses the UA string as part of session management, then this fails. The workaround is to create an exception for the site locally.

- Granularity is provided without issues in most cases when using Internet Explorer or Firefox. However, a few nonbrowser applications that use their own mechanism to connect to the Internet do not pass user credentials using PIM, and the user appears anonymous. Applications that use the Internet Explorer API are less likely to be affected by this issue. Both types of applications may not use a UA string, even if they use the Internet Explorer proxy settings. The workaround is to add an exception for the URL or to allow the URL for anonymous users.