QUANTUM

03 December 2025

IDENTITY AWARENESS

R82

Administration Guide

Check Point Copyright Notice

Important Information

Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page.

Check Point R82

For more about this release, see the R82 home page.

Latest Version of this Document in English

Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.

Feedback

Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments.

Revision History

Date	Description
3 December 2025	Updated: ■ *"Using an Identity Awareness Gateway as an Active Directory Proxy" on page 174* ■ *"Transparent Kerberos Authentication Configuration" on page 234*
17 November 2025	Updated *"Transparent Kerberos Authentication Configuration" on page 234*
09 November 2025	Updated: ■ *"Using an Identity Awareness Gateway as an Active Directory Proxy" on page 174*
28 May 2025	Updated: ■ *"Using an Identity Awareness Gateway as an Active Directory Proxy" on page 174* ■ *"Selecting Identity Sources" on page 95*
12 February 2025	Updated: ■ *"Configuring AD Query" on page 49* ■ *"SAML Identity Provider for Identity Awareness" on page 181*
16 December 2024	Updated: ■ *"SAML Identity Provider for Identity Awareness" on page 181*
21 October 2024	First release of this document

Table of Contents

Introduction to Identity Awareness

In traditional firewall setups, traffic is monitored solely through IP addresses. This method does not reveal the user or machine behind those addresses. Identity Awareness closes this gap by mapping user and computer identities to IP addresses. This approach enables more granular Access Control policies and improves data auditing.

Identity Awareness is a versatile and scalable solution, suitable for both Active Directory and non-Active Directory environments, and encompasses employees and guest users alike. It leverages `Source` and `Destination` IP addresses to identify users and computers, which can be uses as matching criteria in Access Control policy rules.

Use Case: Consider a scenario where a company wants to restrict access to sensitive data based on user roles. With Identity Awareness, the administrator can create rules that allow only specific user groups to access certain resources, regardless of the devices they use. For instance, only employees from the "Finance" group can access financial reports, whether they work from the office or remotely.

You can incorporate the following criteria into your Access Control policies:

- User or User Group Identity
- Computer or Computer Group Identity

With Identity Awareness, you define policy rules for specified users, who send traffic from specified computers or from any computer. Likewise, you can create policy rules for any user on specified computers.

Identity Awareness gets identities from the configured identity sources. See *"Identity Sources" on page 14*.

When Identity Awareness is configured, logs based on IP address, user, and computer name appear in SmartConsole > **Logs & Events** > **Logs** tab. Logs of events appear in the **Logs & Events > Access Control** views.

An Identity Awareness Security Gateway can share the identity information that it acquires with other Identity Awareness Security Gateways. This way, users that need to pass through many Security Gateways are identified only one time. See *"Advanced Identity Awareness Environment" on page 202* for more information.

Known Limitations

- Identity Awareness does not support NAT.

Getting Started with Identity Awareness

1. Install the Management Server.

   See the *Installation and Upgrade Guide* for your version.

2. Install the Security Gateway.

   See the *Installation and Upgrade Guide* for your version.

3. Install the applicable Identity Clients.

   See sk134312.

4. In SmartConsole, configure the Security Gateway:

   a. From the left navigation panel, click **Gateways & Servers**.

   b. Open the Security Gateway object.

   c. Enable the **Identity Awareness** Software Blade and follow the Identity Awareness Configuration wizard.

      See *"Enabling Identity Awareness on the Security Gateway" on page 31*.

   d. From the left, click the **Identity Awareness** page.

   e. Configure the applicable **Identity Sources** and their settings.

      See *"Identity Sources" on page 42*.

   f. Click **OK**.

5. In SmartConsole, configure the applicable Access Roles and Access Control policy.

   See *"Creating Access Roles" on page 33*. and *"Using Identity Awareness in the Firewall Rule Base" on page 37*.

6. In SmartConsole, install the Access Control policy.

7. In SmartConsole, examine the logs on the **Logs & Events** view > **Logs** tab.

Access Role Objects

In SmartConsole, you can create Access Role objects to configure specified users, computers, and network locations as one object.

You can use Access Role objects as a source or a destination parameter in a rule.

Access Role objects include one or more of these objects:

- Networks.
- Users and user groups.
- Computers and computer groups.
- Remote Access Clients.

For example, this rule permits IT Department and Sales Department roles to share files over FTP.

Name	Source	Destination	VPN	Services & Applications	Action
IT and Sales File Sharing	IT_dept	Sales_dept	*Any	ftp	accept

Identity Sources

This section describes the Identity Sources.

Identity Sources determine how the Identity Awareness Security Gateway learns the user names and computers that generate traffic on the network.

You must enable the applicable identity sources in the **Identity Awareness Security Gateway** object > **Identity Awareness** page, and install the Access Control Policy.

Identity Source	Description
Browser-Based Authentication See *"Browser-Based Authentication" on page 18*	Identities are acquired through the authentication web portal on Identity Awareness Gateway (Captive Portal), or Transparent Kerberos Authentication.
Active Directory Query (AD Query) See *"AD Query" on page 20*	Identities are acquired seamlessly from the Microsoft Active Directory. This is a clientless identity acquisition tool.
Identity Agents See *"Identity Agents for a User Endpoint Computer" on page 22*	Identities are acquired using Identity Agents that are installed on the user endpoint computers.

Identity Source	Description
Terminal Servers See *"Terminal Servers" on page 22*	Identities are acquired using Identity Agents that are installed on Windows-based application server that hosts Terminal Servers, Citrix XenApp, and Citrix XenDesktop services. These Identity Agents are used to identify traffic from individual users on Terminal Servers.
RADIUS Accounting See *"RADIUS Accounting" on page 22*	Identities are acquired using RADIUS Accounting directly from a RADIUS Accounting Client.
Identity Collector See *"Identity Collector" on page 23*	Identities are acquired using Identity Agents that are installed on Microsoft Active Directory Domain Controllers, Cisco Identity Services Engine (ISE) Servers, or NetIQ eDirectory Servers.
Identity Web API See *"Identity Web API" on page 24*	Gives you a flexible method for creating identities.
Remote Access See *"Remote Access" on page 25*	Identities are acquired for Mobile Access clients and IPsec VPN clients configured to work in Office Mode, when they connect to the Security Gateway. For this to work, you must enable both the Identity Awareness and IPsec VPN Software Blades on the same Security Gateway.

Identity Sources

An Identity Awareness Gateway gets identities from different identity sources.

An Identity Awareness Gateway gets information from some identity sources directly.

For other identity sources, Identity Clients installed on an endpoint device or Windows server get identities and share them with the Identity Awareness Gateway.

Identity Clients have versions that are different from the versions of Identity Awareness Gateways.

To download the latest Identity Clients, see sk134312.

Identity Source	Documentation	Description
Browser-Based Authentication	See these: ■ *"Browser-Based Authentication" on page 18*. ■ *"Configuring Browser-Based Authentication" on page 44* ■ *"Getting Identities with Browser-Based Authentication" on page 98*	The Identity Awareness Gateway gets identities from one of these: ■ The authentication web portal on the Identity Awareness Gateway (Captive Portal) ■ Transparent Kerberos Authentication
AD Query	See these: ■ *"AD Query" on page 20* . ■ *"Configuring AD Query" on page 49* ■ *"Getting Identities for Active Directory Users" on page 97*	The Identity Awareness Gateway gets identities seamlessly from Microsoft Active Directory. This is a clientless identity acquisition tool (AD Query).
Identity Agents	See the *Identity Awareness Clients Administration Guide*.	The Identity Awareness Gateway gets identities from Identity Agents that are installed on the user endpoint computers.
Terminal Servers	See the *Identity Awareness Clients Administration Guide*.	The Identity Awareness Gateway gets identities from Identity Agents that are installed on a Windows-based application server that hosts Terminal Servers, Citrix XenApp, and Citrix XenDesktop services. These Identity Agents identify individual users.

Identity Source	Documentation	Description
RADIUS Accounting	See these: ■ *"RADIUS Accounting" on page 22* ■ *"Configuring RADIUS Accounting" on page 63*.	The Identity Awareness Gateway gets identities through RADIUS Accounting directly from a RADIUS accounting client.
Identity Collector	See the *Identity Awareness Clients Administration Guide*.	The Identity Awareness Gateway gets identities from Identity Collectors that are installed on these: ■ Microsoft Active Directory Domain Controllers ■ Cisco Identity Services Engine (ISE) Servers ■ NetIQ eDirectory Servers
Identity Web API	See these: ■ *"Identity Web API" on page 24* ■ *"Configuring Identity Awareness API" on page 69*	Gives you a flexible method to create identities.
Remote Access	See these: ■ *"Configuring Remote Access" on page 89* ■ *Mobile Access Administration Guide* for your version ■ *Remote Access VPN Administration Guide* for your version	The Identity Awareness Gateway gets identities from Mobile Access clients and IPsec VPN clients configured to work in Office Mode when they connect to the Security Gateway.

Browser-Based Authentication

Browser-Based Authentication gets identities and authenticates users with one of these acquisition methods:

- **Captive Portal**

  Important - Internal Users and Administrators who authenticate in Multi-Portals on the Security Gateway must have different passwords.
  This applies to:
  - Identity Awareness Captive Portal
  - Data Loss Prevention Portal

  Captive Portal authenticates users with a web interface. When users try to access a protected web resource, they enter authentication information in a form that shows in their web browser.

  The Captive Portal shows when a user tries to get an access to a web resource and all of these conditions apply:

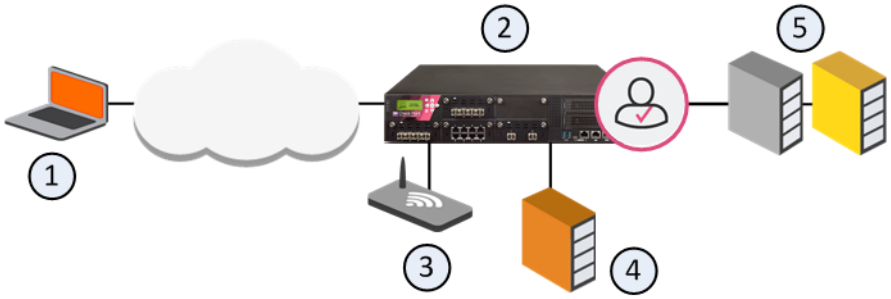
  - Captive Portal is enabled.
  - The **Redirect** option enabled for the applicable policy rule.
  - Firewall or Application & URL Filtering rules stop access by unidentified users to resources that only identified users can get access to.

  In addition, the Captive Portal shows when Transparent Kerberos Authentication is enabled but authentication fails.

  From the Captive Portal, users:

  - Enter their user name and password (which are configured in the Identity Awareness Gateway object > **Identity Awareness** page > near the **Browser-Based Authentication**, click **Settings** > refer to the **Users Access** section).
  - Enter guest user credentials (which are configured in the Identity Awareness Gateway object > **Identity Awareness** page > near the **Browser-Based Authentication**, click **Settings** > refer to the **Users Access** section).
  - Click a link to download an Identity Agent (which is configured in the Identity Awareness Gateway object > **Identity Awareness** page > near the **Browser-Based Authentication**, click **Settings** > refer to the **Identity Agent Deployment from the Portal** section).

Browser-Based Authentication with Captive Portal



Item	Description
1	User
2	Identity Awareness Gateway
3	Captive Portal
4	Active Directory Domain Controller
5	Internal Data Center

Flow of events for Browser-Based Authentication with Captive Portal:

1. A user (1) wants to get an access to the Internal Data Center (5).
2. Identity Awareness Gateway (2) does not recognize the user and redirects the user's web browser to the Captive Portal (3).
3. The user enters regular office credentials, for example, AD, or other Check Point supported authentication methods, for example, LDAP, Check Point internal credentials, or RADIUS.
4. The credentials go to the Identity Awareness Gateway, which finds them in the AD server (4).
5. The user gets an access to the requested URL in the Data Center (5).

- **Transparent Kerberos Authentication**

  To authenticate users, Transparent Kerberos Authentication gets authentication data from the web browser without user input. If authentication is successful, the user goes directly to the specified destination. If authentication fails, the user must enter credentials in the Captive Portal.

Flow of events for Browser-Based Authentication with Transparent Kerberos Authentication:

1. A user wants to get an access to the Internal Data Center.
2. Identity Awareness Gateway does not recognize the user and redirects the user's web browser to the Transparent Authentication page.
3. The Transparent Authentication page asks the web browser to authenticate itself.
4. The web browser gets a Kerberos ticket from Active Directory and presents it to the Transparent Authentication page.
5. The Transparent Authentication page sends the ticket to the Identity Awareness Gateway, which authenticates the user and redirects the user's web browser to the originally requested URL.
6. If Kerberos authentication fails for some reason, Identity Awareness Gateway redirects the user's web browser to the Captive Portal.

AD Query

AD Query is an easy to configure, clientless tool to get identities. Its function is based on Active Directory integration, and it is fully transparent to the user.

AD Query works when:

- An identified user or computer tries to get an access to a resource that creates an authentication request. For example, when a user logs in, unlocks a screen, shares a network drive, reads emails through Exchange, or uses an Intranet portal.
- You select AD Query to get identities.

In this technology, you make a query for the Active Directory Security Event Logs and extract the user and computer mapping to the network address from them. It is based on Windows Management Instrumentation (WMI), a standard Microsoft protocol. The Identity Awareness Gateway communicates directly with the Active Directory domain controllers and does not need a special server.

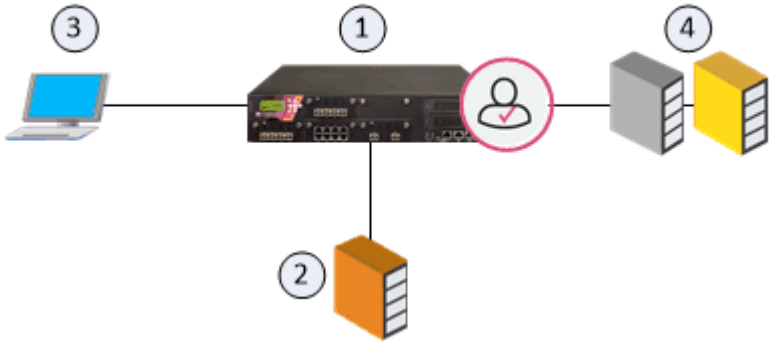
No installation is necessary on the end clients, or on the Active Directory server.

The system generates a Security Event Log entry when a user or a computer connects to a network resource. AD Query extracts user and computer identity information from the Active Directory Security Event Logs. Security Event Logs are not generated when a user logs out because Active Directory cannot detect this action.

These are limitations of AD Query:

- **User/IP association timeout** - After a default period of network inactivity, a user session closes automatically. The user must connect to the Identity Awareness Captive Portal and log in again.
- **Many user accounts connected from the same IP address** - AD Query cannot detect when a user logs out. Therefore, more than one user can have open sessions from the same IP address. When this occurs, the permissions for each account stay active until the session reaches the value configured in the **"User/IP association timeout"**. In this scenario, it is possible for users to access network resources for which they do not have permissions.

How AD Query Works - Firewall Rule Base



Item	Description
1	Identity Awareness Gateway
2	Active Directory Domain Controller
3	An end-computer, on which a user with Active Directory credentials logs on
4	Network resources

Flow of events:

1. The Identity Awareness Gateway (1) gets security event logs from the Active Directory Domain Controllers (2).
2. A user logs in on an end-computer with their Active Directory credentials (3).
3. The Active Directory Domain Controller (2) sends the security event log to the Identity Awareness Gateway (1).
4. The Identity Awareness Gateway (1) gets the user name (`@domain`), computer name, and source IP address).
5. The user on the end-computer (3) opens a connection to the network resource (4).

6. The Identity Awareness Gateway confirms the user identity and allows or blocks access to the resource based on the Security Policy.

Identity Agents for a User Endpoint Computer

Identity Agents are dedicated client agents that are installed on user endpoint computers. These Identity Agents get and report identities to the Identity Awareness Gateway. The administrator configures these Identity Agents. For more information about Identity Agents for a user endpoint computer, see the *Identity Awareness Clients Administration Guide*.

Terminal Servers

Identity Agent for a Terminal Server- An Identity Agent installed on a Windows-based application server that hosts Terminal Servers, Citrix XenApp, and Citrix XenDesktop services. The Identity Awareness Terminal Servers solution lets the system enforce Identity Awareness policies on multiple users that connect from one IP address. This functionality is necessary when an administrator must control traffic created by users of application servers that host Microsoft Terminal Servers, Citrix XenApp, and Citrix XenDesktop.

This Terminal Servers Identity Agent type cannot be used for endpoint computers.

For more information about Identity Agent for a Terminal Server, see the *Identity Awareness Clients Administration Guide*.

RADIUS Accounting

You can configure an Identity Awareness Gateway to use **RADIUS Accounting** (RFC 2866) to get user and computer identities directly from a RADIUS Accounting Client.

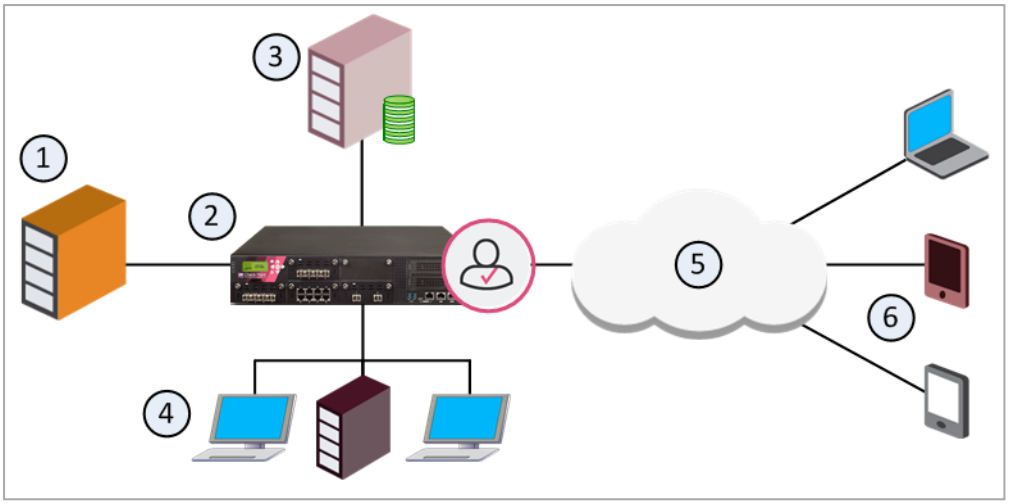
The Identity Awareness Gateway uses this information to apply access permissions to the connection.

General Overflow

The RADIUS Accounting Server gets identity data from **RADIUS Accounting Requests** generated by the RADIUS Accounting Client.

The Identity Awareness Gateway uses the data from these requests to get user and device group information from the LDAP server.

Based on the information from the LDAP server, the Identity Awareness Gateway applies the configured Access Control rules to traffic generated by users and their computers.



Item	Description
1	RADIUS server with RADIUS Accounting Client enabled. Sends RADIUS Accounting Requests to the Identity Awareness Gateway.
2	Identity Awareness Gateway works as a RADIUS Accounting Server.
3	LDAP server. Sends identity data for the user to the Identity Awareness Gateway.
4	Internal network resources.
5	Internet.
6	Remote laptops and mobile devices.

Identity Collector

Check Point Identity Collector is a dedicated client agent installed on Windows Servers in your network. Identity Collector collects information about identities and their associated IP addresses, and sends it to the Check Point Security Gateway for identity enforcement.

The Identity Collector can connect with more than one Identity Source at a time. The Identity Sources are organized in Query Pools.

A Query Pool is an object, which contains a number of Identity Sources. Each Query Pool is assigned to one Identity Awareness Gateway. The Identity Collector collects information from the Identity Sources in the Query Pools and sends the information to the Identity Awareness Gateways.

Example:

An environment has two domains: `Asia.com` and `Euro.com`.

The administrator wants the Asia Identity Awareness Gateway to get the events from all the 4 Active Directory Domain Controllers in the `Asia.com` domain.

The administrator in addition wants the Europe Identity Awareness Gateway 1 and Europe Identity Awareness Gateway 2 to get the events from all the 6 Active Directory Domain Controllers in the `Euro.com` domain.

The administrator, therefore, creates 2 Query Pools:

- One, which contains all the Active Directory Domain Controllers in the `Asia.com` domain.
- One, which contains all the Active Directory Domain Controllers in the `Euro.com` domain.

The administrator configures:

- The Asia Identity Awareness Gateway to get events from the Asia Query Pool.
- The two Europe Identity Awareness Gateways to get events from the Europe Query Pool.

For more information about Identity Collector, see the *Identity Awareness Clients Administration Guide*.

Identity Web API

The Identity Awareness Identity Web API is a flexible identity source that you can use for simple integration with 3rd party security and identity products, such as ForeScout CounterACT and Aruba Networks ClearPass. The Identity Web API identity source provides a flexible method for the creation of identities based on environment needs. With the Identity Web API, you can create and cancel identities, and query the Identity Awareness Software Blade regarding users, IP addresses, and computers.

The Identity Web API uses the REST protocol over HTTPS. The Identity Awareness Gateway authenticates and authorizes the users and computers with the information it gets from the Web API.

You can create associations for users and machines. Identity Awareness Gateway can calculate their group membership and Access Roles, or you can provide that information. The Web API is useful for:

- Integration with 3rd party security products. For example, you can apply a special *restricted* Access Role to quarantine an infected computer detected by a 3rd party security provider.
- Integration with other authentication systems.
- Automation of administrative tasks related to Identity Awareness.

Identity Web API gets JSON requests over HTTPS. Each JSON request contains one Identity Web API command, or a bulk of commands. Each API command must include a shared secret that was pre-configured in SmartConsole.

The Identity Web API supports these commands

Command	Description
`add-identity`	Associates an IP address to a user or a computer for a specified quantity of time.
`delete-identity`	Revokes sessions that match one IP address or an IP range.
`show-identity`	Queries the identities related to an IP address, and other information the Identity Awareness blade saves about this IP address.

Remote Access

Mobile Access clients and IPsec VPN clients configured to work in Office Mode obtain identities when they connect to the Security Gateway.

For more information about Mobile Access clients, see the *Mobile Access Administration Guide* for your version.

For more information about IPsec VPN clients, see the *Remote Access VPN Administration Guide* for your version.

Identity Awareness - Comparison of Acquisition Sources

These tables show how identity sources are different in terms of usage and environment considerations. Based on these considerations, you can configure Identity Awareness to use one or more identity of these identity sources (see *"Selecting Identity Sources" on page 95*).

Browser-Based Authentication - Captive Portal

Unidentified users log in with a user name and password in a Captive Portal. After authentication, the user clicks a link to go to the destination address.

Recommended Usage	Environment Considerations
■ Identity based enforcement for non-AD users (non-Windows and guest users). ■ You can demand environment of Identity Agents.	Use it for identity enforcement (not intended for logging purposes).

Browser-Based Authentication - Transparent Kerberos Authentication

The Transparent Kerberos Authentication Single-Sign On (SSO) solution transparently authenticates users already logged in to the AD. When users authenticate to the domain, they can access all authorized network resources, and do not have to enter credentials again. If Transparent Kerberos Authentication fails, users are redirected to the Captive Portal for manual authentication.

Note - The Identity Agent download link and the **Automatic Logout** option are ignored when Transparent Kerberos Authentication SSO is successful. This is because users do not see the Captive Portal.

Recommended Usage	Environment Considerations
In AD environments, when known users are already logged in to the domain.	■ Used for identity enforcement only (not intended for logging purposes). ■ Transparent Kerberos Authentication does not use Identity Agents or the Keep Alive feature.

AD Query

Gets identity data seamlessly from Active Directory (AD).

Recommended Usage	Environment Considerations
■ Identity-based auditing and logging. ■ Leveraging identity in Internet application control. ■ Basic identity enforcement in the internal network.	■ Easy configuration (AD administrator credentials are necessary). For organizations that prefer not to allow administrator users to be used as service accounts on third party devices, there is an option to configure AD Query without AD administrator privileges, see sk43874. ■ Preferred for Desktop users. ■ Only detects AD users and computers.

Identity Agent

A lightweight Identity Agent authenticates users securely with Single Sign-On (SSO).

Recommended Usage	Environment Considerations
■ Identity enforcement for Data Centers. ■ Protecting highly sensitive servers. ■ When accuracy in detecting identity is crucial.	See *"Selecting Identity Sources" on page 95*.

Terminal Servers Identity Agent

Identifies multiple users, who connect from one IP address. A Terminal Identity Agent is installed on the application server, which hosts the terminal/Citrix services.

Recommended Usage	Environment Considerations
Identify users who use Terminal Servers or a Citrix environment.	See *"Selecting Identity Sources" on page 95*.

RADIUS Accounting

You can configure an Identity Awareness Gateway to use **RADIUS Accounting** to get user and computer identities directly from a RADIUS accounting client. Identity Awareness Gateway uses this information to apply access permissions to the connection.

RADIUS Accounting gets identity data from **RADIUS Accounting Requests** generated by the RADIUS accounting client. Identity Awareness Gateway uses the data from these requests to get user and device group information from the LDAP server. Firewall rules apply these permissions to users, computers and networks.

Recommended Usage	Environment Considerations
In environments, where authentication is handled by a RADIUS server.	■ You must configure the RADIUS accounting client to send RADIUS accounting requests to the Identity Awareness Gateway. ■ You must give the RADIUS client access permissions and create a shared secret.

Identity Collector

The Identity Collector is a Windows-based application, which collects identity information and sends it to the Identity Awareness Gateways for identity enforcement.

Recommended Usage	Environment Considerations
■ Works with Microsoft Active Directory Domain Controller in large-scale environments. ■ Integrates with Cisco Identity Services Engine (ISE). ■ Works with NetIQ eDirectory Servers. ■ Asks for *Event Log Readers* permission credentials.	■ Windows application with prerequisites. ■ Locally managed.

Identity Web API

The Web API is a flexible identity source that you can use for simple integration with 3rd party security and identity products.

Recommended Usage	Environment Considerations
■ Integrates with 3rd party security products, such as ForeScout CounterACT and Aruba Networks ClearPass. ■ Integrates Identity Awareness with authentication systems that Check Point does not regularly support. ■ Does system administration tasks such as quick checks of users' IP address.	■ You must properly configure the accessibility and the list of authorized API clients. ■ You must create a separate shared secret for each API client.

Remote Access

Users who get access using IPsec VPN Office Mode can authenticate seamlessly.

Recommended Usage	Environment Considerations
Identify and apply identity-based security Policy on users that get an access to the organization through VPN.	See *"Selecting Identity Sources" on page 95*.

Identity Awareness Environment

Identity Awareness Software Blade is commonly enabled on a perimeter Security Gateway. It is frequently used in conjunction with Application Control Software Blade.

To protect internal data centers, Identity Awareness Software Blade can be enabled on an internal Security Gateway located in front of internal servers, such as data centers. This can be done in addition to the perimeter Security Gateway, but a perimeter Security Gateway is not necessary.

Identity Awareness can have a Bridge Mode or a Route Mode configuration.

- In Bridge Mode, the Security Gateway can use a current subnet with no change to the hosts' IP addresses.
- In Route Mode, the Security Gateway works as a router with different subnets connected to its network interfaces.

For redundancy, you can configure a cluster of Identity Awareness Security Gateways in High Availability or Load Sharing modes.

You can configure multiple Identity Awareness Security Gateways to share identity information. Common scenarios include:

- Enabling Identity Awareness Software Blade on a perimeter Security Gateway and on a data center Security Gateway.
- Enabling Identity Awareness Software Blade on more than one data center Security Gateway.
- Enabling Identity Awareness Software Blade on a branch office Security Gateway and on a central Security Gateway.

You can have one or more Identity Awareness Gateways get identities and share them with the other Identity Awareness Gateways.

You can in addition share identities between Identity Awareness Gateways that are managed in different Multi-Domain Servers.

Identity Awareness Default Ports

This section shows the default ports used by Identity Awareness features.

Feature	Port
LDAP	389
LDAP over SSL (LDAPS)	636
AD Query	135
Global Catalog	3268
Global Catalog over SSL	3269
Identity Awareness Gateway to AD	135, 389
AD to Identity Awareness Gateway	135
Enforcement Gateway	389

Feature	Port
Identity Sharing Gateway to Enforcement Gateway	15105, 28581
Browser-Based Authentication	443
Identity Agents to Enforcement Gateway	443
RADIUS Accounting	1813

It is possible to configure these features to different ports. For more information about Identity Awareness ports, see sk98561 and sk52421.

Configuring Identity Awareness

This section describes how to configure and work with Identity Awareness.

Enabling Identity Awareness on the Security Gateway

When you enable Identity Awareness Software Blade on a Security Gateway, an Identity Awareness Configuration wizard opens. You can use the wizard to configure one Security Gateway that uses the AD Query, Browser-Based Authentication, and Terminal Servers for acquiring identities. You cannot use the wizard to configure an environment with multiple Security Gateway, or to configure Identity Agent and Remote Access acquisition (other methods for acquiring identities).

When you complete the wizard and install an Access Control Policy, the system is ready to monitor Identity Awareness. You can see the logs for user and computer identity in the SmartConsole **Logs & Events** > **Logs** tab. You can see these events through the Columns Profile **Access Control**.

To enable Identity Awareness Software Blade on a Security Gateway you must select Identity Sources and configure an Active Directory Domain.

Selecting Identity Sources

Procedure:

1. Log in to SmartConsole.
2. From the left navigation toolbar, click **Gateways & Servers**.
3. Double-click the Security Gateway or Security Cluster object.
4. On the **Network Security** tab, select **Identity Awareness**.
5. The **Identity Awareness Configuration** wizard opens.
6. On the **Methods For Acquiring Identity** page, select the applicable Identity Sources:
   - *"AD Query" on page 20*
   - *"Browser-Based Authentication" on page 18*
   - *"Terminal Servers" on page 22*

Notes

- After completing this wizard, you can select additional Identity Sources (see *"Identity Sources" on page 14*).
- When you enable Browser-Based Authentication on Security Gateway that runs on an IP Series appliance with IPSO OS, make sure to set the Voyager management application port to a number other than 443 or 80.

7. Click **Next**

   The **Integration With Active Directory** page opens.

   You can select or configure an Active Directory Domain.

Configuring an Active Directory Domain

Best Practice - We highly recommend that you go to the LDAP Account Unit and make sure that only necessary domain controllers are in the list. If AD Query is not necessary to work with some of the domain controllers, delete them from the LDAP Servers list..

Procedure:

1. If the SmartConsole computer is part of the domain, the Wizard fetches all the domain controllers of the domain and all of the domain controllers are configured.

   If you create a new domain, and the SmartConsole computer is not part of the domain, the LDAP Account Unit that the system creates contains only the domain controller you set manually. If it is necessary for AD Query to fetch data from other domain controllers, you must **add** them later manually to the LDAP Servers list after you complete the wizard.

   To view/edit the LDAP Account Unit object, open **Object Explorer** (CTRL + E), and select **Users/Identities** > **LDAP Account units**.

   The LDAP Account Unit name syntax is: `<domain name>__AD`

   For example, `CORP.ACME.COM__AD`.

2. From the **Select an Active Directory** list, do one of these:

   - Select the Active Directory to configure from the list that shows configured LDAP Account Units.
   - Create a new domain. If you have not set up Active Directory, you need to enter a **domain name**, **username, password** and **domain controller** credentials.

   When the SmartConsole client computer is part of the AD domain, SmartConsole suggests this domain automatically. If you select this domain, the system creates an LDAP Account Unit with **all** of the domain controllers in the organization's Active Directory.

3. Enter the Active Directory credentials and click **Connect** to verify the credentials.

   Important - For AD Query you must enter domain administrator credentials. For Browser-Based Authentication standard credentials are sufficient.

4. **Optional**: If you selected Browser-Based Authentication or Terminal Servers, or do not wish to configure Active Directory, select **I do not wish to configure Active Directory at this time** and click **Next**.

5. Click **Next**.

   If you selected **Browser-Based Authentication** on the **Methods For Acquiring Identity** page, the **Browser-Based Authentication Settings** page opens.

6. In the **Browser-Based Authentication Settings** page, select a URL for the portal, where unidentified users get pointed.

   The list shows all IP addresses configured for the Security Gateway. The IP address selected by default is the Security Gateway main IP address. The same IP address can be used for other portals with different paths. For example:

   - Identity Awareness Browser-Based Authentication - 192.0.2.2/connect
   - DLP Portal - 192.0.2.2/DLP
   - Mobile Access Portal - 192.0.2.2/sslvpn

   By default, access to the portal is only through internal interfaces. To change this, click **Edit**. On a perimeter Security Gateway, we recommend that the Captive Portal can be accessed only through internal interfaces.

7. Click **Next**.

   The **Identity Awareness is Now Active** page opens with a summary of the acquisition methods.

   If you selected Terminal Servers, the page includes a link to download the agent (see the *Identity Awareness Clients Administration Guide*).

8. Click **Finish**.

9. **Optional:** In the Security Gateway or Security Cluster object, go to the **Identity Awareness** page and configure the applicable settings.

10. Click **OK**.

11. Install the Access Control Policy.

Creating Access Roles

After you enable Identity Awareness (see *"Enabling Identity Awareness on the Security Gateway" on page 31*), you create Access Role objects.

You can use Access Role objects as source and/or destination parameter in a rule. Access Role objects can include one or more of these objects:

- Networks
- Users and user groups
- Computers and computer groups
- Remote Access clients

To create an Access Role object:

1. In SmartConsole, open the **Object Explorer** (press the **CTRL+E** keys).
2. Click **New** > **Users** > **Access Role**.

   The **New Access Role** window opens.
3. Enter a **Name** and **Comment** (optional).
4. On the **Networks** page, select one of these:
   - **Any network**.
   - **Specific networks** - Click the plus **[+]** sign and select a network > click the plus **[+]** sign next to the network name, or search for a known network.
5. On the **Users** page, select one of these:
   - **Any user**.
   - **All identified users** - Includes users identified by a supported authentication method.
   - **Specific users/groups** - Click the plus **[+]** sign and select a user > click the plus **[+]** sign next to the username, or search for a known user or user group.
6. On the **Machines** page, select one of these:
   - **Any machine**.
   - **All identified machines** - Includes computers identified by a supported authentication method.
   - **Specific machines/groups** - Click the plus **[+]** sign and select a device > click the plus **[+]** sign next to the device name, or search for a known device or group of devices.

   For computers that use Full Identity Agents, you can select (optional) **Enforce IP Spoofing protection**.
7. On the **Remote Access Clients** page, select one of these:

- **Any Client**.
- **Specific Client** - Select the current allowed client, or create a new allowed client.

Note - For Identity Awareness Gateways R77.xx or lower, you must select **Any Client**.

8. Click **OK**.

Configuring Security Identifier (SID) for LDAP Users

For Access Roles matching for LDAP users, you specify the DN (Distinguished Name) for the LDAP user account, where `CN=UserName, OU=Group, DC=Domain, DC=com`.

In R81, we added a Security Identifier (SID) support feature.

SID is a unique identifier for each object that LDAP holds. With SID support, Check Point Security Gateway matches Access Roles so that if a group name or user name or domain name changes, the user's SID remains the same and the Access Role matching occurs because of policy.

Note - SID support is not activated by default.

Warning - The upgrade process replaces all existing files with default files. You must not copy the customized configuration files from the current version to the upgraded version, because these files can be unique for each version. You must make all the custom configurations again after the upgrade.

To enable SID support on the Check Point Security Gateway:

1. Run *#cpstop* command.
2. Edit the *$CPDIR/tmp/.CPprofile.sh* file.
3. Add the line:

   export LDAP_SID=1
4. Save the file.
5. Reboot the Security Gateway.
6. Run this command:

```
#pdp nested status
```

Note - SID support works only when the status **enabled - mode 2** or **enabled - mode 4** for the nested groups is enabled. If not, run **#pdp nested __set_state 4**.
For more information about the nested groups, see *"Nested Groups" on page 173*.

7. Do this procedure on every Security Gateway and Cluster Member.

Using Identity Tags in Access Role Matching

Identity Tags let you include external identifiers (such as Cisco® Security Group Tags, or any other groups provided by any Identity Source) in Access Role matching. These external identifiers work like a tag that can be assigned to a certain user, machine or group.

To use Identity Tags in Access Role matching:

1. **Create a new Identity Tag**

    a. In SmartConsole, click the **Objects** pane >**New** > **More** > **User/Identity** > **Identity Tag**.

    b. Enter a name for the object.

    Note - If you enter the **External Identifier** first, the Identity Tag object gets the same name.

    c. In the **External Identifier** field, enter one of these:

    - A Cisco Security Group Name, as defined on the Cisco ISE server or acquired through Identity Collector.
    - A custom tag (defined on a third party product) acquired through the Check Point Identity Web API.

    Note - The External Identifier must be a unique name.

    d. Click **OK**.

2. **Include the Identity Tag in an Access Role**

    a. In SmartConsole, click the **Objects** pane >**New** > **More** > **User/Identity** > **New Access Role**.

    b. On the **Users** tab or **Machines** tab, select **Specific users/groups**.

    c. Click the **[+]** icon.

d. Click on the domain name button in the top left corner and select **Identity Tags**.

e. Select the Identity Tag created in Step 1.

f. Click **OK**.

3. Add this Access Role to the **Source** or **Destination** column of an Access Control Policy rule.
4. Install the Access Control Policy.

Using Identity Awareness in the Firewall Rule Base

The Security Gateway examines packets and applies rules in a sequential manner. When a Security Gateway receives a packet from a connection, it examines the packet against the first rule in the Rule Base. If there is no match, it then goes on to the second rule and continues until it matches a rule. If there is no match to any of the explicit or implied rules, Security Gateway drops the packet.

Working with Access Role Objects in the Rule Base

In rules with Access Roles, if the source identity is unknown, and traffic is HTTP, configure the **Action** field to redirect traffic to the Captive Portal. This rule redirects the user to the Captive Portal.

In rules with Access Roles, if the source identity is known, the **Action** in the rule (**Allow**, **Drop**, or **Reject**) is enforced immediately, and the user is not redirected to the Captive Portal. After the system gets the credentials from the Captive Portal, it can examine the rule for the next connection.

In rules with Access Role objects, criteria matching works like this:

- When identity data for an IP address is known:
  - If it matches an Access Role, the rule is enforced and traffic is allowed or blacked based on the action.
  - If it does not match an Access Role, it goes on to examine the next rule.
- When identity data for an IP address is unknown and:
  - All rule fields match, besides the Source field with an Access Role.
  - The connection is HTTP.

- The action is set to redirect to the Captive Portal.

  If all the conditions apply, the traffic is redirected to the Captive Portal to get credentials and make sure there is a match.

  If not all conditions apply, there is no match, and the next rule is examined.

  Note - You can only redirect HTTP traffic to the Captive Portal.

To redirect HTTP traffic to the Captive Portal:

1. In an Access Control Policy rule that uses an Access Role in the **Source** column, right-click the **Action** cell > click **More**.

   The **Action Settings** window opens.
2. In the **Action** field, select **Accept**, **Ask**, or **Inform**.
3. At the bottom, select **Enable Identity Captive Portal**.
4. Click **OK**.
5. The **Action** cell shows that a redirect to the Captive Portal occurs:
   - `Accept (display Captive Portal)`
   - `Ask (display Captive Portal)`
   - `Inform (display Captive Portal)`
6. Install the Access Control Policy.

Important - When you set the option to redirect HTTP traffic from unidentified IP addresses to the Captive Portal, make sure to put the rule in the correct position in the Rule Base, to avoid unwanted behavior.

This is an example of a Firewall Rule Base that describes how matching works:

No.	Source	Destination	Service	Action
1	Finance Dept (Access Role)	Finance Web Server	`*Any`	`Accept (display Captive Portal)`
2	Admin IP Address	`*Any`	`*Any`	`Accept`
3	`*Any`	`*Any`	`*Any`	`Drop`

Example 1 - If an unidentified Finance user tries to get an access to the Finance Web Server over HTTP, a redirect to the Captive Portal occurs. After the user enters credentials, the Identity Awareness Gateway allows access to the Finance Web Server. Access is allowed based on rule number 1, which identifies the user through the Captive Portal as belonging to the Finance Access Role.

Example 2 - If an unidentified administrator tries to get an access to the Finance Web Server over HTTP, a redirect to the Captive Portal occurs despite rule number 2. After the administrator is identified, rule number 2 matches. To let the administrator get an access to the Finance Web Server without redirection to the Captive Portal, switch the order of rules 1 and 2 or add a network restriction to the Access Role.

Identifying Users behind an HTTP Proxy Server

If your organization uses an HTTP proxy server between the users and the Identity Awareness Gateway, the Identity Awareness Gateway cannot see the identities of these users. As a result, the Identity Awareness Gateway cannot enforce policy rules based on user identities.

To let the Identity Awareness Gateway identify users behind a proxy server, you can use the **X-Forward-For HTTP** header, which the proxy server adds.

To do this, you have to:

- Configure the XFF header on the Identity Awareness Gateway
- Configure the XFF header on the Access Control Policy Layer
- Use Access Roles in the Access Control Policy Layer, or use one of these advanced options in the **Track** column: **Log**, **Detailed Log**, **Extended Log**.

How to configure the XFF header on an Identity Awareness Gateway

1. Log in to SmartConsole.
2. From the Navigation Toolbar, click **Gateways & Servers**.
3. Open the Identity Awareness Gateway object.
4. In the **General Properties** page > **Network Security** tab, make sure that **Identity Awareness** is enabled.
5. In the left navigation tree, click on the **[+]** near the **Identity Awareness** and go to the **Proxy** page.
6. Select **Detect users located behind http proxy configured with X-Forwarded-For**.
    - Optional: Select **Hide X-Forwarded-For in outgoing traffic**.

      With this option selected, internal IP addresses are not seen in requests to the internet.

- Optional: Select **Trust X-Forwarded-For from known proxies only** and select the applicable Group object from the drop-down list (you need to configure such Group object in advance).

  The Identity Awareness Gateway reads the XFF header only from the trusted servers.

  Note - If this option is disabled, the Identity Awareness Gateway parses the XFF header only from internal network connections.

7. Click **OK**.
8. Install the Access Control Policy.

How to configure the XFF header on the Access Control Policy Layer

1. Log in to SmartConsole.
2. From the Navigation Toolbar, click **Security Policies**.
3. In the **Access Control** section, right-click **Policy** and select **Edit Policy**.
4. In the **Access Control** section:
   - If you already have Policy Layers configured, in the Policy Layer section, click and select **Edit Layer**.
   - If you do not have Policy Layers configured yet, then:

   a. Click on the plus **[+]** sign **> New Layer**.

   b. Configure the layer.

   c. Click **OK** to close the **Layer Editor** window.

   d. Click **OK** to close the **Policy** window.

   e. In the **Access Control** section, right-click **Policy** and select **Edit Policy**.

   f. In the Policy Layer section, click and select **Edit Layer**.
5. In the **Layer Editor** window, go to **Advanced** page.
6. In the **Proxy Configuration** section, select **Detect users located behind http proxy configured with X-Forwarded-For**.
7. Click **OK** to close the **Layer Editor** window.
8. Click **OK** to close the **Policy** window.
9. Install the Access Control Policy.

How to configure Access Roles in the Access Control Policy Layer

See *"Using Identity Awareness in the Firewall Rule Base" on page 37*.

How to use one of the advanced options in the Track column

1. Right-click in the **Track** column > click **More**.

   The **Track Settings** window opens.

   Note - For more information about each available option, click the **(?)** icon in the top right corner.

2. In the **Track** field, select one of these applicable options:

   - **Log**
   - **Detailed Log**
   - **Extended Log**

   Note - *Detailed Log* and *Extended Log* are only available, if one or more of these Software Blades are enabled on the Layer: **Application & URL Filtering**, **Content Awareness**, or **Mobile Access**.

3. In the **Log Generation** section, select one of these applicable options:

   - **per Connection**
   - **per Session**

4. Click **OK**.

5. Install the Access Control Policy.

Configuring Identity Sources

This section describes how to configure and work with various Identity Sources.

Identity Sources

An Identity Awareness Gateway gets identities from different identity sources.

An Identity Awareness Gateway gets information from some identity sources directly.

For other identity sources, Identity Clients installed on an endpoint device or Windows server get identities and share them with the Identity Awareness Gateway.

Identity Clients have versions that are different from the versions of Identity Awareness Gateways.

To download the latest Identity Clients, see sk134312.

Identity Source	Documentation	Description
Browser-Based Authentication	See these: ■ *"Browser-Based Authentication" on page 18*. ■ *"Configuring Browser-Based Authentication" on page 44* ■ *"Getting Identities with Browser-Based Authentication" on page 98*	The Identity Awareness Gateway gets identities from one of these: ■ The authentication web portal on the Identity Awareness Gateway (Captive Portal) ■ Transparent Kerberos Authentication
AD Query	See these: ■ *"AD Query" on page 20* . ■ *"Configuring AD Query" on page 49* ■ *"Getting Identities for Active Directory Users" on page 97*	The Identity Awareness Gateway gets identities seamlessly from Microsoft Active Directory. This is a clientless identity acquisition tool (AD Query).

Identity Source	Documentation	Description
Identity Agents	See the *Identity Awareness Clients Administration Guide*.	The Identity Awareness Gateway gets identities from Identity Agents that are installed on the user endpoint computers.
Terminal Servers	See the *Identity Awareness Clients Administration Guide*.	The Identity Awareness Gateway gets identities from Identity Agents that are installed on a Windows-based application server that hosts Terminal Servers, Citrix XenApp, and Citrix XenDesktop services. These Identity Agents identify individual users.
RADIUS Accounting	See these: ■ *"RADIUS Accounting" on page 22* ■ *"Configuring RADIUS Accounting" on page 63*.	The Identity Awareness Gateway gets identities through RADIUS Accounting directly from a RADIUS accounting client.
Identity Collector	See the *Identity Awareness Clients Administration Guide*.	The Identity Awareness Gateway gets identities from Identity Collectors that are installed on these: ■ Microsoft Active Directory Domain Controllers ■ Cisco Identity Services Engine (ISE) Servers ■ NetIQ eDirectory Servers
Identity Web API	See these: ■ *"Identity Web API" on page 24* ■ *"Configuring Identity Awareness API" on page 69*	Gives you a flexible method to create identities.

Identity Source	Documentation	Description
Remote Access	See these: ■ *"Configuring Remote Access" on page 89* ■ *Mobile Access Administration Guide* for your version ■ *Remote Access VPN Administration Guide* for your version	The Identity Awareness Gateway gets identities from Mobile Access clients and IPsec VPN clients configured to work in Office Mode when they connect to the Security Gateway.

Configuring Browser-Based Authentication

For the overview, see *"Browser-Based Authentication" on page 18*.

In the **Identity Sources** section of the Identity Awareness page, select **Browser-Based Authentication** to send unidentified users to the Captive Portal.

If you configure Transparent Kerberos Authentication (see *"Transparent Kerberos Authentication Configuration" on page 234*), the browser tries to identify AD users before sending them to the Captive Portal.

If you already have configured the portal in the Identity Awareness Wizard or SmartConsole, its URL shows below **Browser-Based Authentication**.

To configure the Browser-Based Authentication settings:

1. Select **Browser-Based Authentication** and click **Settings**.
2. From the **Portal Settings** window, configure:
   a. **Portal Network Location**

      Select if the portal runs on this Security Gateway or a different Identity Awareness Security Gateway. The default is that the Captive Portal is on the Security Gateway. The Security Gateway redirects unidentified users to the Captive Portal on the same Security Gateway. This is the basic configuration.

      A more advanced configuration is possible where the portal runs on a different Security Gateway. See the *"Identity Awareness Environment" on page 28* section for more details.

b. **Access Settings**

Click **Edit** to open the **Portal Access Settings** window. In this window, you can configure:

- **Main URL** - The primary URL that users are redirected to for the Captive Portal. You might have already configured this in the Identity Awareness Configuration wizard.
- **Aliases** - Click the **Aliases** button to **Add** URL aliases that are redirected to the main portal URL. For example, `ID.yourcompany.com` can send users to the Captive Portal. To make the alias work, it must be resolved to the main URL on your DNS server.
- **Certificate** - Click **Import** to import a certificate for the portal website to use. If you do not import a certificate, the portal uses a Check Point auto-generated certificate. This can cause browser warnings if the browser does not recognize Check Point as a trusted Certificate Authority. See *"Server Certificates" on page 231* for more details.
- **Accessibility** - Click **Edit** to select from where the portal can be accessed. You might have already configured this in the Identity Awareness Wizard. The options are based on the topology configured for the Security Gateway.
- How Users are sent to the Captive Portal if they use networks connected to these interfaces.

  The options are:

  - **Through all interfaces**
  - **Through internal interfaces**
    - **Including undefined internal interfaces**
    - **Including DMZ internal interfaces**
    - **Including VPN Encrypted interfaces** - Interfaces used for establishing route-based VPN tunnels (VTIs)
  - **According to the Firewall policy** - Select this if there is a rule that states who can access the portal.

c. **Authentication Settings**

Click **Settings** to open the **Authentication Settings** window. In this window you can configure:

- **Browser transparent Single Sign-On**

  Select **Automatically authenticate users from computers in the domain** if Transparent Kerberos Authentication is used to identify users.

  Main URL: - Use this URL to start the SSO process. If transparent authentication fails, users are redirected to the configured Captive Portal. This URL contains the DNS name or IP address of Identity Awareness Gateway.

  Note - The Identity Agent download link and the **Automatic Logout** option are ignored when Transparent Kerberos Authentication SSO is successful. This is so because users do not see the Captive Portal.

- **Authentication Method**

  Select one method that known users must use to authenticate.

  - **Defined on user record (Legacy Authentication)** - Takes the authentication method from **Security Gateway Object Properties** > **Other** > **Legacy Authentication**.
  - **User name and password** - This can be configured internally or on an LDAP server.
  - **RADIUS** - A configured RADIUS server. Select the server from the list.

- **User Directories**

  Select one or more places where the Security Gateway searches to find users when they try to authenticate.

  - **Internal users** - The directory of internal users.
  - **LDAP users** - The directory of LDAP users. Either:
    - **Any** - Users from all LDAP servers.
    - **Specific** - Users from an LDAP server that you select.
  - **External user profiles** - The directory of users who have external user profiles.

  The default is that all user directory options are selected. Select only one or two options if users are only from a specified directory or directories and you want to maximize Security Gateway performance when users authenticate. Users with identical user names must log in with domain\user.

d. **Customize Appearance**

Click **Edit** to open the **Portal Customization** window and edit the images that users see in the Captive Portal. Configure the labeled elements of the image below.

Label Number	Name	To do in GUI
1	Portal Title	Enter the title of the portal. The default title is **Network Login**.
2	Company Logo	Select **Use my company logo** and **Browse** to select a logo image for the portal.
2	Company Logo for mobiles	Select **Use my company logo for mobiles** and **Browse** to select a smaller logo image for users who get an access to the portal from mobile devices.

e. **User Access**

Configure what users can do in the Captive Portal to become identified and get an access to the network.

Name and password login

Users are prompted to enter a current username and password. Only known users can authenticate.

Click **Settings** to configure settings for known users after they enter their usernames and passwords successfully.

- **Access will be granted for xxx minutes** - For how long they can get an access to network resources before they have to authenticate again.
- **Ask for user agreement** - You can tell users to sign a user agreement. Click **Edit** to upload an agreement. This option is not selected by default because a user agreement is not usually necessary for known users.
- **Adjust portal settings for specific user groups** - You can add user groups and give them settings that are different from other users. Settings specified for a user group here override settings configured elsewhere in the Portal Settings. The options that you configure for each user group are:
  - If they must accept a user agreement.
  - If they must download an Identity Agent and which one.
  - If they can defer the Identity Agent installation and until when.

You can only configure settings for Identity Agent environment if you select **Identity Agents** on the **Identity Awareness** page.

Unregistered guests login

Let guests who are not known by the Security Gateway get an access to the network after they enter the necessary data.

Click **Settings** to configure settings for guests.

- **Access will be granted for xxx minutes** - For how long they can get an access to network resources before they have to authenticate again.

- **Ask for user agreement** - Makes users sign a user agreement. Click **Edit** to select an agreement, and the **End-user Agreement Settings** page opens. Select an agreement to use:
  - **Default agreement with this company name** - Select this to use the standard agreement. See the text in the **Agreement preview**. Replace **Company Name** with the name of your company. This name is used in the agreement.
  - **Customized agreement** - Paste the text of a customized agreement into the text box. You can use HTML code.
- **Login Fields** - Edit the table shown until it contains the fields that users complete in that sequence. Select **Is Mandatory** for each field that guests must complete before they can get an access to the network. To add a new field, enter it in the empty field and then click **Add**. Use the green arrows to change the sequence of the fields. The first field shows the user name in **Logs & Events** > **Logs**.

f. **Configuring Identity Agent from the Portal**

If you select **Identity Agents** as a method to get identities, you can tell users to download the Identity Agent from the Captive Portal. You can in addition let users install the Identity Agent on a specified later date and not now.

- **Require users to download** - Select this to make users install the Identity Agent. Select which Identity Agent they must install. If this option is selected and the **defer** option is not selected, users can not get access to the network if they install the Identity Agent.
- **Users may defer installation until** - Select this option to give users flexibility to make a choice when to install the Identity Agent. Select the date by which they must install it. Until that date a **Skip Identity Agent installation** option shows in the Captive Portal.

Note - When you enable Browser-Based Authentication on an IPSO Security Gateway that is on an IP Series appliance, make sure to set the Voyager management application port to a port other than 443 or 80.

Configuring AD Query

For the overview, see *"AD Query" on page 20*.

Important - Before you configure AD Query, you must:

- Enable RADIUS Accounting on the Security Gateway / each Cluster Member before it can work as a RADIUS Accounting server. See the *R82 Gaia Administration Guide*.
- Configure the LDAP Account Unit objects for your Active Directory Domain Controllers. See the *R82 Security Management Administration Guide*.

Important - NTLMv1 and NTLMv2 authentication are supported. These are the default authentication modes in an R82 Security Gateway:

Security Gateway Version	Configuration Before the Security Gateway Upgrade	Default Authentication Mode
R82 - Clean Install	N / A **Note** - Starting from R81.20, the default is NTLMv2.	NTLMv2
R82 - Upgrade from a lower version	Authentication mode was **not** changed using the `adlogconfig` command. **Note** - In R81.10 and lower, the default is NTLMv1.	NTLMv2
R82 - Upgrade from a lower version	Authentication mode was changed to NTLMv1 using the `adlogconfig` command. **Note** - In R81.10 and lower, the default is NTLMv1. **Example for R81.10** - An administrator changed the authentication mode from the default NTLMv1 to NTLMv2, and then from NTLMv2 back to NTLMv1.	NTLMv1

Procedure:

1. **Enable AD Query for a Security Gateway**

   a. From the left navigation panel, click **Gateways & Servers**.

   b. Open the Security Gateway or Cluster object.

   c. On the **General Properties** page, select the **Identity Awareness** Software Blade (if did not do so already).

   d. On the **Identity Awareness** page, select **Active Directory Query**.

e. Click the **Settings** button.

The **Active Directory Query** window opens.

f. In the **Active Directory Domains** section:

- Click the **green plus sign [+]** and select an existing LDAP Account Unit object to add it to the list.
- Select an LDAP Account Unit object and click the **red minus sign [-]** to remove it from the list.

2. **Optional: Configure the Single User Assumption**

You can configure AD Query to allow only one active account per IP address.

When user **A** logs out before the timeout and user **B** logs in, user **A**'s session closes automatically and his permissions are canceled.

User **B** is the only active user account and only his permissions are valid.

This feature is called **Single User Assumption**.

Before you activate Single User Assumption, you must exclude all Service Accounts used by user computers.

Note - Another way to reduce the occurrence of these issues is to increase the DHCP lease time.

To activate the Single User Assumption:

a. Exclude Service Accounts (Users, Computers, and Networks).

Procedure

You can manually exclude service accounts (users, computers, and networks) from the AD Query scan. In addition, you can configure AD Query to automatically detect and exclude suspected service accounts. Identity Awareness identifies service accounts as user accounts that are logged in to more than a specified number of computers at the same time.

Excluding objects from Active Directory queries:

i. On the **Identity Awareness** page, select **Active Directory Query** and click **Settings**.

ii. Click the **Advanced** button.

The **Active Directory Query Advanced** window opens.

iii. In the **Excluded Users / Computers** section, enter the user or computer account name and click **Add**.

You can use the ***** and **?** wildcard characters or regular expressions (see *"Appendix: Regular Expressions" on page 342*) to select more than one account.

Use this syntax for regular expressions: `regexp:<Regular Expression>`.

iv. **Optional:** Select **Automatically exclude users which are logged into more than [ ] machines simultaneously**.

Enter the threshold number of computers in the related field.

v. In the **Excluded Networks** section:

- Click the **green plus sign [+]** and select an existing Network object (or click **New** to create an applicable object) to add it to the list.
- Select a Network object and click the **red minus sign [-]** to remove it from the list.

vi. Click **OK** to close the **Active Directory Query Advanced** window.

b. In the **Active Directory Query** window, select **Assume that only one user is connected per computer**.

Note - To deactivate the Single User Assumption, clear this option.

c. Click **OK** to close the **Active Directory Query** window.

d. Click **OK** to close the Security Gateway or Cluster object.

e. Install the Access Control Policy on the Security Gateway or Cluster object.

3. **Optional: Manage the Suspected Service Account List**

When automatic exclusion is enabled, Identity Awareness looks for suspected service accounts every 10 minutes. Suspected Service Accounts are saved to a persistent database that survives reboot. When a new Service Account is detected, a log appears in SmartConsole > **Logs & Events** view > **Logs** tab.

Use these commands to see and manage the suspected service account database:

Notes:

- You must run these commands in the Expert mode on the Identity Awareness Gateway.
- In a Cluster, you must configure all the Cluster Members in the same way.

Action	Syntax
Show all suspected Service Accounts	`adlog a control srv_accounts show`
Run the Service Accounts scan immediately	`adlog a control srv_accounts find` This command is useful before you enable the **Assume that only one user is connected** option.
Remove an account from the Service Account database	`adlog a control srv_accounts unmark <account name>`
Remove all accounts from the suspected Service Account database	`adlog a control srv_accounts clear`

Important - When you use the "`adlog a control`" command, you must run this command to save the configuration:

```
adlog a control reconf
```

For more information, see *"adlog control" on page 250*.

4. **Recommended: Configure the authentication mode to use NTLMv2**

Follow these steps to make sure the authentication mode uses NTLMv2:

a. **On the Security Management Server**

Note - On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:`mdsenv <IP Address or Name of Domain Management Server>`

i. Connect to the command line.

ii. Log in to the Expert mode.

iii. Run:

```
adlogconfig a
```

iv. Examine the section **Authentication mode**:

- If **[x]** appears next to the option **[x] Use NTLMv2**, then skip to the next step, *"Use Automatic LDAP Group Update" on page 56*.
- If **[x]** appears next to the option **[x] Use NTLMv1**, then enter the number of this option:

  Change authentication mode NTLMv1/NTLMv2

  Make sure **[x]** appears next to the option **[x] Use NTLMv2**.

v. Enter the number of this option:

Exit and save

b. **On the Security Gateway / each Cluster Member**

On a Security Gateway / ClusterXL / Scalable Platform Security Group:

i. Connect to the command line.

ii. Log in to the Expert mode.

iii. Run:

```
adlogconfig a
```

iv. Examine the section **Authentication mode**:

- If **[x]** appears next to the option **[x] Use NTLMv2**, then skip to the next step, *"Use Automatic LDAP Group Update" on the next page*.
- If **[x]** appears next to the option **[x] Use NTLMv1**, then enter the number of this option:

  Change authentication mode NTLMv1/NTLMv2

  Make sure **[x]** appears next to the option **[x] Use NTLMv2**.

v. Enter the number of this option:

Exit and save

On a Quantum Spark Gateway / each Quantum Spark Cluster Member:

i. Connect to the command line on the Quantum Spark Gateway / each Quantum Spark Cluster Member.

ii. If the default shell is Gaia Clish, go to the Expert mode:

```
expert
```

iii. Create the required file:

```
touch $FWDIR/conf/ad_log_override.C
```

iv. Edit this file:

```
vi $FWDIR/conf/ad_log_override.C
```

v. Add these lines:

```
(Configuration
    :UseNTLMv2 (true)
)
```

vi. Save the changes in the file and exit the editor.

vii. Run:

```
adlog a control reconf
```

c. **In SmartConsole, restart the Identity Awareness Configuration wizard and configure Identity Awareness**

i. From the left navigation panel, click **Gateways & Servers**.

ii. Open the Security Gateway or Cluster object.

iii. In the **General Properties** pane, clear **Identity Awareness**. Do **not** click **OK**.

iv. In the **General Properties** pane, select **Identity Awareness**.

The **Identity Awareness Configuration** window opens.

v. Follow the Identity Awareness wizard.

vi. Click **OK** to close the Security Gateway or Cluster object.

vii. Install the Access Control Policy on the Security Gateway or Cluster object.

5. **Use Automatic LDAP Group Update**

Identity Awareness automatically recognizes changes to LDAP group membership and updates identity information, including Access Roles.

Warning - When you add, move, or remove an LDAP nested group, the system recalculates LDAP group membership for ALL users in ALL Groups. Be very careful when you deactivate user-related notifications.

Important - Automatic LDAP group update works only with Microsoft Active Directory when AD Query is activated.

LDAP Group Update is activated by default. You can deactivate LDAP Group Update.

Deactivating automatic LDAP group update

a. Connect to the command line on the Security Gateway / each Cluster Member.

b. Log in to the Expert mode.

c. Run:

```
adlogconfig a
```

d. Enter the number of this option:

   Turn LDAP groups update on/off.

   The **LDAP groups update notifications** status changes to **[ ]** (not active).

   If you select the option **Turn LDAP groups update on/off** when automatic LDAP group update is not active, the **LDAP groups update notifications** status changes to **[X]** (active).

e. Enter the number of this option:

   Exit and save

f. In SmartConsole, install the Access Control Policy on the Security Gateway or Cluster object.

Note - You can use `adlogconfig` to configure the time between LDAP change notifications and to send notifications only for changes related to users.

Configuring LDAP group notification options

a. Connect to the command line on the Security Gateway / each Cluster Member.

b. Log in to the Expert mode.

c. Run

```
adlogconfig a
```

d. Enter the number of this option:

   Notifications accumulation time

e. Enter the time between notifications in seconds (default = 10).

f. Enter the number of this option control whether to send notifications only for changes related to users:

   Update only user-related LDAP changes

   Warning - Be very careful when you deactivate only user-related notifications. This can cause excessive CPU load on the Security Gateway / Cluster Member.

g. Enter the number of this option:

   Exit and save

h. In SmartConsole, install the Access Control Policy on the Security Gateway or Cluster object.

Automatic LDAP Group Update does not occur immediately because Identity Awareness looks for users and groups in the LDAP cache first. The information in the cache does not contain the updated LDAP Groups. By default, the cache contains 1,000 users and cached user information is updated every 15 minutes.

To get automatic LDAP Group Update assignments immediately, you must deactivate the LDAP cache. This action can cause Identity Awareness to work slower than expected.

Deactivating the LDAP

a. In SmartConsole, go to **Menu** > **Global properties**.

b. In the left navigation tree, click **User Directory**.

c. Change **Timeout on cached users** to zero.

d. Change **Cache size** to zero.

e. Click **OK**.

f. Install the Access Control Policy on the Security Gateway or Cluster object.

6. **Configure Domain Controllers for each Security Gateway**

An organization Active Directory can have more than one sites, where each site has its own domain controllers that are protected by a Security Gateway. When all of the domain controllers belong to the same Active Directory, one LDAP Account Unit is created in SmartConsole.

When AD Query is enabled on a Security Gateway, you can configure the Security Gateway to communicate with only some of the domain controllers. For each domain controller the AD Query needs to ignore, configure the default priority of the Account Unit to a value that is greater than 1000.

Example:

- The LDAP Account Unit *ad.mycompany.com* has 5 domain controllers - *dc1*, *dc2*, *dc3*, *dc4*, and *dc5*.
- On the Identity Awareness Gateway, it is necessary to enable AD Query for only domain controllers *dc2* and *dc3*. This means that priority of all other domain controllers (*dc1*, *dc4*, and *dc5*) must be set to a number greater than 1000 in the Identity Awareness Gateway object.

To specify Domain Controllers for each Security Gateway (based on the example above):

a. From the left navigation panel, click **Gateways & Servers**.

b. Open the Security Gateway or Cluster object.

c. In the left tree, click on the **[+]** near **Other** and click **User Directory**.

d. Select the option **Selected Account Units list**.

e. Click **Add**.

f. Select the applicable Account Unit object.

> **Important** - The account that connects to Active Directory must be a service account, not a personal user account.

g. Click **OK**.

h. Clear the option **Use default priorities**.

i. Configure the priority **1001** for *dc1*, *dc4*, and *dc5*:

   i. Select the domain controller.

   ii. In the **Priority** field, enter **1001**.

   iii. Click **Set**.

j. Click **OK**.

k. Install the Access Control Policy on the Security Gateway or Cluster object.

7. **Examine the Status of Domain Controllers**

Make sure that the domain controllers are configured correctly.

Examine with which domain controllers the Security Gateway communicates and which domain controllers it ignores.

a. Connect to the command line on the Security Gateway / each Cluster Member.

b. Log in to the Expert mode.

c. Run:

```
adlog a dc
```

For more information, see *"adlog dc" on page 252*.

Troubleshooting for AD Query

If you experience connectivity problems between your domain controllers and Identity Awareness Gateway/Log Servers, perform the following troubleshooting steps:

1. Resolve Connectivity Issues
    a. Ping the domain controller from the Identity Awareness Gateway and Log Server.
    b. Ping the Identity Awareness Gateway and Log Server from your domain controller.
    c. Perform standard network diagnostics as necessary.
    d. Check the **Logs** tab of the **Logs & Events** view and see if there are drops between a Security Gateway defined with AD Query (Source) and the domain controller (Destination). If there are drops, see *"Configuring the Firewall" on page 63* and sk58881.
2. Use Microsoft WBEMTEST utility to verify WMI is functional and accessible:

a. **Connect to the Utility**

i. Click **Start** > **Run**.

ii. Enter `wbemtest.exe` in the **Run** window.

iii. In the **Windows Management Instrumentation Tester** window, click **Connect**.

iv. In the **Connect** window, in the first field, enter the Domain controller, in this format: `\\<IP address>\root\cimv2`

v. In the **Credentials** > **User** field, enter the fully qualified AD user name. For example: *ad.company.com\admin*

vi. Enter a password for the user.

vii. Click **Connect**.

viii. If the **Windows Management Instrumentation Tester** window re-appears with its buttons enabled, WMI is fully functional.

If the connection fails, or you get an error message, check for these conditions:

- Connectivity problems (see *"Resolve Connectivity Issues" on the previous page*)
- Incorrect domain administrator credentials (see *"Verify your domain administrator credentials" on the next page*).
- WMI service is not running (see *"Verify the WMI Service on the Domain Controller" on the next page*).
- A Firewall is blocking traffic between the Identity Awareness Gateway or Log Server and domain controller (see *"Configuring the Firewall" on page 63*).

b. **Verify your domain administrator credentials**

   i. Click **Start** > **Run**.

   ii. In the **Run** window, enter `\\<domain controller IP address>\c$`

   For example: `\\11.22.33.44\c$`

   iii. In the **Logon** window, enter your domain administrator user name and password.

   iv. If the domain controller root directory appears, this indicates that your domain administrator account has sufficient privileges. An error message may indicate that:

      i. If the user does not have sufficient privileges, this indicates that he is not defined as a domain administrator. Obtain a domain administrator credentials.

      ii. You entered the incorrect user name or password. Check and retry.

      iii. The domain controller IP address is incorrect or you are experiencing connectivity issues.

c. **Verify the WMI Service on the Domain Controller**

   i. Click **Start** > **Run**.

   ii. Enter `services.msc` in the **Run** window.

   iii. Find the **Windows Management Instrumentation** service and see that the service started.

   If it did not start, right-click this service and select **Start**.

d. **Configuring the Firewall**

If a Firewall is located between the Identity Awareness Gateway or Log Server, and the Active Directory controller, configure the Firewall to allow WMI traffic.

To create Firewall rules for WMI traffic:

i. In SmartConsole, from the **Security Policies** view, open the **Access Control Policy**.

ii. Create a rule that allows **ALL_DCE_RPC** traffic:

- **Source** = Security Gateway that run AD Query
- **Destination** = Domain Controllers
- **Service** = **ALL_DCE_RPC**
- **Action** = **Accept**

iii. Save the policy and install it on Security Gateway.

Note - If there are connectivity issues on DCE RPC traffic after this policy is installed, see sk37453 for a solution.

3. Confirm that Security Event Logs are Recorded:

If you have checked connectivity (see *"Resolve Connectivity Issues" on page 60*) but still do not see identity information in logs, make sure that the necessary event logs are being recorded to the Security Event Log.

AD Query reads these events from the Security Event log:

- For Windows Server 2003 domain controllers - 672, 673, 674
- For Windows Server 2008 and above domain controllers - 4624, 4769, 4768, 4770

Make sure you see the applicable events in the Event Viewer on the domain controller (My computer > Manage > Event Viewer > Security).

If the domain controller does not generate these events (by default they are generated), refer to Microsoft Active Directory documentation for instructions on how to configure these events.

Configuring RADIUS Accounting

For the overview, see *"RADIUS Accounting" on page 22*.

Configure RADIUS Accounting in the **RADIUS Accounting Settings** window. In the **Check Point Gateway** window > **Identity Awareness** page, click **RADIUS Accounting** > **Settings**.

Enabling RADIUS Accounting on a Security Gateway

You must enable RADIUS Accounting on Security Gateway before they can work as a RADIUS Accounting server:

1. In the **SmartConsole Gateways & Servers** view, open the Security Gateway.
2. On the **General Properties** page, make sure that **Identity Awareness** is enabled.
3. On the **Identity Awareness** page, select **RADIUS Accounting**.

RADIUS Client Access Permissions

Gateway interfaces must be authorized to accept connections from RADIUS Accounting clients:

1. In the **RADIUS Client Access Permissions** section, click **Edit**.
2. Select Security Gateway interfaces that can accept connections from RADIUS Accounting clients:
    a. **All Interfaces** - All Security Gateway interfaces can accept connections from RADIUS Accounting clients (default).
    b. **Internal Interfaces** - Only explicitly defined internal Security Gateway interfaces can accept connections from RADIUS Accounting clients.
        - **Including undefined internal interfaces** - In addition, accepts connections from internal interfaces without a defined IP address.
        - **Including DMZ internal interfaces** - In addition, accepts connections from clients located in the DMZ.
    c. **Firewall Policy** - The Firewall policy allows interface connections.
3. Enter or select the RADIUS server port (default = 1813).

Important - The **All Interfaces** and **Internal Interface** options have priority over Firewall Policy rules. If a Firewall rule is configured to block connections from RADIUS Accounting clients, connections continue to be allowed when one of these options are selected.

Authorized RADIUS Clients

An Identity Awareness Gateway accepts RADIUS Accounting requests only from authorized RADIUS Accounting clients. A RADIUS Accounting client is a host with a RADIUS client software installed:

1. In the **Authorized RADIUS Clients** section of the **RADIUS Accounting** window, click the **+** icon and select a RADIUS Accounting Client from the list.

Click **New** to create a specified new host object for the RADIUS Accounting client. This host object is selected automatically.

Click the **[-]** - icon to remove a current RADIUS client from the list.

2. Click **Generate** to create a strong, shared secret for client authentication. This shared secret applies to all host objects in this list.

   You can manually enter a shared secret. It is not necessary to generate a new shared secret when you add or remove clients from the list.

RADIUS Message Attribute Indices

RADIUS Accounting Messages contain identity, authentication and administrative information for a connection. This information is contained in predefined attributes of the RADIUS Accounting Message packet.

The **Message Attributes Indices** section tells Identity Awareness, which attributes in RADIUS Accounting Messages contain identity information used by Identity Awareness:

- **Device name** - RADIUS device-name attribute.
- **User name** - RADIUS user-name attribute.
- **IP Address** - RADIUS IP address attribute.

Select a message attribute for each of these values. The default attributes are correct for many Identity Awareness configurations.

Note - **Vendor-Specific (26)** is a user-defined attribute. There can be more than one **Vendor-Specific** attribute in a RADIUS Accounting message, each with a different value.

A sub-index value is assigned to each **Vendor-Specific** attribute in a message. This lets Identity Awareness find and use the applicable value.

To configure message attributes:

1. Select a message attribute from the list for each index field.
2. If you use the **Vendor-Specific (26)** attribute, select the applicable sub-index value.

Session Timeout and LDAP Servers

You can create a specified user session timeout. This parameter is the maximum time that a user session stays open without receiving an **Accounting Start** or **Interim-Update** message from the RADIUS Accounting client. To create the specified session timeout, enter or select a value in minutes (default = 720).

You can select, which LDAP Account Units the Security Gateway searches for user or device information, when it gets a RADIUS Accounting request. LDAP Account Units are configured in SmartConsole.

To make the specified authorized LDAP Account Units:

1. Click the **Settings** button, located below the **LDAP Account Units** heading.
2. In the **LDAP Account Units** window, select one of these options:
   - **Any** - Searches all defined LDAP Account Units for user or device information.
   - **Specific** - Searches only the specified LDAP Account Units for user or device information.
     - Click **+** to add an authorized LDAP Account Unit.
     - Click **[-]** - to remove an authorized LDAP Account Unit.
3. If you selected the **Specific** option, click the green **[+]** icon and then select one or more LDAP Account Units.

RADIUS Secondary IP and Dual Stack Support

The RADIUS server can send one message with two IP addresses, rather than a message for each address.

With this feature, you can get two IP addresses from the RADIUS message and two different sessions are created, one for each IP.

To configure secondary IP or dual stack:

1. Use an SSH connection or console to get access to the Security Gateway.
2. Log in to the Expert mode.
3. Run:

   ```
   pdp radius ip set < attribute index >
   ```

   Where < *attribute index* > is the RADIUS index with the secondary IP address value (this is similar to the User IP index that you can set in SmartConsole).

Note

- If the secondary IP index is 26 (Vendor-Specific), you must add the vendor-specific attribute index of the message that contains the secondary IP:

```
pdp radius ip set < attribute index > -a < vendor
specific attribute index >
```

- You can set the server to handle RADIUS messages from a specified Vendor code:

```
pdp radius set ip < attribute index > -a < vendor
specific attribute index> -c <vendor code >
```

This is a sample command to configure a Cisco-AVPair:

```
pdp radius ip set 26 -a 1 -c 9
```

RADIUS Attribute Parsing

This feature allows parsing string or text data in RADIUS messages. The parser finds a string between a predefined prefix and suffix.

For example, if the message is in the form of `###data~~@`, you can set the parser with the prefix `#` and suffix `@` to find `data`.

To configure RADIUS Attribute parsing:

Run:

```
pdp radius parser set< attribute index > [-p < prefix >] [-s <
suffix >]
```

Where < *attribute index* > is the RADIUS index with the value, which needs parsing.

< *prefix* > and < *suffix* > are the parsing options.

If the message is < *text1* >< *prefix* >< *text2* >< *suffix* >< *text3* >, the parser returns < *text2* >.

Example:

message is: `username=test;`
prefix is: `username=`
suffix is: *;* (semi-colon)
parsed text is: `test`

You can specify a prefix, or a suffix. If you specify only one, the parser takes out only what you specified.

Note

- If the attribute index is 26 (vendor-specific), you must add the vendor-specific attribute index:
  `pdp radius parser set < attribute index> -a < vendor specific attribute index> -p < prefix> -s < suffix>`
- You can set the server to handle RADIUS messages from a specified vendor code:
  `pdp radius parser set < attribute index> -a < vendor specific attribute index> -c < vendor code> -p < prefix> -s < suffix>`

Receiving Groups from RADIUS Messages

With this feature, you can read the user or computer groups from the RADIUS message and calculate Access Roles accordingly.

To configure group fetching from RADIUS messages:

- Run:

```
pdp radius group set -u <attribute index> -d <delimiter>
```

- Run:

```
pdp radius group fetch on
```

Where < *attribute index* > is the RADIUS index with the groups value, -u sets user groups and -m sets computer groups and < *delimiter* > is the delimiter used to split multiple groups in one message.

For example, if you want to fetch user groups, and the message is "`group1;group2;group3`", then set the delimiter to ";" using this command:

```
pdp radius groups set -u < attribute index > -d ";"
```

Note

- If the attribute index is 26 (vendor-specific), you must add the vendor-specific attribute index:

```
pdp radius groups set -u < attribute index > -a <
vendor specific attribute index > -d < delimiter >
```

- You can set the server to handle RADIUS messages from a specific vendor code:

```
pdp radius groups set -u < attribute index > -a <
vendor specific attribute index > -c < vendor code >
-d < delimiter >
```

When receiving groups from RADIUS messages is enabled, the Identity Awareness Gateway does not fetch groups from other servers for RADIUS accounting users or computers.

Configuring Identity Awareness API

This section describes how to configure and work with Identity Awareness API.

For the overview, see *"Identity Web API" on page 24*.

Configuring Identity Awareness API Settings

1. From the left navigation panel, click **Gateways & Servers**.
2. Open the Security Gateway / Cluster object.
3. From the left tree, click **Identity Awareness**.
4. In the **Identity Sources** section, select **Identity Web API** and click **Settings**.
5. Go to the **Identity Web API Settings** window and configure:

- **Client Access Permissions**

  You must select Identity Awareness Gateway interfaces that can accept connections from Web API clients:

  a. In the **Client Access Permissions** section of the **Identity Web API Settings** window, click **Edit**.

  b. Select Security Gateway interfaces that can accept connections from Web API clients. The options are based on the topology configured for the Security Gateway. Web API clients can get an access to the Security Gateway, if they use networks connected to these interfaces.

     The options are:

     - **Through all interfaces**
     - **Through internal interfaces**
       - **Including undefined internal interfaces**
       - **Including DMZ internal interfaces**
       - **Including VPN Encrypted interfaces** - Interfaces used for establishing route-based VPN tunnels (VTIs)
     - **According to the Firewall policy** - Select this if there is a rule that states who can access the portal.

  Important -The **Through all interfaces** and **Through internal interfaces** options have priority over Firewall Policy rules. If a Firewall rule is configured to block connections from Identity Collector clients, connections continue to be permitted when one of these options is selected.

- **Authorized Clients and Selected Client Secret**

  An Identity Awareness Gateway accepts connections only from authorized Web API client computers.

  To configure authorized Web API client computers:

  a. In the **Authorized Clients** section of the **Identity Collector Settings** window, click the **green [+]** icon and select a Web API client from the list.

  Notes:
  - To create a specified new host object:
    i. Close the **Web API Settings** window.
    ii. Close the **Identity Awareness Gateway Properties** window.
    iii. From the top toolbar, click the **Objects** menu **> More object types > Network Object > New Host**.
    Or from the right upper corner, click the **Objects** tab **> New > Host**.
  - To remove a current Identity Collector client from the list, select the client and click the **red [-]** icon.

  b. Create an authentication secret for a selected Web API client:

  i. Select the Web API client in the list.

  ii. Click **Generate**, or enter the applicable secret manually.

  Notes:
  - Each client has its own client secret.
  - To modify a client secret, change it manually.

- **Authentication Settings**

  In the **Authentication Settings** section of the **Web API Settings** window, click **Settings**.

  The **LDAP Account Units** window opens.

  Configure where the Identity Awareness Gateway can search for users, when they try to authenticate:

  - **Internal users** - The directory of configured internal users.
  - **LDAP users** - The directory of LDAP users:
    - **All Gateway's Directories** - Users from all configured LDAP servers.
    - **Specific** - Users from configured LDAP servers that you select.
  - **External user profiles** - The directory of users, who have external user profiles.

  By default, all User Directories options are selected. You can select only one or two options, if users are only from a specified directory, and you want to maximize Security Gateway performance, when users authenticate. Users with identical user names must log in with `domain\username`.

Identity Web API Commands

The Identity Web API uses the REST protocol over SSL. The requests and responses are HTTP and in JSON format.

The web API URL has this structure:

`https://<IP Address or FQDN of Gateway>/_IA_API/v1.0/<command>`

For example: `https://gw.acme.com/_IA_API/v1.0/add-identity`

The expected JSON structure is a simple, flat key-value object.

Versioning

To provide backward and forward compatibility, you can include the Web API version in the request URL, as shown in this table:

URL	API Version	Minimum Gateway Version
`https://<GW_IP_or_FQDN>/_IA_API/idasdk/<command>`	1.0	R80.10
`https://<GW_IP_or_FQDN>/_IA_API/v1.0/<command>`	1.0	R80.10

URL	API Version	Minimum Gateway Version
`https://<GW_IP_or_FQDN>/_IA_API/<command>`	Latest	R80.10

Important - URL `https://<GW_IP_or_FQDN>/_IA_API/idasdk/<command>` used by R80.10 EA customers is preserved and serves API version 1.0.

Add Identity (v1.0)

Creates a new Identity Awareness association for a specified IP address.

Syntax

```
POST https://<IP Address or FQDN of Gateway>/_IA_API/v1.0/add-identity
```

Parameter	Type	Description	Default value
`shared-secret`	String	Shared secret	N/A
`ip-address`	String (IP)	Association IP. Supports either IPv4 or IPv6, but not both.	N/A
`user`	String	User name	Empty string
`machine`	String	Computer name	Empty string
`domain`	String	Domain name	Empty string
`session-timeout`	Integer	Timeout (in seconds) for this Identity Awareness association	43200 (12 hours)
`fetch-user-groups`	Boolean (0/1)	Defines whether Identity Awareness fetches the user's groups from the user directories defined in SmartConsole.	1
`fetch-machine-groups`	Boolean (0/1)	Defines whether Identity Awareness fetches the machine's groups from the user directories defined in SmartConsole.	1

Parameter	Type	Description	Default value
`user-groups`	Array of strings	List of groups, to which the user belongs (when Identity Awareness does not fetch user groups).	Empty array
`machine-groups`	Array of strings	List of groups, to which the computer belongs (when Identity Awareness does not fetch computer groups).	Empty array
`calculate-roles`	Boolean (0/1)	Defines whether Identity Awareness calculates the identity's Access Roles.	1
`roles`	Array of strings	List of roles to assign to this identity (when Identity Awareness does not calculate roles).	Empty array
`machine-os`	String	Host operating system. For example: Windows 7.	Empty string
`host-type`	String	Type of host device. For example: Apple iOS device.	Empty string

Response Fields

Parameter	Type	Description
`ipv6-address`	String (IP)	Created IPv6 identity
`ipv4-address`	String (IP)	Created IPv4 identity
`message`	String	Textual description of the command's result

Best Practice - You must include the domain name whenever available, to make sure that the user is authorized by the correct server, improves performance and prevents incorrect authorization, when there are identical user names in more than one domain.

Notes

- The request must include user or computer information or both. The `shared-secret` and `ip-address` fields are mandatory.
- String attributes, for example, user, domain and group names, must not contain curly brackets ("{", "}"), square brackets ("[", "]"), or angle brackets ("<", ">"). Requests that contain these characters fail.
- When you set `fetch-user-groups` or `fetch-machine-groups` or both to 1, you must in addition set `calculate-roles` to 1. If not, there is no assignment of Access Roles and the request fails.
- When you set `fetch-user-groups` or `fetch-machine-groups` or both to 1, user authorization can fail (for example, if the user cannot be found in an Account Unit). Because the gateway sends the response before the authorization process is complete, a successful response does not necessarily mean the gateway created the identity successfully.
- If you know the operating system and host type of the created associations, you can include this information in the `machine-os` and `host-type` fields. This improves the information audit, but does not harm enforcement.
- For Active Directory user and computer groups, which are generated with the Access Role creation tool, include a special prefix:
  - Group prefix is `ad_group_`
  - User prefix is `ad_user_`
  - Machine prefix is `ad_machine_`

  For example, for Active Directory user group *MyGroup* the user group attribute is `ad_group_MyGroup`. For computer group *MyMachinePC*, the machine-groups attribute is `ad_machine_MyMachinePC`.

Examples

Example 1 - Minimum request for user identity generation

Request

```
POST https://gw.acme.com/_IA_API/v1.0/add-identity
```

```
{
 "shared-secret":"****",
 "ip-address":"1.2.3.5",
 "user":"mary"
}
```

Response

```
{
 "ipv4-address":"1.2.3.5",
 "message":"Association sent to PDP."
}
```

Example 2- User-defined groups, calculate roles

Request

```
POST https://gw.acme.com/_IA_API/v1.0/add-identity
```

```
{
 "shared-secret":"****",
 "ip-address":"1.1.1.1",
 "user":"john",
 machine":"",
 "domain":"cme.com",
 "user-groups":["MyUserGroup"],
 "roles":[],"timeout":4,
 "fetch-user-groups":0,
 "calculate-roles":1,
 "identity-source":"ACME API Client"
}
```

Response

```
{
 "ipv4-address":"1.1.1.1",
 "message":"Association sent to PDP."
}
```

Example 3 - User-defined groups and roles, detailed information

Request

```
POST https://gw.acme.com/_IA_API/v1.0/add-identity
```

```
{
 "shared-secret":"****",
 "user":"John",
 "machine":"Laptop_1234",
 "ip-address":"2.2.2.2",
 "identity-source":"ACME API Client",
 "machine-os":"Windows 10 (Build 1176)",
 "host-type":"Laptop",
 "fetch-user-groups":0,
 "fetch-machine-groups":0,
 "calculate-roles":0,
 "session-timeout":43200,
 "user-groups":["EnterpriseFinanceUsers","ad_user_JohnDoe"],
 "machine-groups":["EnterpriseLaptopMachines"],
 "roles":["FinanceUser","StandardLaptop"]
}
```

Response

```
{
 "ipv4-address" : "2.2.2.2",
 "message" : "Association sent to PDP."
}
```

Delete Identity (v1.0)

Delete Identity Awareness associations for one IP address, a range of IP addresses, a subnet, or associations for an IP address and a user name.

Syntax

```
POST https://<IP Address or FQDN of Gateway>/_IA_
API/v1.0/delete-identity
```

Parameter	Type	Description	Default Value
`shared-secret`	String	Shared secret.	N/A
`ip-address`	String (IP)	Association IP address. Necessary when you revoke a single IP address.	Empty
`revoke-method`	String	Type of revoke method. It can be empty for the deletion of a single association by an IP address. If not, then the permitted values are: **mask** - for the deletion of all associations in a subnet. **range** - for the deletion of all associations in a range. **user-name-and-ip** - for the deletion of all associations with a specific user and a given IP address.	Empty
`subnet`	String (IP)	Subnet. Required when the revoke method is mask.	Empty
`subnet-mask`	String (IP)	Subnet mask. Required when the revoke method is mask.	Empty
`ip-address-first`	String (IP)	First IP address in the range. Required when the revoke method is range.	Empty

Parameter	Type	Description	Default Value
`ip-address-last`	String (IP)	Last IP address in the range. Required when the revoke method is range.	Empty
`client-type`	String	Deletes only associations created by the specified identity source. If no value is set for the client-type parameter, or if it is set to any, the Security Gateway deletes all identities associated with the given IP address(es) (the Client Type table has a list of the permitted values). **Note** - When the `client-type` is set to `vpn` (remote access), the Security Gateway deletes all the identities associated with the given IP address(es). This is because when you delete an identity associated with an Office Mode IP address, this usually means that this Office Mode IP address is no longer valid..	Any
`user`	String	User name. Required when the `revoke-method` is set to `user-name-and-ip`.	Empty

List of identity sources for the client-type parameter

Client type	Description
`any`	All identity sources
`captive-portal`	Browser-Based Authentication
`ida-agent`	Identity Agents
`vpn`	Remote Access
`ad-query`	Active Directory query
`multihost-agent`	Terminal Servers (Multi-User Host (MUH) Agent)
`radius`	RADIUS Accounting
`ida-api`	Identity Web API
`identity-collector`	Identity Collector

Response Fields

Parameter	Type	Description
ipv6-address	String (IP)	Deleted IPv6 association
ipv4-address	String (IP)	Deleted IPv4 association
message	String	Textual description of the command's result
count	Unsigned integer	Number of deleted identities

Examples

Example 1 - Delete by IP

Request

```
POST https://gw.acme.com/_IA_API/1.0/delete-identity
```

```
{
 "shared-secret":"****",
 "ip-address":"1.1.1.1"
}
```

Response

```
{
 "count":"1",
 "ipv4-address":"1.1.1.1",
 "message":"Disassociation sent to PDP."
}
```

Example 2 - Delete by IP range

Request

```
POST https://gw.acme.com/_IA_API/v1.0/delete-identity
```

```
{
 "shared-secret":"****",
 "revoke-method":"range",
 "ip-address-first":"1.1.1.2",
 "ip-address-last":"1.1.1.3"
}
```

Response

```
{
 "count":"2",
 "message":"Total of 2 IPs disassociations will be processed."
}
```

Example 3 - Delete by IP subnet

Request

```
POST https://gw.acme.com/_IA_API/idasdk/delete-identity
```

```
{
 "shared-secret":"****",
 "revoke-method":"mask",
 "subnet":"1.1.1.1",
 "subnet-mask":"255.255.255.0"
}
```

Response

```
{
 "count":"100",
 "message":"Total of 100 IPs disassociations will be processed."
}
```

Example 4 - Delete by IP and user name

Request

```
POST https://gw.acme.com/_IA_API/idasdk/delete-identity
```

```
{
 "shared-secret":"****",
 "ipv4-address":"1.1.1.1",
 "revoke-method":"user-name-and-ip",
 "user":"USER_NAME",
}
```

Response

```
{
 "count":"2",
 "ipv4-address":"1.1.1.1",
 "message":"Disassociation sent to PDP."
}
```

Query Identity (v1.0)

Queries the Identity Awareness associations of a given IP address.

Syntax

```
POST https://<IP Address or FQDN of Gateway>/_IA_
API/idasdk/show-identity
```

Parameter	Type	Description	Default Value
shared-secret	String	Shared secret	N/A
ip-address	String (IP)	Identity IP address	N/A

Response Fields

Parameter	Type	Description
ipv6-address	String (IP)	Queried IPv6 identity
ipv4-address	String (IP)	Queried IPv4 identity
message	String	Textual description of the command's result
users	Array	All user identities on this IP. The Information includes these fields: ■ Users' full names (full name if available, falls back to user name if not) ■ Array of groups ■ Array of roles ■ Identity source
machine	String	Computer name, if available
machine-groups	Array	List of computer groups
combined-roles	Array	List of all the Access Roles on this IP, for auditing and enforcement purposes.
machine-identity-source	String	Machine session's identity source, if the machine session is available.

Note - If more than one identity source authenticated the user, the result shows a separate record for each identity source.

Example

Request

```
POST https://gw.acme.com/_IA_API/v1.0/show-identity
```

```
{
 "shared-secret":"****",
 "ip-address":"1.1.1.1"
}
```

Response 1 - User identity is available

```
{
  "combined-roles":[
  "All_Identified_Users",
  "User_John"
  ],
  "domain":"cme.com",
  "ipv4-address":"1.1.1.1",
  "machine":"admin-pc@cme.com",
  "message":"total 1 user records were found.",
  "users":[
    {
      "groups":[
      "All Users",
      "ad_user_John_Smith"
      ],
      "identity-source':AD Query",
      "roles":[
      "All_identified_Users",
      "User_John"
      ],
      "user":"JohnSmith"
    }
  ]
}
```

Response 2 - User and computer identities are available

```
{
 "combined-roles":[
 "Admin-PC_cme.com",
 "All_Identified_Users",
 "User_John"],
 "domain":"cme.com",
 "ipv4-address":"192.168.110.126",
 "machine":"admin-pc@ad.ida",
 "machine-groups":[ "ad_machine_ADMINPC",
 "All Machines"],
 "machine-identity-source":" Identity Awareness API (ACME API
Client):,
 "message":"total 1 user records were found.",
 "users":[
  {
   "groups":[
   "All Users",
   "ad_user_John_Smith"
   ],
   "identity-source":"Identity Awareness API (ACME API Client)",
   "roles":[
   "Admin-PC_ad.ida",
   "All_Identified_Users",
   "User_John"
   ],
   "user":"John Smith"
  }
 ]
}
```


Response 3 - Multiple user identities are available

```
{
 "combined-roles":[
 "Admin-PC",
 "All_Identified_Users",
 "User_John"
 ],
 "domain":"cme.com",
 "ipv4-address":"192.168.110.126",
 "machine":"admin-pc@cme.com",
 "machine-identity-source":"AD Query",
 "ad_machine_ADMINPC",
 "All Machines"
 ],
 "message":"total 2 user records were found.",
 "users":[
  {
   "groups":[
   "All Users"
   ],
   "identity-source": "AD Query",
   "roles":[
   "Admin-PC",
   "All_Identified_Users"
   ],
   "user":"George Black"
  },
  {
   "groups":[
   "All Users",
   "ad_user_John_Smith"
   ],
   "identity-source": "AD Query",
   "roles":[
   "Admin-PC",
   "All_Identified_Users",
   "User_John"
   ],
   "user":"John Smith"
  }
 ]
}
```


Response 4 - No identity found

```
{
 "ipv4-address" : "1.1.1.1",
 "message" : "total 0 user records were found."
}
```

Bulk Commands (v1.0)

You can use a bulk command to send multiple commands in one request. To do this, send the bulk command with a `requests` array, in which each array element contains the parameters of one request. The response returns a `responses` array, in which each array element contains the response for one command. The responses appear in the order of the requests.

Example 1 - Adding multiple associations

Request

Upper left corner

```
{
 "shared-secret" : "****",
 "requests":[
  {"user":"linda","machine":"","ip-address":"1.1.18.1"},
  {"user":"james","ip-address":"1.1.18.2", "domain" :
"cme.com"},
  {"user":"mary","machine":"","ip-address":"1.1.18.3"}
 ]
}
```

Response

```
{
 "responses":[
  {
   "ipv4-address":"1.1.18.1",
   "message":"Association sent to PDP."
  },
  {
   "ipv4-address":"1.1.18.2",
   "message":"Association sent to PDP."
  },
  {
   "ipv4-address":"1.1.18.3",
   "message":"Association sent to PDP."
  }
 ]
}
```

Example 2 - Adding multiple associations, one of which is incorrect

Request

```
{
 "shared-secret":"****",
 "requests":[
  {"user":"john","machine":"","ip-address":"1.1.18.1"},
  {"user":"linda","ip-address":"invalid", "domain" : "cme.com"},
  {"user":"james","machine":"","ip-address":"1.1.18.3"}
 ]
}
```

Response

```
{
 "responses": [
  {
   "ipv4-address": "1.1.18.1",
   "message": "Association sent to PDP."
  },
  {
   "pre": "GENERIC_ERR_INVALID_PARAMETER",
   "message": "No valid IP was provided"
  },
  {
   "ipv4-address": "1.1.18.3",
   "message": "Association sent to PDP."
  }
 ]
}
```

Example 3 - Request multiple identities

Request

```
{
 "shared-secret":"****",
 "requests":[
  {"ip-address":"1.1.18.1"},
  {"ip-address":"1.1.18.2"},
  {"ip-address":"1.1.18.3"}
 ]
}
```

Response

```
{
  "responses":[
   {
    "combined-roles":[],
    "ipv4-address":"1.1.18.1",
    "message":"total 1 user records were found.",
    "users":[
     {
      "groups":[
      "All Users"
      ],
      "identity-source": "AD Query",
      "roles":[],
      "user":"User 1"
     }
    ]
   },
   {
    "combined-roles":[],
    "domain":"cme.com",
    "ipv4-address": "1.1.18.2",
    "message":"total 1 user records were found.",
    "users":[
     {
      "groups":[
      "All Users"
      ],
      "identity-source": "AD Query",
      "roles":[],
      "user":"User 2"
     }
    ]
  },
  {
   "combined-roles": [],
   "ipv4-address": "1.1.18.3",
   "message": "total 1 user records were found.",
   "users":[
    {
     "groups": [],
     "identity-source": "AD Query",
     "roles": [],
     "user": "User 3"
    }
   ]
  }
 ]
}
```

Troubleshooting Web API

Issues with the Web API are usually because of:

- Incorrect configuration. For example, when you enter an incorrect URL or do not authorize the client to use the Web API.
- Incorrect command syntax, such as missing parameters or invalid parameter values.

For standard requests:

- HTTP response code of 200 means that the Identity Awareness service received a valid API command.
- HTTP response code 500 means that the command is invalid, or an internal error prevented the performance of the command by the API.

If the request fails, the JSON response body includes a `code` field, and the `message` field includes a textual description.

- The `message` field - Shows success of the procedure.
- The `code` field - Implies that the procedure failed.

For bulk requests, the HTTP status code is always 200. A granular error code is given for each of the requests.

Statuses and Responses

HTTP status	API response ("code" field)	Possible cause
N/A	N/A	No response is usually the result of a connectivity issue. Make sure the API client can get an access to the gateway and that the gateway does not drop the traffic.
404	N/A	This is the result of these causes: ■ Identity Awareness API is disabled. ■ Identity Awareness API is enabled, but the API client is not authorized. ■ Identity Awareness API is enabled, but the IDA API access settings do not permit access from the API client network. ■ Incorrect or missing shared secret. ■ Incorrect URL.

HTTP status	API response ("code" field)	Possible cause
500	`GENERIC_ERROR_INVALID_SYNTAX`	Syntax error in the JSON request body (for example: redundant comma after the last parameter).
500	`GENERIC_ERROR_INVALID_PARAMETER_NAME`	The request includes a field that is not permitted for this request.
500	`GENERIC_ERR_MISSING_REQUIRED_PARAMETERS`	Missing mandatory parameter.
500	`GENERIC_ERR_INVALID_PARAMETER`	Incorrect parameter value or parameter type (for example: invalid IP address).
500	`GENERIC_INTERNAL_ERROR`	Internal error on the gateway. Contact *Check Point Support*.

Configuring Remote Access

To configure Remote Access:

In the Identity Awareness Gateway object properties > **Identity Awareness** page, select **Remote Access** to enable it, or clear this option to disable it.

Important - If there is more than one Identity Awareness Gateway that share identities with each other and have Office Mode configured, each Identity Awareness Gateway must be configured with different IP ranges for Office Mode.

For the overview, see *"Remote Access" on page 25*.

Infinity Identity Integration

Infinity Identity acts as a unified identity repository across the Check Point ecosystem. In R82, a centralized configuration for Identity Providers lets you define one or more Identity Providers on the Infinity Portal and reuse the IdP configuration on multiple Security Gateways in SmartConsole that have the Identity Awareness Blade enabled.

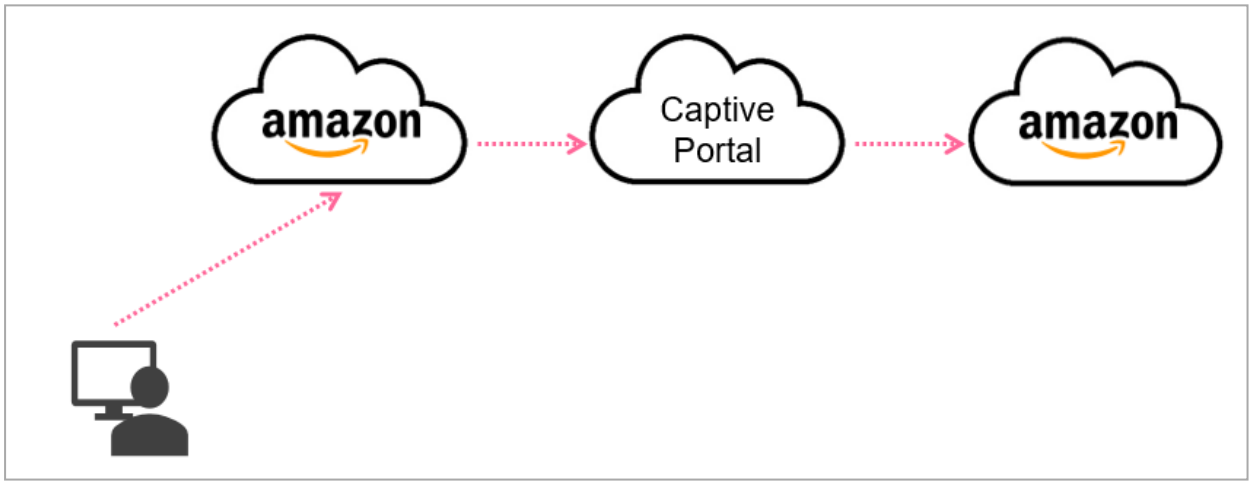
How It Works

This example uses Azure but applies to any IdP supported by the Infinity Portal.

1. A user defined in Azure attempts to access Amazon Web Services.

   Note - If you have more than one IdP configured, the user is redirected to the Captive Portal to select an IdP.

2. Upon successful authentication through the IdP, the user is granted access to Amazon based on your predefined rule.



Prerequisites

- Access to one of these supported cloud platforms.
- An app on your chosen platform with permissions to create groups and assign users.
- SmartConsole is connected to the Infinity Portal.

Supported IdPs

- Microsoft ADFS
- Microsoft Entra ID
- Okta
- RADIUS

- OneLogin
- Ping Identity
- Google Workspace
- Duo
- Generic SAML Server

Important - Only the EU and US regions are supported in Infinity Identity configurations.

How to Configure a Centralized Identity Provider

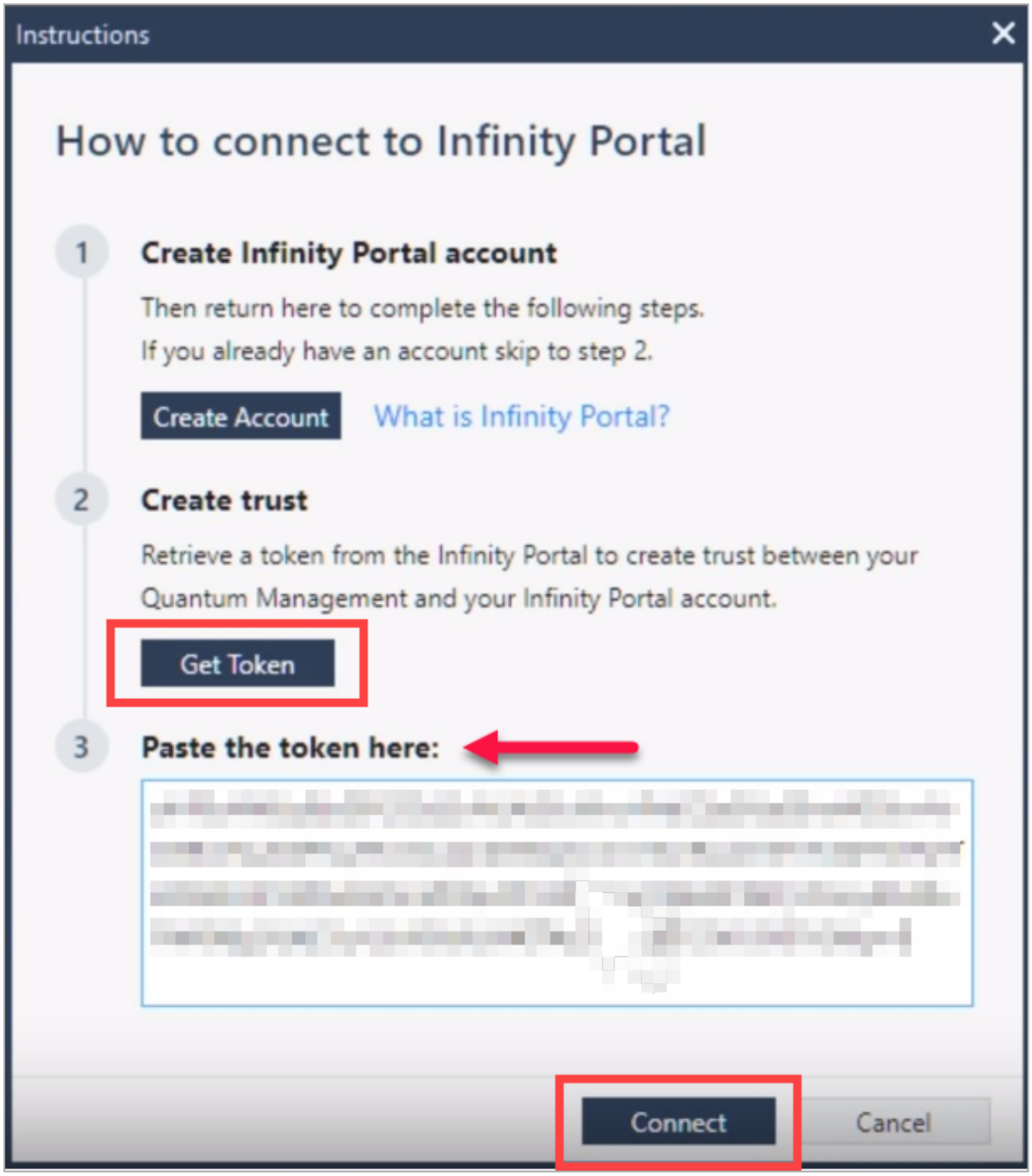
Before you begin, log in to SmartConsole, the Infinity Portal, and your IdP.

Step 1: Define an Identity Provider

Check Point supports multiple Identity Providers. Refer to SSO Authentication Setup with Identity Provider for detailed procedures.

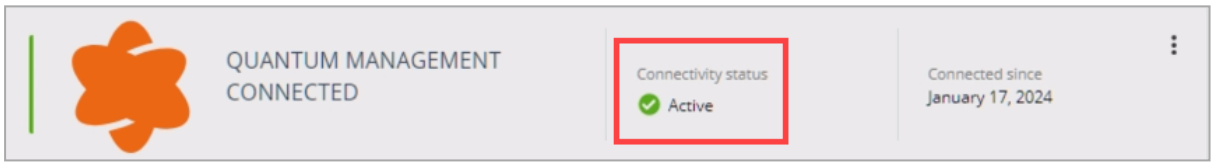
Step 2: Integrating with SmartConsole

1. Open SmartConsole and log in to your Security Management Server.
2. Select Infinity Services > click **Get Started**.
3. In the **Instructions** window **How to connect to the Infinity Portal**, click **Get Token.**
4. Navigate to the Infinity Portal to authenticate and select an account, agree to share your Security Management Server data with the Infinity Portal, and copy the token.
5. Return to SmartConsole, paste the token into the SmartConsole's instructions window and click **Connect**.



6. Wait for the Security Management Server to connect to the Infinity Portal.
7. On the Identity Provider app card, the following Infinity Identity app cards shows for R82 users:

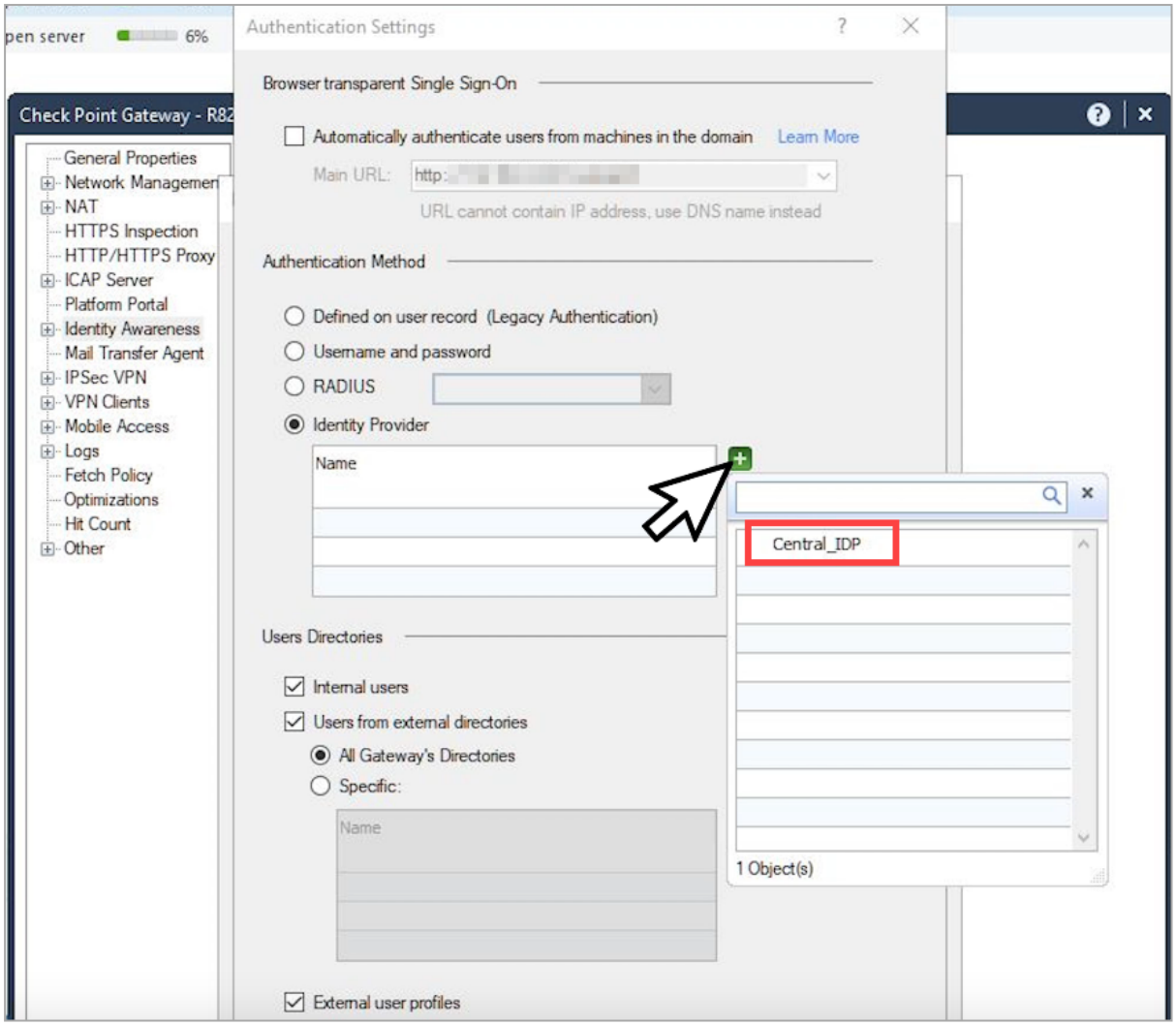
8. In the Infinity Portal, make sure your Security Management Server is connected. The **Connect status** shows **Active**, as in this example:



9. Follow the steps for adding an IdP, see SSO Authentication Setup with Identity Provider.
10. Test connectivity, confirm the Identity Provider, run the connectivity test, and close.
11. The Identity Provider defined on the Infinity Portal is now available as a *read-only* object in SmartConsole.

Step 3: Configure Identity Awareness in SmartConsole

1. In SmartConsole, open the gateway object (the one that you want to connect to the IdP) and enable the Identity Awareness Blade.
2. In the First Time Configuration Wizard, select **Browser-Based Authentication** > **Next.**
3. Select "**I do not wish to configure an Active Directory at this time**" and click **Next** > (again) **Next** > **Finish**.
4. In the navigation tree, select the Identity Awareness property and open the **Browser-Based Authentication** settings.
5. Below **Authentication Settings**, select **Edit**.
6. For the **Authentication Method**, select Identity Provider as the authentication method, and then select the IdP that you configured in the Infinity Portal. In this example, "Central IdP".



7. Click **OK**, and then **OK** again to save the settings.
8. In the **Security Policies** view, create a rule for testing purposes.
   a. **Name** - Give the rule a name, for example, "Central_IdP".
   b. **Source** - Add an **Access Role** that contains the user group assigned to your central IdP (such as Azure). The Access Role gets its *group*s and *users* in those groups from those defined on the IdP. To create an Access Role, see *"Creating Access Roles" on page 33*.
   c. **Destination** - For the **Destination**, select ***Any**.
   d. **Services & Applications** - Select the applicable applications and sites.
   e. **Action** - In the **Action Settings** window, the **Action** is **Accept**.
   Also, make sure to select the checkbox **Enable Identity Captive Portal**.
   f. Track - Track matches on the rule with the **Log**.
9. **Publish** the session changes and click **Install Policy** > **Install**.

Selecting Identity Sources

Identity sources have different security and environment considerations. Depending on your organization's requirements, you can choose to set them separately, or as combinations that supplement each other. For information about how Identity Awareness prioritizes information it receives from different identity sources, see *"Identity Conciliation - PDP" on page 142* and *"Identity Conciliation - PEP" on page 170*.

Here are examples of how to choose identity sources for different organizational requirements:

Requirement	Recommended Identity Source
Logging and auditing with basic enforcement	**AD Query**.
Logging and auditing only	**AD Query**.
Application Control	**AD Query** and **Browser-Based Authentication**. The AD Query finds all AD users and computers. The Browser-Based Authentication identity source is necessary to include all non-Windows users. In addition, it serves as a fallback option, if AD Query cannot identify a user. If you configure Transparent Kerberos Authentication, then the browser attempts to authenticate users transparently by getting identity information before the Captive Portal username/password page is shown to the user.
Data Center, or internal server protection	The options are: ■ **AD Query** and **Browser-Based Authentication** - When most users are desktop users (not remote users) and easy configuration is important. **Note** - You can add Identity Agents if you have mobile users and have users that are not identified by AD Query. Users that are not identified encounter redirects to the Captive Portal. ■ **Identity Agents** and **Browser-Based Authentication** - When a high level of security is necessary. The Captive Portal is used for distributing the Identity Agent. IP Spoofing protection can be set to prevent packets from being IP spoofed.

Requirement	Recommended Identity Source
Terminal Servers and Citrix environments	**Terminal Servers**. Tells you to install the Terminal Servers Identity Agent on each Terminal Server.
Users that get an access to the organization through VPN	**Remote Access**. Lets you identify Mobile Access and IPsec VPN clients that work in Office Mode.
Environment that use a RADIUS server for authentication	**RADIUS Accounting**. Make sure that you configure the Security Gateway as a RADIUS Accounting client and give it access permissions and a shared secret.

Identity Awareness Use Cases

This section describes how to work with Identity Awareness use cases.

Getting Identities for Active Directory Users

Organizations that use Microsoft Active Directory can use AD Query to acquire identities.

When you set the AD Query option to get identities, you are configuring clientless employee access for all Active Directory users. To enforce access options, create rules in the Firewall Rule that contain *Access Role* objects. An Access Role object defines users, computers and network locations as one object.

Active Directory users that log in and are authenticated, get a seamless access to the resources that are based on Firewall rules.

Scenario: Laptop Access

Description:

James Wilson is an HR partner in the ACME organization. ACME IT wants to limit access to HR servers to designated IP addresses to minimize malware infection and unauthorized access risks. Thus, the Security Gateway policy permits access only from James' desktop, which is assigned a static IP address 10.0.0.19.

He received a laptop and wants to get an access to the HR Web Server from anywhere in the organization. The IT department gave the laptop a static IP address, but that limits him to operating it only from his desk. The current Rule Base contains a rule that lets James Wilson get an access to the HR Web Server from his laptop with a static IP (10.0.0.19).

Name	Source	Destination	VPN	Service	Action	Track
Jwilson to HR Server	Jwilson	HR_Web_ Server	`Any Traffic`	`Any`	`accept`	`Log`

He wants to move around the organization and continue to have access to the HR Web Server.

To make this scenario work, the IT administrator does these steps:

1. Enables Identity Awareness on a Security Gateway, selects **AD Query** as one of the **Identity Sources** and installs the policy.

2. Checks the logs in the **Logs & Events** view of SmartConsole to make sure the system identifies James Wilson in the logs.
3. Adds an Access Role object to the Firewall Rule Base that lets James Wilson gets an access to the HR Web Server from any computer and from any location.
4. Sees how the system tracks the actions of the Access Role in the **Logs & Events** view of SmartConsole.

User Identification in the Logs:

The logs in the **Logs & Events** view of SmartConsole show that the system recognizes James Wilson as the user behind IP 10.0.0.19. This log entry shows that the system maps the source IP to the user James Wilson from CORP.ACME.COM. This uses the identity acquired from AD Query.

Note - AD Query maps the users in dependence of their AD activity. This can take some time and depends on user activity. If James Wilson is not identified (the IT administrator does not see the log), he should lock and unlock the computer.

Using Access Roles:

To let James Wilson get an access to the HR Web Server from **any** computer, change the rule in the Access Control Policy Rule Base. Create an Access Role for James Wilson (see *"Creating Access Roles" on page 33*), from **any** network and **any** computer. In the rule, change the source object to be the Access Role object (for example, **HR_Partner**).

Name	Source	Destination	VPN	Services & Applications	Action	Track
HR Partner Access	HR_ Partner	HR_Web_ Server	Any	Any	accept	None

Install the policy. You can remove the static IP address from the laptop of James Wilson and give it a dynamic IP address. The Security Gateway James Wilson configured in the HR_ Partner Access Role gets an access to the HR Web server from his laptop with a dynamic IP address.

Getting Identities with Browser-Based Authentication

Browser-Based Authentication lets you acquire identities from unidentified users such as:

- Managed users connecting to the network from unknown devices such as Linux computers or iPhones.
- Unmanaged, guest users such as partners or contractors.

If unidentified users try to connect to resources in the network that are restricted to identified users, they are automatically sent to the Captive Portal. If Transparent Kerberos Authentication is configured, the browser attempts to identify users that are logged into the domain through SSO before it shows the Captive Portal.

Scenarios

#1: Recognized User from Unmanaged Device

The CEO of ACME recently bought her own personal iPad. She wants to access the internal Finance Web server from her iPad. Because the iPad is not a member of the Active Directory domain, she cannot identify seamlessly with AD Query. But she can enter her AD credentials in the Captive Portal and then get the same access as on her office computer. Her access to resources depends on rules in the Firewall Rule Base.

Necessary SmartConsole Configuration

1. Enable **Identity Awareness** Software Blade on a Security Gateway.
2. Select **Browser-Based Authentication** as one of the **Identity Sources**, and click **Settings**.
3. In the **Portal Settings** window in the **User Access** section, make sure that **Name and password login** is selected.
4. Create a new rule in the Rule Base to let Linda Smith access network destinations. Select **accept** as the **Action**.
5. Right-click the **Action** column and select **More**.

   The **Action Settings** window opens.
6. Select **Enable Identity Captive Portal**.
7. Click **OK**.
8. From the **Source** of the rule, right-click to create an **Access Role**.
   a. Enter a **Name** for the Access Role.
   b. In the **Users** page, select **Specific users** and choose Linda Smith.
   c. In the **Machines** page, make sure that **Any machine** is selected.

d. Click **OK**.

The Access Role is added to the rule.

Name	Source	Destination	VPN	Service	Action	Track
CEO Access	Linda Smith	Finance_ Server	Any Traffic	http	Accept (Enable Identity Captive Portal)	Log

User Experience

For the CEO to access the Finance server from her personal device:

1. She browses to the Finance server from her personal device.

   The Captive Portal opens.

2. She enters her usual system credentials in the Captive Portal.

   A **Welcome to the network** window opens.

3. She can successfully browse to the Finance server.

User Identification in the Logs

The log entry in the **Logs** tab of the Logs & Events view shows how the system recognizes a user from a personal device. This uses the identity acquired from Captive Portal.

#2: Guest Users from Unmanaged Device

Guests frequently come to the ACME company. While they visit, the CEO wants to let them access the Internet on their own laptops.

Amy, the IT administrator configures the Captive Portal to let unregistered guests log in to the portal to get network access. She makes a rule in the Rule Base to let unauthenticated guests access the Internet only.

When guests browse to the Internet, the Captive Portal opens. Guests enter their name, company, email address, and phone number in the portal. They then agree to the terms and conditions written in a network access agreement. Afterward, they are given access to the Internet for a specified time.

Necessary SmartConsole Configuration

To make this scenario work, the IT administrator must:

1. Enable **Identity Awareness** Software Blade on a Security Gateway.
2. Select **Browser-Based Authentication** as one of the **Identity Sources**, and click **Settings**.
3. In the **Portal Settings** window in the **Users Access** section, make sure that **Unregistered guest login** is selected.
4. Click **Unregistered guest login - Settings**.
5. In the **Unregistered Guest Login Settings** window, configure:
   - The data guests must enter.
   - For how long users can access to the network resources.
   - If a user agreement is necessary and its text.
6. Create an **Access Role** rule in the Rule Base, to let identified users access the Internet from the organization:
   a. Right-click **Source** and select **Access Role**.
   b. In the **Users** tab, select **All identified users**.
7. Create an **Access Role** rule in the Rule Base, to let Unauthorized Guests access only the Internet:
   a. Right-click **Source** and select **Access Role**.
   b. In the **Users** tab, select **Specific users** > **Unauthenticated Guests**.
   c. Select **accept** as the **Action**.
   d. Right-click the **Action** column and select **Edit Properties**.

      The Action Properties window opens.
   e. Select **Enable Identity Captive Portal**.
   f. Click **OK**.

User Experience

For a guest at ACME to access the Internet:

1. She browses to an Internet site from her laptop.

   The Captive Portal opens because she is not identified and therefore cannot access the Internet.
2. She enters her identifying data in the Captive Portal and reads through and accepts a network access agreement.

A **Welcome to the network** window opens.

3. She can successfully browse the Internet for a specified time.

Getting Identities in Application Control

You can use the Identity Awareness and Application & URL Filtering together to add user awareness, computer awareness, and application awareness to the Check Point Security Gateway. They work together in these procedures:

- In the Access Control Policy Layer with the Application & URL Filtering Software Blade enabled, use Identity Awareness Access Roles rules as the source of the rule.
- You can use all the types of identity sources to acquire identities of users who try get an access to applications.
- Logs and events display user and IP address accesses, and their applications.

Scenario: Identifying Users in Application Control Logs

Description

The ACME organization uses Identity Awareness to monitor outbound application traffic and learn what their employees are doing. The IT administrator must enable Application Control and Identity Awareness. Logs and events display identity information for the traffic.

- To see the logs, open the **Logs & Events** > **Logs** tab.
- To see the events, open the **Access Control** > **Logs & Events** views.

Next, the IT department can add rules to block specific applications or track them differently in the Application & URL Filtering Layer of the policy to make it even more effective. See the *R82 Quantum Security Gateway Guide*.

Necessary SmartConsole Configuration

To make this scenario work, the IT administrator must:

1. Enable the Application Control blade on a Security Gateway.

   This adds a default rule to the Application Control Rule Base that allows traffic from known applications, with the tracking set to **Log**.

2. Enable Identity Awareness on a Security Gateway, selects **AD Query** as one of the **Identity Sources**.
3. Install the Access Control Policy.

User Identification in the Logs

You can see data for identified users in the Logs and Events that relate to application traffic.

- To see the logs, open the **Logs & Events** > **Logs** tab.
- To see the events, open the **Logs & Events** view > **Access Control** views > **Events**.

The log entry shows that the system maps the source IP address with the user identity. In addition, it shows Application Control data.

Configuring Identity Logging for a Log Server

When you enable Identity Awareness on a Log Server, you add user and computer identification to Check Point logs. Administrators can then analyze network traffic and security-related events better.

The Log Server communicates with Active Directory servers. The Log Server stores the data extracted from the AD in an association map. When Security Gateway generate a Check Point log entry and send it to the Log Server, the server gets the user and computer name from the association map entry that corresponds to the source IP address of the event log. It then adds this identity aware information to the log.

Enabling Identity Awareness on the Log Server for Identity Logging

Preliminary Actions

Before you enable Identity Awareness on the Log Server for Identity Logging:

- Make sure there is network connectivity between the Log Server and the domain controller of your Active Directory environment.
- Get the Active Directory administrator credentials.

To enable Identity Awareness on the Log Server for Identity Logging, you must:

1. Configure an Active Directory Domain.
2. Install the database.

Procedure:

1. Log in to SmartConsole.
2. From the Navigation Toolbar, click **Gateways & Servers**.
3. Open the Log Server object.
4. In the **General Properties** page, in the **Management** section, select **Logging & Status** and **Identity Logging**.

   The **Identity Awareness Configuration** wizard opens.
5. On the **Acquire Identities For Logs** window, click **OK**.

Configuring an Active Directory Domain

On the **Integration With Active Directory** page, select or configure an Active Directory Domain.

1. From the **Select an Active Directory** list, select the Active Directory to configure from the list that shows configured LDAP Account Units or create a new domain. If you have not set up Active Directory, it is necessary to enter a **domain name**, **username, password** and **domain controller** credentials.

   When the SmartConsole client computer is part of the AD domain, SmartConsole suggests this domain automatically. If you select this domain, the system creates an LDAP Account Unit with **all** of the domain controllers in the organization's Active Directory.

2. Enter the Active Directory credentials and click **Connect** to verify the credentials.

   Important - For AD Query you must enter domain administrator credentials. For Browser-Based Authentication standard credentials are sufficient.

3. If you selected Browser-Based Authentication or Terminal Servers, or do not configure Active Directory, select **I do not wish to configure Active Directory at this time**.

4. Click **Next**.

   Best Practice -We highly recommend that you go to the LDAP Account Unit and make sure that only necessary domain controllers are in the list. If AD Query is not necessary to work with some of the domain controllers, erase them from the LDAP Servers list.
   With the Identity Awareness configuration wizard, you can use existing LDAP Account units or create a new one for one AD domain.
   If the SmartConsole computer is part of the domain, the Wizard fetches all the domain controllers of the domain and all of the domain controllers are configured.
   If you create a new domain, and the SmartConsole computer is not part of the domain, the LDAP Account Unit that the system creates contains only the domain controller you set manually. If it is necessary for AD Query to fetch data from other domain controllers, you must **add** them manually to the LDAP Servers list after you complete the wizard.
   To see/edit the LDAP Account Unit object, open **Object Explorer** (CTRL + E), and select **Users/Identities** > **LDAP Account units**.
   The LDAP Account Unit name syntax is: `<domain name>__AD`
   For example, `CORP.ACME.COM__AD`.

5. Click **Next**.

6. The **Identity Awareness is Now Active** page opens with a summary of the acquisition methods.
7. Click **Finish**.
8. **Optional:** In the Log Server object, go to the **Identity Awareness** page and configure the applicable settings.
9. Click **OK**.

Installing the Database

1. In SmartConsole, go to **Menu** and click **Install database**.

   The **Install Database** window opens.
2. Select all Check Point objects on which to install the database.
3. In the **Install database** window, click **Install**.
4. In the **SmartConsole** window, click **Publish & Install**.
5. Wait for the message **Install Database on XXX Succeeded** at the end of the operation.

WMI Performance

Bandwidth between the Log Server and Active Directory Domain Controllers

The quantity of data transferred between the Log Server and domain controllers depends on the quantity of events generated. The generated events include event logs and authentication events. The quantities change based on the applications that run in the network. Programs that have many authentication requests have a larger quantity of logs. The observed bandwidth range varies between 0.1 to 0.25 Mbps for each 1000 users.

CPU Impact

When using AD Query, the impact on the domain controller CPU is less than 3%.

Identity Awareness Environment

This section describes how to configure and work with various instances of Identity Awareness.

Identity Sharing

Best Practice - In a distributed environment with multiple Identity Awareness Security Gateways and AD Query, an Identity Sharing configuration improves performance and flexibility.
In this configuration, Identity Awareness Security Gateways share identity information with other Identity Awareness Security Gateways. You can configure Identity Sharing across multiple Security Gateways if the Security Gateways have Identity Awareness Software Blade enabled.
Without Identity Sharing:

- Identity Agents connect to only one Identity Awareness Security Gateway.
- When traffic goes through more than one Identity Awareness Security Gateway, you can require users to authenticate on each Identity Awareness Security Gateway (for example, in Captive Portal).
- Each Identity Awareness Security Gateway is connected to an identity source (for example, AD Query). Each Identity Awareness Security Gateway makes a query to the Active Directory. Each Identity Awareness Security Gateway queries for the group membership and calculates the Access Role object. This increases the load on the Security Gateways.

Introduction to Identity Sharing

An Identity Awareness Security Gateway configured as a Policy Decision Point gets identity information and shares it with other Identity Awareness Security Gateways configured as Policy Enforcement Points. This way, only one Identity Awareness Security Gateway performs the group membership query and calculates the Access Role object. This reduces the load on the identity sources, on User Directory, or on the two of them.

PDP - Policy Decision Point:

- Gets user/computer identities from the designated identity sources.
- Shares user/computer identities with other Identity Awareness Security Gateways.

PEP - Policy Enforcement Point:

- Provides the applicable Access Roles to the Rule Base process. It enforces the procedure as defined in the policy.

- Receives identities through Identity Sharing.
- Can redirect users to the Identity Awareness Captive Portal.

Supported Configurations for Identity Sharing:

- One PDP shares identities to multiple PEPs.
- One PEP receives identities from multiple PDPs.
- PDP and PEP processes run on different Security Gateways and use Smart-Pull Identity Sharing for the connection.
- PDP and PEP processes run on the same Security Gateway and use Push Identity Sharing for the connection.

When an Identity Server needs to connect to an Identity Awareness Gateway for Identity Sharing, the Identity Server uses the IP Address of the Identity Awareness Gateway object.

If a network configuration does not allow communication with this IP Address of the Identity Awareness Gateway, you can configure a different IPv4 Address for the communication channel between the Identity Server and the Identity Awareness Gateway. For more information, see sk60701.

Identity Sharing Configuration Procedure

1. Open SmartConsole for the Management Server / Multi-Domain Server that manages the Identity Awareness Security Gateways.
2. Configure Identity Awareness Security Gateways that share identities (Policy Decision Points):
    a. From the left navigation panel, click **Gateways & Servers**.
    b. Open the applicable Security Gateway object.
    c. From the left tree, click **Identity Awareness** > **Identity Sharing**.
    d. Click **Share local identities with other gateways**.
    e. Click **OK**.
3. Configure Identity Awareness Security Gateways that receive identities (Policy Enforcement Points):
    a. Open the applicable Security Gateway object.
    b. From the left tree, click **Identity Awareness** > **Identity Sharing**.
    c. Click **Get identities from other gateways**.

d. Below **Get identities from other gateways**, to the right of the table, click the plus button.

   A list of PDP Security Gateways appears.

e. Select the applicable PDP Security Gateway from the list.

   Note - The list contains only Security Gateways that have **Share local identities with other gateways** enabled.

f. Click **OK**.

4. Install the Access Control policy on all these Security Gateways.

Smart-Pull Identity Sharing

In large environments, not all PEPs must have the identities from all PDPs. For example, it is not necessary for small branch offices with a small number of users to keep all of the identities from the PDP in the headquarters office.

When Smart Pull is configured, identities are sent to the PEP only when the PEP requests or pulls them from the PDP. This saves space on the PEP and avoids transactions between the PDP and the PEP that are not necessary.

The Smart-Pull Identity Sharing operation stages are:

1. **Identity Acquisition**

   - The PDP gets identities and keeps them in the PDP repository.
   - The PDP notifies the applicable PEPs about the network (Class C), where the user was identified.

   Notes:
   - The PDP does not publish the identities to the PEPs until the Identity Propagation stage.
   - The `pep show network pdp` command on the PEP shows the PDPs and the networks they identify.
   - The `pdp network info` command on the PDP shows all the networks it publishes.

2. **Sub-Network Registration**

   A user initiates a connection through the PEP. If the policy must have an identity element, the PEP searches for the identity in its local database.

- If the PEP finds the identity in its local database, then:
  a. The PEP registers to the PDP for notification about a smaller network (subnet mask 255.255.255.240).
  b. The PDP publishes all the currently known identities from the networks with the subnet mask 255.255.255.240 to the PEPs that register.
- If the PEP does **not** find the identity in its local database, the PEP searches for a PDP that knows the applicable Class C network to find the identity.

Notes:
- The `pep show network registration` command on the PEP shows the networks with the subnet mask 255.255.255.240, to which the PEP is registered.
- The `pdp network registered` command on the PDP shows the list of the PEPs for the networks with the subnet mask 255.255.255.240.

3. **Identity Propagation**
   a. The PDP gets the identity of a user, who has an IP address from an already registered network with the subnet mask 255.255.255.240.
   b. The PDP immediately publishes the identity to the registered PEPs.

Push Identity Sharing

In Push Identity Sharing, when a PDP gets an identity, the PDP publishes the identity to the PEP.

Note - This is the only supported sharing method for an Identity Awareness Security Gateway that performs PDP and PEP roles.

Monitoring Identity Sharing

When Identity Sharing operates as expected, these are the open connections between the PDP and the PEP:

- Identity connection - shares identity information from the PDP to the PEP. The PDP opens this connection to the PEP on port `15105`. The *pepd* process listens for incoming identity connections on this port.
- Network connection - shares network information from the PEP to the PDP. The PEP opens this connection to the PDP on port `28581`. The *pdpd* process listens for incoming network connections on this port.

If the PEP is configured in Push mode, it receives Identity connections but does not send Network connections.

If the PDP or PEP is a cluster, all members open the outgoing connection but only the active cluster member gets incoming connections. The cluster uses its Virtual IP Address (VIP) for connections.

Important - Check Point Security Gateways have implied rules to allow these connections. If a third-party gateway drops the traffic, Identity Sharing does not work.

For more information, see *"Configuration Scenarios" on page 204*.

Example

In this example, the IP address of the PDP is `10.10.10.10` and the IP address of the PEP is `11.11.11.11`.

To monitor connections on the PDP, on the PDP Gateway or active Cluster Member, run:

```
pdp connections pep
```

For more information, see *"pdp connections" on page 295*.

To monitor connections on the PEP, on the PEP Gateway or active Cluster Member, run:

```
pep show pdp all
```

For more information, see *"pep show" on page 332*.

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Example output of the "`pdp connections pep`" command:

```
[Expert@MyGW1:0]# pdp connections pep
------------------------------------------------------------------
-------------------------------------
| Direction | IP            | Port  | Name  | Type           |
Status    | Location | IPv6 Supported |
------------------------------------------------------------------
-------------------------------------
| Incoming  | 172.23.57.237 | 28581 | MyGW2 | Single Gateway |
Connected | Remote   | No             |
------------------------------------------------------------------
-------------------------------------
| Outgoing  | 127.0.0.1     | 15105 | MyGW3 | Single Gateway |
Connected | Locally  | No             |
------------------------------------------------------------------
-------------------------------------
| Outgoing  | 172.23.57.237 | 15105 | MyGW2 | Single Gateway |
Connected | Remote   | No             |
------------------------------------------------------------------
-------------------------------------
[Expert@MyGW1:0]#
```

Example output of the "`pep show pdp all`" command:

```
[Expert@MyGW1:0]# pep show pdp all
Command: root->show->pdp->all
------------------------------------------------------------------
-----------
| Direction | IP            | ID | Status    | Users | Connect
time       |
------------------------------------------------------------------
-----------
| Incoming  | 127.0.0.1     | 0  | Connected | 0     | 13Oct2022
20:04:46 |
------------------------------------------------------------------
-----------
| Incoming  | 172.23.57.220 | 0  | Connected | 0     | 13Oct2022
 9:44:11 |
------------------------------------------------------------------
-----------
| Outgoing  | 172.23.57.220 | 0  | Connected | N/A   | 13Oct2022
 9:44:09 |
------------------------------------------------------------------
-----------
[Expert@MyGW1:0]#
```

Identity Broker

Identity Broker is an identity sharing method between Policy Decision Points (PDP Gateways). The Policy Decision Points can share identities across different management domains in a distributed environment with multiple Identity Awareness Security Gateways.

In a distributed environment with multiple Identity Awareness Security Gateways, you can use Identity Broker to propagate any received identity from one PDP Gateway to another. This helps to create a more scalable and robust sharing of hierarchy and topologies.

Identity Broker is a Web-API based functional part of the PDP instance. Identity Broker adds a new communication channel between PDPs.

The Identity Broker Solution

Identity Broker propagates identities between PDP Gateways. A PDP Gateway learns the Identities from the Identity Sources. This PDP Gateway performs the group membership query, calculates Access Roles, and then shares the identities to other PDP Gateways. This reduces the load on the PDP Gateways receiving the identities, identity sources, and/or User Directories.

The sharing can be performed between PDP Gateways managed by different Security Management Servers / Domain Management Servers.

Identity sharing between the Identity Brokers can be controlled through filters. You can:

- Filter identities by network , user/machine name, domain, identity source, access roles, and distinguished name.
- Share only local Identity sessions. When enabled, the PDP forwards only its own sessions, and not the sessions it learned from other PDPs.

The Identity Broker solution shares all the received identities by default. By applying filters, you can avoid sharing identities that are not required for other PDPs.

Terms and Descriptions

Publisher

A Security Gateway defined to share identities with one or more Subscribers.

Subscriber

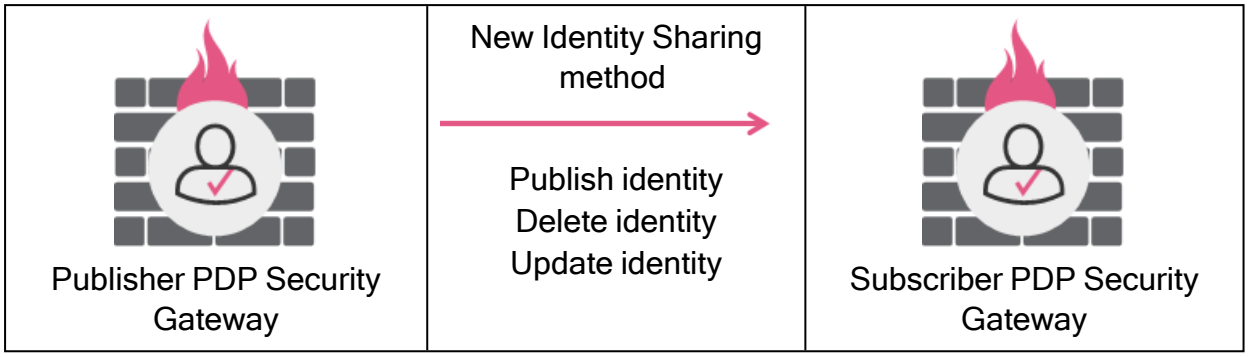
A Security Gateway defined to receive identities from one or more Publishers.

Identity Broker Communication

Identity Broker uses WEB-API to communicate. Security Gateways share information in JSON format over HTTP post requests.

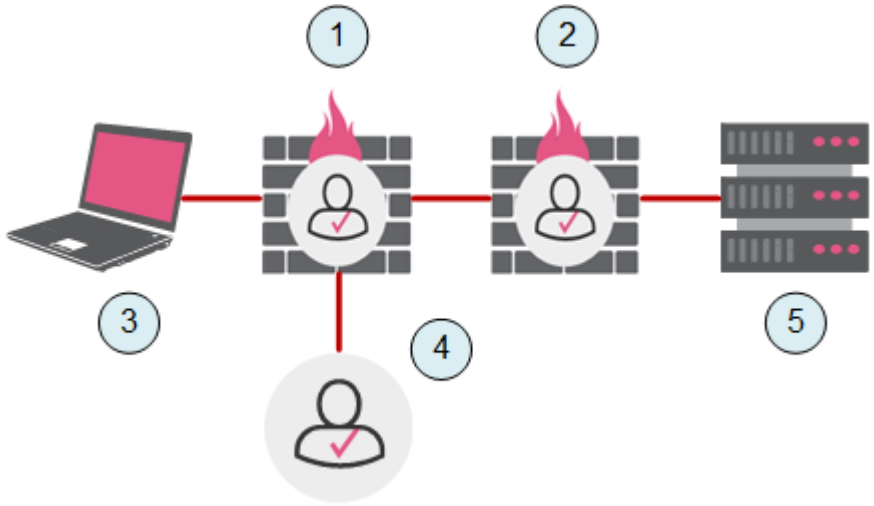
Each Identity Broker node verifies the other:

- The Publisher identifies the Subscriber by verifying the presented SSL Certificate.
- The Subscriber identifies the Publisher by verifying a pre-shared secret key.



Example Scenario

Logical topology:



Item	Description
1	Security Gateway #1
2	Security Gateway #2
3	A user on a computer (3) behind the Security Gateway #1
4	Identity Source (for example, Active Directory)
5	A resource (for example, a server) behind the Security Gateway #2

General Flow of Events:

1. The Security Gateway #1 is configured as an Identity Broker Publisher.

   It gets and learns the identity from the Identity Source (4), and shares it with the remote Security Gateway #2.

2. The Security Gateway #2 is configured as an Identity Broker Subscriber.

   It gets the identities of the users from remote the Security Gateway #1.

3. When the user connects to the resource (5), the Security Gateway #2 identifies the user and enforces identity-based rules.

4. **Optional:** You can apply filters to control which identities the Security Gateway #1 publishes and to which identities the Security Gateway #2 subscribes.

5. **Optional:** You can manage the Security Gateway #1 and Security Gateway #2 with different Management Servers.

Important - In addition to the topology configuration in the presented scenario, you can configure Security Gateway 2 as a Publisher and Security Gateway 1 as a Subscriber. That way, the two Security Gateways simultaneously give and receive identities to each other. Each Broker Publisher to Broker Subscriber relation is independent, and does not change any other Publisher-Subscriber relationship.

Configuration File "identity_broker.C"

You configure the Identity Broker in the file called `$FWDIR/conf/identity_broker.C` that is located on the Security Gateway / each Cluster Member.

Important:

- If this file does not exist, then create it manually in the Expert mode:

  ```
  ls -l $FWDIR/conf/identity_broker.C
  ```

  ```
  touch $FWDIR/conf/identity_broker.C
  ```

- **Each parameter you configure in this file must have a value inside the parentheses ":<parameter> (<value>)"**
  If an optional parameter does not have a value, you must delete it from the file.
- Before you edit this file, create a backup copy:

  ```
  cp -v $FWDIR/conf/identity_broker.C{,_BKP}
  ```

- If you edit this file on Windows OS, then after you transfer it back to the Security Gateway / Cluster Member, you must convert this file from the DOS format to the UNIX format:

  ```
  dos2unix $FWDIR/conf/identity_broker.C
  ```

Templates for the "$FWDIR/conf/identity_broker.C" file

These are the example templates for the *$FWDIR/conf/identity_broker.C* file:

- Security Gateway that works as a PDP Publisher
- Security Gateway that works as a PDP Subscriber
- Security Gateway that works as a PDP Publisher and as a PDP Subscriber

Example template with mandatory parameters for a Security Gateway that works as a PDP Publisher

This template contains the mandatory parameters to configure the Identity Broker on a PDP Publisher that works with two PDP Subscribers.

See:

- *"Configuring an Identity Broker" on page 122*.
- *"Example of a Configured Identity Broker" on page 137*.

```
#################################################################
#  Configuration file for Identity Broker - Identity Distribution
between PDPs.
#  For more information , please refer to Identity Awareness Admin
Guide.
#################################################################
(
  :sharing_id (ENTER_UNIQUE_SHARING_ID_FOR_THIS_PUBLISHER_GATEWAY)
  :identity_subscribers (
    : (
      :Name (DESCRIPTIVE_NAME_OF_SUBSCRIBER_GATEWAY_1)
      :sharing_id (UNIQUE_SHARING_ID_OF_SUBSCRIBER_GATEWAY_1)
      :ipaddr (IP_ADDRESS_OF_INTERFACE_ON_SUBSCRIBER_GATEWAY_1)
      :certificate_subject ("CERTIFICATE_SUBJECT_OF_SUBSCRIBER_
GATEWAY_1")
    )
    : (
      :Name (DESCRIPTIVE_NAME_OF_SUBSCRIBER_GATEWAY_2)
      :sharing_id (UNIQUE_SHARING_ID_OF_SUBSCRIBER_GATEWAY_2)
      :ipaddr (IP_ADDRESS_OF_INTERFACE_ON_SUBSCRIBER_GATEWAY_2)
      :certificate_subject ("CERTIFICATE_SUBJECT_OF_SUBSCRIBER_
GATEWAY_2")
    )
  )
)
```

Example template with mandatory parameters for a Security Gateway that works as a PDP Subscriber

This template contains the mandatory parameters to configure the Identity Broker on a PDP Subscriber that works with two PDP Publishers.

See:

- *"Configuring an Identity Broker" on page 122*.
- *"Example of a Configured Identity Broker" on page 137*.

```
#################################################################
#  Configuration file for Identity Broker - Identity Distribution
between PDPs.
#  For more information , please refer to Identity Awareness Admin
Guide.
#################################################################
(
  :sharing_id (ENTER_UNIQUE_SHARING_ID_FOR_THIS_SUBSCRIBER_GATEWAY)
  :identity_publishers (
    : (
      :Name (DESCRIPTIVE_NAME_OF_PUBLISHER_GATEWAY_1)
      :sharing_id (UNIQUE_SHARING_ID_OF_PUBLISHER_GATEWAY_1)
      :ipaddr (IP_ADDRESS_OF_INTERFACE_ON_PUBLISHER_GATEWAY_1)
    )
    : (
      :Name (DESCRIPTIVE_NAME_OF_PUBLISHER_GATEWAY_2)
      :sharing_id (UNIQUE_SHARING_ID_OF_PUBLISHER_GATEWAY_2)
      :ipaddr (IP_ADDRESS_OF_INTERFACE_ON_PUBLISHER_GATEWAY_2)
    )
  )
)
```

Example template with all supported parameters for a Security Gateway that works as a PDP Publisher and as a PDP Subscriber

This template contains all supported parameters to configure the Identity Broker.

Important:

- Each parameter you configure in this file must have a value inside the parentheses ":<parameter> (<value>)"
- If an optional parameter does not have a value, you must delete it from the file.

See:

- *"Configuring an Identity Broker" on page 122*.
- *"Example of a Configured Identity Broker" on page 137*.

```
##########################################################################
##################
#    Configuration file for Identity Broker - Identity Distribution
between PDPs.    #
#    For more information, see  the Identity Awareness
Administration Guide.         #
##########################################################################
##################
(
  :sharing_id ()
  :identity_subscribers (
    : (
      :Name ()
      :sharing_id ()
      :ipaddr ()
      :certificate_subject ("")
      :crl_validation_config (fail_closed)
      :share_only_local_sessions (false)
      :filter (
        :include_users_and_machines ()
        :exclude_users_and_machines ()
        :include_networks ()
        :exclude_networks ()
        :include_identity_source ()
        :exclude_identity_source ()
        :include_domains ()
        :exclude_domains ()
        :include_roles ()
        :exclude_roles ()
        :include_distinguished_names ()
        :exclude_distinguished_names ()
        :include_owners ()
        :exclude_owners ()
        :include_immediate_publishers ()
        :exclude_immediate_publishers ()
      )
    )
  )
  :identity_publishers (
    : (
      :Name ()
      :sharing_id ()
      :ipaddr ()
      :recalculate_access_roles (false)
      :filter (
```

```
        :include_users_and_machines ()
        :exclude_users_and_machines ()
        :include_networks ()
        :exclude_networks ()
        :include_identity_source ()
        :exclude_identity_source ()
        :include_domains ()
        :exclude_domains ()
        :include_roles ()
        :exclude_roles ()
        :include_distinguished_names ()
        :exclude_distinguished_names ()
        :include_owners ()
        :exclude_owners ()
        :include_immediate_publishers ()
        :exclude_immediate_publishers ()
      )
    )
  )
  :global_outgoing_filter (
    :include_users_and_machines ()
    :exclude_users_and_machines ()
    :include_networks ()
    :exclude_networks ()
    :include_identity_source ()
    :exclude_identity_source ()
    :include_domains ()
    :exclude_domains ()
    :include_roles ()
    :exclude_roles ()
    :include_distinguished_names ()
    :exclude_distinguished_names ()
    :include_owners ()
    :exclude_owners ()
    :include_immediate_publishers ()
    :exclude_immediate_publishers ()
  )
  :global_incoming_filter (
    :include_users_and_machines ()
    :exclude_users_and_machines ()
    :include_networks ()
    :exclude_networks ()
    :include_identity_source ()
    :exclude_identity_source ()
    :include_domains ()
    :exclude_domains ()
    :include_roles ()
    :exclude_roles ()
    :include_distinguished_names ()
```

```
      :exclude_distinguished_names ()
      :include_owners ()
      :exclude_owners ()
      :include_immediate_publishers ()
      :exclude_immediate_publishers ()
    )
  )
```

The sections in the $FWDIR/conf/identity_broker.C file

See *"Example of a Configured Identity Broker" on page 137*.

#	Section	Type	Description
1	Sharing ID `:sharing_id()`	■ Mandatory on a Publisher ■ Mandatory on a Subscriber	Identifies this Security Gateway when it communicates with other Security Gateways. The Sharing ID is an alphanumeric unique identifier for a Security Gateway. You configure the Sharing ID for a PDP Publisher or a PDP Subscriber. See *"Part 2 of 2 - PDP Publisher Configuration in Command Line" on page 123* and *"Part 2 of 2 - PDP Subscriber Configuration in Command Line" on page 126*. **Note** - The sharing_id must be identical to all cluster members and set the IP address to one of the cluster's VIPs. From the subscriber's perspective, the Cluster Publisher is seen as a single publisher in common cluster topologies.

#	Section	Type	Description
2	Identity Subscribers `:identity_ subscribers ()`	Mandatory on a Publisher	Configures Identity Subscribers on a Security Gateway that works as a PDP Publisher. These parameters in the Identity Subscribers section are mandatory: ■ `:Name ()` ■ `:sharing_id ()` ■ `:ipaddr ()` ■ `:certificate_subject ("")` These parameters in the Identity Subscribers section are optional: ■ `:crl_validation_ config ()` ■ `:share_only_local_ sessions ()` ■ `:filter ()` - this subsection can contains many local filters
3	Identity Publishers `:identity_ publishers ()`	Mandatory on a Subscriber	Configures Identity Publishers on a Security Gateway that works as a PDP Subscriber. These parameters in the Identity Publishers section are mandatory: ■ `:Name ()` ■ `:sharing_id ()` ■ `:ipaddr ()` These parameters in the Identity Publishers section are optional: ■ `:recalculate_access_ roles ()` ■ `:filter ()` - this subsection can contains many local filters

#	Section	Type	Description
4	Global Outgoing Filters `:global_ outgoing_filter ()`	Optional on a Publisher	Configures global outgoing filters on a Security Gateway that works as a PDP Publisher. These filters apply to all identity sessions this Publisher sends to all Subscribers that are configured on this Publisher.
5	Global Incoming Filters `:global_ incoming_filter ()`	Optional on a Subscriber	Configures global incoming filters on a Security Gateway that works as a PDP Subscriber. These filters apply to all identity sessions this Subscriber receives from all Publishers that are configured on this Subscriber.

Configuring an Identity Broker

Configuring a PDP Publisher

A Publisher Security Gateway shares identities with other Security Gateways that are considered Identity Subscribers.

For a Publisher Security Gateway to share identities, you must configure the Identity Subscribers in the `$FWDIR/conf/identity_broker.C` file on the Publisher Security Gateway.

Part 1 of 2 - PDP Publisher Configuration in SmartConsole

1. From the left navigation panel, click **Gateways & Servers**.
2. Double-click the Security Gateway / Cluster object.
3. Enable the **Identity Awareness** Software Blade and complete the **Identity Awareness Configuration** wizard.
4. From the left tree, click **Identity Awareness**.
5. Select the applicable **Identity Sources** - the Identity Providers from which to get the identities.

   Near each **Identity Source** you selected, click **Settings** and configure the applicable settings.

6. **Optional:** Configure this Security Gateway / Cluster as a Subscriber of a different Identity Awareness Security Gateway / Cluster.
7. Click **OK**.
8. Install the Access Control Policy on this Security Gateway / Cluster object.

Part 2 of 2 - PDP Publisher Configuration in Command Line

Best Practice - Prepare these files in advance on your computer:

- The `$FWDIR/conf/identity_broker.C` file for the Publisher.
- The `$FWDIR/conf/identity_broker.C` file for each Subscriber of this Publisher.

1. Connect to the command line on this Security Gateway / each Cluster Member.
2. Log in to the Expert mode.
3. Back up the current file:

   ```
   cp -v $FWDIR/conf/identity_broker.C{,_BKP}
   ```

4. Edit the current file:

   ```
   vi $FWDIR/conf/identity_broker.C
   ```

   See *"Example of a Configured Identity Broker" on page 137*.

5. In the section "`:sharing_id()`", enter an alphanumeric unique identifier for this PDP Publisher.

   Enter at minimum 16 characters. You can use a UUID generator.

   You use this identifier in the `$FWDIR/conf/identity_broker.C` file on Subscribers in the section "`:identity_publishers ()`".

   For example:

   ```
   :sharing_id (b2L4Sri5K9HxJw63GjAb)
   ```

6. In the section "`:identity_subscribers ()`", enter the applicable data for **each** Subscriber Security Gateway / Cluster.

Parameter	Description
`Name`	Specifies a descriptive name for this Subscriber Security Gateway / Cluster. **Best Practice** - Use the object name of this Subscriber Security Gateway / Cluster as configured in SmartConsole.
`sharing_id`	Specifies the unique identifier of the Subscriber Security Gateway / Cluster. Get this value from the `$FWDIR/conf/identity_broker.C` file on the Subscriber - from the top section "`:sharing_id ()`". **Note** - The sharing_id must be identical to all cluster members and set the IP address to one of the cluster's VIPs. From the subscriber's perspective, the Cluster Publisher is seen as a single publisher in common cluster topologies.
`ipaddr`	Specifies the IPv4 address of the applicable interface on the Subscriber Security Gateway / Cluster, to which this Publisher connects. **Important** - If this IP address changes in the Subscriber Security Gateway / Cluster object, you must update it in the `$FWDIR/conf/identity_broker.C` file. **Note** - For IPv6, use "`ipaddr6`".

`certificate_subject`	**Note** - You can perform this procedure only after you enable "**Get Identities from Identity Broker**" in the Subscriber Security Gateway object in SmartConsole.
	a. Fetch the Server Certificate from the Subscriber.
	On the Publisher Security Gateway / each Cluster Member, run:
	`$FWDIR/bin/BrokerCertFetcher <IP Address of Subscriber>`
	b. Make sure the CA Fingerprint and the "Subject" for the Subscriber Security Gateway are correct.
	c. Configure the "Subject" for the Subscriber Security Gateway in the "`certificate_subject`" field.
	d. Make sure this file exists:
	`stat $FWDIR/nac/broker_ca_certs/<IP_Address_of_Subscriber>.pem`

Parameter	Description
`crl_validation_config`	**Optional:** Specifies the mode for CRL (Certificate Revocation List) validation. The options are: ■ `fail_closed` - Start to download the CRL list. If the download fails, deny the connection (default). ■ `fail_open` - Start to download the CRL list. If the download fails, allow the connection. ■ `skip_crl_check` - Do not use CRL to validate the Certificate.
`share_only_local_sessions`	**Optional:** Specifies to publish only local sessions to this Subscriber. Identities of local sessions are those identities that are directly learned from the locally connected identity sources. The options are: ■ `true` ■ `false` (default)
`filter`	**Optional:** Specifies an outgoing filter for this specific Subscriber. Follow the instructions in *"Configuring Identity Filters" on page 134*.

Configuring a PDP Subscriber

A Subscriber Security Gateway gets its identities from other Security Gateways. These are considered Identity Publishers.

For a Subscriber Security Gateway to get identities, you must configure the Identity Publishers in the `$FWDIR/conf/identity_broker.C` file on the Subscriber Security Gateway.

Part 1 of 2 - PDP Subscriber Configuration in SmartConsole

1. From the left navigation panel, click **Gateways & Servers**.
2. Double-click the Security Gateway / Cluster object.
3. Enable the **Identity Awareness** Software Blade and complete the **Identity Awareness Configuration** wizard.
4. From the left tree, click **Identity Awareness** > **Identity Sharing**.
5. In the right pane:

a. Enable **Get Identities from Identity Broker**.

b. Click **Settings**.

The **Portal Access Settings** window opens.

6. Import a dedicated internal CA certificate for the Subscriber to present to the Publishers as an HTTPS Server certificate:

a. Connect to the command line on the Management Server.

b. Log in to the Expert mode.

c. Run this command for the Security Gateway / Cluster object you configure:

```
cpca_client create_cert -n "CN=<Name of Security
Gateway / Cluster Object>.broker.portal" -f <Name of
Security Gateway / Cluster Object>_broker.p12 -k IKE -w
"<Password>"
```

d. Transfer this P12 file from the Management Server to the SmartConsole Client computer.

e. In the **Certificate** section, click **Import**.

f. Select the P12 file and click **Open**.

7. Configure the **Accessibility** settings.

By default, the Publisher Security Gateway tries to connect to the internal interface of the Subscriber Security Gateway.

If one of the Publisher Security Gateways connects to the Subscriber Security Gateway through a different interface:

a. In the **Accessibility** section, click **Edit**.

b. Select the applicable option.

c. Click **OK** to close the **Portal Access Settings** window.

8. Click **OK**.

9. Install the Access Control Policy on the Security Gateway / Cluster object.

Part 2 of 2 - PDP Subscriber Configuration in Command Line

Best Practice - Prepare these files in advance on your computer:

- The `$FWDIR/conf/identity_broker.C` file for the Subscriber.
- The `$FWDIR/conf/identity_broker.C` file for each Publisher for this Subscriber.

1. Connect to the command line on the Subscriber Security Gateway / each Cluster Member.
2. Log in to the Expert mode.
3. Back up the current file:

   ```
   cp -v $FWDIR/conf/identity_broker.C{,_BKP}
   ```

4. Edit the current file:

   ```
   vi $FWDIR/conf/identity_broker.C
   ```

   See *"Example of a Configured Identity Broker" on page 137*.

5. In the section "`:sharing_id()`", enter an alphanumeric unique identifier for this PDP Subscriber.

   Enter at minimum 16 characters. You can use a UUID generator.

   You use this identifier in the `$FWDIR/conf/identity_broker.C` file on Publishers in the section "`:identity_subscribers ()`".

   For example:

   ```
   :sharing_id (b2L4Sri5K9HxJw63GjAb)
   ```

6. In the section "`:identity_publishers ()`", enter the applicable data for **each** Publisher Security Gateway / Cluster.

Parameter	Description
`Name`	Specifies a descriptive name for this Publisher Security Gateway / Cluster. **Best Practice** - Use the object name of this Publisher Security Gateway / Cluster as configured in SmartConsole.

Parameter	Description
`sharing_id`	Specifies the unique identifier of the Publisher Security Gateway / Cluster. Get this value from the `$FWDIR/conf/identity_broker.C` file on the Publisher - from the top section "`:sharing_id ()`". **Note** - The sharing_id must be identical to all cluster members and set the IP address to one of the cluster's VIPs. From the subscriber's perspective, the Cluster Publisher is seen as a single publisher in common cluster topologies.
`ipaddr`	Specifies the IPv4 address of the applicable interface on the Publisher Security Gateway to which this Subscriber connects. **Important** - If this IP address changes in the Subscriber Security Gateway / Cluster object, you must update it in the `$FWDIR/conf/identity_broker.C` file. **Note** - For IPv6, use "`ipaddr6`".
`filter`	**Optional:** Specifies an incoming filter for this specific Publisher. Follow the instructions in *"Configuring Identity Filters" on page 134*.
`recalculate_access_roles`	**Optional:** Specifies if recalculation of Access Roles is needed for each shared session from this Publisher. This way, the Subscriber can use the Access Roles from the Access Control Policy instead of the Access Roles from the Publisher. This feature is disabled by default. For more information, see sk164474.

Identity Broker Filters

By default:

- A Publisher sends all Identity Sessions to all its Subscribers.
- A Subscriber receives all Identity Sessions from all its Publishers.

You can configure filters in the `$FWDIR/conf/identity_broker.C` file to control identity sharing between Identity Brokers.

On a **Publisher**, you can configure:

- Global filters that apply to all identity sessions this Publisher sends to all Subscribers that are configured on this Publisher. Global filters take precedence over local filters.
- Local filters that apply to identity sessions this Publisher sends to specific Subscribers that are configured on this Publisher.

On a **Subscriber**, you can configure:

- Global filters that apply to all identity sessions this Subscriber receives from all Publishers that are configured on this Subscriber. Global filters take precedence over local filters.
- Local filters that apply to identity sessions this Subscriber receives from specific Publishers that are configured on this Subscriber.

Best Practice - Configure a filter to control which Identity Sessions a Publisher sends to its Subscribers.
Configure the applicable local filters for specific subscribers, or configure the applicable global filters.

There two types of filters- include filters and exclude filters.

Algorithm on the Security Gateway:

1. Apply the "include" filter, if it is configured.

   "AND"

2. Apply the "exclude" filter, if it is configured.

   When an exclude filter includes multiple statements, the Security Gateway performs a logical "OR" between these "exclude" statements.

Filters

See *"Global Filters (Optional)" on page 134* and *"Example of a Configured Identity Broker" on page 137*.

- **Users/Machines name**

  You can use Regular Expressions. Specify the word `regexp:` in the prefix.

  For example, if you want to exclude user `johndoe` OR all users staring with `srv_`, configure this filter:

  ```
  :exclude_users_and_machines (
    : ("johndoe")
    : ("regexp:^srv_*$")
  )
  ```

- **Network**

  For example, to include only sessions from the 192.168.0.1/24 network, configure this filter:

  ```
  :include_networks (192.168.0.1/255.255.255.0)
  ```

- **Identity Source**

  To exclude or include all identities from any of the available Identity Sources, specify one or more of any of the necessary Sources.

  These are the Identity Sources that you can use in this filter:

  - portal
  - Identity Agent
  - Remote Access
  - AD Query
  - Terminal Servers Identity Agent
  - RADIUS Accounting
  - Identity Awareness API
  - Identity Collector

  For example, to exclude all identities from Identity Collector, configure this filter:

  ```
  :exclude_identity_source (
    : ("Identity Collector")
  )
  ```

- **Domain Name**

  You can use Regular Expressions. Specify the word `regexp:` in the prefix.

For example, to exclude all the identities from the domain name *example.com* OR all the identities from a domain name that ends with *company.com*, configure this filter:

```
:exclude_domains (
  : ("example.com")
  : ("regexp:^.*company\.com$")
)
```

- **Distinguished Name**

  You can use Regular Expressions. Specify the word `regexp:` in the prefix.

  For example, to include all identities with a distinguished name that contains the organization unit "OU_01" ,configure this filter:

```
:include_distinguished_names (
  : ("regexp:^.*OU=OU_01.*$")
)
```

- **Access Role**

  To exclude or include identities matched to specific Access Roles, specify the applicable Access Role object name.

  You can use Regular Expressions. Specify the word `regexp:` in the prefix.

  For example, to send only the identities that match an Access Role named "UK_ Finance" and an Access Role that starts with the phrase "Manager_", configure this filter:

```
:include_roles (
  : ("UK_Finance")
  : ("regexp:^Manager_.*$")
)
```

- **Immediate Publishers**

  An Immediate Publisher propagates identities to an Identity Broker one hop away, In other words, a direct publisher-subscribe connection exists between two Identity Broker peers.

  To exclude or include immediate publishers of the configured subscribers, specify one or more to the filter set:

```
:include_immediate_publishers (
  : ("192.168.1.72")
  : ("192.168.1.66")
)
```

Example - large scale environment scenario:

- Identity Broker A (192.168.1.72) and B publish identity sessions to the Identity Broker peer C.
- Identity Broker C (192.168.1.66) publishes identity sessions to Identity Broker D.
- Without any filtering, Identity Broker D learns about all the Identity Sessions from A, B and C.
- In case Identity Broker D only learns about Identity Sessions from Identity Broker A:

  In the Identity Broker C configuration file, in the section that describes "subscriber D", add a filter to show Identity Broker A as "immediate publishers".

  ```
  :include_immediate_publishers (
    : ("192.168.1.72")
  )
  ```

- If you apply the above filter settings, Identity Broker D learns Identity Sessions from Identity Broker A and Identity Broker C.

Immediate Owners

A PDP instance creates an Identity Session based on a login event learned from an identity source. For example, when an Identity Agent terminates a PDP instance, this PDP instance creates the Identity Session and is the owner of this session.

When this PDP instance publishes this Identity Session to a subscribing Identity Broker peer, it includes its IP address as "owner" in the Identity Session properties.

This example shows the Identity Broker with the IP address 192.168.51.229 that owns the identity session 94a9f4c:

```
Session:  94a9f4c2
Session UUID:  {B4E4634F-E98E-FCE7-A52B-CCB38B5705DB}
Ip:  192.168.51.188
Users:
alice {94fbed73}
  Groups: InternalSales;All Users
  Roles: InternalSalesAccessRole
  Client Type: portal
  Authentication Method: User & Password
  Distinguished Name:
  Connect Time: Thu Jan  9 16:00:27 2020
  Next Reauthentication: -
  Next Connectivity Check: -
  Next Ldap Fetch: -
Packet Tagging Status:  Not Active
Published Gateways:  Local
Owner:  192.168.51.229
Immediate Publisher:  192.168.51.229
Published PDPs:  192.168.51.226
```

To exclude or include identities from a specific owner, set the applicable owner IP address.

Best Practice - Configure a list of "include_owners" for an Identity Broker to only learn Identity Sessions created by dedicated Identity Brokers in the network.

For example, to share only identities whose origin is two specific owners, configure this filter:

```
:include_owners (
  : ("172.23.106.72")
  : ("172.23.106.66")
)
```

Global Filters (Optional)

Filters can be configured globally for Identity Brokers using the **global_outgoing_filter** and **global_incoming_filter** parameters:

Important - Global filters take precedence over local filters. For example, if you configure an outgoing global filter to exclude Identities from network 10.10.10.0/24 and configure a contradicting local filter to include and publish the 10.10.10.0/24 network identities, this network's identities are not published.

Parameter	Description
`global_outgoing_filter`	Specify global outgoing filters on the *Publisher*. These filters apply to all the identity sessions published to **ALL** the configured Subscribers.
`global_incoming_filter`	Specify global incoming filters for the *Subscribers*. These filters apply to all the identity sessions received from **ALL** configured *Publishers*.

Configuring Identity Filters

These are all the Possible Filter configuration templates.

Note - All fields are optional.

Important:

- Each parameter you configure in this file must have a value inside the parentheses "`:<parameter> (<value>)`"
- If an optional parameter does not have a value, you must delete it from the file.

:filter

```
:filter (
  :include_users_and_machines ()
  :exclude_users_and_machines ()
  :include_networks ()
  :exclude_networks ()
  :include_identity_source ()
  :exclude_identity_source ()
  :include_domains ()
  :exclude_domains ()
  :include_roles ()
  :exclude_roles ()
  :include_distinguished_names ()
  :exclude_distinguished_names ()
```

```
    :include_owners ()
    :exclude_owners ()
    :include_immediate_publishers ()
    :exclude_immediate_publishers ()
  )
```

:global_outgoing_filter

```
  :global_outgoing_filter (
    :include_users_and_machines ()
    :exclude_users_and_machines ()
    :include_networks ()
    :exclude_networks ()
    :include_identity_source ()
    :exclude_identity_source ()
    :include_domains ()
    :exclude_domains ()
    :include_roles ()
    :exclude_roles ()
    :include_distinguished_names ()
    :exclude_distinguished_names ()
    :include_owners ()
    :exclude_owners ()
    :include_immediate_publishers ()
    :exclude_immediate_publishers ()
  )
```

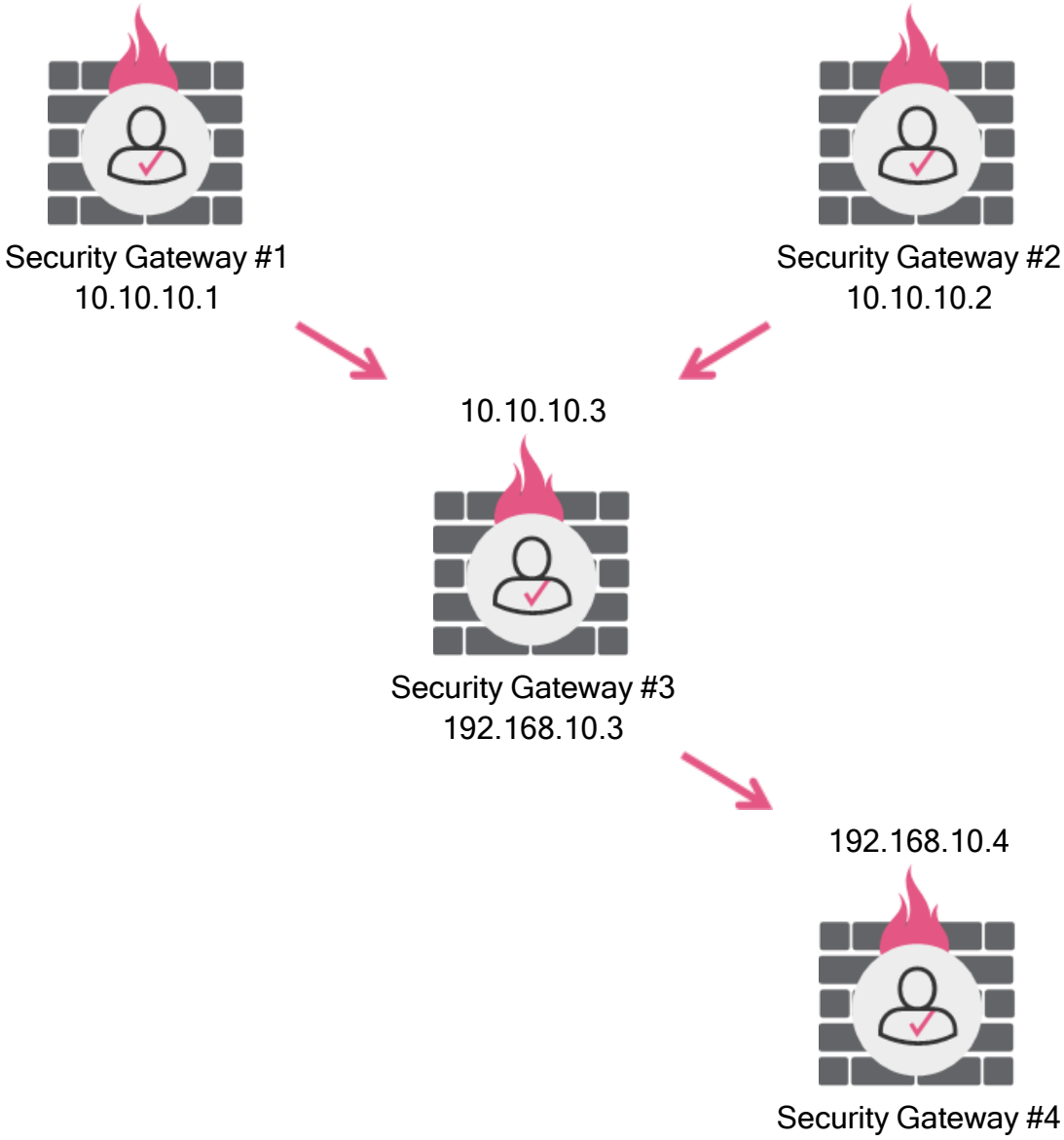
:global_incoming_filter

```
  :global_incoming_filter (
    :include_users_and_machines ()
    :exclude_users_and_machines ()
    :include_networks ()
    :exclude_networks ()
    :include_identity_source ()
    :exclude_identity_source ()
    :include_domains ()
    :exclude_domains ()
    :include_roles ()
    :exclude_roles ()
    :include_distinguished_names ()
    :exclude_distinguished_names ()
    :include_owners ()
    :exclude_owners ()
```

```
    :include_immediate_publishers ()
    :exclude_immediate_publishers ()
  )
```

Example of a Configured Identity Broker

Logical topology:



Security Gateway	Gets identities from these PDP Publishers	Shares identities with these PDP Subscribers
Security Gateway #1	None	Security Gateway #3 over 10.10.10.x
Security Gateway #2	None	Security Gateway #3 over 10.10.10.x

Security Gateway	Gets identities from these PDP Publishers	Shares identities with these PDP Subscribers
Security Gateway #3	Security Gateway #1 over 10.10.10.x Security Gateway #2 over 10.10.10.x	Security Gateway #4 over 192.168.10.x
Security Gateway #4	Security Gateway #3 over 192.168.10.x	None

Example of a configured Identity Broker on Security Gateway #1

The `$FWDIR/conf/identity_broker.C` file configured on Security Gateway #1:

```
(
  :sharing_id (z8JXd28t0taHnhifKnYm8)
  :identity_subscribers (
    : (
      :Name (GW3)
      :sharing_id (Ac65e4dCc4aBa06b140dE)
      :ipaddr (10.10.10.3)
      :certificate_subject ("GW3.broker.portal")
      :share_only_local_sessions (false)
      :filter ()
    )
  )
  :global_outgoing_filter (
    :exclude_identity_source (
      : ("Identity Collector")
    )
  )
)
```

Example of a configured Identity Broker on Security Gateway #2

The `$FWDIR/conf/identity_broker.C` file configured on Security Gateway #2:

```
(
  :sharing_id (Y2l885i5u49xJw63hHACP)
  :identity_subscribers (
    : (
      :Name (GW3)
      :sharing_id (Ac65e4dCc4aBa06b140dE)
      :ipaddr (10.10.10.3)
      :certificate_subject ("GW3.broker.portal")
      :share_only_local_sessions (false)
      :filter ()
    )
  )
  :global_outgoing_filter (
    :exclude_identity_source (
      : ("Identity Collector")
    )
  )
)
```

Example of a configured Identity Broker on Security Gateway #3

The `$FWDIR/conf/identity_broker.C` file configured on Security Gateway #3:

```
(
  :sharing_id (Ac65e4dCc4aBa06b140dE)
  :identity_subscribers (
    : (
      :Name (GW4)
      :sharing_id (0N8NbkP0XMuvAw3F62d20)
      :ipaddr (192.168.10.4)
      :certificate_subject ("GW4.broker.portal")
      :share_only_local_sessions (false)
      :filter ()
    )
  )
  :identity_publishers (
    : (
      :Name (GW1)
      :sharing_id (z8JXd28t0taHnhifKnYm8)
      :ipaddr (10.10.10.1)
      :filter ()
    )
    : (
      :Name (GW2)
      :sharing_id (Y2l885i5u49xJw63hHACP)
      :ipaddr (10.10.10.2)
      :filter ()
    )
  )
  :global_outgoing_filter (
    :exclude_identity_source (
      : ("Identity Collector")
    )
  :global_incoming_filter (
    :exclude_networks (
      : (192.168.1.0/255.255.255.0)
    )
    :exclude_identity_source (
      : ("Radius Accounting")
    )
  )
)
```

Example of a configured Identity Broker on Security Gateway #4

The `$FWDIR/conf/identity_broker.C` file configured on Security Gateway #4:

```
(
  :sharing_id (0N8NbkP0XMuvAw3F62d20)
  :identity_publishers (
    : (
      :Name (GW3)
      :sharing_id (Ac65e4dCc4aBa06b140dE)
      :ipaddr (10.10.10.3)
      :filter ()
    )
  )
  :global_incoming_filter (
    :exclude_networks (
      : (172.33.40.0/255.255.255.0)
    )
    :exclude_identity_source (
      : ("Radius Accounting")
    )
  )
)
```

CLI Commands

You can use the "`pdp broker <commands>`" commands to monitor and do an inspection on the Identity Broker.

For full syntax and description of all the available CLI commands, see *"Command Line Reference" on page 245*.

Identity Conciliation - PDP

A Policy Decision Point (PDP) Security Gateway uses the PDP Identity Conciliation mechanism.

Note - Identity Conciliation is supported for Security Gateway versions R80.40 and higher.

PDP Identity Conciliation - Actions

When the PDP Security Gateway receives an update about an identity (user identity or machine identity) on an IP address, from which the PDP has an active session, it does one of these actions:

Action	Description
Override	Deletes the current identity session. Keeps the new identity session.
Reject	Rejects the new identity session. Keeps the current identity session.
Append	Adds the new identity information to the current identity session.

PDP Identity Conciliation - Terms

Type of Identity Session	Description
Per-Entity	The PDP Security Gateway receives the session from an identity source other than an Identity Agent for a User Endpoint Computer. The session comes from: ■ AD Query ■ RADIUS Accounting ■ Identity Collector ■ Identity Web API
Per-Host	The PDP Security Gateway receives the session from an identity source directly on the user host: ■ Identity Agent for a User Endpoint Computer ■ Identity Agent for a Terminal Server (MUH) ■ Remote Access VPN client ■ Captive Portal
Between PDP Security Gateways in the same Management Domain	The PDP Security Gateway receives the session in one of these ways: ■ Locally - the PDP Security Gateway) receives the identity directly from the identity source. ■ From an Identity Broker Publisher, when the same Management Server manages the two Security Gateways - this Identity Subscriber and the Identity Publisher
Between PDP Security Gateways in different Management Domains ("external session")	The PDP Security Gateway receives the session from an Identity Broker Publisher, when different Management Servers manage the two Security Gateways - this Identity Subscriber and the Identity Publisher

PDP Identity Conciliation - PDP Session Parameters

Parameter	Description
Office Mode IP Address	If the current session, or the new session comes from a Remote Access VPN client, then the PDP Security Gateway gives a higher priority to the session from a Remote Access VPN client.
Confidence	The PDP Security Gateway gives a higher priority to a session that has a higher score. These are the default scores for different identity sources: ■ 40 - Remote Access VPN client, or Identity Agent for a Terminal Server ■ 30 - Identity Agent ■ 20 - Captive Portal ■ 15 - Identity Web API ■ 10 - Identity Collector, or RADIUS Accounting ■ 0 - AD Query, or IFMAP
Locality	The Security Gateway gives a higher priority to a session that was shared by fewer Gateways (lower hop count). **Example**: **Session A** Identity Source => PDP Identity Publisher (Hop Count = 0) => PDP Identity Subscriber (Hop Count = 1) Total Hop Count = 1 **Session B** Identity Source => PDP Identity Publisher (Hop Count = 0) => PDP Identity Subscriber/Publisher (Hop Count -1) => PDP Identity Subscriber (Hop Count = 2) Total Hop Count = 2 Because Session A has a lower hop count, the PDP Gateway gives higher priority to Session A.

Parameter	Description
Time To Live (TTL)	The PDP Security Gateway gives a higher priority to a session that has a more recent time stamp (created more recently). The timestamp is in the Epoch Time format.
Full Session	The PDP Security Gateway gives a higher priority to a session that has a user identity and a machine identity (comparing to a session that has only one of these attributes).
PDP Preference	The PDP Security Gateway gives a higher priority to a session that it receives from a specific PDP Identity Publisher. By default, there are no preferred Identity Publishers.

PDP Identity Conciliation - Possible Session Scenarios

The PDP Identity Conciliation supports these scenarios:

Scenario	Internal Session Category	Current Session	New Session	Management Domains of PDP Security Gateways	Identity Conciliation Action	Description
1	PerEntityInDomain	Per-Entity	Per-Entity	Same	Always **Append**	■ The two identity sessions are Per-Entity sessions. ■ The same Management Server manages the two PDP Security Gateways. ■ The default action is "Append" (administrator cannot change this behavior). ■ Priorities of session parameters: • Value 0 - Confidence • Value 1 - Time to Live (TTL) • Value 2- Locality

Scenario	Internal Session Category	Current Session	New Session	Management Domains of PDP Security Gateways	Identity Conciliation Action	Description
						• Value 3 - PDP Preference

Scenario	Internal Session Category	Current Session	New Session	Management Domains of PDP Security Gateways	Identity Conciliation Action	Description
2	PerEntityExternal	Per-Entity	Per-Entity	Different	Based on the configured priorities of session parameters	■ The two identity sessions are Per-Entity sessions. ■ Different Management Servers manage the two PDP Security Gateways. ■ Priorities of session parameters: • Value 0 - Locality • Value 1 - Confidence • Value 2 - Time to Live (TTL) • Value 3 - PDP Preference

Scenario	Internal Session Category	Current Session	New Session	Management Domains of PDP Security Gateways	Identity Conciliation Action	Description
3	PerHostInDomain	Per-Host or Per-Entity	Per-Host	Same	If the new session arrives directly from the Identity Source , the decision is **Override**. If the new session arrives from an Identity Broker, the decision is based on the configured priorities of session parameters	■ The current session is a Per-Host session or a Per-Entity session. ■ The new session is a Per-Host session. ■ The same Management Server manages the two PDP Security Gateways. ■ When the PDP Security Gateway receives the session directly from the Identity Source (**not** from an Identity Broker, the decision is **Append**.

Scenario	Internal Session Category	Current Session	New Session	Management Domains of PDP Security Gateways	Identity Conciliation Action	Description
						■ When the PDP Security Gateway receives the session from an Identity Broker, the decision is according to the configured priorities of the session parameters. ■ Priorities of session parameters: • Value 0 - Office Mode IP Address • Value 1 - Confidence • Value 2 - Time to Live (TTL)

Scenario	Internal Session Category	Current Session	New Session	Management Domains of PDP Security Gateways	Identity Conciliation Action	Description
						• Value 3 - Locality • Value 4 - Full Session • Value 5 - PDP Preference

Scenario	Internal Session Category	Current Session	New Session	Management Domains of PDP Security Gateways	Identity Conciliation Action	Description
4	PerHostInDomain	Per-Host	Per-Entity	Same	Based on the configured priorities of session parameters	■ The current session is a Per-Host session. ■ The new session is a Per-Entity session. ■ The same Management Server manages the two PDP Security Gateways. ■ Priorities of session parameters: • Value 0 - Office Mode IP Address • Value 1 - Confidence • Value 2 - Time to Live (TTL)

Scenario	Internal Session Category	Current Session	New Session	Management Domains of PDP Security Gateways	Identity Conciliation Action	Description
						• Value 3 - Locality • Value 4 - Full Session • Value 5 - PDP Preference

Scenario	Internal Session Category	Current Session	New Session	Management Domains of PDP Security Gateways	Identity Conciliation Action	Description
5	PerHostExternal	Per-Host or Per Entity	Per-Host	Different	If the new session arrives directly from the Identity Source , the decision is **Override**. If the new session arrives from an Identity Broker, the decision is based on the configured priorities of session parameters	■ The current session is a Per-Host session or a Per-Entity session ■ The new session is a Per-Host session. ■ The same Management Server manages the two PDP Security Gateways. ■ When the PDP Security Gateway receives the session directly from the Identity Source (**not** from an Identity Broker, the decision is **Append**.

Scenario	Internal Session Category	Current Session	New Session	Management Domains of PDP Security Gateways	Identity Conciliation Action	Description
						■ When the PDP Security Gateway receives the session from an Identity Broker, the decision is according to the configured priorities of the session parameters. ■ Priorities of session parameters: • Value 0 - Locality • Value 1 - Confidence • Value 2 - Time to Live (TTL)

Scenario	Internal Session Category	Current Session	New Session	Management Domains of PDP Security Gateways	Identity Conciliation Action	Description
						• Value 3 - Full Session • Value 4 - PDP Preference

Scenario	Internal Session Category	Current Session	New Session	Management Domains of PDP Security Gateways	Identity Conciliation Action	Description
6	PerHostExternal	Per-Host	Per-Entity	Different	Based on the configured priorities of session parameters	■ The current session is a Per-Host session. ■ The new session is a Per-Entity session. ■ Different Management Servers manage the two PDP Security Gateways. ■ Priorities of session parameters: • Value 0 - Locality • Value 1 - Confidence • Value 2 - Time to Live (TTL) • Value 3 - Full Session

Scenario	Internal Session Category	Current Session	New Session	Management Domains of PDP Security Gateways	Identity Conciliation Action	Description
						• Value 4 - PDP Preference

PDP Identity Conciliation - Decision Flow

In cases when PDP Security Gateway does not make the default action, it examines the configured priorities of the session parameters.

1. The Security Gateway decides which Session Scenario applies.
2. The Security Gateway compares the two identity sessions based on the first session parameter:
   - If the current session gets higher priority based on the session parameter, the Security Gateway decides to **Reject** the new session.
   - If the new session gets higher priority based on the session parameter, the Security Gateway decides to **Override** the current session.
3. If neither the current, nor the new session gets higher priority (the sessions are in a "tie"), the Security Gateway compares the next session parameter until it makes a decision.

PDP Identity Conciliation - Examples

#	Current Session	New Session	Management Domain	PDP Conciliation Decision
1	Identity source - Identity Collector. The Security Gateway received this identity session through the Identity Broker sharing mechanism. The same Management Server manages the two PDP Security Gateways.	Identity source - RADIUS Accounting. The Security Gateway received this identity session directly.	The same Management Server manages the two PDP Security Gateways.	**Append** the new session to the current session. Internal session category - PerEntityInDomain.
2	Identity source - Identity Agent for a Terminal Server. The Security Gateway received this identity session through the Identity Broker sharing mechanism. The same Management Server manages the two PDP Security Gateways.	Identity source - Remote Access VPN client. The Security Gateway received this identity session directly.	The same Management Server manages the two PDP Security Gateways.	**Override** the current session with the new session. Internal session category - PerHostInDomain.

#	Current Session	New Session	Management Domain	PDP Conciliation Decision
3	Identity source - Identity Web API. The Security Gateway received this identity session through the Identity Broker sharing mechanism.	Identity source - Captive Portal. The Security Gateway received this identity session through the Identity Broker sharing mechanism.	Different Management Servers manage the two PDP Security Gateways	Internal session category - PerHostExternal. The Security Gateway compares the two session based on these session parameters: ■ Value0 - Locality (hop count) ■ Value1 - Confidence ■ Value2 - Time to Live (TTL) ■ Value3 - Full Session ■ Value4 - PDP Preference Example: 1. The Security Gateway compares the two session based on the first session parameter on the list - "Locality": ■ If the current session has a lower hop count, then it has the higher priority. The decision is to **Reject** the new session. ■ If the new session has a lower hop count, then it has the lower priority. The decision is to **Override** the current session with the new session.

#	Current Session	New Session	Management Domain	PDP Conciliation Decision
				2. If the sessions have the same hop count (a "tie"), the Security Gateway compares the two session based on the second session parameter on the list - "Confidence": ■ The Confidence score of Captive Portal (20) is greater than the Confidence score of Identity Web API (15). The decision is to **Override** the current session with the new session.

PDP Identity Conciliation - Configuration

Warning - We recommend to use the default values in the configuration file. Wrong configuration can lead to connectivity issues for end-users.

Note - In a Cluster, you must configure all the Cluster Members in the same way.

Editing the configuration file:

1. Connect to the command line on the Security Gateway / each Cluster Member / Scalable Platform Security Group.
2. Log in to the Expert mode.
3. Back up the current configuration file:

   ```
   cp -v $FWDIR/conf/pdp_session_conciliation.C{,_BKP}
   ```

4. Edit the current configuration file:

   ```
   vi $FWDIR/conf/pdp_session_conciliation.C
   ```

5. Make the applicable changes.

   Warning - Be careful when you edit this file. If the syntax of this file is wrong, the Security Gateway uses the default values for all parameters.

6. Save the changes in the file and exit the editor.
7. On a Scalable Platform Security Group - copy the updated file to all Security Group Members:

   ```
   asg_cp2blades $FWDIR/conf/pdp_session_conciliation.C
   ```

8. In SmartConsole, install the Access Control Policy on this Security Gateway / Cluster object.

Parameters in the configuration file:

Section	Parameter	Parameter and Default Value	Description
PDPPreferencesConfig			Contains the IP addresses and preference values for preferred PDP Identity Publishers. The higher the preference value, the higher the priority.
		127.0.0.1 (0)	Default value.
ConfidenceConfig	ScorePerAttribute	:HasLogoutNotification (0) :HasAuthorization (0) :HasAuthentication (0) :HasKeepAlive (0) :HasIpSpoofingDetection (0) :HasRoamingDetection (0) :HasLogout (0)	Advanced parameters related to the session state. **Warning** - Change these values only if Check Point Support or R&D explicitly told you to do so. Contact *Check Point Support*.
	ScorePerIdentitySource		Scores for Identity Sources.

Section	Parameter	Parameter and Default Value	Description
		`:portal (20)`	Score for Captive Portal.
		`:ida_agent (30)`	Score for Identity Agent for a User Endpoint Computer.
		`:vpn (40)`	Score for Remote Access VPN clients.
		`:adq (0)`	Score for AD Query.
		`:ifmap (0)`	Score for IFMAP
		`:muh_agent (40)`	Score for Identity Agent for a Terminal Server v1.
		`:radius (10)`	Score for RADIUS Accounting.
		`:ida_api (15)`	Score for Identity Web API.
		`:idc (10)`	Score for Identity Collector.
		`:muh_agent2 (40)`	Score for Identity Agent for a Terminal Server v2.

Section	Parameter	Parameter and Default Value	Description
`ConciliationConfig`			Session parameters and their priority for the possible session scenarios. See: ■ *"PDP Identity Conciliation - Terms" on page 143* ■ *"PDP Identity Conciliation - PDP Session Parameters" on page 144* ■ *"PDP Identity Conciliation - Possible Session Scenarios" on page 145*

Section	Parameter	Parameter and Default Value	Description
	PerHostInDomain	:0 (OfficeModeIp) :1 (Confidence) :2 (Ttl) :3 (Locality) :4 (FullSession) :5 (PdpPreference)	
	PerEntityInDomain	:0 (Confidence) :1 (Ttl) :2 (Locality) :3 (PdpPreference)	
	PerHostExternal	:0 (Locality) :1 (Confidence) :2 (Ttl) :3 (FullSession) :4 (PdpPreference)	
	PerEntityExternal	:0 (Locality) :1 (Confidence) :2 (Ttl) :3 (PdpPreference)	

Examples:

PDP Identity Conciliation Configuration File - Example 1

All Security Gateways in the environment are in the same Management domain.

One PDP Publisher shares information from Identity Collector.

A second PDP Publisher shares information from Identity Agent for a Terminal Server.

The administer wants to prefer the PDP Publisher that sends information from Identity Collector.

The relevant Internal Session Category is PerHostInDomain. By default, the session from the PDP Publisher that sent the Identity Agent session remains because it has the higher Confidence priority.

To prefer the PDP Publisher that sends information from Identity Collector,make these changes in the `$FWDIR/conf/ pdp_session_conciliation.C` file in the PDP Gateway.

1. Change the ordered set of PerHostInDomain behavior as shown. Put " (PdpPreference)" in position `:0` and decrease the position of other parameters by one.

   :PerHostInDomain (

   :0 (PdpPreference)

   :1 (OfficeModeIp)

   :2 (Confidence)

   :3 (Ttl)

   :4 (Locality)

   :5 (FullSession)

)

2. Change the score of the relevant PDP Publisher (Identity Collector) in the `PDPPreferencesConfig` sub-section to be higher than the score of the other PDP Publisher (Identity Agent for a Terminal Server).
3. Install policy.

PDP Identity Conciliation Configuration File - Example 2

This example shows how to configure Remote Access VPN and Identity Agent on the same user endpoint computer. With this configuration, the PDP Gateway can identify users when they log in through Remote Access VPN. If Identity Agent is installed on the user endpoint computer, the PDP Gateway does not stop the previous connection.

Without this configuration, there is flapping of the identity between Identity Agent and Remote Access VPN. Each causes the other to log off every 10-15 minutes.

To configure Remote Access VPN and Identity Agent on the same user endpoint computer and prevent flapping, make these changes in the `$FWDIR/conf/ pdp_session_ conciliation.C` file in the PDP Gateway.

1. In the section `PerHostInDomain`:
   a. Put "`(Confidence)`" in the position `:0`
   b. Put "`(OfficeModeIP)`" in the position `:1`
2. In the section `ScorePerIdenitiySource`:

a. Increase the score of `ida_agent` so that it is higher than the score of `vpn`

   Example: If the score of `vpn` is `30`, make the score of `ida_agent` `40`.

3. Save the changes in the file.
4. In SmartConsole install policy.
5. On the Security Gateway / each Cluster Member / Security Group, restart the `pdpd` daemon with the "`fw kill pdpd`" command.

PDP-Only

Identity Awareness is composed of two main processes.

1. The Policy Decision Point (PDP) handles the Identity Acquisition logic and serves as the termination point for various identity sources. It is responsible for authentication and authorization by querying group membership against the User Directory and matching relevant access roles. The PDP propagates identities to configured enforcement points PEPs to enforce identity-based policies or other PDPs with the Identity Broker.

2. Policy Enforcement Point (PEP) runs the Identity-Based enforcement logic. It learns the identities and their matching Access Roles from local/remote PDPs, based on the configuration.

In large-scale Identity Awareness deployments, dedicated Gaia machines are used only to run the Identity Acquisition and propagation logic. Those machines do not enforce traffic, so there is no real need for Identity-Based enforcement logic to run.

Use PDP-Only mode to streamline identity-related functions in your Identity Awareness architecture. Administrators can reduce resource overhead and enhance efficiency with the deployment of dedicated PDP Security Gateways. This optimization minimizes memory and CPU consumption and ensures more efficient resource utilization within the broader security of your infrastructure.

The PEP process consumes additional resources:

- Memory consumption.
- CPU consumption.
- Access to the Identity Awareness databases in the kernel.
- Redundant logic that runs in the PDP process to share the identities with the local PEP process.

Solution - To decrease resource utilization, you can enable the PDP-Only mode on the Identity Awareness Gateways that only acquire and propagate identities. In this mode, the PDP Identity Awareness Gateways do not run the PEPD process.

Notes:

- This feature is supported from R81.20 Jumbo Hotfix Accumulator Take 38 and higher.
- In R82, a schema and Security Management API support were added to control the feature's state. Configuration for R81.20 differs and is documented in sk181605. If you upgrade from R81.20 with this feature enabled, re-enable it with the Security Management's API commands in the documentation below.

To enable or disable PDP-Only mode, the administrator must execute the appropriate Management API call on the Management Server. An Access Control policy installation is necessary for the changes to take effect.

Enabling or Disabling PDP-Only Mode

Example command:

```
mgmt_cli set simple-gateway name <Name> identity-awareness-
settings.identity-based-enforcement off
```

To check whether the feature is enabled or disabled, run the following command:

```
mgmt_cli show simple-gateway name <Name> identity-awareness-
settings.identity-based-enforcement
```

Operation:	Parameter	Description
Enable/Disable Identity-Based Enforcement	`simple-gateway name`	Specifies the name of the Security Gateway object.
	`<Name>`	Placeholder for the actual name of the Security Gateway object.
	`identity-awareness-settings.identity-based-enforcement on`	`On` enables identity-based enforcement (PDP-Only disabled). `Off` disables (PDP Only Enabled).
For a Single Security Gateway	`simple-gateway name`	Specifies the name of the Security Gateway object.
For a Cluster	`simple-cluster name`	Specifies the name of the cluster object.

Operation:	Parameter	Description
For VSX	`legacy-virtual-system name`	Specifies the name of the VSX object to configure.

Identity Conciliation - PEP

A Policy Enforcement Point (PEP) Security Gateway uses the PEP Identity Conciliation mechanism.

Note - Identity Conciliation is supported for Security Gateway versions R80.40 and higher.

PEP Identity Conciliation - Actions

When the PEP Security Gateway receives an update about an identity (user identity or machine identity) on an IP address, from which the PEP has an active session, it does one of these actions:

Action	Description
Override	Deletes the current identity session. Keeps the new identity session.
Reject	Rejects the new identity session. Keeps the current identity session.

PEP Identity Conciliation - Default Configuration

By default, the PEP Identity Conciliation decides based on Confidence.

The PDP Security Gateway gives a higher priority to a session that has a higher score.

These are the default scores for different identity sources:

- Captive Portal - 20
- Identity Agent -30
- Remote Access VPN client - 40
- Active Directory Query - 0
- Ifmap - 0
- Identity Agent for a Terminal Server - 40
- RADIUS Accounting - 10

- Identity Web API -15
- Identity Collector -10

To change the confidence scores, contact *Check Point Support*.

PEP Identity Conciliation - Custom Configuration

In a custom configuration, the PEP Identity Conciliation can compare the two sessions based on a global score that considers Confidence and one or more of these other factors:

Factor	Description
PDP Preference	This is the PDP Security Gateway from which the PDP receives the identity session. The session that comes from a PDP with higher priority gets points based on this factor. By default, no PDP is preferred.
Time to Live	The PDP Security Gateway gives a higher priority to a session that has more time remaining until the session expiration time.
Full Session	If one session has user identity and machine identity, and the other session has one kind of identity, the session with user identity and machine identity gets points based on this factor.
Connect_ Time	The session with the newer connect timestamp gets a higher store. This factor does not exist in default and basic configurations.

To make a custom configuration, contact *Check Point Support*.

Configuring Identity Awareness for a Domain Forest (Subdomains)

Create a separate LDAP Account Unit for each domain in the forest (subdomain). You cannot add domain controllers from two different subdomains into the same LDAP Account Unit.

You can use the Identity Awareness Configuration Wizard to make **one** specified subdomain. This automatically creates an LDAP Account Unit that you can easily configure to have more settings. You must manually create all other domains that you want Identity Awareness to relate to. In the **Objects** panel, select > **New** > **More** .> **User/Identity** > **LDAP Account Unit**.

When you create an LDAP Account Unit for each domain in the forest

1. Make sure the username is one of these:
   - A Domain administrator account that is a member of the Domain Admins group in the subdomain. Enter the username as *subdomain**user*.
   - An Enterprise administrator account that is a member of the Enterprise Admins group in the domain. If you use an Enterprise administrator, enter the username as *domain**user*.

     For example, if the domain is `ACME.COM`, the subdomain is `SUB.ACME.COM`, and the administrator is `John_Doe`:

     - If the admin is a Domain administrator, **Username** is: `SUB.ACME.COM\John_Doe`
     - If the admin is an Enterprise administrator, **Username** is: `ACME.COM\John_Doe`

     Note - In the wizard, this is the **Username** field. In the LDAP Account Unit, go to **LDAP Server Properties** tab > **Add** > **Username**.
2. In **LDAP Server Properties** tab > **Add** > **Login DN**, add the login DN.
3. In **Objects Management** tab > **Branches in use**, edit the base DN

   from: `DC=DOMAIN_NAME,DC=DOMAIN_SUFFIX`

   to: `DC=SUB_DOMAIN_NAME,DC=DOMAIN_NAME,DC=DOMAIN_SUFFIX`

   For example, change `DC=ACME,DC=local` to `DC=SUB,DC=ACME,DC=local`

Non-English Language Support

To support non-English user names on an Identity Awareness Gateway, you must set a parameter in the LDAP Account Unit object in SmartConsole.

It is not necessary to set this parameter when you enable Identity Awareness on the Security Management Server or Log Server.

To configure non-English language support:

1. In SmartConsole, click **Open Object Explorer (Ctrl+E)**.
2. From the **Categories** tree, select **Servers** > **LDAP Account Unit** and select the LDAP Account Unit.
3. In the **General** tab of the LDAP Account Unit, make sure **Enable Unicode support** is

selected. It is selected by default.

4. Click **OK**.

Nested Groups

Identity Awareness Security Gateway supports the use of LDAP nested groups. When a group is nested in a different group, users in the nested group are identified as part of the parent group.

For example, if Group_B is a member of Group_A, then Security Gateway identifies Group_B members as part of Group_A.

This table shows the available queries for nested groups:

Nested Groups Query	Description	CLI Command on Security Gateway
Recursive nested groups query	The gateway sends a query with the user name to the LDAP server. Query results include all the groups that the user is a member of. To know if a group is nested in a different group, and for each nesting level, you must send a new query. This configuration is enabled by default. The default nesting depth is 20. For details, see sk66561.	`pdp nested_ groups __set_ state 1`
Per-user nested groups query	With one LDAP query, the response includes all groups for the given user, with all nesting levels. Query results include groups from all branches in the forest. The LDAP server sends the groups of a given user as a flat list. The gateway sends this type of query to Global Catalog ports 3268/3269. For details, see sk134292. **Best Practice** - Use this query if you work with multiple branches in the account unit or if you use cross-domain trees with group membership. For example, a user belongs in the domain tree *example1.com* and in the domain tree *example2.com*.	`pdp nested_ groups __set_ state 2`

Nested Groups Query	Description	CLI Command on Security Gateway
Per-user nested groups query	With one LDAP query, the response includes all groups for the given user, with all nesting levels. Query results include groups from the branch specified in the LDAP account unit. The LDAP server sends the groups of a given user as a flat list. You can use one of these ports reserved for LDAP communication: 3268, 3269, 389, 636. **Best Practice** - Use this query if you work with a single branch in each account unit.	`pdp nested_ groups __set_ state 4`
Multi per-group nested groups query	The gateway sends one LDAP query, which includes the user name and the group. In response, the LDAP server indicates if the user is a member of this group or not. **Best Practice** - Use this query in a Microsoft Active Directory environment with many defined users and groups, and fewer groups defined in SmartConsole.	`pdp nested_ groups __set_ state 3`

To see the configuration status of nested groups, run this command:

```
pdp nested_groups status
```

Using an Identity Awareness Gateway as an Active Directory Proxy

If a Security Management Server is not currently connected to your Active Directory environment, an Identity Awareness Gateway can work as an Active Directory Proxy. This lets you use the Identity Awareness User Picker in an Access Role object (see *"Working with Access Role Objects in the Rule Base" on page 37*). To work as an Active Directory Proxy, the Identity Awareness Gateway must be connected to your Active Directory server.

Known Limitations

- This feature works only with Microsoft Active Directory.
- This feature supports only the user picker in the Access Role object.
- This feature works only with Security Gateway R80.20 and above running on Gaia OS.

- This feature supports only Virtual Systems that belong to the same domain as the VSX Gateway or VSX Cluster (context of VS0).

  This feature does not support Virtual Systems that belong to a different domain than the VSX Gateway or VSX Cluster (context of VS0).
- This feature does not support Scalable Platforms (41000 / 44000 / 61000 / 64000).
- This feature does not support DAIP gateways or Externally managed gateways.
- Available connection types:
  - **Clear** - Connection between the Security Management Server and the Security Gateway is encrypted by SIC. The connection from the Security Gateway to the Active Directory server is not encrypted.
  - **SSL** - Active Directory domain controller needs to allow SSL.
- In a Multi-Domain Security Management environment, this feature is not available for Account Units that are configured in the Global SmartConsole.
- Necessary Active Directory permissions for the account, you use them to configure the Account Unit:
  - For user picker functionality, the account should have permission to perform LDAP queries.
  - For Security Gateway functionality - depends on the identity sources that are used on the Security Gateway.
  - To acquire identities through the AD Query, without domain admin credentials, refer to sk93938.

Configuring an Identity Awareness Gateway as an Active Directory Proxy

Procedure:

1. Create a new Host object for each Active Directory Domain Controller in your Active Directory environment:
   a. In the top left corner, click **Objects** > **New Host**.
   b. Configure the object name and IP address.
   c. Click **OK**.
2. Install the Access Control Policy on the Identity Awareness Gateway.
3. Configure an LDAP Account Unit object:

a. In the top left corner, click **Objects** > **Object Explorer**.

   The Object Explorer window opens.

b. In the left navigation tree, click **Servers**.

c. From the toolbar, click **New** > **More** > **User/Identity** > **LDAP Account Unit**.

   The **LDAP Account Unit Properties** window opens.

d. Configure properties on each tab in the window.

- **General tab**

  I. In the **Name** field, enter the applicable object name (for example, `mycompany.com_LDAP_ACC_UNIT`).

  II. In the **Profile** field, select **Microsoft_AD**.

  III. In the **Prefix** field, enter your domain name (for example, `mycompany.com`).

  IV. In the **Account Unit usage** section, select all the options.

  V. In the **Additional configuration** section, select **Enable Unicode support**.

- **Servers tab**

  I. Click **Add**.

  II. The **LDAP Server Properties** window opens.

  III. Go to the **General** tab.

  i. In the **Host** field, select the host object you created for this Domain Controller in Step 1.

  ii. In the **Username** field, enter the username for this Domain Controller (for example, `John.Smith`).

  iii. In the **Login DN** field, enter the user's distinguished name (DN) for this Domain Controller (see RFC1779).

  Note - Refer to the official Microsoft documentation. For example, use the PowerShell `Get-ADUser` command.

  iv. In the **Password** field, enter the password for this Domain Controller.

  v. In the **Confirm password** field, enter the password again.

IV. In the **Encryption** tab, you can configure LDAPS.

Configure these settings:

i. Select **Use Encryption (SSL)** - Enables LDAPS.

ii. **Encryption port** - The LDAPS port is automatically populated. You can modify it as needed.

iii. Click **Fetch** to retrieve this information:

- **Server Name** - The subject of the LDAPS server certificate.
- **CA** - Certificate of the root CA that signed the LDAPS server certificate.

  Note - If you renew or replace the LDAPS server certificate using the same CA and Server Name, Security Gateways version R82 or higher trust the new certificate automatically.
- **Server** - Fingerprint of the LDAPS server certificate.

iv. Verify that the fetched information is correct.

v. Optional: Select **CRL check** to have the Security Gateway verify that the server certificate is not revoked.

Note - If you enable CRL check, you must make sure that the LDAPS server certificate contains a CRL Distribution Point extension of type HTTP, and that the Security Gateway can access this URL.

vi. **Min/Max Encryption Strength** - Use the default values provided:

- **Export** for minimum encryption strength
- **Strong** for maximum encryption strength

V. Click **OK** to close the LDAP Server Properties window.

Note - The order in which these LDAP Servers come to the view, is the default order in which they are queried. You can configure the applicable priority for these LDAP Servers.

- **Objects Management tab**

  I. In the **Server to connect** field, select the host object you created for this Domain Controller in Step 1.

  II. Manually add the branch(es).

  Note - This feature does not support fetching on branches.

  III. The branch name is the suffix of the Login DN that begins with `DC=`.

  IV. For example, if the Login DN is `CN=John.Smith,CN=Users,DC=mycompany,DC=com`

  V. then the branch name is `DC=mycompany,DC=com`

  VI. Select **Management Server needs proxy to reach AD server**.

  VII. In the **Proxy through** field, select the Security Gateway / Security Cluster that has a route to your AD server.

  VIII. Configure other applicable settings.

- **(Optional) Authentication tab**

  I. Clear **Use common group path for queries**.

  II. In the **Allowed authentication schemes** section, select all the options.

  III. In the **Users' default values** section:

  - Clear **Use user template**.
  - Select **Default authentication scheme** > **Check Point Password**.

e. Click **OK** to complete the configuration of the new LDAP Account Unit object and to close the LDAP Account Unit Properties window.

Manually Retrieving the Active Directory Server Fingerprint

1. Open a plain-text editor on your device.

2. Copy and paste this command to the plain-text editor:

```
cpopenssl s_client -connect 192.168.1.2:636 2>&1 </dev/null |
sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' |
cpopenssl x509 -noout -md5 -fingerprint
```

3. In the text editor, replace `192.168.1.2` with the IP address of your Active Directory Domain Controller.
4. Connect to the command line on the Security Gateway.
5. Log in to the Expert mode.
6. In case of a VSX Gateway, switch to the context of the applicable Virtual System that has connectivity to the Active Directory Domain Controller.
7. Make sure there is connectivity between the Security Gateway, or Virtual System and the Active Directory Domain Controller.
8. Copy and paste the modified command from the text editor on your device to the Security Gateway console, and press **Enter**.

   MD5 Fingerprint is displayed. For example:

```
MD5
Fingerprint=0B:84:D1:28:A5:19:6A:4D:24:57:72:5A:32:9B:2D:4D
```

9. Copy the displayed Active Directory fingerprint (after the = sign) from the Security Gateway console.
10. Paste the copied fingerprint in the **CA** field.

SAML Identity Provider for Identity Awareness

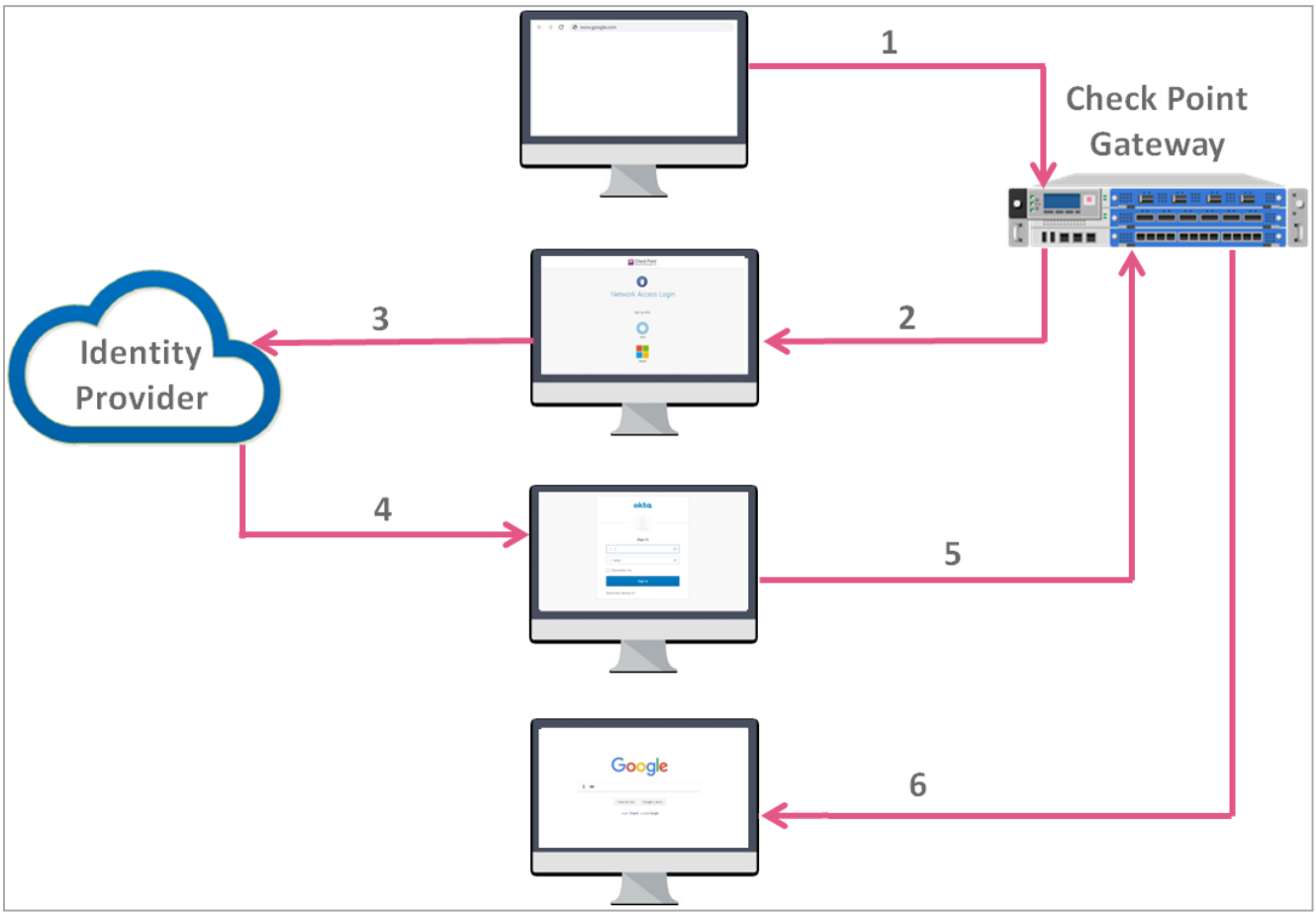
This section describes how to configure authentication using a 3rd party Identity Provider over the SAML protocol as an authentication method for an Identity Awareness Gateway (Captive Portal) as a Service Provider.

An Identity Provider is a system entity that creates, maintains, and manages identity information and provides authentication services. A Service Provider is a system entity that provides services for users authenticated by the Identity Provider.

SAML Authentication Process Flow

In the example diagram below:

- The service is `google.com`.
- The service provider is Identity Awareness Gateway (Captive Portal).
- The Identity Provider is Okta.



1. An end-user asks for a service through the client browser.

   In our example - the end user enters `google.com` in the browser address bar.

2. The Identity Awareness Gateway opens its Captive Portal.
3. The Identity Awareness Gateway redirects the end-user browser to the 3rd party Identity Provider portal to acquire the end user's identity.

   In our example - Okta.

4. The Identity Provider portal opens, and the end-user authenticates.

   In our example - Okta portal.

   The Identity Provider generates a digitally-signed SAML assertion and sends it back to the end-user browser.

5. The end-user browser forwards the SAML assertion to the Identity Awareness Gateway.

6. The Identity Awareness Gateway validates the SAML assertion and provides the end user with the requested service.

   In our example - `google.com` opens in the end-user browser.

Important - When you sign out from the Check Point service portal, it does **not** automatically sign out from the Identity Provider's session.

Basic SAML Configuration for Identity Awareness

1. **Configure the Identity Awareness Software Blade**

   a. Enable the Identity Awareness Software Blade (see *"Getting Started with Identity Awareness" on page 13*).

   b. Configure the Identity Awareness Captive Portal (see *"Configuring Browser-Based Authentication" on page 44*).

2. **Configure an External User Profile object**

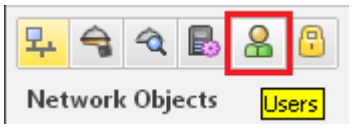
   External User Profile represents all the users authenticated by the Identity Provider.

   a. In SmartConsole, click **Manage & Settings** > **Blades**.

   b. In the **Mobile Access** section, click **Configure in SmartDashboard**.

      Legacy SmartDashboard opens.

   c. In the bottom left pane, click **Users**.



   d. In the bottom left pane, right click on an empty space below the last folder in the pane and select **New** > **External User Profile** > **Match all users**.

e. Configure the **External User Profile** properties:

i. On the **General Properties** page:

In the **External User Profile name** field, leave the default name **generic***.

In the **Expiration Date** field, set the applicable date.

ii. On the **Authentication** page:

From the **Authentication Scheme** drop-down list, select and configure the applicable option.

iii. On the **Location**, **Time**, and **Encryption** pages, configure other applicable settings.

iv. Click **OK**.

f. From the top toolbar, click **Update** (or press **Ctrl + S**).

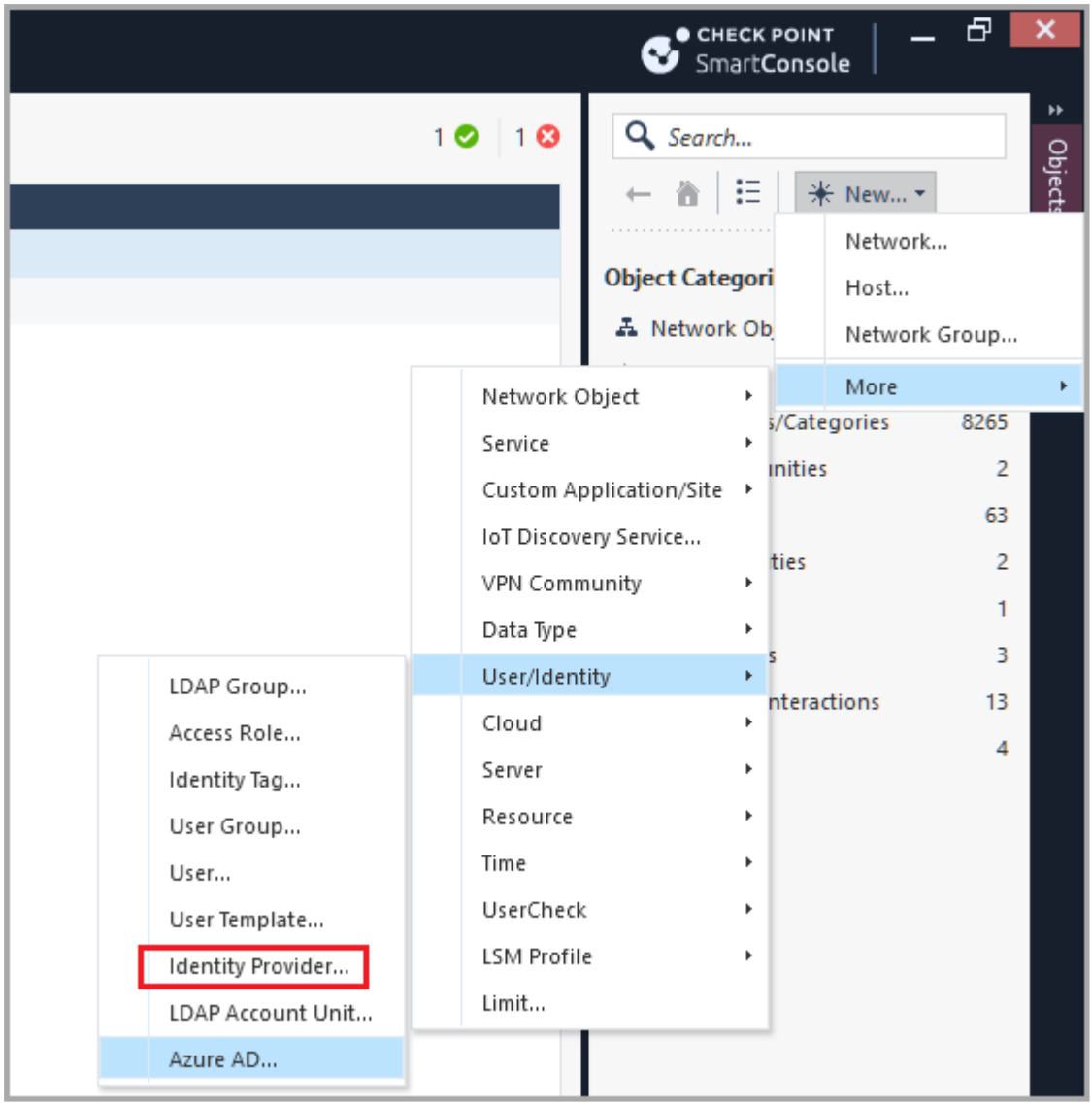
g. Close SmartDashboard.

h. In SmartConsole, install the Access Control Policy.

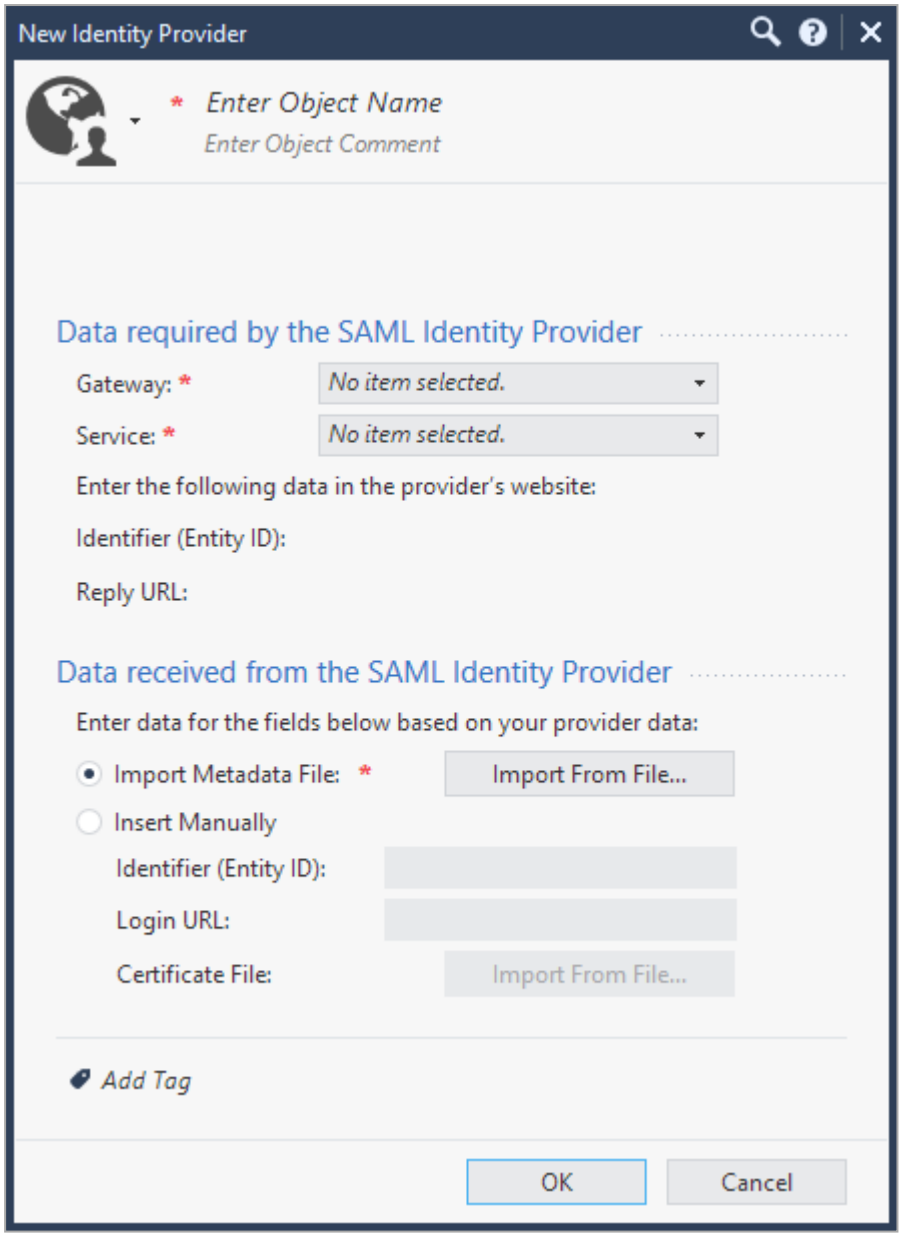
Note - It is not mandatory to install policy at the end of this step.

3. **Configure an Identity Provider object**

a. In SmartConsole, from the **Gateways & Servers** view click **New** > **More** > **User/Identity** > **Identity Provider**.



A **New Identity Provider** window opens:



b. In the **New Identity Provider** window, in the **Data required by the SAML Identity Provider** section, configure these settings:

   - In the **Gateway** field, select the Security Gateway, which needs to perform the SAML authentication.
   - In the **Service** field, select **Identity Awareness**.

   SmartConsole automatically generates the data in these fields based on the previous two fields:

   - **Identifier (Entity ID)** – This is a URL that uniquely identifies a service provider (the Security Gateway, in our case)
   - **Reply URL** – This is a URL, to which the SAML assertions are sent

c. Configure SAML Application on an Identity Provider website.

Important:
- Do **not** close the **New Identity Provider** window while you configure the SAML application in your Identity Provider's website. You continue the configuration later with the information you receive from the Identity Provider.
- Follow the Identity Provider's instructions.

- You must provide the values from the **New Identity Provider** window from the **Identifier (Entity ID)** and the **Reply URL** fields.

  Copy these values from SmartConsole and paste them in the corresponding fields on the Identity Provider's website.

  Note - The exact names of the target fields on the Identity Provider's website might differ between Identity Providers.

- Make sure to configure the Identity Provider to send the authenticated username in the email format (`alias@domain`).

- **Optional:** If you wish to receive the Identity Provider's groups, in which the user is defined, make sure to configure the Identity Provider to send the group names as values of the attribute called **group_attr**.

  Note - When the user logs in to Microsoft Entra ID PDP returns a username that is an email address, and no groups.
  You must replace the *userLoginAttr* with email:
  - Do this:
    i. Go to **Edit > network objects** and select the Gateway object.
    ii. Go to **realms_for_blades > identity_portal**, select *userLoginAttr* and replace it with email.
  - If you want PDP to return user groups, the Active Directory user must use the Azure username as an email address.

- Make sure that at the end of the configuration process you get this information from the Identity Provider:
  - **Entity ID** - a URL that uniquely identifies the application
  - **Login URL** - a URL to access the application
  - **Certificate** – for validation of the data exchanged between the Security Gateway and the Identity Provider

  Note - Some Identity Providers supply a metadata XML file, which contains this information.

d. In the **New Identity Provider** window, in the **Data received from the SAML Identity Provider** section, configure one of these settings:

   - Select **Import the Metadata File** to upload the metadata file supplied by the Identity Provider.
   - Select **Insert Manually** to paste manually the **Entity ID** and **Login URL** into the corresponding fields, and to upload the **Certificate File**. All these are supplied by the Identity Provider.

Note - Identity Provider object in SmartConsole does not support the import of RAW Certificate.

Important - If later you change the settings of the Browser-Based Authentication in the Identity Awareness Gateway object, then you must update the applicable settings in the SAML application on the Identity Provider's website.

4. **Configure the Identity Provider as an authentication method**

   To use the SAML Identity Provider object as an authentication method, you must configure the authentication settings for the Identity Awareness:

   a. In SmartConsole, click the **Gateways & Servers** panel.

   b. Open the Security Gateway object.

   c. From the left tree, click **Identity Awareness**.

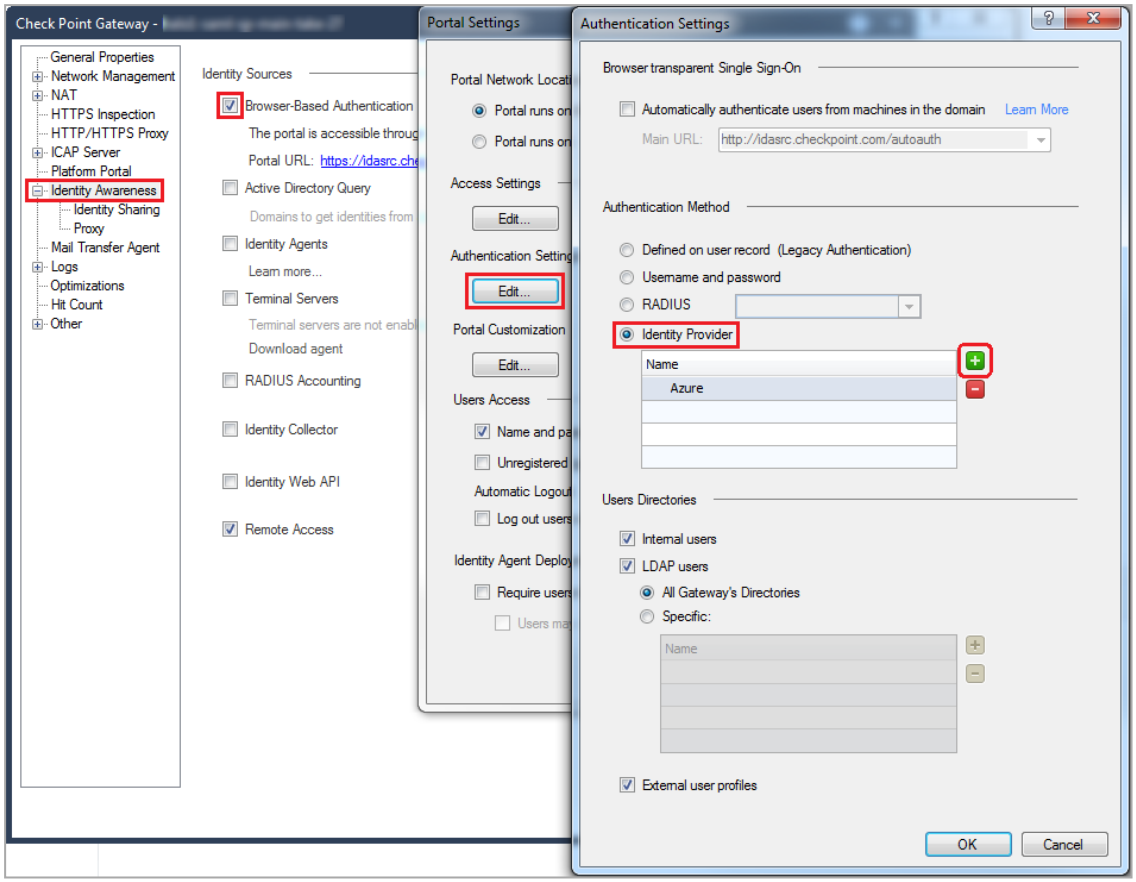
   d. Near the **Browser-Based Authentication**, click **Settings**.

   e. In the **Authentication Settings** section, click **Edit**.

   f. In the **Authentication Method** section, select **Identity Provider**.

g. Click the green **[+]** button and select the SAML **Identity Provider** object.

Example:



h. Click **OK**.

Notes:

- If you configure only one Identity Provider object, the end user is redirected to that Identity Provider's portal.
- If you configure more than one Identity Provider object, the end user is asked to choose the Identity Provider for authentication.

5. **Optional: Configure group authorization**

Part A - Configuring Identity Tags

For each group configured in your SAML application, you must create an equivalent Identity Tag object in SmartConsole.

The value of the Identity Tag must be identical to the value of the provided group or to the Object ID.

Note - If you use Microsoft Entra ID (formerly Azure AD), you must create the Identity Tag in SmartConsole by the Microsoft Entra ID Group Object ID and not by the User Group name:

a. Open your Microsoft Entra ID.
b. Go to the User Group you created in Azure.
c. Copy the Object ID and paste it in the **Identity Tag > External Identifier** field in SmartConsole.

For more information, see *"Using Identity Tags in Access Role Matching" on page 36*.

Part B - Configuring group authorization behavior

Important - In a Cluster, you must configure all the Cluster Members in the same way.

A Security Gateway can authorize groups in different ways.

Authorization can refer to two types of groups:

- Identity Provider groups - these are groups the Identity Provider sends
- Internal groups - these are groups received from User Directories configured in SmartConsole

Available options to configure the authorization behavior:

Option Name	Numerical Value	Authorization Behavior on Security Gateway
Only SAML Groups	0	Consider only Identity Provider groups. Ignore internal groups.
Prefer SAML Groups	1	This is the default. Prefer Identity Provider groups. If there are no external groups in the Identity Provider, use **Ignore SAML Groups** option.
Union with SAML Groups	2	Consider both internal groups and Identity Provider groups.
Ignore SAML Groups	3	Consider only internal groups. Ignore Identity Provider groups.

Note - This configuration is for each Realm.

You can view and change the authorization behavior on the Security Gateway.

Viewing the configured authorization behavior

You see the configured behavior in one of these ways:

- On the Identity Awareness Gateway / each Cluster Member, examine the applicable value in Check Point Registry in the Expert mode:

```
ckp_regedit -p SOFTWARE/Checkpoint/Ex_Groups "<Realm Name>"
```

- On the Identity Awareness Gateway / each Cluster Member (in the Expert mode or Gaia Clish):

```
pdp idp groups status
```

Configuring the authorization behavior

You can set the behavior in one of these ways:

- On the Identity Awareness Gateway / each Cluster Member, change the applicable value in Check Point Registry in the Expert mode:

```
ckp_regedit -a SOFTWARE/Checkpoint/Ex_Groups "<Realm Name>" -n {0 | 1 | 2 | 3}
```

- On the Identity Awareness Gateway / each Cluster Member (in the Expert mode or Gaia Clish):

```
pdp idp groups set {only | prefer | union | ignore}
```

Notes:

- Make sure SAML directory and the applicable User Directory can synchronize with each other.
- Make sure that the LDAP lookup type of the applicable realm is set to "`mail`".

Part C - Configuring an internal User Group "EXT_ID_<name>"

a. In SmartConsole top right corner, click the **Objects** panel.

b. Click **New** > **More** > **User/Identity** > **User Group**.

c. In the name field, enter:

EXT_ID_<Name_of_User_Group_in_Azure>

Example name: `EXT_ID_AzureAD_Users`

d. **Optional:** In the **Comment** field, enter the applicable text.

e. Do not add any users in this group object (leave it empty).

f. Click **OK**.

6. **Install the Access Control Policy**

   a. In SmartConsole, click **Install Policy**.

   b. Select the applicable policy.

   c. Select **Access Control**.

   d. Click **Install**.

Important - Before you use SAML configuration, make sure that your Security Policy allows access to the 3rd party Identity Provider web sites.

Advanced SAML Configuration for Identity Awareness

You can configure these advanced SAML features:

- Request Signing: Verifies authenticity of SAML requests.
- Assertion Decryption: Protects confidentiality of user attributes.
- Forced Re-authentication: Enables mandatory login for each session.

For configuration instructions, refer to sk182042.

Using Microsoft Entra ID for Authorization

By incorporating SAML for user authentication, you can leverage Microsoft Entra ID entities to control access to corporate resources.

Microsoft Entra ID is a Microsoft cloud-based identity and access management service that offers identity and access capabilities for applications that run in Microsoft Azure.

Best Practice:
To use Microsoft Entra ID, your Management Server and Security Gateways that work as PDPs must have an Internet access.

- If your Management Server does not have a direct access, configure a proxy server:
  1. From you browser, log in to the Gaia Portal.
  2. From the left tree, go to **System Management > Proxy**.
  3. Select the **Use proxy server** option and enter the applicable proxy server configuration.
  4. Click **OK**.
  5. Publish the SmartConsole session.

- If your Security Gateway that works as PDP does not have a direct access, configure a proxy server:
  1. In SmartConsole, open the **Global Properties**.
  2. From the left tree, click **Proxy**.
  3. Select the **Use proxy server** option and enter the applicable proxy server configuration.
  4. Click **OK**.
  5. Publish the SmartConsole session.

Configuring

This section describes the procedure for configuring Microsoft Entra ID.

The procedure has two parts. Each part consists of these steps:

- Part 1 - Configuration in Microsoft Azure Portal.
- Part 2 - Configuration in Check Point SmartConsole.

Configuration in Microsoft Azure Portal

Note - For more information about configuration on the Microsoft Azure portal, refer to Microsoft Azure documentation.

1. **Configuring Azure application**

   a. Log in to your Azure account in https://portal.azure.com/, click the username the top-right side, and make sure that the directory is correct.

   Note - You must have at least one user and one group defined.

b. Make specified user group(s).

   i. From the left-side menu, select **Microsoft Entra ID**.

   ii. Click **Users**.

   iii. In the **Overview** window, select the users from the list.

   iv. Click **Home**.

c. Select **Enterprise Applications**.

d. Click **New Application > Non-gallery application**.

e. In the **Add your own application** window, enter a name for your application (for example, *checkpoint*). Click **Add**.

f. In your application **Overview** window, click on your application and select **App registrations** option.

g. Click **Owned applications >*checkpoint***.

h. Copy and save these parameters:

   - **Application (client) ID**
   - **Directory (tenant) ID**

i. Go to **Certificates & Secrets > New client secret** and set these parameters:

   - **Description** - Enter a free-text description (for example, Check Point).
   - **Expires** - Set an applicable expiration date.

j. Click **Add**.

k. Copy and save the client secret.

   Note - You cannot retrieve this value after you perform a different operation or leave this blade.

2. **Configuring SAML as a Single Sign-On for your Azure application**

   a. Click on **Home** and select **Microsoft Entra ID** from the menu.

   b. Click on **Enterprise applications** and go to **All applications**.

   c. Select your application.

      The application **Overview** window opens.

   d. Click **Single Sign-On**.

   e. Select **SAML** as the Single Sign-On method.

f. In the **Set up Sign-On with SAML** window, go to the **User Attributes & Claims** section and click the pencil icon to edit the claims.

The **User Attributes & Claims** window opens.

g. In the **Required claim** section, click **Unique User Identifier (Name ID)**.

h. In the **Manage claim** window:

- **Attribute** option - Select.
- **Source Attribute** drop-down menu - Select **user.localuserprincipalname**.

i. Click **Save** to save the user claims, then close the window.

j. Back on the **SAML Signing Certificate** page, go to the **Federation Metadata XML** file and click **Download**.

The Federation Metadata XML is downloaded.

Note - Stay logged in to Azure and come back to it in the next steps.

3. **Registering your application**

a. Click **App Registrations > New registration**.

b. Click **Owned applications**.

c. Select your application and click **Register**.

d. Click **API permissions > Add a permission** and select these permissions:

- **Microsoft Graph**
- **Device.Read.All**
- **Group.Read.All**
- **User.Read.All**

e. Click **Add permissions > Configured permissions > Grant admin consent** for approval of your app API permissions. Click **Yes**.

Your application gets the granted permissions.

Configuration in Check Point SmartConsole

1. **Configuring Azure object**

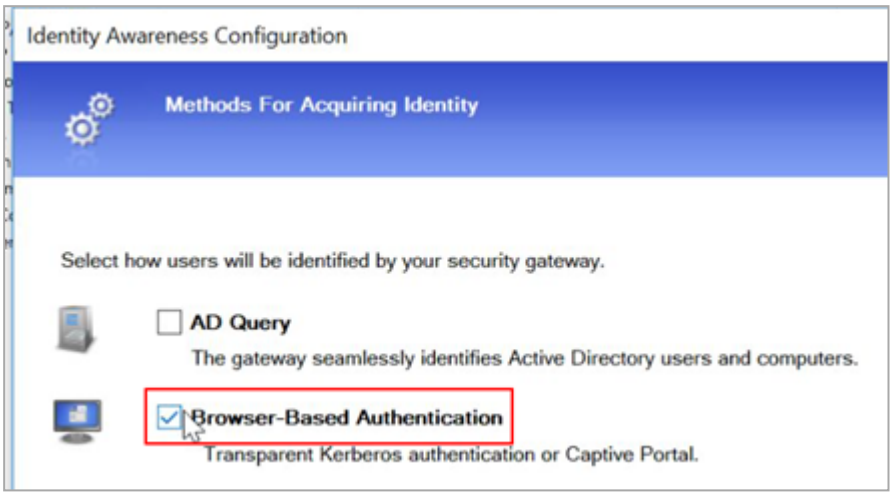
Use one of the following configuration options:

- **Configure the Microsoft Entra ID through the IDA wizard**

  a. In **SmartConsole**, open the Gateway and click **Identity Awareness**.

  b. On the **Identity Awareness Configuration** wizard, select only Browser-Based Authentication option.

  Example:



  c. Click **Next**.

  d. From the **Select Active Directory** drop-down menu, select **Create new Microsoft Entra ID**.

  e. Enter these settings that you created in *"Configuration in Microsoft Azure Portal" on page 193*:

  - **Name** - Enter a name for your application.
  - **Application ID field** - Enter the **Application ID** of the Service Principal in the UUID format `[xxxxxxx-xxxx-xxxx-xxxxxx]`.
  - **Application Key** - Enter the Client Secret created for the Service Principal.
  - **Directory ID** - Enter the Directory ID of the Service Principal in the UUID format `[xxxxxxx-xxxx-xxxx-xxxxxx]`.

    Important - Do not configure specified multiple Microsoft Entra ID objects with same Directory ID.

  f. Click **Test Connection**.

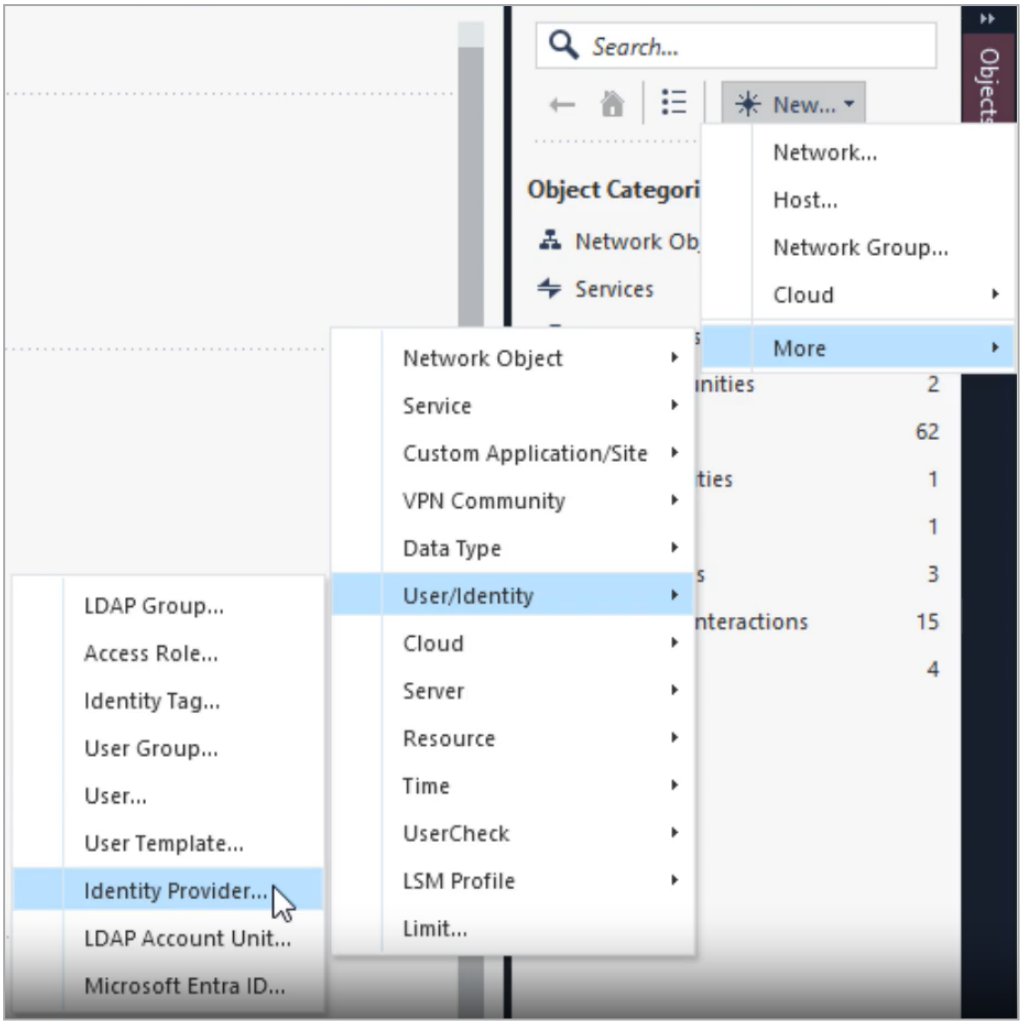
g. After the connection is active, click **Next > Next >Finish**.

   You can now select the new created Microsoft Entra ID from the **Users/Identities** menu.

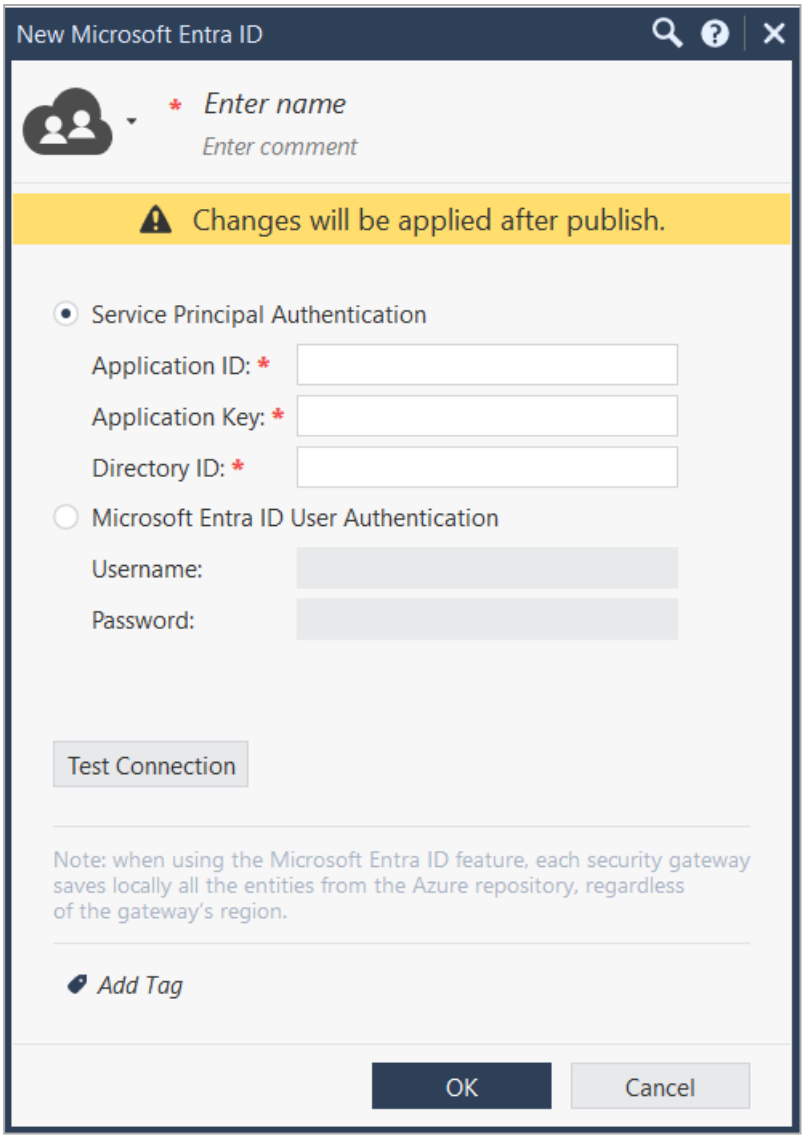
h. Publish the SmartConsole session.

- **Configure a new server on the Objects bar**

a. On Check Point SmartConsole, click **New > More > User/Identity > Microsoft Entra ID**.



A **New Microsoft Entra ID** window opens.



b. In the **New Microsoft Entra ID** window, in the **Service Principal Authentication** section, configure these settings that you created in *"Configuration in Microsoft Azure Portal" on page 193*:

   - **Name** - Enter a name for your application.
   - **Application ID field** - Enter the **Application ID** of the Service Principal in the UUID format `[xxxxxxx-xxxx-xxxx-xxxxxx]`.
   - **Application Key** - Enter the Client Secret created for the Service Principal.
   - **Directory ID** - Enter the Directory ID of the Service Principal in the UUID format `[xxxxxxx-xxxx-xxxx-xxxxxx]`.

c. Click **Test Connection**.

d. Publish the SmartConsole session.

2. **Creating the Access Role with the Azure directory**

    a. In the object tree, click **New> More > User/Identity > Access Role**.

    b. Click **[+]** to add a new Access Role.

    c. In the **New Access Role** window:

    - Enter a **Name** for the access.
    - Enter a **Comment** (optional).
    - Select a **Color** for the object (optional).

    d. In the **Users** pane, select one of these:

    - **Any user**.
    - **All identified users** - Includes all users identified by a supported authentication method (internal users, Active Directory users, or LDAP users).
    - **Specific users/groups** - You can select the Microsoft Entra ID and select users or groups of users from the list.

    e. Click **OK**.

    f. Publish the SmartConsole session.

    g. Use the created Azure Access Role to add the rules in the Access Control policy.

Best Practice - If you use Azure for the two of authentication and authorization, then Microsoft Entra ID performs authentication through the SAML protocol with the SAML Identity Provider.
To configure SAML for authentication, refer to *"SAML Identity Provider for Identity Awareness" on page 181*.

Advanced Identity Awareness Environment

Configure a Check Point Security Gateway with enabled Identity Awareness Software Blade for better security for your network environment and corporate data. This section describes environment configuration with Identity Awareness that we recommend.

Important:

- NAT between two Identity Awareness Security Gateways that share data with each other, is not supported.
- Perimeter Identity Awareness Security Gateway is the most standard environment. Configure the Security Gateway at the perimeter where it protects an access to the DMZ and the internal network. The perimeter Security Gateway in addition controls and inspects internal traffic going to the Internet. In this environment, create an identity-based Access Control Policy .
- Data Center protection - If you have a Data Center or server farm separately from the users' network, then protect the access to the servers with the Security Gateway. Configure the Security Gateway in front of the Data Center. The Security Gateway inspects all traffic. An identity-based Access Control Policy controls the access to resources and applications. Configure the Security Gateway in Bridge Mode to protect the Data Center without important changes to the current network infrastructure.
- Large-scale enterprise environment - In large networks, configure multiple Security Gateway. For example: configure a perimeter Firewall and multiple Data Centers. Install an identity-based policy on all Identity Awareness Security Gateway. The Identity Awareness Gateways share user and computer data of the whole environment.
- Network segregation - The Security Gateway helps you migrate or create internal network segregation. Identity Awareness lets you control access between different segments in the network with an identity-based policy. Configure the Security Gateway near to the network to prevent malware threats and access that is not approved to general resources in the global network.
- Distributed enterprise with branch offices - For an enterprise with remote branch offices connected to the headquarters with VPN, configure the Security Gateway at the remote branch offices. When you enable Identity Awareness on the branch office Security Gateway, users are authenticated before they get to internal resources. The branch office Security Gateway shares the identity data with other Security Gateway to prevent authentication that is not necessary.
- Wireless campus - Wireless networks have built-in security challenges. To give an access to wireless-enabled corporate devices and guests, configure Identity Awareness Security Gateway in front of the wireless switch. Install an Identity Awareness policy. The Security Gateway gives a guest access after authentication in the web Captive Portal, and then they inspect the traffic from WLAN users.

Advanced Configuration

There are more ways to configure an Identity Awareness Security Gateway:

- IP routing mode
- Transparent mode (Bridge Mode)

IP routing mode - This is a regular and standard method to configure Identity Awareness Gateways. Use this mode when you configure the Identity Awareness Security Gateway at the perimeter. In this case, the Identity Awareness Security Gateway behaves as an IP router that examines and forwards traffic between the internal interface and the external interface in both directions. Use different network subnets and ranges to locate both interfaces.

Transparent mode - Has an additional name "Bridge Mode". Use this configuration method to install the Identity Awareness Security Gateway as a Layer 2 device, rather than an IP router. The benefit of this method is that it is not necessary to make changes in the network infrastructure. It lets you configure the Identity Awareness Security Gateway inline in the same subnet. This configuration is mostly applicable when you must configure an Identity Awareness Gateway for network segregation and Data Center protection purposes.

Configuring a Test Environment

Best Practice - If you want to examine how Identity Awareness works in a Security Gateway, we recommend that you configure it in a simple environment. In this setup, you can examine all identity sources and create an identity-based policy.

We recommend to install these main components in the setup:

1. User host (Windows)
2. Check Point Security Gateway R75.20 or higher
3. Microsoft Windows server with Active Directory, DNS and IIS (Web resource)

Put the Security Gateway in front of the protected resource, the Windows server that runs IIS (web server). The user host computer gets an access to the protected resource through the Security Gateway.

Testing Identity Agents

Enable and configure Identity Agents, and configure Identity Agents self-provisioning through Captive Portal.

1. Open a browser and connect to the web resource.

   The resource redirects you to the Captive Portal.
2. Enter user credentials.
3. Install the client as prompted by the Captive Portal.
4. In the authentication window, enter the user credentials through the client.
5. Examine the connection.

Configuration Scenarios

You can configure Identity Awareness Gateway in different ways.

Perimeter Identity Awareness Gateway

Security Challenge

The Security Gateway at the perimeter behaves as a primary gate for all incoming and outgoing traffic to and from your corporate network. Users in internal networks get access to Internet resource and applications daily. Not all Internet applications and web sites are secure and some are restricted based on corporate policy. If you forbid all internal access, it affects productivity of employees that must have access as part of their daily work definition. You can control access to allowed applications with the Application Control blade. But you must have a more granular Access Control Policy for user and computer identity.

Use Access Roles to configure an Identity Awareness policy with Application Control to let an access to the applications on the Internet only to specified user groups.

Enable Identity Awareness on the perimeter Security Gateway.

Configuration Scenario

1. Configure the Security Gateway at the perimeter in Routing Mode. Create a specified external interface to the ISP (the Internet) and an internal interface points to the internal corporate network LAN.

   Optional: You can create a different specified internal interface that protects DMZ servers.
2. Make sure there are no NAT or Proxy servers between the gateway and your network.

Best Practice - We recommend to use the Proxy server that is in the DMZ network.

3. Make sure that the Security Gateway connects to the internal AD domain controllers.
4. Make sure that users have an access to the internal interface of the Security Gateway.
5. Configure the Application Control blade.

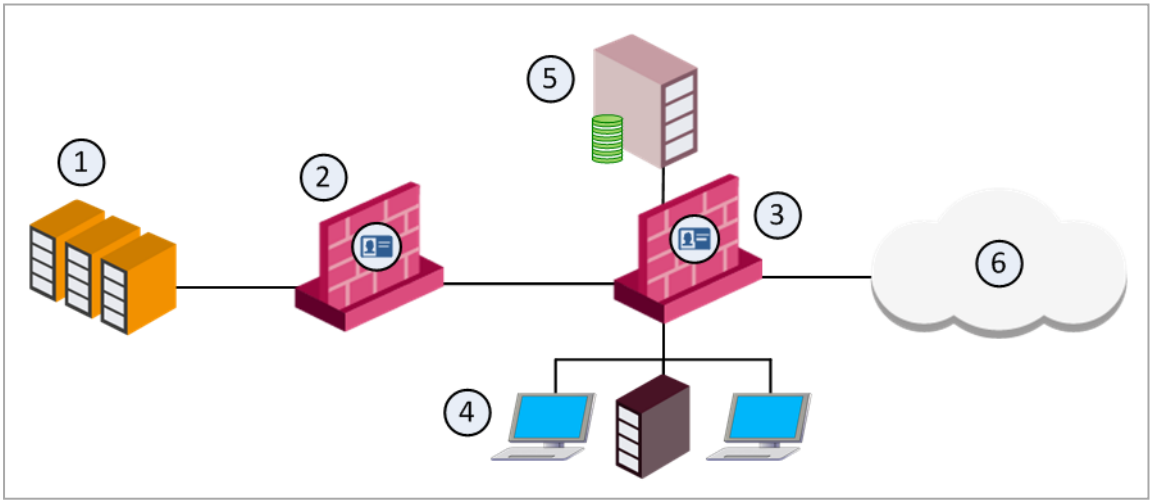
   See the *R82 Quantum Security Gateway Guide*.

Best Practice - If you have more than one perimeter Security Gateways that connect to the Internet, we recommend that you manage these Security Gateways with one Security Management Server and use SmartConsole to configure the applicable Security Policy.

Configuration Procedure

1. Enable Identity Awareness and select the applicable identity sources.
2. Create Access Roles functions that are based on Users and Computers. You can create multiple Access Roles that show different departments, user and computer groups and their location in the network.
3. Add the Access Roles to the source column of the applicable Firewall and application control policies.

This is a sample diagram for a small to medium corporate headquarters.



Item	Description
1	Corporate data center.
2	Identity Awareness Gateway protects the data center.

Item	Description
3	Perimeter Identity Awareness Gateway User IDs go to the gateway that protects the data center.
4	Internal network resources.
5	LDAP server (for example, Active Directory).
6	Internet.

Data Center Protection

Security Challenge

The Data Center contains sensitive corporate resources and information that you must safely protect from access that is not approved. You must in addition protect it from malware and viruses that can harm databases and steal corporate information. Only compliant users and computers must get access to the Data Center and especially to some applications.

Configuration Scenario

1. Configure the Security Gateway inline in front of the Date Center core switch.

   This procedure protects access to the Data Center from the LAN.

   Best Practice - We recommend that you configure the Security Gateway in the Bridge Mode to prevent all the changes in the network.

2. Specify minimum two interfaces on the Security Gateway and configure them to be internal or bridged.
3. Make sure that the Security Gateway has connectivity to the Active Directory and all applicable internal domain controllers in the network (LAN).
4. Make sure that users from the LAN can connect to the Data Center through the Security Gateway with an "Any Any Any Accept" policy.
5. Make sure that you do not have a proxy or NAT device between the Security Gateway and users or the LAN.

Configuration Procedure

1. Enable Identity Awareness on the Security Gateway and select identity sources.
2. Create Access Roles for users and apply the Access Roles to applicable Access Control Policy rules.

Large Scale Enterprise Environment

Security Challenge

In complex large-scale enterprise networks, you must control access from the local network to the Internet and to multiple Data Center resources. The Data Center contains sensitive corporate resources and information that must be securely protected from unauthorized access. Grant access only to policy-compliant users and computers. Protect your network and Data Center from malware, bots, and viruses.

Users in the internal networks access Internet resources and applications daily. Not all Internet applications and web sites are secure, and some are restricted by the corporate policy. If you block all internal access, it affects productivity of employees who must have access in the context of their daily work definition. You can control access to the allowed applications with the Application Control blade. If you require a granular Access Control Policy works because of user and computer identity, use Access Roles with Application Control.

Configuration Scenario

1. Configure or use current Security Gateway at the perimeter and in front of the Data Center.
2. Install the Security Gateway at the perimeter in routing mode, and use at least one external interface to the Internet and one to the internal network (make it an internal interface).

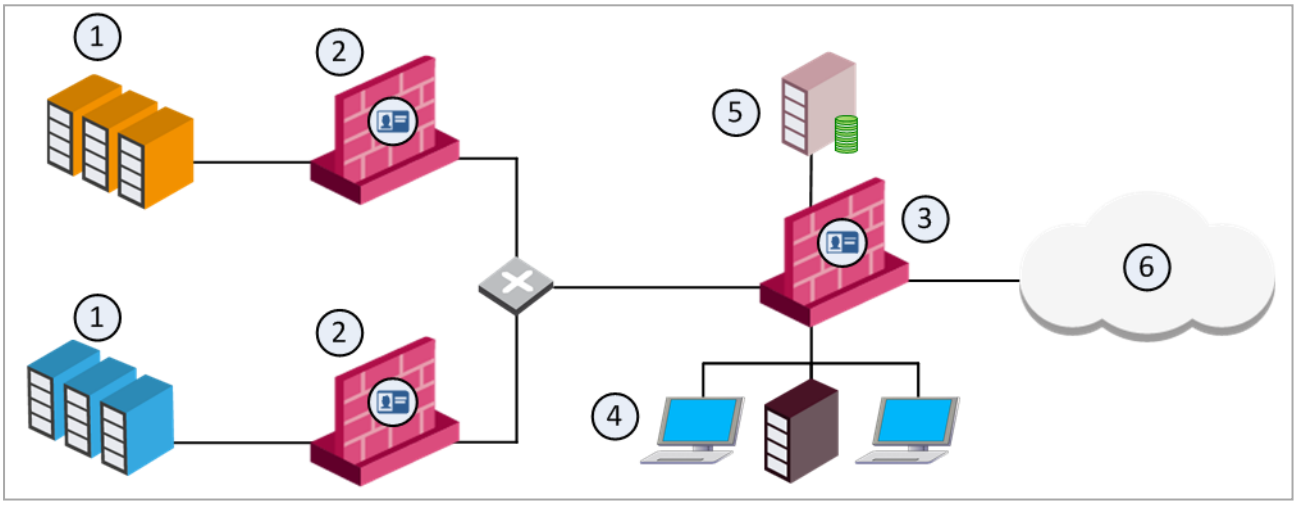
   Best Practice -We recommend that you configure the Security Gateway as an inline device in front of the Data Center in Bridge Mode to avoid network changes.
3. Make sure that all Security Gateway in the Data Centers and perimeter can communicate directly with each other.

   Best Practice - We recommend that you manage the Security Gateway from one Security Management Server and SmartConsole.
4. Make sure that there is connectivity from each Security Gateway to the Active Directory internal domain controllers.
5. Make sure that in an "Any Any Any Accept" Policy, users from the LAN can connect to the applicable resources.
6. Make sure there are no NAT or Proxy servers between the gateway and your network.

   Best Practice - We recommend that you put your Proxy server in the DMZ network.

Configuration Procedure

1. Enable Identity Awareness on the Security Gateway.
2. Select the identity source method for each Security Gateway, at the perimeter and at the Data Center.
3. Create Access Roles for users, and apply Access Roles to the applicable Firewall security rules.
4. Add Access Roles to the Policy.
5. On the **Gateway Properties > Identity Awareness** tab, select **Share local identities with other gateways**.
6. Install the Policy on the perimeter Security Gateway.



Item	Description
1	Corporate data centers.
2	Identity Awareness Gateway protects the data center.
3	Perimeter Identity Awareness Gateway. User IDs go to the gateways that protect the data centers.
4	Internal network resources.
5	LDAP server (for example Active Directory).
6	Internet.

Best Practice:

- **AD Query Recommended Configuration:**
  When you enable AD Query to get user and computer identity, we recommend that you enable the feature on all Security Gateway that participate in the network environment. All Security Gateway should have the Active Directory domain defined with the list of all applicable domain controllers in the internal network.
- **Identity Agents Recommended Configuration:**
  - If you use Identity Agents for a User Endpoint Computer to authenticate users and computers, you must select the Security Gateway to maintain Identity Agents.
  - For a single Data Center and perimeter Security Gateway, we recommend you to configure Identity Agents forthat connect to a single Security Gateway. Then the Security Gateway gets the identity and shares it with the other Security Gateways in the network. Select a high capacity / performance Security Gateway that in addition can behave as an authentication server, and configure this Security Gateway's IP / DNS on the Identity Agents (for more information, see *"Identity Agents for a User Endpoint Computer" on page 22*).
  - For complex environments with many Data Centers, with more than one Security Gateways that protect different Data Centers and the perimeter, we recommend that you balance Identity Agents authentication through different Security Gateway. You can configure a list of Security Gateways in the Identity Agent settings, where the Identity Agent connects to different Security Gateways. This provides load balancing across the Security Gateways. All Security Gateways share between them the identities learned from the agents in the network.

To make a specified list of Security Gateways that share between them identity information:

1. Open **Gateway Properties > Identity Awareness**.
2. Select **Get identities from other gateways**.
3. Select the Security Gateway with the identities.

Network Segregation

Security Challenge

Networks consist of different network segments and subnets where your internal users reside. Users that connect to the network can potentially spread viruses and malware across the network. It can infect other computers and servers on the network. Your purpose:

- Make sure that only compliant users and computers pass and connect across multiple network segments.
- Authenticate users who connect to the servers and to the Internet.

Best Practice - We recommend that you configure Security Gateway close to the access networks before the core switch.

- Access between the segments is controlled by the Security Gateway.
- Access between the LAN and Data Center is controlled by the Security Gateway.
- Access between the LAN and the Internet is controlled by the Security Gateway either at each segment or at the perimeter Security Gateway.

Best Practice - We recommend that you configure the Security Gateway in Bridge Mode to avoid network and routing changes.

- Each Security Gateway of a particular segment authenticates users with the selected method.
- Each Security Gateway of a particular segment authenticates users with the selected method.

Configuration

1. Configure Security Gateway in each segment in Bridge Mode.
2. Make sure that there is no proxy or NAT device between the Security Gateway and the LAN.
3. Make sure that the Security Gateway can communicate with the Active Directory domain controller configured in each segment (replicated domain controllers).

   If there is a general domain controller that serves all users across the segments, make sure that all Security Gateway can connect to this domain controller.
4. Enable Identity Awareness on each Security Gateway and select an appropriate identity source method.
5. In the Identity Awareness tab, clear the **Share local identities with other gateways** option.

   If you want to share identities with one Security Gateway, for example, the perimeter Security Gateway, keep this option selected and disable **Get identities from other gateways** in the segment Security Gateway. Then go to the perimeter Security Gateway and select **Get identities from other gateways**.
6. If you want to use Identity Agents, then make the particular Security Gateway DNS/IP in the agent Security Gateway configuration per access segment.

Distributed Enterprise with Branch Offices

Security Challenge

Distributed enterprises have a potential risk of malware and viruses that go from remote branch offices over VPN links to the corporate internal networks.

In addition, you must provide authorized access to users who come from remote branch offices and request an access to the Data Center and the Internet.

Configuration Scenario

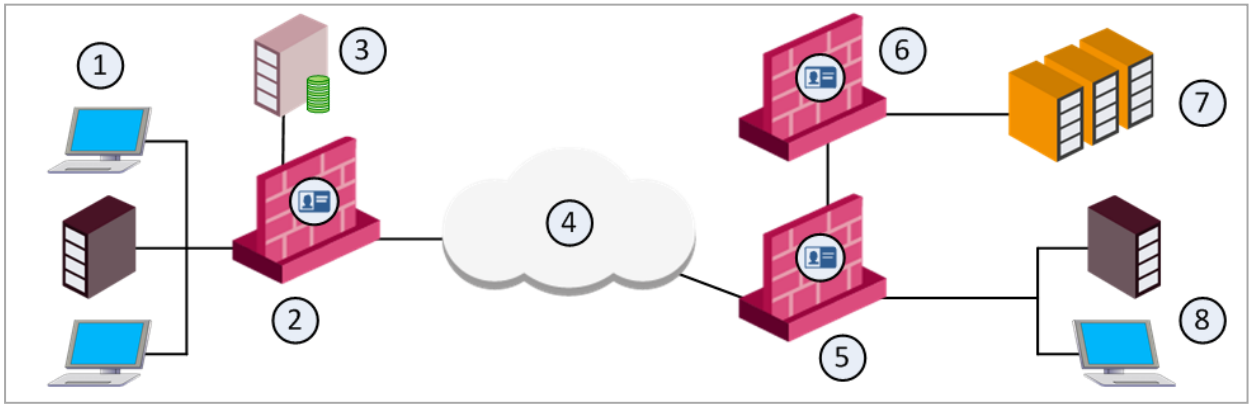
Best Practice - We recommend that you configure Security Gateway at the remote branch offices and at headquarters in front of the Data Center and at the perimeter.

- At remote branch offices, you can configure low capacity Security Gateway because of a relatively low number of users.

  You configure the remote branch Security Gateway in IP Routing Mode and establish a VPN link to the corporate Security Gateway. The remote branch Security Gateways now works as a perimeter Firewall and VPN gateway.

  Best Practice - At the corporate headquarters, we recommend that you configure Data Center Security Gateway to protect access to Data Center resources and applications, and to a perimeter Security Gateway. You can install the Data Center Security Gateway in Bridge Mode to prevent changes to the current network.

- The local branch office Security Gateway identifies users from the branch office, learns their identities, and then connects to the corporate network over VPN.
- The branch office Security Gateway shares these user identities with the headquarters' internal and perimeter Security Gateway. When a user from a branch office attempts to connect to the Data Center, the Security Gateway identifies this user at the headquarters Data Center without the need for additional authentication.



Item	Description
1	Internal network resources - branch office
2	Branch Identity Awareness Gateway User IDs go to the corporate gateways
3	LDAP server (for example Active Directory)
4	Internet
5	Perimeter corporate Identity Awareness Gateway
6	Identity Awareness Gateway that protects the data center
7	Corporate data center
8	Internal network resources - corporate office

Configuration

1. Select a Security Gateway in accordance with the performance guideline for your remote branch offices.
2. Configure the Security Gateway at the branch offices in Routing Mode. Make a specified VPN site-to-site if necessary.
3. Configure Security Gateway inline at the Data Center. We recommend to use Bridge Mode.
4. Configure a Security Gateway at the perimeter that protects the internal network in Routing Mode. This perimeter Security Gateway can serve as a VPN Security Gateway for branch offices.

   Best Practice
   - If you have Active Directory domain controllers replicated across your branch offices, make sure that local Security Gateway can connect to the domain controller.
   - If you do not have a local domain controller, make sure that the Security Gateway has an access to the headquarters' internal domain controller over VPN.
5. Enable Identity Awareness and select the appropriate methods to get identity.
6. Create an Access Role and apply the roles in the Security Policy on the branch office Security Gateway, perimeter and Data Center Security Gateway.
7. Share identities between the branch offices with the headquarters and Data Center Security Gateway:

a. Go to the Identity Awareness tab.

b. Select **Get identities from other gateways** and **Share local identities with other gateways**.

Best Practice
We recommend these configurations:

- AD Query Configuration:
  If you use AD Query to authenticate users from the local and branch offices, we recommend you to configure only a local domain controller list per site in the applicable Security Gateway.
  For example, if you have a branch office Security Gateway and a Data Center Security Gateway, enable AD Query on all Security Gateways:
  1. On the branch office Security Gateway, select the Active Directory domain controllers replications installed in the branch office only.
  2. On the Data Center Security Gateway, configure a list of domain controllers installed in the internal headquarters network.

  It is not necessary to configure all domain controllers available in the network, because branch and internal Security Gateways share the identity information between themselves as applicable.
- Identity Agents Configuration:
  If you use Identity Agents, we recommend you to configure the local branch office Security Gateway DNS/IP on the agent. The agents connect to the local Security Gateway, then they authenticate the user and share the identities with the internal headquarters Security Gateway.

Wireless Campus

Security Challenge

You use wireless networks to grant access to employees that use Wi-Fi enabled devices, to guests, and to contractors. Guests and contractors in some cases cannot use the corporate wired network connection and must connect through WLAN. Guests and contractors have no permission to install other endpoint agents on their devices.

In addition, mobile devices such as smartphones intensively use wireless access. You can install agents in these devices.

These devices are not part of the Active Directory domain. Wireless networks do not give an applicable level of security in terms of network access.

Configuration Scenario

1. Configure the Security Gateway in Bridge Mode in front of the Wireless Switch.
2. Make sure that the Security Gateway gets an access to the Internet or other necessary resources in the network.
3. Make sure that the Security Gateway connects to the authentication server, such as Active Directory or RADIUS.
4. Make sure that the Security Gateway and the WLAN network have no NAT or proxy device between them.

Configuration Procedure

1. Enable Identity Awareness on the Security Gateway.
2. Select Browser-Based Authentication as an identity source.
3. In the Gateway properties, register your guests:
   a. Go to Identity Awareness tab.
   b. In the **Browser-Based Authentication Settings**, select **Unregistered guests login**.
   c. In **Settings**, select the fields for your guests to enter their credentials.
4. Select **Log out users when they close the portal browser**.

Dedicated Identity Acquisition Security Gateway

Security Challenge

You have more than one Security Gateways that protect the Data Center or Internet access where access depends on identity acquisition. The Security Gateways run different blades and deal with heavy traffic inspection.

To prevent an impact on performance of the Security Gateways in terms of user identity acquisition and authentication, it is possible to offload this functionality to a separate Security Gateway.

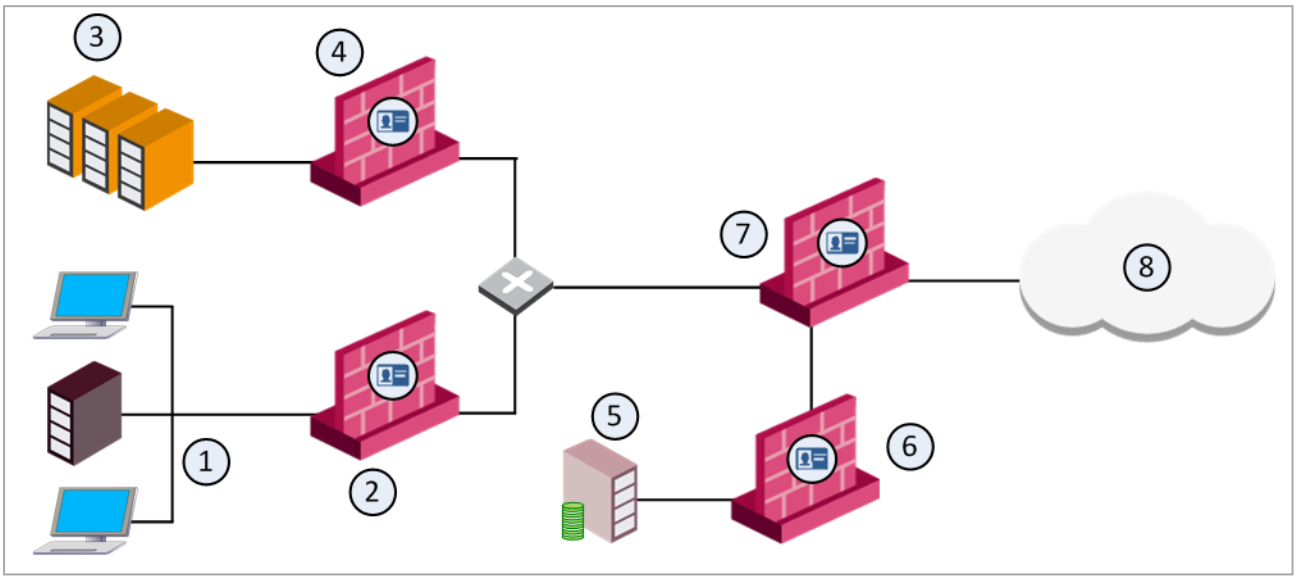
The dedicated Security Gateway:

- Gets user identity.
- Authenticates users.
- Shares learned identities with all Security Gateways in the network.

Configuration Scenario

You select an applicable appliance to be the dedicated Identity Awareness Security Gateway. All users authenticate with this Security Gateway.

If you enable AD Query, the dedicated Security Gateway communicates with all Active Directory domain controllers over WMI.



Item	Description
1	Internal network resources.
2	Identity Awareness Gateway that protects the internal network. User IDs go to the corporate gateways.
3	Corporate data center.
4	Identity Awareness Gateway that protects the data center.
5	LDAP server (for example Active Directory).
6	Dedicated Identity Awareness Security Gateway.
7	Perimeter corporate Identity Awareness Gateway.
8	Internet.

Configuration Procedure

1. On the dedicated identity acquisition Security Gateway, enable the Identity Awareness feature and select the identity method.

2. On the Security Gateway, enable Identity Awareness and select **Get identities from other gateways** and **Share local identities with other gateways**.

Identity Cache Mode for Identity Sharing Protocols

Overview

Identity Awareness operates with a default setting that adheres to a stringent approach to handle acute error flows.

This involves implementing the "prefer to delete" principle, which leads to the widespread deletion of identities in specific error scenarios.

- Disconnection from the PDP for longer than 10 minutes.
  - When a PDP (Policy Decision Point) or PEP (Policy Enforcement Point) becomes disconnected, all the identities it has learned are deleted.
  - When information is shared between PDP Security Gateways through an Identity Broker, any deletions made should be efficiently communicated and reflected in the downstream layers of Identity Broker Subscribers.

    This ensures a synchronized and accurate data state throughout the entire identity management ecosystem.
- If the PDP encounters a failure and reboots, there is a risk that it might synchronize an empty database with its peer systems.

The outcome of the behavior described above:

- No Identity-based enforcement, and connectivity is broken.
- Performance impact as a result of running and propagating the massive identity deletion logic.
- Lack of resiliency, even in cases where the environment was designed to have alternative identity propagation paths.
- In large scale environments, it may take hours until the system is fully recovered.

Identity Awareness Gateway R82 and higher uses the Identity Cache Mode for Identity Sharing protocols.

Important - In R82 and higher, the Identity Cache Mode is **enabled** by default with a cache duration of 1 hour.

The Identity Cache Mode follows the "prefer to keep" principle, enabling Identity Awareness to regain stability without causing the aforementioned disruptions.

This approach prioritizes maintaining system integrity while addressing the issues highlighted earlier.

- Instead of conducting extensive deletions, the relevant identities are kept in the database.
  - PDP-to-PEP sharing - By default, 24 hours.
  - PDP-to-PDP sharing - By default, 1 hour (configurable).
- Allows identity propagation from alternative paths to overrun existing information at all times.
  - Conciliation decision for the existing relevant Identity Sessions is "overwrite".
- Upon the restoration of connectivity, assuming that the Identity Session has not been overwritten, the pertinent Identity Sessions undergo a "refresh" process, reverting to their initial state and logic.

Upgrade from the R81.20 Jumbo Hotfix Accumulator to R82

The Identity Cache Mode feature is available in the R81.20 Jumbo Hotfix Accumulator, Take 70 and higher.

In the R81.20 Jumbo Hotfix Accumulator, this feature is disabled by default and has a different default timeout for PDP-to-PDP sharing (24 hours).

During an upgrade to R82, the previous configuration is preserved.

Viewing the Current Status of the Identity Cache Mode

Procedure

1. Connect to the command line on the Security Gateway / each Cluster Member / Scalable Platform Security Group.
2. Log in to the Expert mode.
3. In the VSNext / Traditional VSX mode, go to the context of the applicable Virtual Gateway / Legacy Virtual System:

   ```
   vsenv <VS ID>
   ```

4. Examine the current Identity Cache Mode status:

   - To see the status for the PDP-to-PDP sharing protocol (Identity Broker), run:

     ```
     pdp broker identity_cache_mode status
     ```

   - To see the status for the PDP-to-PEP sharing protocol, run:

     ```
     pep control identity_cache_mode status
     ```

   Possible outputs:

   - "`Identity Cache Mode is enabled`" (this is the default)
   - "`Identity Cache Mode is disabled`"

Configuring the Identity Cache Mode on All Security Gateways

The default configuration for all Identity Awareness Gateways managed by a Security Management Server / Domain Management Server:

1. The Identity Cache Mode is enabled.
2. The timeout for the PDP-to-PDP sharing protocol (Identity Broker) is 60 minutes.

You can change the global configuration in SmartConsole or with the Management API.

To configure the global Identity Cache Mode settings in SmartConsole for all managed Identity Awareness Gateways

1. Connect with SmartConsole to the Security Management Server / Domain Management Server.
2. In the top left corner, click Menu > **Global properties**.
3. In the left tree, click **Identity Awareness**.
4. In the **Cache Duration** section:
   - To disable the Identity Cache Mode, clear the checkbox **In case of connectivity loss, extend identity cache for up to [ ] minutes**.

     Warning - Do not disable the Identity Cache Mode unless Check Point Support explicitly asked you to do so.
   - To enable the Identity Cache Mode again, select the checkbox **In case of connectivity loss, extend identity cache for up to [ ] minutes**.
   - To change the timeout for the PDP-to-PDP sharing protocol (Identity Broker), enter the required value.
5. Click **OK**.
6. Install the Access Control Policy on all Identity Awareness Gateways.
7. On each Identity Awareness Gateway, examine the current Identity Cache Mode status.

   Run these commands in the Expert mode.

- To see the status for the PDP-to-PDP sharing protocol (Identity Broker), run:

```
pdp broker identity_cache_mode status
```

- To see the status for the PDP-to-PEP sharing protocol, run:

```
pep control identity_cache_mode status
```

To configure the global Identity Cache Mode settings with Management API for all managed Identity Awareness Gateways

Note - See one of these Management API references (chapter "**Manage & Settings**" > section "**Global Properties**"):

- The online *Check Point Management API Reference*.
- The local *Management API Reference* (first, you must follow sk174606 to allow access to this local Management API reference):

```
https://<IP Address or Gaia Management
Interface>/api_docs/#introduction
```

1. Examine the current Identity Awareness global properties:

```
mgmt_cli show global-properties
```

Example (default output):

```
[Expert@MyMgmt:0]# mgmt_cli show global-properties
Username: ******
Password: ************

... ... ...

identity-awareness:
  cache-mode: true
  cache-mode-duration: 60

[Expert@MyMgmt:0]#
```

2. Configure the required Identity Cache Mode global status:

```
mgmt_cli set global-properties identity-awareness.cache-mode
{true | false}
```

Where:

- `true` - Enables the Identity Cache Mode globally
- `false` - Disables the Identity Cache Mode globally

  Warning - Do not disable the Identity Cache Mode unless Check Point Support explicitly asked you to do so.

3. Configure the required Identity Cache Mode global timeout (in minutes) for the PDP-to-PDP sharing protocol (Identity Broker):

   ```
   mgmt_cli set global-properties identity-awareness.cache-mode-duration <1-2880>
   ```

4. Install the Access Control policy on all Identity Awareness Gateways:

   ```
   mgmt_cli install-policy <parameters>
   ```

Configuring the Identity Cache Mode on Specific Security Gateways

You can override the global Identity Cache Mode configuration on each managed Security Gateway / Cluster / Scalable Platform Security Group / VSNext Virtual Gateway / Traditional VSX Virtual System.

Important:

- To override the global configuration, you must use the Management API to configure the applicable Identity Awareness Gateway object.
- After you change the configuration of an Identity Awareness Gateway object, you must install the Access Control Policy on that object.

Explanation

Note - See one of these Management API references:

- The online *Check Point Management API Reference*.
- The local *Management API Reference* (first, you must follow sk174606 to allow access to this local Management API reference):

```
https://<IP Address or Gaia Management Interface>/api_docs/#introduction
```

Override Scenario	Scenario Description	Required API Parameter in the Identity Awareness Gateway Object
Override the global status	■ The Identity Cache Mode is enabled globally (this is the default). It is necessary to disable the Identity Cache Mode on an individual Identity Awareness Gateway. ■ The Identity Cache Mode is disabled globally. It is necessary to enable the Identity Cache Mode on an individual Identity Awareness Gateway.	`identity-awareness-settings.identity-sharing-settings.cache-mode.override-profile true`

Override Scenario	Scenario Description	Required API Parameter in the Identity Awareness Gateway Object
Restore the global status	■ The Identity Cache Mode is enabled globally (this is the default). Previously, you disabled the Identity Cache Mode on an individual Identity Awareness Gateway. It is now necessary to enable the Identity Cache Mode again on that individual Identity Awareness Gateway. ■ The Identity Cache Mode is disabled globally. Previously, you enabled the Identity Cache Mode on an individual Identity Awareness Gateway. It is now necessary to disable the Identity Cache Mode again on that individual Identity Awareness Gateway.	`identity-awareness-settings.identity-sharing-settings.cache-mode.override-profile false`

Override Scenario	Scenario Description	Required API Parameter in the Identity Awareness Gateway Object
Override the timeout for the PDP to-PDP sharing protocol (Identity Broker)	■ The Identity Cache Mode is enabled globally (this is the default). It is necessary to configure a different timeout value on a specific Identity Awareness Gateway. ■ The Identity Cache Mode is enabled on a specific Identity Awareness Gateway. It is necessary to configure a different timeout value.	`identity-awareness-settings.identity-sharing-settings.cache-mode-duration.value <Timeout in Minutes>`

To override the Identity Cache Mode global status on a specific Identity Awareness Gateway

- Example for a Simple Gateway object:

```
mgmt_cli set simple-gateway name <Name of Object> identity-awareness-settings.identity-sharing-settings.cache-mode.override-profile true
```

- Example for a Cluster object:

```
mgmt_cli set simple-cluster name <Name of Object> identity-awareness-settings.identity-sharing-settings.cache-mode.override-profile true
```

- Example for a Traditional VSX Virtual System object:

```
mgmt_cli set legacy-virtual-system name <Name of Object> identity-awareness-settings.identity-sharing-settings.cache-mode.override-profile true
```

To restore the Identity Cache Mode global status and timeout for PDP to-PDP sharing on a specific Identity Awareness Gateway

- Example for a Simple Gateway object:

```
mgmt_cli set simple-gateway name <Name of Object> identity-
awareness-settings.identity-sharing-settings.cache-
mode.override-profile false
```

- Example for a Cluster object:

```
mgmt_cli set simple-cluster name <Name of Object> identity-
awareness-settings.identity-sharing-settings.cache-
mode.override-profile false
```

- Example for a Traditional VSX Virtual System object:

```
mgmt_cli set legacy-virtual-system name <Name of Object>
identity-awareness-settings.identity-sharing-settings.cache-
mode.override-profile false
```

To override the Identity Cache Mode global timeout for PDP to-PDP sharing on a specific Identity Awareness Gateway

Note - This timeout override is supported only if you override the global Identity Cache Mode configuration on the Identity Awareness Gateway.

- Example for a Simple Gateway object:

```
mgmt_cli set simple-gateway name <Name of Object> identity-
awareness-settings.identity-sharing-settings.cache-
mode.override-profile true identity-awareness-
settings.identity-sharing-settings.cache-mode.value <Timeout
in Minutes>
```

- Example for a Cluster object:

```
mgmt_cli set simple-cluster name <Name of Object> identity-
awareness-settings.identity-sharing-settings.cache-
mode.override-profile true identity-awareness-
settings.identity-sharing-settings.cache-mode.value <Timeout
in Minutes>
```

- Example for a Traditional VSX Virtual System object:

```
mgmt_cli set legacy-virtual-system name <Name of Object>
identity-awareness-settings.identity-sharing-settings.cache-
mode.override-profile true identity-awareness-
settings.identity-sharing-settings.cache-mode.value <Timeout
in Minutes>
```

Advanced Browser-Based Authentication Configuration

This section describes how to configure and work with more options for Browser-Based Authentication.

Customizing Text Strings

You can customize some aspects of the web interface. This includes changes to the text strings shown on the Captive Portal Network Login page. You can make changes to the default English language or edit files to show text strings in other languages.

You can change English text that is shown on the Captive Portal to different English text through the SmartConsole. The changes are saved in the database and can be upgraded.

To configure other languages to show text strings in a specified language on the Captive Portal, you must configure language files. These language files are saved on the Security Gateway and cannot be upgraded. If you upgrade the Security Gateway, these files must be configured again.

To help you understand what each string ID means, you can set the Captive Portal to String ID Help Mode. This mode lets you view the string IDs used for the text captions.

Setting Captive Portal to String ID Help Mode

1. On the Security Gateway, open the file:

   `/opt/CPNacPortal/phpincs/utils/L10N.php`

2. Replace the line `// return $stringID;` with `return $stringID;` (delete the two backslashes before the text `return $stringID`).

3. Reload the Captive Portal in your web browser.

   The Captive Portal opens showing the string IDs.

4. To revert to regular viewing mode, open the file `L10N.php` and put backslashes before the text `return #stringID`.

Changing Portal Text in SmartConsole

1. In SmartConsole, go to **Menu > Global properties**.
2. In the left navigation tree, click **Advanced** > **Configure**.
3. Go to **Identity Awareness** > **Portal Texts**.
4. Delete the word `DEFAULT` and type the new English text in the necessary field.

5. Click **OK**.
6. Install the policy.

Adding a New Language

You can configure the Captive Portal to show the Network Login pages in different languages. After you set the language selection list, users can choose the language they prefer to log in with from a list at the bottom of the page.

To configure a language for Captive Portal you must do these operations:

1. **Edit the language array for the new language locale**

   The supported language file contains entries for languages that you can see in the list on the Captive Portal page.

   By default, English is the only language entry in the list. It has a corresponding language file. For each new language, you must create an entry in the supported languages file and create a new language file.

   Creating a new language

   Add an entry to the supported languages file:

   a. Open the file:

      `/opt/CPNacPortal/phpincs/conf/L10N/supportedLanguages.php`

   b. In the `$arLanguages` array, create a new locale entry with the syntax: `"xx_XX" => "XName"`.

      For example: "de_DE" => "German".

   Disabling a language

   Comment out the line of the specific language or delete the line.

2. **Create New Language Files**

   Use the English language file as a template to create new language files. Then translate the strings in the new language file.

   To create new language files, use the English language file (`portal_en_US.php`) as a template and refer to it for the source language. The file contains the message strings. It is not necessary to translate all strings, but you must include all strings in the new language file.

When you translate a string, make sure that the string's length is almost the same in size as the initial English string. This is important to prevent breaks in the page layout. If this is not possible, consult with technical support.

You cannot use HTML special character sequences such as `  / < / &gt` in the translated strings.

Creating a new language file

a. Make a copy of the English language file:

   `/opt/CPNacPortal/phpincs/conf/L10N/portal_en_US.php`

b. Rename it to the new language. Use the syntax `portal_xx_XX.php.`

   For example, `portal_de_DE.php`

c. Translate the strings in the new language file.

d. Make sure that the read permissions for the new language file are the same as those for the original language file. Run this command to set the permissions for read and write:
   `chmod 666 <file name>`.

3. **Save New language files**

   You must save the language file with UTF-8 encoding.

Saving a file with UTF-8 encoding

a. Use Notepad, Microsoft Word or a different editor to save the file with UTF-8 encoding. When you use Microsoft Word, save the file as a '.txt' file with UTF-8 as the encoding method and rename it to `portal_xx_XX.php`. For example: `portal_de_DE.php`.

b. Move the file to `/opt/CPNacPortal/phpincs/conf/L10N` if it is not already there.

4. **Set the language selection list to show on the Network Login page**

   When you only use the English language, the language selection list does not show at the bottom of the Captive Portal Network Login page. When you configure additional languages, you must show the language selection list on the Network Login page. Captive Portal users can then select the language, with which to log in.

Seeing the language list on the Network Login page

a. On the Security Gateway, open the file:

`/opt/CPNacPortal/phpincs/view/html/Authentication.php`

b. Back up the file (for possible future revert).

c. In `<label for="language_selection">`, remove the lines that start with `<?PHP /*` and end with `*/ ?>`

The lines to remove are in the square:

d. Save the file.

The language selection list shows on the Network Login page.

To revert to not showing the language selection list, replace the current file with the backup of the original file.

5. **Make sure the text strings are shown correctly**

a. Browse to the Captive Portal and select the new language.

b. Browse from different operating systems with different locale setups.

c. Make sure that the text is shown correctly on the Captive Portal pages.

d. Browse to the Captive Portal from a different browser and use a different font size.

Server Certificates

For secure SSL connection, gateways must establish trust with endpoint computers by showing a *Server Certificate*. This section discusses the procedures necessary to generate and install server certificates.

Check Point gateways, by default, use a certificate created by the Internal Certificate Authority on the Security Management Server as their server certificate. Browsers do not trust this certificate. When an endpoint computer tries to connect to the gateway with the default certificate, certificate warning messages open in the browser. To prevent these warnings, the administrator must install a server certificate signed by a trusted certificate authority.

All portals on the same Security Gateway IP address use the same certificate.

Obtaining and Installing a Trusted Server Certificate

To be accepted by an endpoint computer without a warning, gateways must have a server certificate signed by a known certificate authority (such as Entrust, VeriSign or Thawte). This certificate can be issued directly to the gateway, or be a chained certificate that has a certification path to a trusted root certificate authority (CA).

Follow the next procedures to get a certificate for a gateway that is signed by a known Certificate Authority (CA).

Generating the Certificate Signing Request

First, generate a *Certificate Signing Request* (CSR). The CSR is for a *server* certificate, because the gateway works as a server to the clients.

Note - This procedure creates private key files. If private key files with the same names already exist on the computer, they are overwritten without warning.

1. From the gateway command line, log in to the Expert mode.
2. Run:

   ```
   cpopenssl req -new -out <CSR file> -keyout <private key
   file> -config $CPDIR/conf/openssl.cnf
   ```

   This command generates a private key. This output comes into view:

   ```
   Generating a 2048 bit RSA private key
   .+++
   ...+++
   writing new private key to 'server1.key'
   Enter PEM pass phrase:
   ```

3. Enter a password and confirm.

   Fill in the data.

   - The **Common Name** field is mandatory. This field must have the Fully Qualified Domain Name (FQDN). This is the site that users access. For example: `portal.example.com`.
   - All other fields are optional.

4. Send the CSR file to a trusted certificate authority. Make sure to request a *Signed Certificate* in PEM format. Keep the `.key` private key file.

Generating the P12 File

After you get the Signed Certificate for the gateway from the CA, generate a P12 file that has the Signed Certificate and the private key.

1. Get the Signed Certificate for the gateway from the CA.

   If the signed certificate is in P12 or P7B format, convert these files to a PEM (Base64 encoded) formatted file with a CRT extension.

2. Make sure that the CRT file has the full certificate chain up to a trusted root CA.

   Usually you get the certificate chain from the signing CA. Sometimes it split into separate files. If the signed certificate and the trust chain are in separate files, use a text editor to combine them into one file. Make sure the server certificate is at the top of the CRT file.

3. From the gateway command line, log in to the Expert mode.

4. Use the `*.crt` file to install the certificate with the `*.key` file that you generated.

   a. Run:

   ```
   cpopenssl pkcs12 -export -out <output file> -in <signed
   cert chain file> -inkey <private key file>
   ```

   For example:

   ```
   cpopenssl pkcs12 -export -out server1.p12 -in
   server1.crt -inkey server1.key
   ```

   b. Enter the certificate password when prompted.

Installing the Signed Certificate

1. Log in to SmartConsole.
2. From the left Navigation Toolbar, click **Gateways & Servers**.
3. Open the Identity Awareness Gateway object.
4. In the navigation tree, click the applicable Software Blade page:
   - **Mobile Access** > **Portal Settings**
   - **Platform Portal**
   - **Data Loss Prevention**
   - **Identity Awareness > Captive Portal > Settings > Access Settings**

   In the **Certificate** section, click **Import** or **Replace**.
5. Install the Access Control Policy on the gateway.

Note - The **Repository of Certificates** on the IPsec VPN page of the gateway object is only for self-signed certificates. It does not affect the certificate installed manually using this procedure.

Viewing the Certificate

To see the new certificate from a Web browser:

The Security Gateway uses the certificate when you connect with a browser to the portal. To see the certificate when you connect to the portal, click the lock icon that is next to the address bar in most browsers.

The certificate that users see depends on the actual IP address that they use to get an access to the portal - not only the IP address configured for the portal in SmartConsole.

To see the new certificate from SmartConsole:

From a page that contains the portal settings for that blade/feature, click **View** in the **Certificate** section.

Transparent Kerberos Authentication Configuration

The Transparent Kerberos Authentication Single-Sign On (SSO) solution transparently authenticates users already logged into AD. This means that a user authenticates to the domain one time and has access to all authorized network resources without having to enter credentials again. If Transparent Kerberos Authentication fails, the user is redirected to the Captive Portal for manual authentication.

Note - The Identity Agent download link and the **Automatic Logout** option are ignored when Transparent Kerberos Authentication SSO is successful. The user does not see the Captive Portal.

SSO in Windows domains works with the Kerberos authentication protocol.

The Kerberos protocol is based on the concept of *tickets*, encrypted data packets issued by a trusted authority, Active Directory (AD). When a user logs in, the user authenticates to a domain controller that gives an initial *ticket granting ticket* (TGT). This ticket vouches for the user's identity.

In this solution, when an unidentified user is about to be redirected to the Captive Portal for identification:

1. Captive Portal asks the browser for authentication.
2. The browser shows a Kerberos ticket to the Captive Portal.

3. Captive Portal sends the ticket to the gateway (the Identity Awareness Gateway).
4. The gateway decrypts the ticket, extracts the user's identity, and publishes it to all Security Gateway with Identity Awareness.
5. The authorized and identified user is redirected to the originally requested URL.
6. If transparent automatic authentication fails (steps 2-5), the user is redirected to the Captive Portal for identification.

Transparent Kerberos Authentication uses the GSS-API Negotiation Mechanism (SPNEGO) internet standard to negotiate Kerberos. This mechanism works like the mechanism that Identity Agents use to present the Kerberos ticket (see the *Identity Awareness Clients Administration Guide*).

You can configure SSO Transparent Kerberos Authentication to work with HTTP and/or HTTPS connections. HTTP connections work transparently with SSO Transparent Kerberos Authentication at all times. HTTPS connections work transparently only if the Security Gateway has a signed `.p12` certificate. If the Security Gateway does not have a certificate, the user sees, and must respond to, the certificate warning message before a connection is made.

Configuration Overview

Transparent Kerberos Authentication SSO configuration includes these steps. They are described in details in this section.

- AD configuration - Creating a user account and mapping it to a Kerberos principal name
  - For HTTP connections: (`HTTP/<captive portal full dns name>@DOMAIN`)
  - For HTTPS connections: (`HTTPS/<captive portal full dns name>@DOMAIN`)
- SmartConsole configuration:
  - Creating an LDAP Account Unit and configuring it with SSO.
  - Enabling Transparent Kerberos Authentication on the Identity Awareness Gateway.
- Endpoint client configuration - Configuring trusted sites in the browsers.

Where applicable, the procedures give instructions for both HTTP and HTTPS configuration.

Creating a New User Account

1. In Active Directory, open **Active Directory Users and Computers** (**Start** > **Run** > **dsa.msc**)
2. Add a new user account.

You can select one username and password. For example: a user account named `ckpsso` with the password `qwe123!@#` to the domain `corp.acme.com`.

3. Clear the **User must change password at next logon** option and select **Password Never Expires**.

Mapping the User Account to a Kerberos Principal Name

Run the `setspn` utility to create a Kerberos principal name, used by the Security Gateway and the AD. A Kerberos principal name contains a service name (for the Security Gateway that browsers connect to) and the domain name (to which the service belongs).

`setspn` is a command line utility that is available for Windows Server 2000 and higher.

Installing setspn.exe

Install the correct `setspn.exe` version on the AD server. The `setspn.exe` utility is not installed by default in Windows 2003.

On Windows 2003:

1. Get the correct executable for your service pack from the Microsoft Support site before installation. It is part of the Windows 2003 support tools. For example, AD 2003 SP2 must have support tools for 2003 SP2.
2. Download the `support.cab` and `suptools.msi` files to a new folder on your AD server.
3. Run the `suptools.msi`.

If you use Active Directory with Windows Server 2008 and above, the `setspn` utility is installed on your server in the `Windows\System32` folder. Run the command prompt as an Administrator.

Using setspn

Important - If you used the `setspn` utility before, with the same principal name, but with a different account, you must delete the different account or remove the association to the principal name.
To remove the association, run:

```
setspn -D HTTP/ <captive_portal_full_dns_name> <old_account name>
```

If you do not do this, authentication fails.

1. Open the command line (**Start** > **Run** > **cmd**).
2. Run `setspn` with this syntax:

   For HTTP connections:

```
> setspn -A HTTP/<captive_portal_full_dns_name> <username>
```

Important - Make sure that you enter the command exactly as shown. All parameters are case sensitive.

Example:

```
> setspn -A HTTP/mycaptive.corp.acme.com ckpsso
```

The AD is ready to support Kerberos authentication for the Security Gateway.

To see users associated with the principle name, run: `setspn -Q HTTP*/*`

Configuring an Account Unit

If you already have an Account Unit from the Identity Awareness First Time Configuration Wizard, use that unit. Do not do the first five steps. Start with Step 6.

1. Add a new host to represent the AD domain controller: In SmartConsole, open the **Object Explorer (Ctrl+E)** and click **New** > **Host**.
2. Enter a name and IP address for the AD object.
3. Click **OK**.
4. Add a new LDAP Account Unit:

   In the **Object Explorer**, click **New** > **More** > **User/Identity** > **LDAP Account Unit**.
5. In the **General** tab of the LDAP Account Unit:
   a. Enter a name.
   b. In **Profile**, select **Microsoft_AD**.
   c. In **Domain**, enter the domain name.

      Best Practice - Enter the domain for existing Account Units to use for Identity Awareness. If you enter a domain, it does not affect existing LDAP Account Units.
   d. Select **CRL retrieval** and **User management**.
6. Click **Active Directory SSO configuration** and configure the values:
   a. Select **Use Kerberos Single Sign On**.
   b. Enter the domain name.
   c. Enter the account username you created in *"Creating a New User Account" on page 235*.

d. Enter the account password for that user (the same password you configured for the account username in AD) and confirm it.

e. Leave the default settings for **Ticket encryption method**.

f. Click **OK**.

7. In the **Servers** tab:

a. Click **Add** and enter the LDAP Server properties.

b. In **Host**, select the AD object you configured.

c. In **Login DN**, enter the login DN of a predefined user (added in the AD) used for LDAP operations.

d. Enter the LDAP user password and confirm it.

e. In the **Check Point Gateways are allowed to** section, select **Read data from this server**.

f. In the **Encryption** tab, you can configure LDAPS.

Configure these settings:

I. Select **Use Encryption (SSL)** - Enables LDAPS.

II. **Encryption port** - The LDAPS port is automatically populated. You can modify it as needed.

III. Click **Fetch** to retrieve this information:

- **Server Name** - The subject of the LDAPS server certificate.
- **CA** - Certificate of the root CA that signed the LDAPS server certificate.

Note - If you renew or replace the LDAPS server certificate using the same CA and Server Name, Security Gateways version R82 or higher trust the new certificate automatically.

- **Server** - Fingerprint of the LDAPS server certificate.

IV. Verify that the fetched information is correct.

V. Optional: Select **CRL check** to have the Security Gateway verify that the server certificate is not revoked.

Note - If you enable CRL check, you must make sure that the LDAPS server certificate contains a CRL Distribution Point extension of type HTTP, and that the Security Gateway can access this URL.

VI. **Min/Max Encryption Strength** - Use the default values provided:

- **Export** for minimum encryption strength
- **Strong** for maximum encryption strength

8. In the **Objects Management** tab:
   a. In **Server to connect**, select the AD object you configured.
   b. Click **Fetch Branches** to configure the branches in use.
   c. Set the number of entries supported.
9. In the **Authentication** tab, select **Default authentication scheme > Check Point Password**.
10. Click **OK**.

Enabling Transparent Kerberos Authentication

1. Log in to SmartConsole.
2. From the left Navigation Toolbar, click **Gateways & Servers**.

3. Open the Identity Awareness Gateway object.
4. In the left tree, go to the **Identity Awareness** page.
5. Click **Browser-Based Authentication** > **Settings**.

   The **Captive Portal Settings** window opens.
6. In the **Authentication Settings** section, click **Edit**.
7. Select **Automatically authenticate users from machines in the domain**.

   The **Main URL** field contains the URL (with IP address or Hostname) that is used to begin the SSO process. If transparent authentication fails, users are redirected to the configured Captive Portal.
8. Click **OK** to close all windows.
9. Install the Access Control Policy.

Browser Configuration

To work with Transparent Kerberos Authentication, it is necessary to configure your browser to trust Captive Portal URL. If the portal is working with HTTPS, you must in addition enter the URL in the **Local Internet** field through HTTPS.

Internet Explorer

It is not necessary to add the Captive Portal URL to Trusted Sites.

To configure Internet Explorer for Transparent Kerberos Authentication:

1. Open Internet Explorer.
2. Go to Internet **Tools** > **Options** > **Security** > **Local intranet** > **Sites** > **Advanced**.
3. Enter the Captive Portal URL in the applicable and then click **Add**.

Google Chrome

If your Internet Explorer for Transparent Kerberos Authentication is already configured, then this configuration works with Chrome. Use this procedure only if you did not configure Internet Explorer for Transparent Kerberos Authentication.

To configure Google Chrome for Transparent Kerberos Authentication:

1. Open Chrome.
2. Click the menu (wrench) icon and select **Settings**.
3. Click **Show advanced settings**.
4. In the **Network** section, click **Change Proxy Settings**.

5. In the **Internet Properties** window, go to **Security** > **Local intranet** > **Sites** > **Advanced**.
6. Enter the Captive Portal URL in the applicable field.

Firefox

For Firefox, the **Negotiate authentication** option is disabled by default. To use Transparent Kerberos Authentication, you must enable this option.

To configure Firefox for Transparent Kerberos Authentication:

1. Open Firefox.
2. In the URL bar, enter `about:config`
3. Search for the `network.negotiate-auth.trusted-uris` parameter.
4. Set the value to the DNS name of the Captive Portal Security Gateway. You can enter multiple URLs by separating them with a comma.

Two Factor Authentication

Check Point Captive Portal authenticates users easily with a web interface. When users try to get an access to a protected resource, they are prompted to enter authentication credentials in a browser.

Captive Portal Two Factor Authentication adds support for an additional challenge-response authentication from the user through the RADIUS protocol.

Follow all the procedures below to configure Captive Portal Two Factor Authentication.

1. **Configure a RADIUS server object in SmartConsole**
   a. In the top left corner, click **Objects** > **Object Explorer**.

      The Object Explorer window opens.

   b. In the left navigation tree, click **Servers**.
   c. From the toolbar, click **New** > **More** > **User/Identity** > **RADIUS**.
   d. Enter a name for your designated RADIUS server.
   e. In the **Host** field, add the appropriate host object with your RADIUS server IP address.

      If the host is not yet defined, click the star icon > **Host**, and enter the host Name and IP Address.

f. In the **Version** field, select the appropriate RADIUS version.

g. In the **Protocol** field, select the appropriate authentication protocol.

h. Click **OK**.

i. Close the **Object Explorer** window.

j. Install the Access Control Policy.

2. **Configure Captive Portal in SmartConsole**

a. From the left Navigation Toolbar, click **Gateways & Servers**.

b. Double-click the Security Gateway object.

c. On the **General Properties** pane, select the **Identity Awareness** Software Blade.

Identity Awareness Configuration Wizard opens.

d. On the **Methods For Acquiring Identity** wizard screen, select the **Browser-Based Authentication**.

e. Click **Next**.

f. On the **Integration With Active Directory** wizard screen, select **I do not wish to configure an Active Directory at this time**.

g. Click **Next**.

h. On the **Browser-Based Authentication Settings** wizard screen, configure the accessibility settings.

i. Click **Next**.

j. Click **Finish** to close the Identity Awareness Configuration Wizard.

k. In the left navigation tree, click **Identity Awareness**.

l. Next to the **Browser-Based Authentication** check box, click **Settings**.

m. In the **Authentication Settings** section, click **Edit**.

n. In the **Authentication Method** section, select **RADIUS** and then select the RADIUS server object you created earlier.

o. In the **User Directories** section, select the **LDAP users** option, if user groups are fetched directly from an LDAP server.

If not, clear this option.

p. Click **OK** to close the Security Gateway object properties.

q. Install the Access Control Policy.

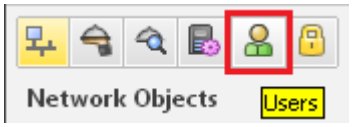
3. **Configure a generic user profile in the Legacy SmartDashboard**

    a. In SmartConsole, click **Manage & Settings** > **Blades**.

    b. In the **Mobile Access** section, click **Configure in SmartDashboard**.

    Legacy SmartDashboard opens.

    c. In the bottom left pane, click **Users**.



    d. In the bottom left pane, right click on an empty space below the last folder in the pane and select **New** > **External User Profile** > **Match all users**.

    e. Configure the **External User Profile** properties:

        i. On the **General Properties** page:

        In the **External User Profile name** field, leave the default name **generic***.

        In the **Expiration Date** field, set the applicable date.

        ii. On the **Authentication** page:

        From the **Authentication Scheme** drop-down list, select and configure the applicable option.

        iii. On the **Location**, **Time**, and **Encryption** pages, configure other applicable settings.

        iv. Click **OK**.

    f. From the top toolbar, click **Update** (or press **Ctrl + S**).

    g. Close SmartDashboard.

    h. In SmartConsole, install the Access Control Policy.

4. **Configure Access Roles that are based on LDAP users and groups**

    a. Make sure you have an *LDAP Account Unit* object for the LDAP server:

        i. In SmartConsole, in the top left corner, go to **Objects** > **Object Explorer**.

        Object Explorer window opens.

        ii. In the left navigation tree, click **Servers**.

    If not, from the toolbar, click **New** > **More** > **User/Identity** > **LDAP Account Unit**, and configure the object.

    b. Configure Access Roles based on LDAP users and LDAP groups.

c. Install the Access Control Policy.

5. **Configure Access Roles that are based on RADIUS groups**

   a. Configure the Global Properties:

      i. In SmartConsole, go to **Menu** > **Global properties**.

      The Global Properties window opens.

      ii. In the left navigation tree, click **Advanced** > **Configure**.

      The Advanced Configuration window opens.

      iii. In the left navigation tree, click **SecuRemote/SecureClient**.

      iv. Select **add_radius_groups**.

      v. Click **OK** to close the Advanced Configuration window.

      vi. Click **OK** to close the Global Properties window.

   b. Configure the internal user groups:

      i. In the top left corner, click **Objects** > **Object Explorer**.

      Object Explorer window opens.

      ii. In the left navigation tree, click **Users**.

      iii. From the toolbar, click **New** > **User** > **User Group**.

      iv. For each RADIUS group `<grp>` on your RADIUS server, create an internal user group named `RAD_<grp>` (case-sensitive).

      For example, for RADIUS group `MyGroup`, create an internal user group named `RAD_MyGroup`.

      v. Close the **Object Explorer** window.

   c. Configure Access Roles with the internal user groups you created in the previous step.

   d. Install the Access Control Policy.

Command Line Reference

See the *R82 CLI Reference Guide*.

Below is a limited list of applicable commands.

These terms are used in the CLI commands:

Term	Description
PDP	Identity Awareness Policy Decision Point. This is an Identity Awareness Security Gateway, which is responsible to collect and share identities.
PEP	Identity Awareness Policy Enforcement Point. This is an Identity Awareness Security Gateway, which is responsible to enforce network access restrictions. It makes its decisions based on identity data it collected from the **PDP**.
ADLOG	The module responsible for the acquisition of identities of entities (users or computers) from the Active Directory. The `adlog` runs on: ▪ An Identity Awareness Security Gateway, for which you enabled the AD Query. The AD Query serves the Identity Awareness Software Blade, which enforces the policy and logs identities. ▪ A Log Server. The `adlog` logs identities. The `adlog` is the command line process used to control and monitor the ADLOG feature. The command line tool helps control users' statuses, as well as troubleshoot and monitor the system.

The **PEP** and **PDP** processes are key components of the system. Through them, administrators control user access and network protection.

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Syntax Legend for CLI Commands

Whenever possible, this guide lists commands, parameters and options in the alphabetical order.

This guide uses this convention in the Command Line Interface (CLI) syntax:

Character	Description

TAB	Shows the available nested subcommands:
	`main command`
	`→ nested subcommand 1`
	`→ → nested subsubcommand 1-1`
	`→ → nested subsubcommand 1-2`
	`→ nested subcommand 2`
	Example:
	`cpwd_admin`
	`config`
	`-a <options>`
	`-d <options>`
	`-p`
	`-r`
	`del <options>`
	Meaning, you can run only **one** of these commands:
	■ This command: `cpwd_admin config -a <options>`
	■ Or this command: `cpwd_admin config -d <options>`
	■ Or this command: `cpwd_admin config -p`
	■ Or this command: `cpwd_admin config -r`
	■ Or this command: `cpwd_admin del <options>`

Curly brackets or braces **{ }**	Enclose a list of available commands or parameters, separated by the vertical bar **|**. User can enter only one of the available commands or parameters.

Character	Description
Angle brackets **< >**	Enclose a variable. User must explicitly specify a supported value.
Square brackets or brackets **[ ]**	Enclose an optional command or parameter, which user can also enter.

adlog

Description

Provides commands to control and monitor the AD Query (formerly AD Log) process.

Syntax

- When the `adlog` runs on a Security Gateway, the AD Query serves the Identity Awareness Software Blade, which enforces policy and logs identities.

  In this case, the command syntax is:

  ```
  adlog a <parameter> [<option>]
  ```

- When the `adlog` runs on a Log Server with Identity Logging enabled, it logs identities.

  In this case, the command syntax is:

  ```
  adlog l <parameter> [<option>]
  ```

Note - Parameters for the "`adlog a`" and "`adlog l`" commands are identical.

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description
No Parameters	Displays available options for this command and exits.

`a`
or
`l`
	Sets the working mode:
	■ `adlog a`- If you use the AD Query for Identity Awareness.
	■ `adlog l` - If you use a Log Server (Identity Logging).

`control <parameter> <option>`	Sends control commands to the AD Query. See *"adlog control" on page 250*.

Parameter	Description
`dc`	Shows the status of a connection to the AD domain controller. See *"adlog dc" on page 252*.
`debug <parameter>`	Enables and disables the `adlog` debug output. See *"adlog debug" on page 253*.
`query <parameter> <option>`	Shows the database of identities acquired by the AD Query, according to the specified filter. See *"adlog query" on page 254*.
`statistics`	Shows statistics about NT Event logs received by `adlog`, for each IP address and total. Also shows the number of identified IP addresses. See *"adlog statistics" on page 255*.

adlog control

Description

Sends control commands to the AD Query (formerly AD Log).

Syntax

```
adlog {a | l} control
      muh <options>
      reconf
      srv_accounts <options>
      stop
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description

`muh <options>`	Manages the list of Multi-User Hosts.
	The available <*options*> are:
	■ Show all known Multi-User Hosts (MUHs):
	`adlog {a | l} control muh show`
	■ Add an IP address as a Multi-User Host (MUH):
	`adlog {a | l} control muh mark`
	■ Removes an IP address from the list of Multi-User Hosts (MUHs):
	`adlog {a | l} control muh unmark`

`reconf`	Sends a reconfiguration command to the AD Query. Resets the policy configuration to the one defined in SmartConsole.

Parameter	Description

`srv_ accounts <options>`	Manages service accounts.
	Service accounts are accounts that do not belong to actual users, rather they belong to services that run on a computer. Service accounts are suspected, if they are logged in more than a certain number of times.
	The available <*options*> are:
	■ Show all known service accounts:
	`adlog {a | l} control srv_accounts show`
	■ Clear all the accounts from the list of service accounts:
	`adlog {a | l} control srv_accounts clear`
	■ Manually update the list of service accounts:
	`adlog {a | l} control srv_accounts find`
	■ Remove an account name from the list of service accounts:
	`adlog {a | l} control srv_accounts unmark`

`stop`	Stops the AD Query. Security Gateway does not acquire new identities with the AD Query anymore.

adlog dc

Description

Shows the status of a connection to the Active Directory Domain Controller.

Syntax

```
adlog a dc
```

```
adlog l dc
```

Important:

- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

adlog debug

Description

Enables and disables the `adlog` debug output.

Feature	Output Debug File
Identity Awareness on a Security Gateway	`$FWDIR/log/pdpd.elg`
Identity Logging on a Log Server	`$FWDIR/log/fwd.elg`

Syntax

```
adlog {a | l} debug
      extended
      mode
      off
      on
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description
`extended`	Turns on the debug and adds extended debug topics.
`mode`	Shows the debug status ("`on`", or "`off`").
`off`	Turns off the debug.
`on`	Turns on the debug.

adlog query

Description

Shows the database of identities acquired by the AD Query (formerly AD Log), according to the specified filter.

Syntax

```
adlog {a | l} query
      all
      ip <IP Address>
      machine <Computer Name>
      string <String>
      user <Username>
```

Important:

- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description
`all`	No filter. Shows the entire identity database.
`ip <IP Address>`	Filters identities that relate to the specified IP address.
`machine <Computer Name>`	Filters identity mappings based on the specified computer name.
`string <String>`	Filters identity mappings based on the specified text string.
`user <Username>`	Filters identity mappings based on the specified user.

Example - Show the entry that contains the string "jo" in the user name

```
adlog a query user jo
```

adlog statistics

Description

Shows statistics about NT Event logs received by `adlog`, for each IP address and total.

Also shows the number of identified IP addresses.

Syntax

```
adlog a statistics
```

```
adlog l statistics
```

Important:

- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

adlogconfig

Description

Configures advanced AD Query (formerly AD Log) settings through a text menu.

Each setting has a default value.

If you change the default value or manually configure the default value, then the change is saved in the `$FWDIR/conf/ad_log_override.C` file.

Syntax

- On a Security Gateway / each Cluster Member / Security Group, run:

  ```
  adlogconfig a
  ```

- On a Log Server with Identity Logging enabled, run:

  ```
  adlogconfig l
  ```

Note - Menu options in the "`adlogconfig a`" and "`adlogconfig l`" commands are identical.

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Default Output

```
[ ] Override default AD Query configuration
   [ ] Enable AD Query
      [ ] Create logs also for logoff events
      [ ] Create logs with timestamp from AD
          Timeout for username-and-IP association (minutes,
0=disabled): 0
          Interval for fetching Full Name for known users (days,
0=disabled): 0
          Hour of the day for fetching Full Name for known users
(0=disabled): 0
          Threshold for Multi-User Host detection (logged in
users): 7
          Timeout for revoked users on single user hosts
(seconds): 14400
      [X] Mark hosts as Multi-User Hosts after X users logged in
          Timeout for Multi-User Host mark (seconds): 2592000
          Threshold for Service Account detection (logins): 10
      [ ] Automatically exclude Service Accounts
[ ] Override default parameters for AD communication
          Interval between AD queries for login events (seconds,
0=disabled): 0
          Max returned objects for each AD query data chunk
(0=unlimited): 0
[ ] Ignore login events received from other AD Domains
[X] Do not check if AD password expired
[ ] AD authentication mode
   [ ] Use NTLMv1
   [X] Use NTLMv2
[ ] Assume that all hosts are for single users
[ ] Ignore hostnames of users' computers
[X] Use automatic AD updates about LDAP groups membership
          Timeout for accumulating LDAP group updates (seconds):
10
      [X] Use LDAP group updates about users only
[ ] Prefer IPv6 addresses for Domain Controllers
[1] WMI query Type

====================================================

 1 - Use / Do not use the AD Query 'override' file
 2 - Enable / Disable the AD Query feature
 3 - Create logs also for logoff events
 4 - Create logs with timestamp from AD
 5 - Timeout for username-and-IP association
```

```
 6 - Query interval (in days) for fetching Full Name for known
users
 7 - Query hour of the day for fetching Full Name for known
users
 8 - Add AD Domain and its Domain Controllers
 9 - Delete AD Domain and its Domain Controllers
10 - Reconfigure AD username
11 - Reconfigure AD Password
12 - Reconfigure AD Domain Controllers
13 - Number of logged in users for Multi-User Host detection
14 - Timeout for revoked users on single user hosts
15 - Mark / Do not mark hosts as Multi-User Hosts after X users
logged in
16 - Timeout for Multi-User Host mark
17 - Override / Do not override parameters for communication
with AD
18 - Interval between AD queries for login events
19 - Max returned objects per data chunk in each AD query for
login events
20 - Check / Do not check if AD password expired (every 24 hrs)
21 - AD authentication mode - NTLMv1 / NTLMv2
22 - Assume / Do not assume that all hosts are for single users
23 - Threshold for Service Account detection
24 - Ignore / Do not ignore login events received from other AD
Domains
25 - Exclude / Do not exclude Service Accounts automatically
from user association
26 - Ignore / Do not ignore hostnames of users' computers
27 - Ignore / Do not ignore automatic AD updates about LDAP
groups membership
28 - Timeout for accumulating LDAP group updates
29 - Use LDAP group updates about users only / about all changes
30 - Prefer / Do not prefer IPv6 addresses for Domain
Controllers
31 - WMI query type
32 - Exit without saving
33 - Save configuration and exit

Enter the option number:
```

Explanations for the top section of the menu

Explanations

Option (with the default value)	Description
`[ ] Override default AD Query configuration`	Shows whether this option is enabled: *"1 - Use / Do not use the AD Query 'override' file" on page 263*
`[ ] Enable AD Query`	Shows whether this option is enabled: *"2 - Enable / Disable the AD Query feature" on page 263*
`[ ] Create logs also for logoff events`	Shows whether this option is enabled: *"3 - Create logs also for logoff events" on page 264*
`[ ] Create logs with timestamp from AD`	Shows whether this option is enabled: *"4 - Create logs with timestamp from AD" on page 264*
`Timeout for username-and-IP association (minutes, 0=disabled): 0`	Shows the value that was configured with this option: *"5 - Timeout for username-and-IP association" on page 265*
`Interval for fetching Full Name for known users (days, 0=disabled): 0`	Shows the value that was configured with this option: *"6 - Query interval (in days) for fetching Full Name for known users" on page 265*
`Hour of the day for fetching Full Name for known users (0=disabled): 0`	Shows the value that was configured with this option: *"7 - Query hour of the day for fetching Full Name for known users" on page 266*
`Threshold for Multi-User Host detection (logged in users): 7`	Shows the value that was configured with this option: *"13 - Number of logged in users for Multi-User Host detection" on page 268*
`Timeout for revoked users on single user hosts (seconds): 14400`	Shows the value that was configured with this option: *"14 - Timeout for revoked users on single user hosts" on page 268*

Option (with the default value)	Description
`[X] Mark hosts as Multi-User Hosts after X users logged in`	Shows whether this option is enabled: *"15 - Mark / Do not mark hosts as Multi-User Hosts after X users logged in" on page 269*
`Timeout for Multi-User Host mark (seconds): 2592000`	Shows the value that was configured with this option: *"16 - Timeout for Multi-User Host mark" on page 269*
`Threshold for Service Account detection (logins): 10`	Shows the value that was configured with this option: *"23 - Threshold for Service Account detection" on page 273*
`[ ] Automatically exclude Service Accounts`	Shows whether this option is enabled: *"25 - Exclude / Do not exclude Service Accounts automatically from user association" on page 274*
`[ ] Override default parameters for AD communication`	Shows whether this option is enabled: *"17 - Override / Do not override parameters for communication with AD" on page 270*
`Interval between AD queries for login events (seconds, 0=disabled): 0`	Shows the value that was configured with this option: *"18 - Interval between AD queries for login events" on page 270*
`Max returned objects for each AD query data chunk (0=unlimited): 0`	Shows the value that was configured with this option: *"19 - Max returned objects per data chunk in each AD query for login events" on page 271*
`[ ] Ignore login events received from other AD Domains`	Shows whether this option is enabled: *"24 - Ignore / Do not ignore login events received from other AD Domains" on page 273*
`[X] Do not check if AD password expired`	Shows whether this option is enabled: *"20 - Check / Do not check if AD password expired (every 24 hrs)" on page 271*

Option (with the default value)	Description
`[ ] AD authentication mode`	Always appears as cleared "`[ ]`"
`[ ] Use NTLMv1`	Shows whether "`NTLMv1`" was selected with this option: *"21 - AD authentication mode - NTLMv1 / NTLMv2" on page 272*
`[X] Use NTLMv2`	Shows whether "`NTLMv21`" was selected with this option: *"21 - AD authentication mode - NTLMv1 / NTLMv2" on page 272*
`[ ] Assume that all hosts are for single users`	Shows whether this option is enabled: *"22 - Assume / Do not assume that all hosts are for single users" on page 272*
`[ ] Ignore hostnames of users' computers`	Shows whether this option is enabled: *"26 - Ignore / Do not ignore hostnames of users' computers" on page 274*
`[X] Use automatic AD updates about LDAP groups membership`	Shows whether this option is enabled: *"27 - Ignore / Do not ignore automatic AD updates about LDAP groups membership" on page 275*
`Timeout for accumulating LDAP group updates (seconds): 10`	Shows the value that was configured with this option: *"28 - Timeout for accumulating LDAP group updates" on page 275*
`[X] Use LDAP group updates about users only`	Shows whether this option is enabled: *"29 - Use LDAP group updates about users only / about all changes" on page 276*
`[ ] Prefer IPv6 addresses for Domain Controllers`	Shows whether this option is enabled: *"30 - Prefer / Do not prefer IPv6 addresses for Domain Controllers" on page 276*
`[1] WMI query Type`	Shows the value that was configured with this option: *"31 - WMI query type" on page 277*

Explanations for the bottom section of the menu

1 - Use / Do not use the AD Query 'override' file

Description:

Specifies whether to use the non-default settings from the `$FWDIR/conf/ad_log_override.C` file that you configure in this menu.

Default: disabled (does not use this file).

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	Boolean
Default implicit value	`:Override (false)`
Non-Default explicit value	`:Override (true)`

2 - Enable / Disable the AD Query feature

Description:

Specifies whether to use the non-default AD Query (formerly AD Log) settings that you configure in this menu.

Default: disabled (does not use the values configured in the `$FWDIR/conf/ad_log_override.C` file).

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	Boolean
Default implicit value	`:EnableAdLog (false)`
Non-Default explicit value	`:EnableAdLog (true)`

3 - Create logs also for logoff events

Description:

Specifies whether the Identity Awareness Gateway needs to create a log for a logoff event in addition to a login event.

Default: disabled (does not create logs for logoff events).

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	Boolean
Default implicit value	`:EnableLogForLoginOrLogoff (false)`
Non-Default explicit value	`:EnableLogForLoginOrLogoff (true)`

4 - Create logs with timestamp from AD

Description:

Specifies whether to use the time when the event was created on the Active Directory (original creation time) instead of the time when the event is handled on the Identity Awareness Gateway.

Default: disabled (does not use the timestamp from the Active Directory).

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	Boolean
Default implicit value	`:UseLogOriginalCreationTime (false)`
Non-Default explicit value	`:UseLogOriginalCreationTime (true)`

5 - Timeout for username-and-IP association

Description:

Specifies the timeout (in minutes) for the association of the user's IP address and the username.

Default: 0 (disabled).

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	Integer
Default implicit value	`:AssociationTimeout (0x0)`
Non-Default explicit value	`:AssociationTimeout (0x<Hex Number>)`

6 - Query interval (in days) for fetching Full Name for known users

Description:

Specifies the interval (in days) for fetching the full name of the known users from Active Directory.

Default: 0 days (disabled).

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	Integer
Default implicit value	`:FullNameQueryInterval (0x0)`
Non-Default explicit value	`:FullNameQueryInterval (0x<Hex Number>)`

7 - Query hour of the day for fetching Full Name for known users

Description:

Specifies the round hour of the day for fetching the full name of the known users from Active Directory.

Default: 0 days (disabled).

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	Integer
Default implicit value	`:FullNameFetchHour (0x0)`
Non-Default explicit value	`:FullNameFetchHour (0x<Hex Number>)`

8 - Add AD Domain and its Domain Controllers

Description:

Specifies the Active Directory Domain, Domain Controllers, Username, and Password.

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	String

Example:

```
:Domains (
        : (
                :DomainName (example.com)
                :Username (admin)
                :Password (<Hashed Password>)
                :DomainControllers (
                        : (dc1.example.com)
                        : (dc2.example.com)
                )
        )
)
```

9 - Delete AD Domain and its Domain Controllers

Description:

In the `$FWDIR/conf/ad_log_override.C` file, deletes the Active Directory Domain and its Domain Controllers you configured with this option:

"8 - Add AD Domain and its Domain Controllers" on the previous page

10 - Reconfigure AD username

Description:

In the `$FWDIR/conf/ad_log_override.C` file, overwrites the Active Directory Domain username you configured with this option:

"8 - Add AD Domain and its Domain Controllers" on the previous page

11 - Reconfigure AD Password

Description:

In the `$FWDIR/conf/ad_log_override.C` file, overwrites the Active Directory Domain password you configured with this option:

"8 - Add AD Domain and its Domain Controllers" on the previous page

12 - Reconfigure AD Domain Controllers

Description:

In the `$FWDIR/conf/ad_log_override.C` file, overwrites the Active Directory Domain Controllers you configured with this option:

"8 - Add AD Domain and its Domain Controllers" on the previous page

13 - Number of logged in users for Multi-User Host detection

Description:

Specifies the number of logged on users from the same IP address, after which this IP address is considered a Multi-User Host (MUH) computer.

Default: 7 users.

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	Integer
Default implicit value	`:MultiUserThreshold (0x7)`
Non-Default explicit value	`:MultiUserThreshold (0x<Hex Number>)`

14 - Timeout for revoked users on single user hosts

Description:

Note - Applies only when you enable this option:
"22 - Assume / Do not assume that all hosts are for single users" on page 272

Specifies the time interval, during which the Identity Awareness Gateway ignores an association of a previously logged in user on a computer to a new IP address.

This means that during this interval, the previously logged in users cannot pass traffic through the Identity Awareness Gateway if they log in on a different computer.

Default: 14400 seconds (240 minutes).

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	Integer
Default implicit value	`:RevokedUserTimout (0x3840)`
Non-Default explicit value	`:RevokedUserTimout (0x<Hex Number>)`

15 - Mark / Do not mark hosts as Multi-User Hosts after X users logged in

Description:

If you disable this option, then the Identity Awareness Gateway does not mark a source IP address as a Multi-User Host (MUH) computer when there are more than X users logged in on the computer.

"X" is the value you configure with the option *"13 - Number of logged in users for Multi-User Host detection" on the previous page*.

Default: enabled (marks a source IP address as a Multi-User Host).

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	Boolean
Default implicit value	`:DisableMultiUserPersistDB (false)`
Non-Default explicit value	`:DisableMultiUserPersistDB (true)`

16 - Timeout for Multi-User Host mark

Description:

Specifies the time interval, during which the Identity Awareness Gateway keeps a source IP address marked as Multi-User Host (MUH) computer when there are more than X users logged in on the computer.

"X" is the value you configure with the option *"13 - Number of logged in users for Multi-User Host detection" on the previous page*.

Default: 2592000 seconds (43200 minutes = 720 hours = 30 days)

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	Integer
Default implicit value	`:MultiUserPersistMachineTimeout (0x278d00)`
Non-Default explicit value	`:MultiUserPersistMachineTimeout (0x<`*`Hex Number`*`>)`

17 - Override / Do not override parameters for communication with AD

Description:

Specifies whether to use the settings configured with these options:

- *"18 - Interval between AD queries for login events" below*
- *"19 - Max returned objects per data chunk in each AD query for login events" on the next page*

Default: disabled (uses the default parameters).

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	Boolean
Default implicit value	`:QueryWhitinCount (false)`
Non-Default explicit value	`:QueryWhitinCount (true)`

18 - Interval between AD queries for login events

Description:

How frequently (in seconds) the Identity Awareness Gateway asks the Active Directory for login events.

Default: 1 second.

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	Integer
Default implicit value	`:FullNameQueryInterval (0x0)`
Non-Default explicit value	`:FullNameQueryInterval (0x<Hex Number>)`

19 - Max returned objects per data chunk in each AD query for login events

Description:

When the Identity Awareness Gateway asks the Active Directory for login events, this controls the number of returned users in each data chunk

Default: 100 users per data chunk.

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	Integer
Default implicit value	`:QueryMaxReturnedObjects (0x64)`
Non-Default explicit value	`:QueryMaxReturnedObjects (0x<Hex Number>)`

20 - Check / Do not check if AD password expired (every 24 hrs)

Description:

Specifies whether to check (every 24 hours) if the password had expired for the account the Identity Awareness Gateway uses to connect to the Active Directory to query for new login events.

Default: disabled (does not check).

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	Boolean
Default implicit value	`:DisablePassExpCheck (true)`
Non-Default explicit value	`:DisablePassExpCheck (false)`

21 - AD authentication mode - NTLMv1 / NTLMv2

Description:

Controls which authentication mode to use when connecting to Active Directory - NTLMv1 or NTLMv2.

Default: NTLMv2.

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	Boolean
Default implicit value	`:UseNTLMv2 (true)`
Non-Default explicit value	`:UseNTLMv2 (false)`

22 - Assume / Do not assume that all hosts are for single users

Description:

Specifies whether to keep only one association between the source IP address and the username.

If another user logs in on the same computer, then the new username replaces the previous username in the Identity Awareness Gateway.

Default: disabled (does not assume).

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	Boolean
Default implicit value	`:SingleUserAssumption (false)`
Non-Default explicit value	`:SingleUserAssumption (true)`

23 - Threshold for Service Account detection

Description:

Specifies the number of a user logins from different IP addresses to identify the user as a Service Account.

Default:10 logins.

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	Integer
Default implicit value	`:ServiceAccountThreshold (0xa)`
Non-Default explicit value	`:ServiceAccountThreshold (0x<Hex Number>)`

24 - Ignore / Do not ignore login events received from other AD Domains

Description:

Specifies whether to ignore login events received from different domains than configured for AD Query.

Default: disabled (does not ignore).

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	Boolean
Default implicit value	`:IgnoreDifferentDomains (false)`
Non-Default explicit value	`:IgnoreDifferentDomains (true)`

25 - Exclude / Do not exclude Service Accounts automatically from user association

Description:

Controls whether to exclude Service Accounts from user association.

Default: disabled (does not exclude).

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	Boolean
Default implicit value	`:ExcludeServiceAccounts (false)`
Non-Default explicit value	`:ExcludeServiceAccounts (true)`

26 - Ignore / Do not ignore hostnames of users' computers

Description:

Controls whether to ignore the hostname of the computer, on which a user logged in.

Default: disabled (does not ignore).

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	Boolean
Default implicit value	`:DontReportMachines (false)`
Non-Default explicit value	`:DontReportMachines (true)`

27 - Ignore / Do not ignore automatic AD updates about LDAP groups membership

Description:

Controls whether to ignore the automatic Active Directory updates about LDAP groups membership.

Default: enabled (does not ignore).

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	Boolean
Default implicit value	`:LdapGroupsUpdateEnable (true)`
Non-Default explicit value	`:LdapGroupsUpdateEnable (false)`

28 - Timeout for accumulating LDAP group updates

Description:

Note - Applies only when you enable this option:
"27 - Ignore / Do not ignore automatic AD updates about LDAP groups membership" above

Controls the amount of time (in seconds) during which the Identity Awareness Gateway accumulates LDAP group notifications before recalculating the users' access.

Default: 10 seconds.

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	Integer
Default implicit value	`:LdapGroupsUpdateDelay (0x0)`
Non-Default explicit value	`:LdapGroupsUpdateDelay (0x<Hex Number>)`

29 - Use LDAP group updates about users only / about all changes

Description:

Warning - If you disable the default behavior, the CPU load on the Identity Awareness Gateway increases significantly.

Note - Applies only when you enable this option:
"27 - Ignore / Do not ignore automatic AD updates about LDAP groups membership" on the previous page

Controls whether to process LDAP group notifications only for changes related to users, or process all LDAP group notifications.

Default: enabled (uses notifications only for changes related to users).

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	Boolean
Default implicit value	`:LdapGroupsUpdateAll (false)`
Non-Default explicit value	`:LdapGroupsUpdateAll (true)`

30 - Prefer / Do not prefer IPv6 addresses for Domain Controllers

Description:

Specifies whether to use IPv6 addresses if a DNS query for the specified domain controllers returns IPv4 addresses and IPv6 addresses.

Default: disabled (does not prefer).

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	Boolean
Default implicit value	`:PreferIPv6DCAddresses (false)`
Non-Default explicit value	`:PreferIPv6DCAddresses (true)`

31 - WMI query type

Description:

Specifies the WMI Query Type for Active Directory.

Default: 1.

WMI Query Type ID	WMI Query Name	WMI Query Description
1	Admin query	Regular Query. Includes reading forwarded security events logs. Requires the account to be a member of the "Server Operators" group.
2	Fallback from Admin query to non-Admin query	Fallback Configuration. Identity Awareness Gateway will first try the default regular query, and in case it fails following a WMI permissions error, it will try the Non-Admin query (reduced query).
3	Non-Admin query	Reduced Query. Identity Awareness Gateway will always use the query without forwarded events. Membership in the "Server Operators" group is not needed. **Important** - Using the reduced query in Active Directory environments, in which forwarding of security event logs between Domain Controllers is configured, might lead to missing relevant security event logs. As a result, some users and/or machines may not be recognized.

Configuration in the *$FWDIR/conf/ad_log_override.C* file:

Item	Value
Parameter type	Integer
Default implicit value	`:WmiQueryType (0x1)`
Non-Default explicit value	`:WmiQueryType (0x<Hex Number>)`

32 - Exit without saving

Description:

Exits from this menu without saving any changes you made.

33 - Save configuration and exit

Description:

Saving the changes you made and exits from this menu.

pdp

Description

These commands control and monitor the *pdpd* process.

Syntax

```
pdp <command> [<parameter> [<option>]]
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Commands

Parameter	Description
No Parameters	Shows available options for this command and exits.
`ad <parameter> <option>`	For the AD Query, adds (or removes) an identity to the Identity Awareness database on the Security Gateway. See *"pdp ad" on page 282*.
`auth <parameter> <option>`	Shows authentication or authorization options. See *"pdp auth" on page 284*.
`broker <parameter> <option>`	Controls the PDP Identity Broker. See *"pdp broker" on page 288*.
`conciliation <parameter> <option>`	Controls the session conciliation mechanism. See *"pdp conciliation" on page 293*.
`connections <parameter>`	Shows the PDP connections with the PEP gateways, Terminal Servers, and Identity Collectors. See *"pdp connections" on page 295*.
`control <parameter> <option>`	Controls the PDP parameters. See *"pdp control" on page 296*.

Parameter	Description
`debug <parameter> <option>`	Controls the PDP debug. See *"pdp debug" on page 297*.
`idc <parameter> <option>`	Operations related to Identity Collector. See *"pdp idc" on page 300*.
`idp <parameter> <option>`	Operations related to SAML-based authentication. See *"pdp idp" on page 304*.
`monitor <parameter> <option>`	Monitors the status of connected PDP sessions. See *"pdp monitor" on page 305*.
`muh <parameter> <option>`	Shows Multi-User Hosts (MUHs). See *"pdp muh" on page 308*.
`nested_groups <parameter>`	Shows LDAP Nested groups configuration. See *"pdp nested_groups" on page 309*.
`network <parameter>`	Shows information about network related features. See *"pdp network" on page 312*.
`radius <parameter> <option>`	Shows and configures the RADIUS accounting options. See *"pdp radius" on page 313*.
`roles <parameter> <option>`	Shows the user role information. See *"pdp roles" on page 316*.
`status <parameter>`	Shows PDP status information, such as start time or configuration time. See *"pdp status" on page 319*.
`tasks_manager <parameter>`	Shows the status of the PDP tasks. See *"pdp tasks_manager" on page 320*.
`timers <parameter>`	Shows PDP timers information for each session. See *"pdp timers" on page 321*.
`topology_map`	Shows topology of all PDP and PEP addresses. See *"pdp topology_map" on page 322*.
`tracker <parameter>`	Adds the TRACKER topic to the PDP logs. See *"pdp tracker" on page 323*.

Parameter	Description
`update <parameter>`	Recalculates users and computers group membership. See *"pdp update" on page 324*.
`vpn <parameter>`	Shows connected VPN gateways that send identity data from VPN Remote Access Clients. See *"pdp vpn" on page 325*.

pdp ad

General Syntax

```
pdp ad
      associate <options>
      disassociate <options>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

The 'pdp ad associate' command

Description

For the AD Query, adds an identity to the Identity Awareness database on the Security Gateway.

The group data must be in the AD.

Syntax

```
pdp ad associate ip <IP Address> u <Username> d <Domain> [m
<Computer Name>] [t <Timeout>] [s]
```

Parameters

Parameter	Description
`ip <IP Address>`	Specifies the IP address for the identity.
`u <Username>`	Specifies the username for the identity.
`d <Domain>`	Specifies the Domain of the ID server.
`m <Computer Name>`	Specifies the computer that is defined for the identity.
`t <Timeout>`	Specifies the timeout for the AD Query. Default timeout is 5 hours.

Parameter	Description
`s`	Associates the "`u <Username>`" and the "`m <Computer>`" parameters sequentially. First, adds the "`<Computer>`" and then adds the "`<Username>`" to the database.

The 'pdp ad disassociate' command

Description

For the AD Query, removes the identity from the Identity Awareness database on the Security Gateway.

Identity Awareness does not authenticate a user that is removed.

Syntax

```
pdp ad disassociate ip <IP Address> {u <Username> | m <Computer
Name>} [r {override | probed | timeout}]
```

Parameters

Parameter	Description
`ip <IP Address>`	Specifies the IP address for the identity.
`u <Username>`	Specifies the username for the identity.
`m <Computer Name>`	Specifies the computer that is defined for the identity.
`r {override | probed | timeout}`	Specifies the reason to show in SmartConsole on the **Logs & Events** > **Logs** tab.

pdp auth

Description

Configures authentication/authorization options for PDP.

Syntax

```
pdp auth
      allow_empty_result <options>
      count_in_non_ldap_group <options>
      fetch_by_sid <options>
      force_domain <options>
      kerberos_any_domain <options>
      kerberos_encryption <options>
      reauth_agents_after_policy <options>
      recovery_interval <options>
      username_password <options>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description

`allow_empty_result <options>`	Shows the current configuration of fetching of local groups from the AD server based on SID.
	Configures that the fetching of local groups from the AD server based on SID should succeed, even if all SIDs are foreign.
	The available <*options*> are:
	■ Disable the fetching of local groups:
	`pdp auth allow_empty_result disable`
	■ Enable the fetching of local groups:
	`pdp auth allow_empty_result enable`
	■ Show the current configuration:
	`pdp auth allow_empty_result status`

`count_in_non_ldap_group <options>`	Shows and configures the identification of membership to individual users that are selected in the user picker and LDAP branch groups in SmartConsole.
	The available <*options*> are:
	■ Disable the identification of membership:
	`pdp auth count_in_non_ldap_group disable`
	■ Enable the identification of membership:
	`pdp auth count_in_non_ldap_group enable`
	■ Show the current configuration:
	`pdp auth count_in_non_ldap_group status`

`fetch_by_sid <options>`	Shows and configures the fetching of local groups from the AD server based on SID.
	The available <*options*> are:
	■ Disable the fetching of local groups:
	`pdp auth fetch_by_sid disable`
	■ Enable the fetching of local groups:
	`pdp auth fetch_by_sid enable`
	■ Show the current configuration:
	`pdp auth fetch_by_sid status`

Parameter	Description

`force_domain <options>`	Shows and configures the PDP to match the identity's source, based on the reported domain and authorization domain.
	The available <*options*> are:
	■ Disable the match the identity's source:
	`pdp auth force_domain disable`
	■ Enable the match the identity's source:
	`pdp auth force_domain enable`
	■ Show the current configuration:
	`pdp auth force_domain status`

`kerberos_any_domain <options>`	Shows and configures the use of all available Kerberos principles.
	The available <*options*> are:
	■ Disable the use of all available Kerberos principles:
	`pdp auth kerberos_any_domain disable`
	■ Enable the use of all available Kerberos principles:
	`pdp auth kerberos_any_domain enable`
	■ Show the current configuration:
	`pdp auth kerberos_any_domain status`

`kerberos_encryption <options>`	Shows and configures the Kerberos encryption type.
	Note - In SmartConsole, go to **Objects** menu > **Object Explorer** > **Servers** > open the **LDAP Account Unit** object > go to **General** tab > click **Active Directory SSO Configuration**).
	The available <*options*> are:
	■ Configure the Kerberos encryption type:
	`pdp auth kerberos_encryption set`
	■ Show the current configuration:
	`pdp auth kerberos_encryption get`

Parameter	Description

`reauth_agents_after_policy <options>`	Shows and configures the automatic reauthentication of Identity Agents after policy installation.
	The available <*options*> are:
	■ Disable the automatic reauthentication:
	`pdp auth reauth_agents_after_policy disable`
	■ Enable the automatic reauthentication:
	`pdp auth reauth_agents_after_policy enable`
	■ Show the current configuration:
	`pdp auth reauth_agents_after_policy status`

`recovery_interval <options>`	Shows and configures the frequency of attempts to connect back to the higher-priority PDP gateway.
	The available <*options*> are:
	■ Disable the reconnect attempts:
	`pdp auth recovery_interval disable`
	■ Enable the reconnect attempts:
	`pdp auth recovery_interval enable`
	■ Configure the frequency or reconnect attempts:
	`pdp auth recovery_interval set <Number of Seconds>`
	■ Show the current configuration:
	`pdp auth recovery_interval show`

`username_password <options>`	Shows and configures the username and password authentication.
	The available <*options*> are:
	■ Disable the username and password authentication:
	`pdp auth username_password disable`
	■ Enable the username and password authentication:
	`pdp auth username_password enable`
	■ Show the current configuration:
	`pdp auth username_password status`

pdp broker

Description

These commands control the PDP Identity Broker.

Syntax

```
pdp broker
      debug {set | unset} <options>
      discard <options>
      identity_cache_mode status
      reconnect <options>
      session <options>
      status [-e]
      sync <options>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description
`debug set <options>` `debug unset <options>`	Controls the debug of the PDP Identity Broker. The available <*options*> are:

	■ Print the logs related to remote Publisher PDPs:
	`pdp broker debug set pub <IP Address of Publisher PDP>`
	■ Disable the logs related to remote Publisher PDPs:
	`pdp broker debug unset pub <IP Address of Publisher PDP>`

Parameter	Description

	■ Print the extended logs related to remote Publisher PDPs:
	`pdp broker debug set pub_ext <IP Address of Publisher PDP>`
	■ Disable the extended logs related to remote Publisher PDPs:
	`pdp broker debug unset pub_ext <IP Address of Publisher PDP>`

	■ Print the logs related to communication with remote Publisher PDPs:
	`pdp broker debug set pub_transport <IP Address of Publisher PDP>`
	Enable this debug on the Subscriber PDP side to observe the Publisher PDP's JSON requests in these cases:
	• To monitor networking issues in case the message was not received.
	• To monitor the JSON requests from the Publisher PDPs and related message-parsing issues.
	• To monitor if the content of the JSON does not meet the requirements (for example: Sharing ID).
	■ Disable the logs related to communication with remote Publisher PDPs:
	`pdp broker debug unset pub_transport <IP Address of Publisher PDP>`

	■ Print the logs related to remote Subscriber PDPs:
	`pdp broker debug set sub <IP Address of Subscriber PDP>`
	■ Disable the logs related to remote Subscriber PDPs:
	`pdp broker debug unset sub <IP Address of Subscriber PDP>`

	■ Print the extended logs related to remote Subscriber PDPs:
	`pdp broker debug set sub_ext <IP Address of Subscriber PDP>`
	■ Disable the extended logs related to remote Subscriber PDPs:
	`pdp broker debug unset sub_ext <IP Address of Subscriber PDP>`

Parameter	Description

	■ Print the logs related to communication with remote Subscriber PDPs:
	`pdp broker debug set sub_transport <IP Address of Subscriber PDP>`
	■ Disable the logs related to communication with remote Subscriber PDPs:
	`pdp broker debug unset sub_transport <IP Address of Subscriber PDP>`

	Notes:
	■ For more information about the debug, see *"pdp debug" on page 297*.
	■ To see the HTTP related issues, run this command to enable the debug on the Publisher PDP side:
	`pdp debug set HttpClient all`
	To see more information for some errors, run this command:
	`pdp broker status [-e]`

`discard <option>`	Controls the timeout for discarding sessions received from the specified Publisher PDP during a disconnection.
	The available <*options*> are:
	■ Show the current timeout:
	`pdp broker discard show_timeout <IP Address of Publisher PDP>`
	■ Configure the new timeout (in seconds):
	`pdp broker discard set_timeout <IP Address of Publisher PDP> <Timeout>`

`identity_ cache_mode status`	Shows the current status of the Identity Cache Mode for the PDP-to-PDP sharing protocol (Identity Broker). For more information, see the *R82 Identity Awareness Administration Guide* > Chapter "**Advanced Identity Awareness Environment**" > Section "**Identity Cache Mode for Identity Sharing Protocols**".

Parameter	Description
`reconnect <IP Address of Subscriber PDP>`	Forces the reconnection to the specified Subscriber PDP immediately. If you run this command, the PDP ignores the keep-alive intervals and exponential backoff timeouts, and sends the handshake / keep-alive immediately. **Best Practice** - You can use this command when a long time passed since the PDP disconnected, and it is necessary to establish the connection again immediately.
`session <IP Address of Subscriber PDP>`	Shows the Identity Broker session information for the specified Subscriber PDP.
`status [-e]`	Shows the status of remote Publisher PDPs and Subscriber PDPs. The option "`-e`" adds more information (Subscriber PDP port and the last error time and description).

`sync <option>`	Synchronizes identities with the specified Publisher PDPs or Subscriber PDPs.
	The available <*options*> are:
	■ Send the synchronization request (in the next broker message) to the specified remote Publisher PDP:
	`pdp broker sync pub <IP Address of Publisher PDP>`
	■ Send the synchronization request (in the next broker message) to all remote Publisher PDPs:
	`pdp broker sync pub all`

Parameter	Description

	Control the schedule for synchronization with remote Publisher PDPs:
	`pdp broker sync schedule {add <option> | remove <option>| show <option>}`
	■ To add new synchronization time:
	`pdp broker sync schedule add <IP Address of Publisher PDP> "<HH:MM>"`
	■ To remove the current schedule:
	`pdp broker sync schedule remove <IP Address of Publisher PDP> "<HH:MM>"`
	■ To show the current schedule:
	`pdp broker sync schedule show [<IP Address of Publisher PDP>]`

	■ Initiate the synchronization with the specified remote Subscriber PDP:
	`pdp broker sync sub <IP Address of Subscriber PDP>`
	■ Initiate the synchronization with all remote Subscriber PDPs:
	`pdp broker sync sub all`

pdp conciliation

Description

Controls the session conciliation mechanism.

Syntax

```
pdp conciliation
      adq_single_user <option>
      api_multiple_users <option>
      idc_multiple_users <option>
      rad_multiple_users <option>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description

`adq_single_user <option>`	Shows and controls the assumption that single AD Query user is connected on each computer.
	The available <*options*> are:
	■ Disable this behavior:
	`pdp conciliation adq_single_user disable`
	■ Enable this behavior:
	`pdp conciliation adq_single_user enable`
	■ Show the current status (enabled or disabled):
	`pdp conciliation adq_single_user stat`

Parameter	Description

`api_multiple_users <option>`	Shows and controls the assumption that multiple Web-API users are connected on each computer.
	The available <*options*> are:
	■ Disable this behavior:
	`pdp conciliation api_multiple_users disable`
	■ Enable this behavior:
	`pdp conciliation api_multiple_users enable`
	■ Show the current status (enabled or disabled):
	`pdp conciliation api_multiple_users stat`

`idc_multiple_users <option>`	Shows and controls the assumption that multiple Identity Collector users are connected on each computer.
	The available <*options*> are:
	■ Disable this behavior:
	`pdp conciliation idc_multiple_users disable`
	■ Enable this behavior:
	`pdp conciliation idc_multiple_users enable`
	■ Show the current status (enabled or disabled):
	`pdp conciliation idc_multiple_users stat`

`rad_multiple_users <option>`	Shows and controls the assumption that multiple RADIUS users are connected on each computer.
	The available <*options*> are:
	■ Disable this behavior:
	`pdp conciliation rad_multiple_users disable`
	■ Enable this behavior:
	`pdp conciliation rad_multiple_users enable`
	■ Show the current status (enabled or disabled):
	`pdp conciliation rad_multiple_users stat`

pdp connections

Description

Shows the PDP connections with PEP gateways, Terminal Servers, and Identity Collectors.

Syntax

```
pdp connections
      idc
      pep
      ts
```

Important:

- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description
`idc`	Shows a list of connected Identity Collectors.
`pep`	Shows the connection status of all the PEPs, which the current PDP should update.
`ts`	Shows a list of all connected Terminal Servers.

pdp control

Description

Provides commands to control the PDP.

Syntax

```
pdp control
      revoke_ip <IP address>
      sync
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description
`revoke_ip <IP address>`	Logs out the session that is related to the specified IP address.
`sync`	Forces an initiated synchronization operation between the PDPs and the PEPs. When you run this command, the PDP informs its related PEPs of the up-to-date information of all connected sessions. At the end of this operation, the PDP and the PEPs contain the same and latest session information.

pdp debug

Description

Controls the debug of the PDP.

Syntax

```
pdp debug
      async1
      ccc {off | on}
      memory
      off
      on
      reset
      rotate
      set <Topic Name> <Severity>
      spaces [<0 - 5>]
      stat
      unset <Topic Name>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description
`async1`	Tests the `async` command line with the `echo` command for 30 seconds.
`ccc {off | on}`	Configures whether to write the CCC debug logs into the PDP log file - `$FWDIR/log/pdpd.elg` ■ `on` - Writes the CCC debug logs ■ `off` - Does not write the CCC debug logs
`memory`	Shows the memory consumption by the *pdpd* daemon.
`off`	Disables the PDP debug.

Parameter	Description
`on`	Enables the PDP debug. **Important** - After you run this command "`pdp debug on`", you must run the command "`pdp debug set ...`" to configure the required filter.
`reset`	Resets the PDP debug options for Debug Topic and Severity. **Important** - After you run this command "`pdp debug reset`", you must run the command "`pdp debug off`" to turn off the debug.
`rotate`	Rotates the PDP log files - increases the index of each log file: 1. `$FWDIR/log/pdpd.elg` becomes `$FWDIR/log/pdpd.elg.0` 2. `$FWDIR/log/pdpd.elg.0` becomes `$FWDIR/log/pdpd.elg.1` 3. And so on.
`set <Topic Name> <Severity>`	Filters which debug logs PDP writes to the log file based on the specified Debug Topics and Severity: The available Debug Topics are: ■ `all` ■ *Check Point Support* provides more specific topics, based on the reported issue The available Severities are: ■ `all` ■ `critical` ■ `events` ■ `important` ■ `surprise` **Best Practice** - We recommend to enable all Topics and all Severities. Run: `pdp debug set all all`

Parameter	Description
`spaces [<0 - 5>]`	Shows and configures the number of indentation spaces in the `$FWDIR/log/pdpd.elg` file. You can specify the number of spaces: ■ 0 (this is the default) ■ 1 ■ 2 ■ 3 ■ 4 ■ 5
`stat`	Shows the PDP current debug status.
`unset <Topic Name>`	Unsets the specified Debug Topic(s).

Important - When you enable the debug, it affects the performance of the *pdpd* daemon. Make sure to disable the debug after you complete your troubleshooting.

pdp idc

Description

Operations related to Identity Collector.

Syntax

```
pdp idc
      groups_consolidation <options>
      groups_update <options>
      muh <options>
      service_accounts <options>
      status
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description

`groups_ consolidation <options>`	Shows and configures the consolidation of external groups with fetched groups.
	The available <*options*> are:
	■ Enable the consolidation (this is the default):
	`pdp idc groups_consolidation enable`
	■ Disable the consolidation:
	`pdp idc groups_consolidation disable`
	■ Show the current status:
	`pdp idc groups_consolidation status`

Parameter	Description

`groups_update <options>`	Shows and configures the automatic update of Identity Collector's LDAP Groups.
	For more information, see *Identity Awareness Clients Administration Guide* > chapter "Identity Collector" > section "Identity Collector - Automatic LDAP Group Update"
	The available <*options*> are:
	■ Perform "update all" to get the current LDAP group status:
	`pdp idc groups_update on`
	■ Disable the feature (default):
	`pdp idc groups_update off`
	■ Show the current status of the feature:
	`pdp idc groups_update status`

`muh <options>`	Shows and configures the Multi-User Host detection.
	The available <*options*> are:
	■ Mark an IP address as a Multi-User Host:
	`pdp idc muh mark <IP Address>`
	■ Show known Multi-User Host machines:
	`pdp idc muh show`
	■ Unmark an IP address as a Multi-User Host:
	`pdp idc muh unmark <IP Address>`

Parameter	Description

`service_accounts <options>`	Shows and configures the suspected Service Accounts.
	Important - This feature is enabled by default.
	For more information, see the *Identity Awareness Clients Administration Guide*.
	The available <*options*> are:
	■ Show service account statistics -the current mode, known Service Accounts, and excluded accounts:
	`pdp idc service_accounts show`
	■ Configure the number of simultaneous logins (default is 100), after which all usernames are detected as Service Accounts:
	`pdp idc service_accounts set_threshold <2-1000>`
	■ Enable (this is the default) or disable the Prevent Mode (Auto-Exclude Mode):
	`pdp idc service_accounts set_auto_prevention {enable | disable}`
	Notes:
	• If you disable the Prevent Mode, then Identity Collector works in the Detect Mode.
	• When you change the work mode from Detect to Prevent, all sessions that are marked as a Service Account are revoked.
	■ Mark specific usernames as a Service Account (if prevention is enabled, the sessions for these users are revoked):
	`pdp idc service_accounts mark <username>`
	■ Configure specific usernames **not** to be detected as Service Accounts (continue to enforce identity):
	`pdp idc service_accounts add_exception <username_1> <username_2> ... <username_N>`
	■ Configure specific usernames **to be** detected as Service Accounts, if users log in the specified number of times:
	`pdp idc service_accounts delete_exception <username_1> <username_2> ... <username_N>`
	■ Remove specific usernames from the list of Service Accounts:
	`pdp idc service_accounts unmark_service_accounts`

Parameter	Description
	Note - You must put at least one space between account names. Do not put punctuation between account names. ■ Remove all usernames from the list of Service Accounts: `pdp idc service_accounts unmark_service_accounts_all`
`status`	Shows the status of configured identity sources (Identity Collectors).

pdp idp

Description

Operations related to SAML-based authentication.

Syntax

```
pdp idp groups <options>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description

`groups <options>`	Shows and configures the consolidation of external groups with the fetched groups.
	The available <*options*> are:
	■ Configure the authorization behavior for user groups:
	`pdp idp groups set {only | prefer | union | ignore}`
	• `only` - Considers only groups the Identity Provider sends. Ignore groups received from configured User Directories.
	• `prefer` -Prefers groups the Identity Provider sends. Considers groups received from configured User Directories only if the Identity Provider sends no group. This is the default.
	• `union` - Considers both groups received from configured User Directories and groups the Identity Provider sends.
	• `ignore` - Considers only groups received from configured User Directories. Ignores groups the Identity Provider sends.
	■ Shows the configured behavior:
	`pdp idp groups status`

pdp monitor

Description

Monitors the status of connected PDP sessions.

You can run different queries with the commands below to get the output, in which you are interested.

Syntax

```
pdp monitor
      all
      client_type <Client Type>
      cv_ge <Version>
      cv_le <Version>
      groups <Group Name>
      ip <IP address>
      machine <Computer Name>
      machine_exact
      mad
      network
      s_port
      summary
      user <Username>
      user_exact
```

Important:

- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description
`all`	Shows information for all connected sessions.

Parameter	Description
`client_type <Client Type>`	Shows all sessions that connect through the specified client type. Possible client types are: ■ `"AD Query"` - User was identified by the AD Query. ■ `"Identity Agent"` - User or computer was identified by an Identity Awareness Agent. ■ `portal` - User was identified by the Captive Portal. ■ `unknown` - User was identified by an unknown source.
`cv_ge <Version>`	Shows all sessions that are connected with a client version that is higher than (or equal to) the specified version.
`cv_le <Version>`	Shows all sessions that are connected through a client version that is lower than (or equal to) the specified version.
`groups <Group Name>`	Shows all sessions of users or computers that are members of the specified group.
`ip <IP address>`	Shows session information for the specified IP address.
`machine <Computer Name>`	Shows session information for the specified computer name.
`machine_exact`	Shows sessions filtered by the exact computer name.
`mad`	Shows all sessions that relate to a managed asset. For example, all sessions that successfully performed computer authentication.
`network`	Shows sessions filtered by a network wildcard. For example: `192.168.72.*`
`s_port`	Shows sessions filtered by the assigned source port (MUH sessions only).
`summary`	Shows the summary monitoring data.
`user <Username>`	Shows session information for the specified user name.
`user_exact`	Shows sessions filtered by the exact user.

Example - Show the connected user behind the IP address 192.0.2.1

```
pdp monitor ip 192.0.2.1
```

Note - The last field "`Published`" indicates whether the session information was already published to the Gateway PEPs, whose IP addresses are listed.

pdp muh

Description

Shows Multi-User Hosts (MUHs).

Syntax

```
pdp muh status
```

Important:

- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

pdp nested_groups

Description

Configures the Security Gateway queries LDAP Nested Groups.

Shows the current configuration LDAP Nested Group queries.

Syntax

```
pdp nested_groups
      auto_tune {enable | disable}
      clear
      depth <options>
      disable
      enable
      show
      status
      __set_state <options>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description
`auto_tune {enable | disable}`	Enables and disables the auto-tune feature. This feature calculates and automatically selects the state of Nested Groups based on the LDAP configuration on the Security Gateway and the Management Server. **Notes:** ■ When you enable this feature, the Security Gateway automatically configures the best the state of Nested Groups it calculated. ■ When you disable this feature, the Security Gateway automatically returns to the state of Nested Groups you configured earlier with the "`__set_state`" parameter. **Best Practice** - Enable this feature on the Policy Decision Point (PDP) to increase the performance.
`clear`	Clears the list of users, for which the depth was not enough.
`depth <1 - 40>`	Configures the nested groups depth (between 1 and 40).
`disable`	Disables the nested groups.
`enable`	Enables the nested groups.
`show`	Shows a list of users, for which the depth was not enough.
`status`	Shows the configuration status of nested groups.

Parameter	Description
`__set_state {1 | 2 | 3 | 4}`	Configures the nested groups state: ■ `1` - Recursive (this is the default) • The Security Gateway queries each user to find out its group memberships, and then queries each group recursively until it determines the nested groups. • We recommend this method for environments that have few nested groups or no nested groups configured on the LDAP server. ■ `2` - Per-user • The Security Gateway sends one LDAP query. The response includes all groups for the specified user, including the nesting levels. The response includes all groups for the given user, including nesting levels. This query shows groups from any branch in the Active Directory forest. This type of query are sent to the Global Catalog ports (TCP 3268 or 3269). • We recommend this method for environments that have a policy that includes access roles with nested groups in them. • Use this state if you work with multiple branches in the account unit, or if you use group membership cross-domain trees. For example, a user belongs to the domain tree `example1.com` and belongs to the different domain tree `example2.com`. See sk134292. ■ `3` - Multi per-group • The Security Gateway sends one LDAP query. This LDAP query includes a user and a group. The response shows if the user is included in this group. • We recommend this method for environments that have all types of users and groups and have a small number of access roles with nested groups in them. ■ `4` - Per user, if there is a single branch in each Account Unit • The Security Gateway sends one LDAP query. The response includes all groups for the specified user, including the nesting levels. This query shows groups from the branch specified in the LDAP account unit. This type of query can work over all LDAP ports (TCP 3268 or 3269, TCP 389 or 636). • Use this state if you work with a single branch on each account unit.

pdp network

Description

Shows information about network related features.

Syntax

```
pdp network {info | registered}
```

Important:

- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description
`info`	Shows a list of networks known by the PDP.
`registered`	Shows the mapping of a network address to the registered gateways (PEP module).

pdp radius

Description

Shows and configures the RADIUS accounting options.

Syntax

```
pdp radius
      ip
            reset
            set <options>
      groups
            fetch <options>
            reset
            set <options>
      parser
            reset
            set <options>
      roles
            fetch <options>
            reset
            set <options>
      status
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description

`ip <options`	Configures the secondary IP options.
	The available <*options*> are:
	■ Set the secondary IP index:
	`pdp radius ip set <attribute index> [-a <vendor specific attribute index>] [-c <vendor code>]`
	■ Reset the secondary IP settings:
	`pdp radius ip reset`

`groups <options`	Configures the options for user groups.
	The available <*options*> are:
	■ Control whether to fetch groups from RADIUS messages:
	`pdp radius groups fetch {off | on}`
	• `off` - Do not fetch.
	• `on` - Fetch.
	■ Reset user groups options:
	`pdp radius groups reset`
	■ Set group index:
	`pdp radius groups set <options>`
	• To set group index for machines:
	`pdp radius groups set -m <attribute index> [-a <vendor specific attribute index>] [-c <vendor code>] [-d <delimiter>]`
	• To set group index for users:
	`pdp radius groups set -u <attribute index> [-a <vendor specific attribute index>] [-c <vendor code>] [-d <delimiter>]`

Parameter	Description

`parser <options`	Configures the parsing options.
	The available <*options*> are:
	■ Reset parsing options:
	`pdp radius parser reset`
	■ Set parsing options for attributes:
	`pdp radius parser set <attribute index> [-c <vendor code> -a <vendor specific attribute index>] -p <prefix> -s <suffix>`

`roles <options>`	Configures how to obtain roles from RADIUS messages.
	The available <*options*> are:
	■ Control whether to fetch roles from RADIUS messages:
	`pdp radius roles fetch {off | on}`
	• `off` - Do not fetch.
	• `on` - Fetch.
	■ Reset role fetch options:
	`pdp radius roles reset`
	■ Set role index:
	`pdp radius roles set <options>`
	• Set role index for machines:
	`pdp radius roles set -m <attribute index> [-a <vendor specific attribute index>] [-c <vendor code>] [-d <delimiter>]`
	• Set role index for users:
	`pdp radius roles set -u <attribute index> [-a <vendor specific attribute index>] [-c <vendor code>] [-d <delimiter>]`

`status`	Shows the current status.

pdp roles

General Syntax

```
pdp roles
      extract
      fetch <options>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

The 'pdp roles extract' command

Description

Extracts and shows the roles from the file `$FWDIR/tmp/roles_command_output.txt` that was created with the "`pdp roles fetch`" command.

Syntax

```
pdp roles extract
```

The 'pdp roles fetch' command

Description

Fetches the roles that match the provided Access Role information and saves the output in the `$FWDIR/tmp/roles_command_output.txt` file.

Syntax

```
pdp roles fetch [-ip <IP Address>]
      -u "<Username>" -is "<Identity Source>"
      -ug "<User Group 1>","<User Group 2>",...
      -mg "<Machine Group 1>","<Machine Group 2>",...
```

Parameters

Parameter	Description
`-ip <IP Address>`	**Optional.** Specifies the IP address of identity, host, or session to calculate and fetch Access Roles that also contain explicitly selected objects in the **Networks** pane. Example for an Access Role object, in which a Host object with the IPv4 address 5.5.5.5 was selected in the **Networks** pane: `pdp roles fetch -i 5.5.5.5 -u "user_1" -is "AD_Query"`

`-u "<Username>" -is "<Identity Source>"`	Specifies the username and the identity source.
	The available identity sources are (case-sensitive):
	▪ `portal`
	▪ `Identity_Agent`
	▪ `Remote_Access`
	▪ `AD_Query`
	▪ `IFMAP`
	▪ `Terminal_Server_Identity_Agent`
	▪ `Radius_Accounting`
	Important - If in the Access Role object you explicitly selected objects in the **Networks** and **Users** panes, you must also use the parameter "`-ip <IP Address>`".
	Examples:
	`pdp roles fetch -u "user_1" -is "AD_Query"`
	`pdp roles fetch -i 5.5.5.5 -u "user_1" -is "AD_Query"`

`-ug "<User Group 1>","<User Group 2>",...`	Specifies the user group. Enter the comma separated list of group names. For Active Directory groups, you must enter the prefix "`ad_group_`". Example for an AD group called "LaptopUsers": `pdp roles fetch -ug "ad_group_LaptopUsers"`

Parameter	Description
`-mg "<Machine Group 1>","<Machine Group 2>", ...`	Specifies the machine group. Enter the comma separated list of group names. For Active Directory groups, you must enter the prefix "`ad_group_`". Example for an AD group called "Laptops": `pdp roles fetch -mg "ad_group_Laptops"`

pdp status

Description

Shows PDP status information, such as start time or configuration time.

Syntax

```
pdp status show
```

Important:

- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description
`show`	Shows PDP information.

pdp tasks_manager

Description

Shows the status of the PDP tasks (current running, previous, and pending tasks).

Syntax

```
pdp tasks_manager status
```

Important:

- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description
`status`	Shows the status of the PDP tasks.

pdp timers

Description

Shows PDP timers information for each PDP session.

Syntax

```
pdp timers show
```

Important:

- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description
`show`	Shows PDP timers information for each PDP session: ■ `User Auth Timer` ■ `Machine Auth Timer` ■ `Pep Cache Timer` ■ `Compliance Timer` ■ `Keep Alive Timer` ■ `Ldap Fetch Timer`

pdp topology_map

Description

Shows topology of all PDP and PEP addresses.

Syntax

```
pdp topology_map
```

Important:

- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

pdp tracker

Description

During the PDP debug, adds the `TRACKER` debug topic to the PDP logs (this is enabled by default).

This is very useful when you monitor the PDP-to-PEP identity sharing and other communication in distributed environments.

You can set this manually if you add the `TRACKER` topic to the PDP debug.

Syntax

```
pdp tracker {off | on}
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description
`off`	Disables the logging of `TRACKER` events in the PDP log.
`on`	Enables the logging of `TRACKER` events in the PDP log.

pdp update

Description

Initiates a recalculation of group membership for all users and computers.

Important - This command does **not** update deleted accounts.

Syntax

```
pdp update {all | specific}
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description
`all`	Recalculates group membership for all users and computers.
`specific`	Recalculates group membership for a specified user or a computer.

pdp vpn

Description

Shows the connected VPN Gateways that send identity data for VPN Remote Access Client.

Syntax

```
pdp vpn show
```

Important:

- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description
`show`	Shows the connected VPN gateways.

pep

Description

Provides commands to control and monitor the *PEPD* process (see below for options).

Syntax

```
pep <command> [<parameter> [<option>]]
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Commands

Command	Description
`control <parameter> <option>`	Controls the PEP parameters. See *"pep control" on page 327*.
`debug <parameter> <option>`	Controls the PEP debug. See *"pep debug" on page 330*.
`show <parameter> <option>`	Shows PEP information. See *"pep show" on page 332*.
`tracker <parameter>`	During the PEP debug, adds the `TRACKER` debug topic to the PEP logs. See *"pep tracker" on page 335*.

pep control

Description

Provides commands to control the PEP.

Syntax

```
pep control
      extended_info_storage <options>
      gbuf_cache <option>
      identity_cache_mode status
      kbuf_cache <option>
      portal_dual_stack <options>
      tasks_manager status <options>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description
`extended_info_storage <options>`	Controls whether PEP stores the extended identities information for debug. The available <*options*> are: ▪ `disable` - PEP does not store the information. ▪ `enable` - PEP stores the information.

Parameter	Description

`gbuf_cache <option>`	Controls the global buffer cache for Identity Awareness kernel tables.
	Warning - Do not change the default values, unless Check Point Support explicitly instructed you to do so.
	The available <*options*> are:
	■ Show the current status:
	`pep control gbuf_cache status`
	■ Enable the global buffer cache (this is the default):
	`pep control gbuf_cache enable`
	■ Disable the global buffer cache:
	`pep control gbuf_cache disable`
	■ Show the current memory limit for the global buffer cache:
	`pep control gbuf_cache memory_limit show`
	■ Configure the memory limit for the global buffer cache (default is 100 megabytes - 104,857,600 bytes):
	`pep control gbuf_cache memory_limit set <Number of Bytes>`

`identity_ cache_mode status`	Shows the current status of the Identity Cache Mode for the PDP-to-PEP sharing protocol. For more information, see the *R82 Identity Awareness Administration Guide* > Chapter "**Advanced Identity Awareness Environment**" > Section "**Identity Cache Mode for Identity Sharing Protocols**".

Parameter	Description

`kbuf_cache <option>`	Controls the kernel buffer cache for Identity Awareness kernel tables.
	Warning - Do not change the default values, unless Check Point Support explicitly instructed you to do so.
	The available <*options*> are:
	■ Show the current status:
	`pep control kbuf_cache status`
	■ Enable the kernel buffer cache (this is the default):
	`pep control kbuf_cache enable`
	■ Disable the kernel buffer cache:
	`pep control kbuf_cache disable`
	■ Show the current memory limit for the kernel buffer cache:
	`pep control kbuf_cache memory_limit show`
	■ Configure the memory limit for the kernel buffer cache (default is 100 megabytes - 104,857,600 bytes):
	`pep control kbuf_cache memory_limit set <Number of Bytes>`

`portal_ dual_stack <options>`	Controls the support for portal dual stack (IPv4 and IPv6). The available <*options*> are: ■ `disable` - Disables the support. ■ `enable` - Enables the support.
`tasks_ manager <options>`	Shows the status of the PEP tasks (current running, previous, and pending tasks). The available <*options*> are: ■ `status` - Shows the status.

pep debug

Description

Controls the debug of the PEP.

Syntax

```
pep debug
      memory
      off
      on
      reset
      rotate
      set <options>
      spaces [<options>]
      stat
      unset <options>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description
`memory`	Displays the memory consumption by the *pepd* daemon.
`off`	Disables the PEP debug.
`on`	Enables the PEP debug. **Important** - After you run this command "`pep debug on`", you must run the command "`pep debug set ...`" to determine the required filter.
`reset`	Resets the PEP debug options for Debug Topics and Severities. **Important** - After you run this command "`pep debug reset ...`", you must run the command "`pep debug off`" to turn off the debug.

Parameter	Description
`rotate`	Rotates the PEP log files - increases the index of each log file: ■ `$FWDIR/log/pepd.elg` becomes `$FWDIR/log/pepd.elg.0`, ■ `$FWDIR/log/pepd.elg.0` becomes `$FWDIR/log/pepd.elg.1` ■ And so on.
`set <Topic Name> <Severity>`	Filters which debug logs PEP writes to the log file based on the specified Debug Topics and Severity. Available Debug Topics are: ■ `all` ■ Check Point Support provides more specific topics, based on the reported issue Available Severities are: ■ `all` ■ `critical` ■ `events` ■ `important` ■ `surprise` **Best Practice** - We recommend to enable all Topics and all Severities. Run: `pep debug set all all`
`spaces [0 | 1 | 2 | 3 | 4 | 5]`	Displays and sets the number of indentation spaces in the `$FWDIR/log/pepd.elg` file. The default is 0 spaces.
`stat`	Shows the PEP current debug status.
`unset <Topic Name>`	Unsets the specified Debug Topic(s).

Important - When you enable the debug, it affects the performance of the *pepd* daemon. Make sure to turn off the debug after you complete your troubleshooting.

pep show

Description

Shows information about PEP.

Syntax

```
pep show
    conciliation_clashes
        all
        clear
        ip <Session IP Address>
    network
        pdp
        registration
    pdp
        all
        id <ID of PDP>
    stat
    topology_map
    user
        all
        query
                cid <IP[,ID]>
                cmp <Compliance>
                mchn <Computer Name>
                mgrp <Group>
                pdp <IP[,ID]>
                role <Identity Role>
                ugrp <Group>
                uid <UID String>
                usr <Username>
```

Important:

- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description
`conciliation_clashes <options>`	Shows session conciliation clashes. The available <*options*> are: ■ `all` - Show all conciliation clashes. ■ `clear` - Clears all session clashes. ■ `ip <Session IP Address>` - Show all conciliation clashes filtered by the specified session IP address.
`network <options>`	Shows network related information. The available <*options*> are: ■ `pdp` - Shows the Network-to-PDP mapping table. ■ `registration` - Shows the networks registration table.
`pdp <options>`	Shows the communication channel between the PEP and the PDP. Available <*options*> are: ■ `all` - Shows all connected PDPs. ■ `id` - Shows the information for the specified PDP.
`stat`	Shows the last time the *pepd* daemon was started and the last time a policy was received. **Important** - Each time the *pepd* daemon starts, it loads the policy and the two timers. The times between the *pepd* daemon start and when it fetched the policy are very close.
`topology_map`	Shows topology of all PDP and PEP addresses.

Parameter	Description
`user <options>`	Shows the status of sessions that PEP knows. You can perform various queries to get the applicable output (see below). The available <*options*> are: ■ `all` - Shows the list of all clients. ■ `query` - Queries the list of users based on the specified filters: • `cid <IP[,ID]>` - Matches entries of clients with the specified Client ID. • `cmp <Compliance>` - Matches entries with the specified compliance. • `mchn <Computer Name>` - Matches entries with the specified computer name. • `mgrp <Group>` - Matches entries with the specified machine group. • `pdp <IP[,ID]>` - Matches entries, which the specified PDP updated. • `role <Identity Role>` - Matches entries with the specified identity role. • `ugrp <Group>` - Matches entries with the specified user group. • `uid <UID String>` - Matches entries with the specified full or partial UID. • `usr <Username>` - Matches entries with the specified username. **Note** - You can use multiple query filters at the same time to create a logical *AND* correlation between them. For example, to show all users that have a sub-string of "`jo`" AND are part of the user group "`Employees`" you can use this query syntax: `# pep show user query usr jo ugrp Employees`

pep tracker

Description

During the PEP debug, adds the `TRACKER` debug topic to the PEP logs (this is enabled by default).

This is very useful when you monitor the PDP-to-PEP identity sharing and other communication in distributed environments.

You can set this manually if you add the `TRACKER` topic to the PEP debug.

Syntax

```
pep tracker {off | on}
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description
`off`	Disables the logging of `TRACKER` events in the PEP log.
`on`	Enables the logging of `TRACKER` events in the PEP log.

test_ad_connectivity

Description

This utility runs connectivity tests from the Security Gateway to an AD domain controller.

You can define the parameters for this utility in one of these ways:

- In the command line as specified below
- In the `$FWDIR/conf/test_ad_connectivity.conf` configuration file.

  Parameters you define in the `$FWDIR/conf/test_ad_connectivity.conf` file cannot contain white spaces and cannot be within quotation marks.

Important:

- Parameters you enter in the command line override the parameters you enter in the configuration file.
- This utility saves its output in the file you specify with the "`-o`" parameter.
  In addition, examine the `$FWDIR/log/test_ad_connectivity.elg` file.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Syntax

```
[Expert@HostName:0]# $FWDIR/bin/test_ad_connectivity -h
```

```
[Expert@HostName:0]# $FWDIR/bin/test_ad_connectivity <Parameter_1 Value_1> <Parameter Value_2> ... <Parameter_N Value_N>
 ...<Parameters And Options>
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Mandatory / Optional	Description
`-h`	Optional	Shows the built-in help.

Parameter	Mandatory / Optional	Description
`-a`	**Mandatory** Use only one of these options: ■ `-a` ■ `-c` ■ `-p`	Prompts the user for the password on the screen.
`-b <LDAP Search Base String>`	Optional	Specifies the LDAP Search Base String.
`-c <Password in Clear Text>`	**Mandatory** Use only one of these options: ■ `-a` ■ `-c` ■ `-p`	Specifies the user's password in clear text.
`-d <Domain Name>`	**Mandatory**	Specifies the domain name of the AD (for example, `ad.mycompany.com`).
`-D <User DN>`	**Mandatory**	Overrides the LDAP user DN (the utility does not try to figure out the DN automatically).
`-f <AD Fingerprint for LDAPS>`	Optional	Specifies the AD fingerprint for LDAPS.
`-i <IPv4 address of DC>`	**Mandatory**	Specifies the IPv4 address of the AD domain controller to tested.
`-I <IPv6 address of DC>`	**Mandatory**	Specifies the IPv6 address of the AD domain controller to test.
`-o <File Name>`	**Mandatory**	Specifies the name of the output file. This utility always saves the output file in the `$FWDIR/tmp/` directory.

Parameter	Mandatory / Optional	Description
`-p <Obfuscated Password>`	**Mandatory** Use only one of these options: ■ `-a` ■ `-c` ■ `-p`	Specifies the user's password in obfuscated text.
`-l`	Optional	Runs LDAP connectivity test only (no WMI test).
`-L <Timeout>`	Optional	Specifies the timeout (in milliseconds) for the LDAP test only. If this timeout expires, and the LDAP test still runs, then both LDAP connectivity and WMI connectivity tests fail.
`-M`	Optional	Run the utility in demo mode.
`-r <Port Number>`	Optional	Specifies the LDAP or LDAPS connection port number. The default ports are: ■ LDAP - 389 ■ LDAPS - 636
`-s`	Optional	Specifies that LDAP connection must be over SSL.
`-t <Timeout>`	Optional	Specifies the total timeout (in milliseconds) for both LDAP connectivity and WMI connectivity tests.
`-u <Username>`	**Mandatory**	Specifies the administrator user name on the AD.
`-v`	Optional	Prints the full path to the specified output file.
`-x <Domain Name>`	**Mandatory**	Specifies the domain name of the AD (for example, `ad.mycompany.com`). Utility prompts the user for the password.
`-w`	Optional	Runs WMI connectivity test only (no LDAP test).

Example

IPv4 of AD DC	`192.168.230.240`
Domain	`mydc.local`
Username	`Administrator`
Password	`aaaa`
Syntax	`[Expert@GW:0]# $FWDIR/bin/test_ad_connectivity -u "Administrator" -c "aaaa" -D "CN=Administrator,CN=Users,DC=mydc,DC=local" -d mydc.local -i 192.168.230.240 -b "DC=mydc,DC=local" -o test.txt` `[Expert@GW:0]#`

Output	`[Expert@GW:0]# cat $FWDIR/tmp/test.txt`
	`(`
	`:status (SUCCESS_LDAP_WMI)`
	`:err_msg ("WMI_SUCCESS;LDAP_SUCCESS")`
	`:ldap_status (LDAP_SUCCESS)`
	`:wmi_status (WMI_SUCCESS)`
	`:timestamp ("Mon Feb 26 10:17:41 2018")`
	`)`
	`[Expert@GW:0]#`

Note - In order to know the output is authentic, pay attention that the timestamp is the same as the local time.

Working with Kernel Parameters

See the *R82 Quantum Security Gateway Guide* > Chapter "Working with Kernel Parameters".

Kernel Debug

See the *R82 Quantum Security Gateway Guide* > Chapter "Kernel Debug on Security Gateway".

Appendix: Regular Expressions

Regular Expression Syntax

This table shows the Check Point implementation of standard regular expression metacharacters.

Metacharacter	Name	Description
\	Backslash	escape metacharacters non-printable characters character types
[ ]	Square Brackets	character class definition
( )	Parenthesis	sub-pattern, to use metacharacters on the enclosed string
{min,[max]}	Curly Brackets	min/max quantifier {n} - exactly n occurrences {n,m} - from n to m occurrences {n,} - at least n occurrences
.	Dot	match any character
?	Question Mark	zero or one occurrences (equals {0,1})
*	Asterisk	zero or more occurrences of preceding character
+	Plus Sign	one or more occurrences (equals {1,})
|	Vertical Bar	alternative
^	Circumflex	anchor pattern to beginning of buffer (usually a word)
$	Dollar	anchor pattern to end of buffer (usually a word)
-	hyphen	range in character class

Using Non-Printable Characters

To use non-printable characters in patterns, escape the reserved character set.

Character	Description
\a	alarm; the BEL character (hex code 07)
\cX	"control-X", where X is any character
\e	escape (hex code 1B)
\f	formfeed (hex code 0C)
\n	newline (hex code 0A)
\r	carriage return (hex code 0D)
\t	tab (hex code 09)
\ddd	character with octal code ddd
\xhh	character with hex code hh

Using Character Types

To specify types of characters in patterns, escape the reserved character.

Character	Description
\d	any decimal digit [0-9]
\D	any character that is not a decimal digit
\s	any whitespace character
\S	any character that is not whitespace
\w	any word character (underscore or alphanumeric character)
\W	any non-word character (not underscore or alphanumeric)

Glossary

A

Access Role
Access Role objects let you configure network access according to: Networks, Users and user groups, Computers and computer groups, Remote Access Clients. After you activate the Identity Awareness Software Blade, you can create Access Role objects and use them in the Source and Destination columns of Access Control Policy rules.

AD Query
Check Point clientless identity acquisition tool. It is based on Active Directory integration and it is completely transparent to the user. The technology is based on querying the Active Directory Security Event Logs and extracting the user and computer mapping to the network address from them. It is based on Windows Management Instrumentation (WMI), a standard Microsoft protocol. The Check Point Security Gateway communicates directly with the Active Directory domain controllers and does not require a separate server. No installation is necessary on the clients, or on the Active Directory server.

Anti-Bot
Check Point Software Blade on a Security Gateway that blocks botnet behavior and communication to Command and Control (C&C) centers. Acronyms: AB, ABOT.

Anti-Spam
Check Point Software Blade on a Security Gateway that provides comprehensive protection for email inspection. Synonym: Anti-Spam & Email Security. Acronyms: AS, ASPAM.

Anti-Virus
Check Point Software Blade on a Security Gateway that uses real-time virus signatures and anomaly-based protections from ThreatCloud to detect and block malware at the Security Gateway before users are affected. Acronym: AV.

Application Control
Check Point Software Blade on a Security Gateway that allows granular control over specific web-enabled applications by using deep packet inspection. Acronym: APPI.

Audit Log
Log that contains administrator actions on a Management Server (login and logout, creation or modification of an object, installation of a policy, and so on).

B

Bridge Mode
Security Gateway or Virtual System that works as a Layer 2 bridge device for easy deployment in an existing topology.

Browser-Based Authentication
Authentication of users in Check Point Identity Awareness web portal - Captive Portal, to which users connect with their web browser to log in and authenticate.

C

Captive Portal
A Check Point Identity Awareness web portal, to which users connect with their web browser to log in and authenticate, when using Browser-Based Authentication.

Cloud Credentials
Specific credentials from identity providers used by the Identity Collector to connect seamlessly to the Infinity Portal. These credentials are essential for establishing a secure and efficient connection between the Identity Client and the Infinity Portal.

Cloud Services
Refers to a centralized identities solution provided by Infinity Identity and Directory Sync. These services offer identity management and directory synchronization capabilities, hosted and managed in the cloud.

Cluster
Two or more Security Gateways that work together in a redundant configuration - High Availability, or Load Sharing.

Cluster Member
Security Gateway that is part of a cluster.

Compliance
Check Point Software Blade on a Management Server to view and apply the Security Best Practices to the managed Security Gateways. This Software Blade includes a library of Check Point-defined Security Best Practices to use as a baseline for good Security Gateway and Policy configuration.

Content Awareness
Check Point Software Blade on a Security Gateway that provides data visibility and enforcement. Acronym: CTNT.

CoreXL
Performance-enhancing technology for Security Gateways on multi-core processing platforms. Multiple Check Point Firewall instances are running in parallel on multiple CPU cores.

CoreXL Firewall Instance
On a Security Gateway with CoreXL enabled, the Firewall kernel is copied multiple times. Each replicated copy, or firewall instance, runs on one processing CPU core. These firewall instances handle traffic at the same time, and each firewall instance is a complete and independent firewall inspection kernel. Synonym: CoreXL FW Instance.

CoreXL SND
Secure Network Distributer. Part of CoreXL that is responsible for: Processing incoming traffic from the network interfaces; Securely accelerating authorized packets (if SecureXL is enabled); Distributing non-accelerated packets between Firewall kernel instances (SND maintains global dispatching table, which maps connections that were assigned to CoreXL Firewall instances). Traffic distribution between CoreXL Firewall instances is statically based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type. The CoreXL SND does not really "touch" packets. The decision to stick to a particular FWK daemon is done at the first packet of connection on a very high level, before anything else. Depending on the SecureXL settings, and in most of the cases, the SecureXL can be offloading decryption calculations. However, in some other cases, such as with Route-Based VPN, it is done by FWK daemon.

CPUSE
Check Point Upgrade Service Engine for Gaia Operating System. With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself.

D

DAIP Gateway
Dynamically Assigned IP (DAIP) Security Gateway is a Security Gateway, on which the IP address of the external interface is assigned dynamically by the ISP.

Data Loss Prevention
Check Point Software Blade on a Security Gateway that detects and prevents the unauthorized transmission of confidential information outside the organization. Acronym: DLP.

Data Type
Classification of data in a Check Point Security Policy for the Content Awareness Software Blade.

Directory Sync
A solution that holds static Directory information regarding users, groups, devices, and memberships. .

Distributed Deployment
Configuration in which the Check Point Security Gateway and the Security Management Server products are installed on different computers.

Dynamic Object
Special object type, whose IP address is not known in advance. The Security Gateway resolves the IP address of this object in real time.

E

Endpoint Policy Management
Check Point Software Blade on a Management Server to manage an on-premises Harmony Endpoint Security environment.

Expert Mode
The name of the elevated command line shell that gives full system root permissions in the Check Point Gaia operating system.

G

Gaia
Check Point security operating system that combines the strengths of both SecurePlatform and IPSO operating systems.

Gaia Clish
The name of the default command line shell in Check Point Gaia operating system. This is a restricted shell (role-based administration controls the number of commands available in the shell).

Gaia Portal
Web interface for the Check Point Gaia operating system.

H

Hotfix
Software package installed on top of the current software version to fix a wrong or undesired behavior, and to add a new behavior.

HTTPS Inspection
Feature on a Security Gateway that inspects traffic encrypted by the Secure Sockets Layer (SSL) protocol for malware or suspicious patterns. Synonym: SSL Inspection. Acronyms: HTTPSI, HTTPSi.

I

ICA
Internal Certificate Authority. A component on Check Point Management Server that issues certificates for authentication.

Identity Agent
Check Point dedicated client agent installed on Windows-based user endpoint computers. This Identity Agent acquires and reports identities to the Check Point Identity Awareness Security Gateway. The administrator configures the Identity Agents (not the end users). There are two types of Identity Agents - Full and Light. You can download the Full and Light Identity Agent package from the Captive Portal - 'https://<Gateway_IP_Address>/connect' or from Support Center.

Identity Agent Configuration Utility
Check Point utility that creates custom Identity Agent installation packages. This utility is installed as a part of the Identity Agent: go to the Windows Start menu > All Programs > Check Point > Identity Agent > right-click the 'Identity Agent' shortcut > select 'Properties' > click 'Open File Location' ('Find Target' in some Windows versions > double-click 'IAConfigTool.exe').

Identity Agent Distributed Configuration Tool
Check Point Identity Agent control tool for Windows-based client computers that are members of an Active Directory domain. The Distributed Configuration tool lets you configure connectivity and trust rules for Identity Agents - to which Identity Awareness Security Gateways the Identity Agent should connect, depending on its IPv4 / IPv6 address, or Active Directory Site. This tool is installed a part of the Identity Agent: go to the Windows Start menu > All Programs > Check Point > Identity Agent > open the Distributed Configuration. Note - You must have administrative access to this Active Directory domain to allow automatic creation of new LDAP keys and writing.

Identity Awareness
Check Point Software Blade on a Security Gateway that enforces network access and audits data based on network location, the identity of the user, and the identity of the computer. Acronym: IDA.

Identity Broker
Identity Sharing mechanism between Identity Servers (PDP): (1) Communication channel between PDPs based on Web-API (2) Identity Sharing capabilities between PDPs - ability to add, remove, and update the identity session.

Identity Collector
Check Point dedicated client agent installed on Windows Servers in your network. Identity Collector collects information about identities and their associated IP addresses and sends it to the Check Point Security Gateways for identity enforcement, you can download the Identity Collector package from the Support Center.

Identity Collector Identity Sources
Identity Sources for Check Point Identity Collector - Microsoft Active Directory Domain Controllers, Cisco Identity Services Engine (ISE) Servers, or NetIQ eDirectory Servers.

Identity Collector Query Pool
A list of Identity Sources for Check Point Identity Collector.

Identity Logging
Check Point Software Blade on a Management Server to view Identity Logs from the managed Security Gateways with enabled Identity Awareness Software Blade.

Identity Server
Check Point Security Gateway with enabled Identity Awareness Software Blade.

Internal Network
Computers and resources protected by the Firewall and accessed by authenticated users.

IPS
Check Point Software Blade on a Security Gateway that inspects and analyzes packets and data for numerous types of risks (Intrusion Prevention System).

IPsec VPN
Check Point Software Blade on a Security Gateway that provides a Site to Site VPN and Remote Access VPN access.

J

Jumbo Hotfix Accumulator
Collection of hotfixes combined into a single package. Acronyms: JHA, JHF, JHFA.

K

Kerberos
An authentication server for Microsoft Windows Active Directory Federation Services (ADFS).

L

Log Server
Dedicated Check Point server that runs Check Point software to store and process logs.

Logging & Status
Check Point Software Blade on a Management Server to view Security Logs from the managed Security Gateways.

M

Management Interface
(1) Interface on a Gaia Security Gateway or Cluster member, through which Management Server connects to the Security Gateway or Cluster member. (2) Interface on Gaia computer, through which users connect to Gaia Portal or CLI.

Management Server
Check Point Single-Domain Security Management Server or a Multi-Domain Security Management Server.

Manual NAT Rules
Manual configuration of NAT rules by the administrator of the Check Point Management Server.

Mobile Access
Check Point Software Blade on a Security Gateway that provides a Remote Access VPN access for managed and unmanaged clients. Acronym: MAB.

Multi-Domain Log Server
Dedicated Check Point server that runs Check Point software to store and process logs in a Multi-Domain Security Management environment. The Multi-Domain Log Server consists of Domain Log Servers that store and process logs from Security Gateways that are managed by the corresponding Domain Management Servers. Acronym: MDLS.

Multi-Domain Server
Dedicated Check Point server that runs Check Point software to host virtual Security Management Servers called Domain Management Servers. Synonym: Multi-Domain Security Management Server. Acronym: MDS.

N

NAC
Network Access Control. This is an approach to computer security that attempts to unify endpoint security technology (such as Anti-Virus, Intrusion Prevention, and Vulnerability Assessment), user or system authentication and network security enforcement. Check Point's Network Access Control solution is called Identity Awareness Software Blade.

Network Object
Logical object that represents different parts of corporate topology - computers, IP addresses, traffic protocols, and so on. Administrators use these objects in Security Policies.

Network Policy Management
Check Point Software Blade on a Management Server to manage an on-premises environment with an Access Control and Threat Prevention policies.

O

Open Server
Physical computer manufactured and distributed by a company, other than Check Point.

P

PDP
Check Point Identity Awareness Security Gateway that acts as Policy Decision Point: acquires identities from identity sources; shares identities with other gateways.

PEP
Check Point Identity Awareness Security Gateway that acts as Policy Enforcement Point: receives identities via identity sharing; redirects users to Captive Portal.

Provisioning
Check Point Software Blade on a Management Server that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: SmartProvisioning, SmartLSM, Large-Scale Management, LSM.

Publisher PDP
Check Point Identity Awareness Security Gateway that gets identities from an identity source/remote PDP and shares identities to a remote PDP. The Publisher PDP: (1) Initiates an HTTPS connection to the Subscriber PDP for each Identity to be shared (2) Verifies the CN and OU present in the subject field of the certificate presented (3) Verifies that the CA's certificate matches the certificate that was approved in advance by the administrator (4) Checks if the certificate presented is revoked (5) Shares identities including the information about user(s), machine(s) and Access Roles in the form of HTTP POST requests.

Q

QoS
Check Point Software Blade on a Security Gateway that provides policy-based traffic bandwidth management to prioritize business-critical traffic and guarantee bandwidth and control latency.

R

Rule
Set of traffic parameters and other conditions in a Rule Base (Security Policy) that cause specified actions to be taken for a communication session.

Rule Base
All rules configured in a given Security Policy. Synonym: Rulebase.

S

SecureXL
Check Point product on a Security Gateway that accelerates IPv4 and IPv6 traffic that passes through a Security Gateway.

Security Gateway
Dedicated Check Point server that runs Check Point software to inspect traffic and enforce Security Policies for connected network resources.

Security Management Server
Dedicated Check Point server that runs Check Point software to manage the objects and policies in a Check Point environment within a single management Domain. Synonym: Single-Domain Security Management Server.

Security Policy
Collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.

Service Account
In Microsoft® Active Directory, a user account created explicitly to provide a security context for services running on Microsoft® Windows® Server.

SIC
Secure Internal Communication. The Check Point proprietary mechanism with which Check Point computers that run Check Point software authenticate each other over SSL, for secure communication. This authentication is based on the certificates issued by the ICA on a Check Point Management Server.

SmartConsole
Check Point GUI application used to manage a Check Point environment - configure Security Policies, configure devices, monitor products and events, install updates, and so on.

SmartDashboard
Legacy Check Point GUI client used to create and manage the security settings in versions R77.30 and lower. In versions R80.X and higher is still used to configure specific legacy settings.

SmartProvisioning
Check Point Software Blade on a Management Server (the actual name is "Provisioning") that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: Large-Scale Management, SmartLSM, LSM.

SmartUpdate
Legacy Check Point GUI client used to manage licenses and contracts in a Check Point environment.

Software Blade
Specific security solution (module): (1) On a Security Gateway, each Software Blade inspects specific characteristics of the traffic (2) On a Management Server, each Software Blade enables different management capabilities.

Standalone
Configuration in which the Security Gateway and the Security Management Server products are installed and configured on the same server.

Subscriber PDP
Check Point Identity Awareness Security Gateway that gets identities from a remote PDP. The Subscriber PDP: (1) Presents the configured SSL certificate to the Publisher PDP (2) Receives the information from the Publisher PDP after verifying the pre-shared secret in the POST requests.

T

Terminal Servers Identity Agent
Dedicated client agent installed on Microsoft® Windows-based application server that hosts Terminal Servers, Citrix XenApp, and Citrix XenDesktop services. This client agent acquires and reports identities to the Check Point Identity Awareness Security Gateway. In the past, this client agent was called Multi-User Host (MUH) Agent. You can download the Terminal Servers Identity Agent from Support Center.

Threat Emulation
Check Point Software Blade on a Security Gateway that monitors the behavior of files in a sandbox to determine whether or not they are malicious. Acronym: TE.

Threat Extraction
Check Point Software Blade on a Security Gateway that removes malicious content from files. Acronym: TEX.

Transactions
In the context of the Identity Collector, involves the aggregation of events from identity sources, the creation of a request, and the sending of this request to a target. The target then replies with a response. A transaction refers to this request-response.

U

Updatable Object
Network object that represents an external service, such as Microsoft 365, AWS, Geo locations, and more.

URL Filtering
Check Point Software Blade on a Security Gateway that allows granular control over which web sites can be accessed by a given group of users, computers or networks. Acronym: URLF.

User Directory
Check Point Software Blade on a Management Server that integrates LDAP and other external user management servers with Check Point products and security solutions.

V

VSX
Virtual System Extension. Check Point virtual networking solution, hosted on a computer or cluster with virtual abstractions of Check Point Security Gateways and other network devices. These Virtual Devices provide the same functionality as their physical counterparts.

VSX Gateway
Physical server that hosts VSX virtual networks, including all Virtual Devices that provide the functionality of physical network devices. It holds at least one Virtual System, which is called VS0.

Z

Zero Phishing
Check Point Software Blade on a Security Gateway (R81.20 and higher) that provides real-time phishing prevention based on URLs. Acronym: ZPH.