13 March 2017

Identity Awareness

R80.10

Administration Guide

Check Point
SOFTWARE TECHNOLOGIES LTD.

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.

Check Point R80.10

For more about this release, see the R80.10 home page http://supportcontent.checkpoint.com/solutions?id=sk111841.

Latest Version of this Document

Download the latest version of this document http://supportcontent.checkpoint.com/documentation_download?ID=TBD.

To learn more, visit the Check Point Support Center http://supportcenter.checkpoint.com.

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Identity Awareness R80.10 Administration Guide.

Searching in Multiple PDFs

To search for text in all the R80.10 PDF documents, download and extract the complete R80.10 documentation package http://supportcontent.checkpoint.com/documentation_download?ID=TBD.
Use **Shift-Control-F** in Adobe Reader or Foxit reader.

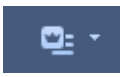
Revision History

Date	Description
13 March 2017	First release of this document

SmartConsole Toolbars

For a guided tour of SmartConsole, click **What's New** in the left bottom corner of SmartConsole.

Global Toolbar (top left of SmartConsole)

	Description and Keyboard Shortcut
	The main SmartConsole Menu
	The **Objects** menu. Also leads to the Object Explorer **Ctrl+E**

	Description and Keyboard Shortcut
	Install policy on managed gateways **Ctrl+Shift+Enter**

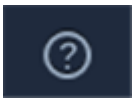
Navigation Toolbar (left side of SmartConsole)

	Description and Keyboard Shortcut
	Gateway configuration view **Ctrl+1**
	Security Policies Access Control view Security Policies Threat Prevention view **Ctrl+2**
	Logs & Monitor view **Ctrl+3**
	Manage & Settings view - review and configure the Security Management Server settings **Ctrl+4**

Command Line Interface Button (left bottom corner of SmartConsole)

	Description and Keyboard Shortcut
	Open a command line interface for management scripting and API **F9**

What's New Button (left bottom corner of SmartConsole)

	Description and Keyboard Shortcut
	Open a tour of the SmartConsole

Objects and Validations Tabs (right side of SmartConsole)

	Description
Objects	Manage security and network objects
Validations	Validation warnings and errors

System Information Area (bottom of SmartConsole)

	Description
Task List	Management activities, such as policy installation tasks
Server Details	The IP address of the Security Management Server

	Description
Connected Users	The administrators that are connected to the Security Management Server

Contents

Terms

AD

Active Directory. Microsoft directory information service. Stores data about user, computer, and service identities for authentication and access.

AD Query

A clientless identity acquisition technology that gets user and device identities from the Active Directory server.

Captive Portal

Also Browser-Based Authentication. A feature where users can authenticate and log in with a special Web page that shows in a browser.

Identity Agent

A dedicated software client installed on user computers that gets identity information and sends it to the Security Gateway.

RADIUS Accounting

A client/server protocol for getting user and device information from RADIUS authentication servers.

Rule

A set of traffic parameters and other conditions that cause specified actions to be taken for a communication session.

Rule Base

The database that contains the rules in a security policy and defines the sequence in which they are enforced.

Security Gateway

A computer or an appliance that inspects traffic and enforces Security Policies for connected network resources.

Security Management Server

The server that manages, creates, stores, and distributes the security policy to Security Gateways.

Service Account

In AD, a user account created explicitly to provide a security context for services running on Microsoft® Windows® Server.

SmartConsole

A Check Point GUI application used to manage security policies, monitor products and events, install updates, provision new devices and appliances, and manage a multi-domain environment.

Introduction to Identity Awareness

In This Section:

Traditionally, firewalls use IP addresses to monitor traffic and are unaware of the user and computer identities behind those IP addresses. Identity Awareness removes this notion of anonymity since it maps users and computer identities. This lets you enforce access and audit data based on identity.

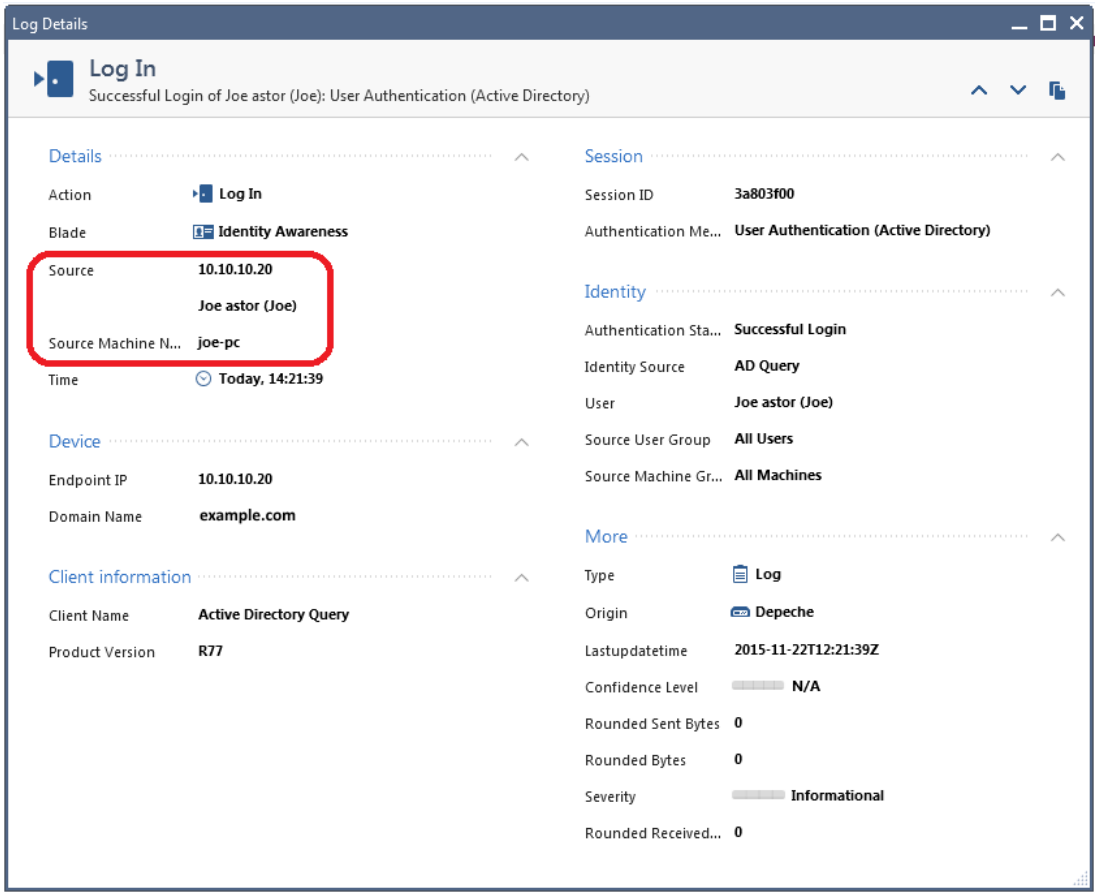
Identity Awareness is an easy to deploy and scalable solution. It is applicable for both Active Directory and non-Active Directory based networks as well as for employees and guest users.

Identity Awareness uses the Source and Destination IP addresses of network traffic to identity users and computers. You can use these elements as matching criteria in the Source and Destination fields of your policy rules:

- The identity of users or user groups
- The identity of computers or computer groups

Identity Awareness lets 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.

You can see the logs based on user and computer name, and not just IP addresses, in the **Logs & Monitor** > **Logs** tab. You can see events in the **Logs & Monitor** Access Control views.



Identity Awareness gets identities from these identity sources. You must enable them on the Gateway, from the **Identity Awareness** page of the Gateway object:

- Active Directory (AD) Query
- Browser-Based Authentication
- Identity Agents (installed on the Endpoint)
- Terminal Servers Agents
- Radius Accounting
- Remote Access
- Identity Collector
- Web API

Identity Awareness Security Gateways can share the identity information that they acquire with other Identity Awareness Security Gateways. This way, users that need to pass through many Security Gateways are only identified once. See Advanced Deployment ("Advanced Identity Awareness Deployment" on page 83) for more information.

Access Role Objects

In SmartConsole, you can create Access Role objects to define 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 can include one or more of these objects:

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

For example, a rule that allows file sharing between the IT department and the Sales department access roles.

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

Identity Sources

AD Query

AD Query is an easy to deploy, clientless identity acquisition tool. It is based on Active Directory integration and it is completely transparent to the user.

AD Query works when:

- An identified user or computer tries to access 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.
- AD Query is selected as a way to acquire identities.

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 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.

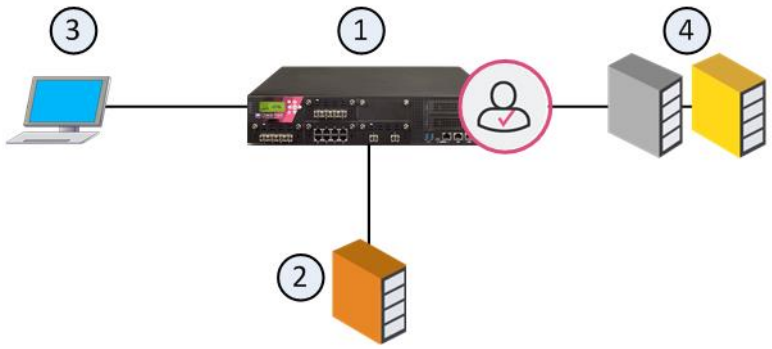
AD Query extracts user and computer identity information from the Active Directory Security Event Logs. The system generates a Security Event Log entry when a user or a computer accesses a network resource. For example, this occurs when a user logs in, unlocks a screen, or accesses a network drive. Security Event Logs are not generated when a user logs out because Active Directory cannot detect this action.

When you work with AD Query, it is important that you understand and comply with these limitations:

- **User/IP association timeout -** After a predefined period of network inactivity, a user session closes automatically. The user must log in again with the Captive Portal.
- **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 remain active until their **User/IP association timeout** occurs. In this scenario, there is a risk that currently connected users can access network resources for which they do not have permissions.

How AD Query Works- Firewall Rule Base



Item	Description
1	Security Gateway
2	Active Directory domain controller
3	User with Active Directory credentials
4	Network resources

The Security Gateway (1) gets security event logs from the Active Directory domain controllers (2).

A user logs in to a computer with Active Directory credentials (3).

The Active Directory domain controller (2) sends the security event log to the Security Gateway (1). The Security Gateway gets the user name (@domain), computer name and source IP address).

The user opens a connection to the network resource (4).

The Security Gateway confirms the user identity and allows or blocks access to the resource based on the policy.

Browser-Based Authentication

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

- Captive Portal
- Transparent Kerberos Authentication

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

Transparent Kerberos Authentication authenticates users by getting authentication data from the browser without any 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.

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

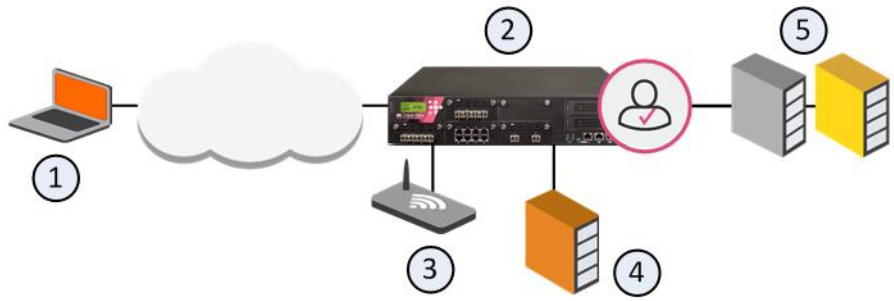
- Captive Portal is enabled.
- The **redirect** option enabled for the applicable rule.
- Firewall or Application Control and URL Filtering rules block access by unidentified users to resources that would be allowed if they were identified.

The Captive Portal also shows when Transparent Kerberos Authentication is enabled, but authentication fails.

From the Captive Portal, users can:

- Enter their user name and password.
- Enter guest user credentials (Configured in the **Portal Settings**).
- Click a link to download an Identity Awareness agent (Configured in the **Portal Settings**).

How Captive Portal Works - Firewall Rule



Item	Description
1	User
2	Security Gateway with Identity Awareness
3	Captive Portal
4	Active Directory domain controller
5	Internal Data Center

A user (1) wants to access the Internal Data Center (5).

Identity Awareness (2) does not recognize the user and redirects the browser to the Captive Portal (3)

The user enters regular office credentials. The credentials can be AD or other Check Point supported authentication methods, such as LDAP, Check Point internal credentials, or RADIUS.

The credentials go to the Security Gateway, which finds them in the AD server (4).

The user can access the requested URL in the Data Center (5).

How Transparent Kerberos Authentication Works

1. A user wants to access the Internal Data Center.

2. Identity Awareness does not recognize the user and redirects the browser to the Transparent Authentication page.
3. The Transparent Authentication page asks the browser to authenticate itself.
4. The 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 Security Gateway, which authenticates the user and redirects it to the originally requested URL.
6. If Kerberos authentication fails for some reason, Identity Awareness redirects the browser to the Captive Portal.

Identity Agents

Endpoint Identity Agents are dedicated client agents installed on user computers that acquire and report identities to the Security Gateway. As the administrator, you, not the users, configure the Agents.

There are three types of Endpoint Identity Agents, Full, Light and Custom:

- **Full** – Predefined Endpoint Identity Agent that includes packet tagging and computer authentication. It applies to all users of the computer that it is installed on. Administrator permissions are required to use the Full Endpoint Identity Agent type. For the Full Endpoint Identity Agent you can enforce IP spoofing protection. You can also leverage computer authentication if you define computers in access roles.
- **Light** – Predefined Endpoint Identity Agent that does not include packet tagging and computer authentication. You can install this Endpoint Identity Agent individually for each user on the target computer. Administrator permissions are not required.
- **Custom** - Configure custom features for all computers that use this agent, such as MAD services and packet tagging ("Creating Custom Endpoint Identity Agents" on page 113).The Custom Endpoint Identity Agent is a customized installation package.

Make sure to use the correct Agent for your environment ("Creating Custom Endpoint Identity Agents" on page 113).

This table shows the similarities and differences of the Light and Full Endpoint Identity Agent types.

		Endpoint Identity Agent Light	**Endpoint Identity Agent Full**
Installation Elements	Endpoint Identity Agent format	Resident application	Resident application + service + driver
	Installation permissions	None	administrator
	Upgrade permissions	None	None
Security Features	User identification	SSO	SSO
	Computer identification	No	Yes
	IP change detection	Yes	Yes

		Endpoint Identity Agent Light	Endpoint Identity Agent Full
	Packet tagging	No	Yes

The installation file size is 7MB for both types and the installation takes less than a minute.

The Capabilities of Endpoint Identity Agents

Using Endpoint Identity Agents gives you:

- **User identification** - Users that log in to the Active Directory domain are transparently authenticated (with SSO) and identified when using an Endpoint Identity Agent. If you do not configure SSO or you disable it, the Endpoint Identity Agent uses username and password authentication with a standard LDAP server. The system opens a window for entering credentials.
- **Computer identification** - You get computer identification when you use the Full Endpoint Identity Agent as it requires to install a service.
- **Seamless connectivity** - Transparent authentication using Kerberos Single Sign-On (SSO) when users are logged in to the domain. Users who do not want to use SSO, enter their credentials manually. You can let them save these credentials.
- **IP change detection** - When an endpoint IP address changes (interface roaming or DHCP assigns a new address), the Endpoint Identity Agent automatically detects the change and reconnects.
- **Added security** - You can use the patented *packet tagging* technology to prevent IP Spoofing. Packet tagging is available for the full Endpoint Identity Agent because it requires installation of a driver. Endpoint Identity Agents also gives you strong (Kerberos-based) user and computer authentication.
- **Packet tagging** - A technology that prevents IP spoofing is available only for the Full Endpoint Identity Agent as it requires installing a driver.

Packet Tagging for Anti-Spoofing

IP Spoofing happens when an unauthorized user assigns an IP address of an authenticated user to an endpoint computer. By doing so, the user bypasses identity access enforcement rules. It is also possible to poison ARP tables that let users do ARP "man-in-the-middle attacks" that keep a continuous spoofed connectivity status.

To protect packets from IP spoofing attempts, you can enable *Packet Tagging*. Packet Tagging is a patent pending technology that prevents spoofed connections from passing through the Security Gateway. This is done by a joint effort between the Endpoint Identity Agent and the Security Gateway that uses a unique technology that sign packets with a shared key.

To see Packet Tagging logs, click **Logs & Monitor** > **Logs**, and then click **Favorites** > **Identity Awareness Blade**.

The Success status indicates that a successful key exchange happened.

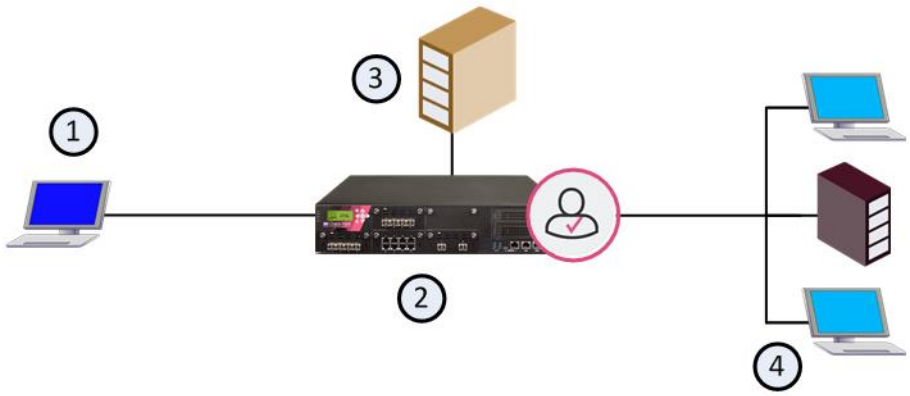
Note - Packet Tagging can only be set on computers installed with the Full Endpoint Identity Agent.

To enable IP Spoofing protection:

1. Make sure users have the Full Endpoint Identity Agent installed.
2. Create an Access Role ("Working with Access Roles" on page 27).
3. In the **Machines** tab, select **Enforce IP spoofing protection (requires full Endpoint Identity Agent)**.
4. Click **OK**.

Downloading Endpoint Identity Agent

Users download the Endpoint Identity Agent from the Captive Portal and then authenticate to the Security Gateway



Item	Description
1	User that is trying to connect to the internal network
2	Security Gateway with Identity Awareness
3	Active Directory domain controller
4	Internal network

This is a high-level overview of the Identity Awareness authentication process:

1. A user logs in to a computer with credentials, and tries to access the Internal Data Center.
2. The Security Gateway with Identity Awareness does not recognize the user and redirects to the Captive Portal.
3. The user sees the Portal page, with a link to download the Endpoint Identity Agent.
4. The user downloads the Endpoint Identity Agent from the Captive Portal and installs it.
5. The Endpoint Identity Agent client connects to the Security Gateway.

   Note - If SSO with Kerberos is configured, the user is automatically connected.
6. The user is authenticated and the Security Gateway sends the connection to its destination according to the Firewall Rule Base.

Terminal Servers

Terminal Servers Endpoint Identity Agent - An Endpoint Identity Agent installed on an application server that hosts Citrix/Terminal 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.

The Terminal Servers solution is based on reserving a set of TCP/UDP ports for each user. Each user that is actively connected to the application server that hosts the Terminal/Citrix services is dynamically assigned a set of port ranges. The gateway receives that information. Then, when a user attempts to access a resource, the packet is examined and the port information is mapped to the user.

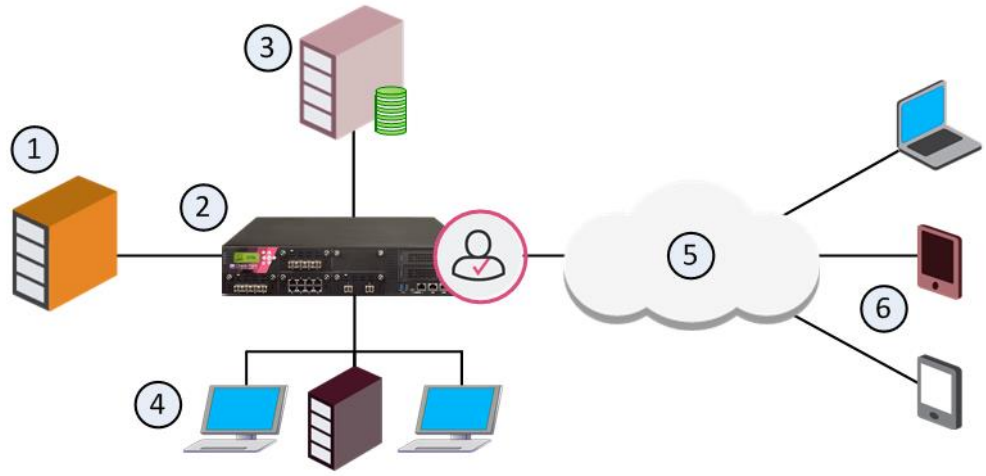
This Endpoint Identity Agent type cannot be used for endpoint computers.

For more information, see sk66761 http://supportcontent.checkpoint.com/solutions?id=sk66761.

Radius Accounting

You can configure a Security Gateway with Identity Awareness to use **RADIUS Accounting** to get user and computer identities directly from a RADIUS accounting client. Identity Awareness 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 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.



Item	Description
1	RADIUS authentication server with RADIUS Accounting client enabled Sends RADIUS accounting request to the gateway
2	Security Gateway with Identity Awareness configured as a RADIUS Accounting server
3	LDAP server Sends identity data for the user to the gateway
4	Internal network resources
5	Internet

Item	Description
6	Remote laptops and mobile devices

Remote Access

Identities are acquired for Mobile Access clients and IPSec VPN clients configured to work in Office Mode when they connect to the Security Gateway. This option is enabled by default.

Identity Collector

Check Point Identity Collector is a Windows-based application which collects information from Identity Sources about identities and their associated IP addresses. The Identity Collector then sends this information to the Check Point Firewalls for identity enforcement.

The Identity Collector supports these Identity Sources:

- Microsoft Active Directory Domain Controllers
- Cisco Identity Services Engine (ISE) Servers, versions 2.0 and 2.1

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 gateway. The Identity Collector collects information from the Identity Sources in the Query Pools and sends the information to the gateways.

For example: An environment has two domains: Asia.com and Euro.com.
The administrator wants the Asia Gateway to get the events from all the 4 domain controllers in the Asia.com domain. He also wants the Euro Gateway 1 and Euro Gateway 2 to get the events from all the 6 domain controllers in the Euro.com domain.
The administrator, therefore, creates 2 Query Pools: one which contains all the domain controllers in the Asia.com domain and another one which contains all the domain controllers in the Euro.com domain.
The administrator will configure the Asia Gateway to get events from the Asia Query Pool, and the two Euro Security Gateways to get events from the Euro Query Pool.

Web API

The web API identity source provides a flexible method for the creation of identities based on environment needs. With the Identity Awareness web API, you can create and revoke identities, and query the Identity Awareness Software Blade regarding users, IPs, and computers.

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

Identity Awareness web API gets JSON requests over HTTPS, and each HTTP request contains one Identity Awareness web API command or a bulk of commands. Each API command must include a shared secret pre-configured in SmartConsole.

The Identity Awareness web API supports 3 commands:

- add-identity - Associates an IP address to a user or a computer for a specified amount 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.

Comparison of Acquisition Sources

These tables show how identity sources are different in terms of usage and deployment considerations. Based on these considerations, you can configure Identity Awareness to use one or more identity of these identity sources ("Selecting Identity Sources" on page 69).

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	Deployment Considerations
• Identity based enforcement for non-AD users (non-Windows and guest users) • You can require deployment of Endpoint Identity Agents	• Used for identity enforcement (not intended for logging purposes).

AD Query Gets identity data seamlessly from Active Directory (AD).

Recommended Usage	Deployment Considerations
• Identity based auditing and logging • Leveraging identity in Internet application control • Basic identity enforcement in the internal network	• Easy configuration (requires AD administrator credentials). 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 http://supportcontent.checkpoint.com/solutions?id=sk43874. • Preferred for desktop users • Only detects AD users and computers

Endpoint Identity Agent

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

Recommended Usage	Deployment Considerations
• Identity enforcement for Data Centers • Protecting highly sensitive servers • When accuracy in detecting identity is crucial	• See Choosing Identity Sources ("Selecting Identity Sources" on page 69).

Terminal Servers Endpoint Identity Agent

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

Recommended Usage	Deployment Considerations
• Identify users who use Terminal Servers or a Citrix environment.	• See Choosing Identity Sources ("Selecting Identity Sources" on page 69).

Browser-Based Authentication - Transparent Kerberos Authentication

The Transparent Kerberos Authentication Single-Sign On (SSO) solution transparently authenticates users already logged into the AD. This means that when a user authenticates to the

domain, he gets access to all authorized network resources and does not have to enter credentials again. If Transparent Kerberos Authentication fails, the user is redirected to the Captive Portal for manual authentication.

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

Recommended Usage	Deployment 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 Endpoint Identity Agents or the Keep Alive feature.

RADIUS Accounting

You can configure a Security Gateway with Identity Awareness to use **RADIUS Accounting** to get user and computer identities directly from a RADIUS accounting client. Identity Awareness 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 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	Deployment 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 Security Gateway. • You must give the RADIUS client access permissions and create a shared secret.

Remote Access

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

Recommended Usage	Deployment Considerations
• Identify and apply identity-based security Policy on users that access the organization through VPN.	• See Choosing Identity Sources ("Selecting Identity Sources" on page 69).

Deployment

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

To protect internal data centers, Identity Awareness can be enabled on an internal Security Gateway in front of internal servers, such as data centers. This can be in addition to on the perimeter Security Gateway but does not require a perimeter Security Gateway.

Identity Awareness can be deployed in Bridge mode or Route mode.

- In the Bridge mode, it can use an existing subnet with no change to the hosts' IP addresses.
- In the Route mode, the Security Gateway acts as a router with different subnets connected to its network interfaces.

For redundancy, you can deploy a Security Cluster in Active-Standby (HA) or Active-Active (LS) modes. Identity awareness supports ClusterXL HA and LS modes.

If you deploy Identity Awareness on more than one Security Gateway, you can configure the

Security Gateways to share identity information. Common scenarios include:

- Deploy on your perimeter Security Gateway and data center Security Gateway.
- Deploy on several data center Security Gateways.
- Deploy on branch office Security Gateways and central Security Gateways.

You can have one or more Security Gateways acquire identities and share them with the other Security Gateways.

You can also share identities between Security Gateways 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	636
AD Query	135
Global Catalog	3268
Global Catalog over SSL	3269
Gateway to AD	135, 389
AD to gateway	135
Enforcement gateway	389
Identity Sharing gateway to Enforcement gateway	15105, 28581
Browser-based Authentication	443
Identity Agents/Terminal Server Agents	443
Radius Accounting	1813

It is possible to configure these features to different ports. For more information about Identity Awareness ports, see sk98561 http://supportcontent.checkpoint.com/solutions?id=sk98561 and sk52421 http://supportcontent.checkpoint.com/solutions?id=sk52421.

Configuring Identity Awareness

In This Section:

Enabling Identity Awareness on the Security Gateway

When you enable Identity Awareness on a Security Gateway, a 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 a multiple Security Gateway environment or to configure Endpoint Identity Agent and Remote Access acquisition (other methods for acquiring identities).

When you complete the wizard and install a policy, the system is ready to monitor Identity Awareness. You can see the logs for user and computer identity in the **Manage & Settings** > **Logs** tab. You can see events in the **Logs & Monitor** Access Control views.

To enable Identity Awareness:

1. Log in to SmartConsole.
2. From the **Gateways & Servers** view, double-click the Security Gateway on which to enable Identity Awareness.
3. On the Network Security tab, select **Identity Awareness**.

   The **Identity Awareness** Configuration wizard opens.
4. Select one or more options. These options set the methods for the acquisition of identities of managed and unmanaged assets.
   - **AD Query** - Lets the Security Gateway seamlessly identify Active Directory users and computers.
   - **Browser-Based Authentication** - Sends users to a Web page to acquire identities. If Transparent Kerberos Authentication is configured, AD users may be identified transparently.
   - **Terminal Servers** - Identify users in a Terminal Server environment (who originate from one IP address).

   These are the methods of acquiring identities you can choose in the wizard. However, other identity sources are supported ("Selecting Identity Sources" on page 69).

   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.
5. Click **Next**.

   The **Integration with Active Directory** window opens.

   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.

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 required to operate with some of the domain controllers, delete 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 at a later time 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 **Servers > LDAP Account units** in the **Categories** tree.

The LDAP Account Unit name syntax is: <domain name>_ _ AD

For example, CORP.ACME.COM_ _ AD.

6. 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, you need to enter a **domain name**, **username, password** and **domain controller** credentials.
7. 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.
8. If you selected Browser-Based Authentication or Terminal Servers and do not wish to configure Active Directory, select **I do not wish to configure Active Directory at this time** and click **Next.**
9. Click **Next**.

   If you selected Browser-Based Authentication on the first page, the **Browser-Based Authentication Settings** page opens.
10. In the **Browser-Based Authentication Settings** page, select a URL for the portal, where unidentified users will be directed.

    All IP addresses configured for the Security Gateway show in the list. 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
11. By default, access to the portal is only through internal interfaces. To change this, click **Edit**. We do not recommend that you let the portal be accessed through external interfaces on a perimeter Security Gateway.
12. 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 ("Configuring Terminal Servers" on page 43).
13. Click **Finish**.
14. Select **Install Policy** (Ctrl+Shift+Enter).

Working with Access Roles

After you enable Identity Awareness, 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** (Ctrl+E).
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 -** 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 -** 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 Endpoint Identity Agents, you can select (optional) **Enforce IP Spoofing protection**.
7. On the **Remote Access Clients** page, select the **Allowed Clients** or add new ones. For R77.xx Gateways or lower, you must choose **Any**.
8. Click **OK**.

Using Identity Awareness in the 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.

Working with Access Role Objects in the Rule Base

In rules with access roles, add a property in the **Action** field to redirect traffic to the Captive Portal. When the source identity is unknown and traffic is HTTP, this property redirects the user to the Captive Portal. If the source identity is known, the **Action** in the rule (**Allow** or **Block**) is enforced immediately and the user is not sent to the Captive Portal. After the system gets the credentials from the Captive Portal, it can examine the rule for the next connection.

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.

In rules with access role objects, criteria matching works like this:

- When identity data for an IP 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 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 see if 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** column and select **Edit Properties**.

   The Action Properties window opens.
2. Select the **Redirect http connections to an authentication (captive) portal. Note: redirection will not occur if the source IP is already mapped to a user** checkbox.
3. Click **OK**.

   The Action column shows that a redirect to the Captive Portal occurs.

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

No.	Source	Destination	Service	Action
1	Finance_Dept (Access Role)	Finance_Web_Server	Any	Accept (display Captive Portal)
2	Admin_IP	Any	Any	Accept
3	Any	Any	Any	Drop

Example 1 - If an unidentified Finance user tries to access the Finance Web Server with http, a redirect to the Captive Portal occurs. After the user enters credentials, the Security 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 access the Finance Web Server with 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 access 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.

Negate and Drop

When you negate a source or destination parameter, it means that a given rule applies to all sources/destinations of the request *except* for the specified source/destination object. When the object is an access role, this includes all unidentified entities as well.

When you negate an access role, it means that the rule is applied to "all except for" the access role and unidentified entities. For example, let's say that the below rule is positioned above the Any, Any, Drop rule. The rule means that everyone (including unidentified users) can access the Intranet Web Server except for temporary employees. If a temporary employee is not identified when she accesses the system, she will have access to the Intranet Web Server. Right-click the cell with the access role and select **Negate Cell**. The word *[Negated]* is added to the cell.

Source	Destination	VPN	Services & Applications	Action
Temp_employees *[Negated]*	Intranet_web_server	Any	http	accept

To prevent access to unidentified users, add another rule that ensures that only identified employees are allowed access.

Source	Destination	VPN	Services & Applications	Action
Temp_employees	Intranet_web_server	Any	http	drop
Any_identified_employee	Intranet_web_server	Any	http	accept

Identifying Users Behind an HTTP Proxy Server

If your organization uses an HTTP proxy server behind the Security Gateway, the Security Gateway cannot see the identities of the users behind the proxy server. As a result, the gateway cannot enforce policy rules based on user identities.

To let the Security 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 Security Gateway
- Configure the XFF header on the Access Control Policy Layer
- Use Access Roles in the Access Control Policy Layer or use one of the these log track options: Detailed, Extended or Full.

To configure the XFF header on a Security Gateway:

1. In the **Gateways & Servers** view, open the Security Gateway.
2. In the **General Properties** page > **Network Security** tab, make sure that **Identity Awareness** is enabled.
3. In the navigation tree, go to **Identity Awareness** > **Proxy**.
4. Enable **Detect users located behind http proxy configured with X-Forwarded-For**.
   - Optional: Enable **Hide X-Forwarded-For in outgoing traffic**. With this option selected, internal IP addresses are not seen in requests to the internet.
   - Optional: Enable **Trust X-Fowarded-For from known proxies only** to configure a list of trusted proxy servers. Select **Known proxy groups** from the drop-down list.

     The Identity Awareness blade will read the XFF header only from the trusted servers.

     Note - If this option is disabled , the gateway will parse the XFF header only from internal network connections.

To configure the XFF header on the Access Control Policy Layer:

1. Go to **<tp_sec>** > **Access Control** > **Policy** > right-click **Policy** and select **Edit Policy**.
2. Click  and select **Edit Layer**.
3. In the **Proxy Configuration** section, enable **Detect users located behind http proxy configured with X-Forwarded-For**.
4. Click **OK**.

Configuring Identity Sources

In This Section:

Configuring AD Query

Enabling AD Query

You must enable RADIUS Accounting on Security Gateways before they can work as a RADIUS Accounting server.

To enable RADIUS Accounting for a Security Gateway:

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**.

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, the user **A** 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 keep these issues to a minimum is to increase the DHCP lease time.

To activate single user assumption:

1. Exclude service accounts ("Excluding Users, Computers and Networks" on page 32).
2. On the **Identity Awareness** page, select **Settings** for AD Query.
3. Select **Assume that only one user is connected per computer**.
4. Click **OK**.

To deactivate Single User Assumption, clear **Assume that only one user is connected per computer**.

Excluding Users, Computers and Networks

You can manually exclude service accounts, users, computers and networks from the AD Query scan. You can also 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.

To exclude objects from Active Directory queries:

1. From the Security Gateway object **Identity Awareness** page, select **Active Directory Query** > **Settings**.
2. Click **Advanced**.
3. In the **Excluded Users / Computers** section, enter the user or computer account name. You can use the ***** and **?** wildcard characters or regular expressions ("Appendix: Regular Expressions" on page 128) to select more than one account. Use this syntax for regular expressions: `regexp:<regular expression>`.
4. Optional: Select **Automatically exclude users which are logged into more than n machines simultaneously**. Enter the threshold number of computers in the related field.
5. In the **Excluded Networks** section:
   - Click the **plus sign (+)** and select a network to add the Excluded Network list.
   - Select an excluded network and click the **minus sign (-)** to remove a network from the list.
6. Click **Add**.
7. Click **OK**.

Managing 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 message shows in **Logs & Monitor** > **Logs**.

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

To show all suspected service accounts, run: `adlog a control srv_accounts show`

To run the service accounts scan immediately, run: `adlog a control srv_accounts find`
This command is useful before you enable the **Assume that only one user is connected** option.

To remove an account from the service account database, run: `adlog a control srv_accounts unmark` *<account name>*

To remove all accounts from the suspected service account database, run: `adlog a control srv_accounts clear`

Important - When you use the `adlog a control` command, you must run `adlog a control reconf` to save the configuration.

Using AD Query with NTLMv2

NTLMv2 for AD Query is supported from R76 versions and higher. Earlier releases are only supported NTLM. By default, NTLMv2 support is disabled.

To enable NTLMv2 support for AD Query:

1. Enable Identity Awareness without using the wizard.
2. Install a policy.
3. From the Security Management Server command line, go to the expert mode.
4. Run: `adlogconfig a`
5. Select: `Use NTLMv2`
6. Select: `Exit and save`
7. Restart the Identity Awareness wizard and continue configuring Identity Awareness.

Automatic LDAP Group Update

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

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.

LDAP Group Update is activated by default. You can manually deactivate LDAP Group Update with the CLI.

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

To deactivate automatic LDAP group update:

1. From the Security Gateway command line, run:
   `adlogconfig a`
   The **adlog** status screen and menu opens.
2. Select **Turn LDAP groups update on/off**.
   LDAP groups update notifications status changes to **[ ]** (not active). If you enter **Turn LDAP groups update on/off** when automatic LDAP group update is not active, **LDAP groups update notifications** status changes to **[X]** (active).
3. Enter **Exit and save** to save this setting and close the **adlogconfig** tool.
4. Install policy.

You can use `adlogconfig` to set the time between LDAP change notifications and to send notifications only for user related changes.

To configure LDAP group notification options:

1. From the Security Gateway command line, run:
   `adlogconfig a`
   The **adlog** status screen and menu opens.
2. Enter the **Notifications accumulation time** to set the time between LDAP change notifications.
3. Enter the time between notifications in seconds (default = 10).
4. Enter **Update only user-related LDAP changes** to/not to send notifications only for user related changes.
   Be very careful when you deactivate only user-related notifications. This can cause excessive gateway CPU load.

5. Enter **Exit and save** to save these settings and close the **adlogconfig** tool.
6. Install policy.

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.

You must deactivate the LDAP cache to get automatic LDAP Group Update assignments immediately. This action can cause Identity Awareness to work slower.

To deactivate the LDAP cache:

1. In SmartConsole, go to **Menu** > **Global Properties > User Directory**.
2. Change **Timeout on cached users** to 0.
3. Change **Cache size** to zero.
4. Install policy.

Specifying Domain Controllers per Security Gateway

An organization Active Directory can have several 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 Security Gateways, you may want to configure each Security Gateway to communicate with only some of the domain controllers.

This is configured in the User Directory page of the **Gateway Properties**. For each domain controller that is to be ignored, the default priority of the Account Unit must be set to a value higher than 1000.

For example, let's say that the LDAP Account Unit *ad.mycompany.com* has 5 domain controllers.

On the Security Gateway we want to enable AD Query only for domain controllers dc2 and dc3. This means that all other domain controllers must be set to a priority higher than 1000 in the Security Gateway properties.

To specify domain controllers for each Security Gateway:

1. Log in to SmartConsole.
2. From the **Gateways & Servers** view, double-click the Security Gateway.
3. Select the page **Other** > **User Directory**.
4. Click **Selected Account Units list** and click **Add**.
5. Select your Account Unit.
6. Clear the **Use default priorities** option and set the priority **1001** to dc1, dc4 and dc5.
7. Click **OK**.
8. **Install Policy**.

Checking the Status of Domain Controllers

You can make sure that the domain controllers are set properly by using the adlog CLI. You can see the domain controllers that the Security Gateway is set to communicate with as well as the domain controllers it ignores.

The CLI command is: `adlog a dc`

Troubleshooting

If you experience connectivity problems between your domain controllers and Security Gateway with Identity Awareness/log servers, perform the following troubleshooting steps:

In this section:

Connectivity Issues

1. Ping the domain controller from the Security Gateway with Identity Awareness/Log Server.
2. Ping the Security Gateway with Identity Awareness/Log Server from your domain controller.
3. Perform standard network diagnostics as required.
4. Check the **Logs** tab of the **Logs & Monitor** 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 36) and sk58881 http://supportcontent.checkpoint.com/solutions?id=sk58881.

Use wbemtest to Verify WMI

To use the Microsoft **wbemtest** utility to verify that WMI is functional and accessible.

1. Click **Start** > **Run**.
2. Enter `wbemtest.exe` in the **Run** window.
3. In the **Windows Management Instrumentation Tester** window, click **Connect**.
4. In the **Connect** window, in the first field, enter the Domain controller, in this format: `\\<IP address>\root\cimv2`
5. In the **Credentials** > **User** field, enter the fully qualified AD user name. For example: *ad.company.com\admin*
6. Enter a password for the user.
7. Click **Connect**.
8. 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 ("Connectivity Issues" on page 35) problems
- Incorrect domain administrator credentials (on page 35).
- WMI service ("Verify the WMI Service" on page 36) is not running
- A Firewall is blocking traffic ("Configuring the Firewall" on page 36) between the Security Gateway with Identity Awareness/log server and domain controller.

Domain administrator Credentials

To verify your domain administrator credentials:

1. Click **Start > Run**.

2. Enter `\\<domain controller IP>\c$` in the **Run** window. For example: `\\11.22.33.44\c$`.
3. In the **Logon** window, enter your domain administrator user name and password.
4. If the domain controller root directory appears, this indicates that your domain administrator account has sufficient privileges. An error message may indicate that:
   a) If the user does not have sufficient privileges, this indicates that he is not defined as a domain administrator. Obtain a domain administrator credentials.
   b) You entered the incorrect user name or password. Check and retry.
   c) The domain controller IP is incorrect or you are experiencing connectivity issues.

Verify the WMI Service

To verify if the WMI service is running on the domain controller:

1. Click **Start** > **Run**.
2. Enter `services.msc` in the **Run** window.
3. Find the **Windows Management Instrumentation** service and see that the service started.
   If it did not start, right-click this service and select **Start**.

Configuring the Firewall

If a Security Gateway is located between the Security Gateway with Identity Awareness/log server and the Active Directory controller, configure the Firewall to allow WMI traffic.

To create Firewall rules for WMI traffic:

1. In SmartConsole, from the **Security Policies** view, open the **Access Control Policy**.
2. Create a rule that allows **ALL_DCE_RPC** traffic:
   - **Source** = Security Gateways that run AD Query
   - **Destination** = Domain Controllers
   - **Service** = **ALL_DCE_RPC**
   - **Action** = **Accept**
3. Save the policy and install it on Security Gateways.
   Note - If there are connectivity issues on DCE RPC traffic after this policy is installed, see sk37453 http://supportcontent.checkpoint.com/solutions?id=sk37453 for a solution.

Confirm that Security Event Logs are Recorded

If you have checked connectivity ("Connectivity Issues" on page 35) 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 higher 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 Browser-Based Authentication in SmartConsole

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 ("Transparent Kerberos Authentication Configuration" on page 100), the browser tries to identify AD users before sending them to the Captive Portal.

If you already 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:
   - Portal Network Location (on page 37)
   - Access Settings (on page 37)
   - Authentication Settings (on page 38)
   - Customize Appearance (on page 39)
   - User Access (on page 39)
   - Endpoint Identity Agent Deployment from the Portal (on page 40)

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.

Portal Network Location

Select if the portal runs on this Security Gateway or a different Identity Awareness enabled 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 deployment is possible where the portal runs on a different Security Gateway. See the Deployment section for more details.

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 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 97) 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.

  Users are sent to the Captive Portal if they use networks connected to these interfaces.
  - **Through all interfaces**
  - **Through internal interfaces**
    - **Including undefined internal interfaces**
    - **Including DMZ internal interfaces**
    - **Including VPN encrypted interfaces**
  - **According to the Firewall policy** - Select this if there is a rule that states who can access the portal.

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:** The URL used to begin the SSO process. If transparent authentication fails, users are redirected to the configured Captive Portal.
  - **IP Address:** The IP address to which the Portal URL is resolved if DNS resolution fails.

  Notes:

  The Endpoint 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.

  The **IP Address** option only shows when you select **Browser-based Authentication** as an identity source.
- **Authentication Method** - Select one method that known users must use to authenticate.
  - **Defined on user record (Legacy Authentication) -** Takes the authentication method from **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. You might choose 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.

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 access the portal from mobile devices.

User Access

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

- **Name and password login**- Users are prompted to enter an existing username and password. This will only let known users authenticate.
- **Unregistered guests login** - Let guests who are not known by the Security Gateway access the network after they enter required data.

Name and Password Login Settings

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 can they access network resources before they have to authenticate again.
- **Ask for user agreement** - You can require that users 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 Endpoint Identity Agent and which one.
  - If they can defer the Endpoint Identity Agent installation and until when.

  You can only configure settings for Endpoint Identity Agent deployment if **Endpoint Identity Agents** is selected on the **Identity Awareness** page.

Unregistered Guest Login Settings

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

- **Access will be granted for xxx minutes** - For how long can they access network resources before they have to authenticate again.
- **Ask for user agreement** - Makes users sign a user agreement. Click **Edit** to choose 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 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 will show the user name in **Logs & Monitor** > **Logs**.

Endpoint Identity Agent Deployment from the Portal

If **Endpoint Identity Agents** is selected as a method to acquire identities, You can require users to download the Endpoint Identity Agent from the Captive Portal. You can also let users install the Endpoint Identity Agent on a specified later date and not right away.

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

Configuring Endpoint Identity Agents

Endpoint Identity Agent Deployment Methods

There are different Endpoint Identity Agent deployment methods:

- **Using Captive Portal** - You can require users to download the Endpoint Identity Agent from the Captive Portal. You can also let users install the Endpoint Identity Agent on a specified later date and not right away. During installation, the Endpoint Identity Agent automatically detects if there are administrator permissions on the computer or not and installs itself accordingly.

  Notes:
  - When you deploy the Full Endpoint Identity Agent, the user that installs the client must have administrator rights on the computer. If the user does not have administrator permissions, the Light Endpoint Identity Agent is installed instead.
  - When users authenticate with the transparent portal, the download link does not show. They must install the agent from the distribution media.
- **Using distribution software** - You can deploy the Endpoint Identity Agent with distribution software. You can find the msi installation files (Light and Full) in `$NACPORTAL_HOME/htdocs/nac/nacclients/customAgent.msi` on the gateway.

Configuring Endpoint Identity Agent Deployment from Captive Portal

To configure Endpoint Identity Agent deployment from Captive Portal:

1. From the Identity Awareness page, select the **Endpoint Identity Agents** checkbox.
2. Select **Browser-Based Authentication** and click **Settings**.
3. From the **Portal Settings** window, select the **Require users to download** checkbox to make users install the Endpoint Identity Agent. Select which Endpoint Identity Agent they must install. If you select this option and you do not select the defer option, users will can only access the network if they install the Endpoint Identity Agent.
4. To give users flexibility to choose when they install the Endpoint Identity Agent, select **Users may defer installation until**. Select the date by which they must install it. Until that date a Skip Endpoint Identity Agent installation option shows in the Captive Portal.
5. Click **OK**.

Configuring Endpoint Identity Agent Deployment for User Groups

When necessary, you can configure specific groups to download the Endpoint Identity Agent. For example, if you have a group of mobile users that roam and it is necessary for them to stay connected as they move between networks.

To configure Endpoint Identity Agent deployment for user groups:

1. From the Identity Awareness page, select the **Endpoint Identity Agent** checkbox.
2. Select **Browser-Based Authentication** and click **Settings**.
3. Select **Name and password login** and click **Settings**.
4. Select **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 the Endpoint Identity Agent and which one.
   - If they can defer the Endpoint Identity Agent installation and until when.
5. Click **OK**.

Configuring Endpoint Identity Agents in SmartConsole

In the **Identity Sources** section of the Identity Awareness page, select **Endpoint Identity Agents** to configure Endpoint Identity Agent settings.

To configure the Endpoint Identity Agent settings:

1. Select **Endpoint Identity Agents** and click **Settings**.
2. From the **Endpoint Identity Agents Settings** window, configure:
   - Endpoint Identity Agent Access
   - Authentication Settings (on page 38)
   - Session details
   - Endpoint Identity Agent Upgrades

Endpoint Identity Agent Access

Click **Edit** to select from where the Endpoint Identity Agent can be accessed. The options are based on the topology configured for the Security Gateway.

Users can communicate with the servers if they use networks connected to these interfaces.

- **Through all interfaces**
- **Through internal interfaces**
  - **Including undefined internal interfaces**
  - **Including DMZ internal interfaces**
  - **Including VPN encrypted interfaces**
- **According to the Firewall Policy** - the Endpoint Identity Agent is accessible through interfaces associated with source networks that appear in access rules used in the Firewall Policy**.**

Session

Configure data for the logged in session using the Endpoint Identity Agent.

- **Agents send keepalive every X minutes** - The interval at which the Endpoint Identity Agent sends a keepalive signal to the Security Gateway. The keepalive is used as the server assumes the user logged out if it is not sent. Lower values affect bandwidth and network performance.
- **Users should re-authenticate every XXX minutes** - For how long can users access network resources before they have to authenticate again. When using SSO, this is irrelevant.
- **Allow user to save password** - When SSO is not enabled, you can let users save the passwords they enter in the Endpoint Identity Agent login window.

Endpoint Identity Agent Upgrades

Configure data for Endpoint Identity Agent upgrades.

- **Check agent upgrades for** - You can select all users or select specific user groups that should be checked for Endpoint Identity Agent upgrades.
- **Upgrade only non-compatible versions** - the system will only upgrade versions that are no longer compatible.
- **Keep agent settings after upgrade** - settings made by users before the upgrade are saved.
- **Upgrade agents silently (without user intervention)** - the Endpoint Identity Agent is automatically updated in the background without asking the user for upgrade confirmation.

Note - When you install or upgrade the Full Endpoint Identity Agent version, the user will experience a momentary loss of connectivity.

Troubleshooting Authentication Issues

Some users cannot authenticate with the Endpoint Identity Agent

This issue can occur in Kerberos environments with a very large Domain Controller database. The authentication failure occurs when the CCC message size is larger than the default maximum size. You can increase the maximum CCC message size to prevent this error.

To increase the maximum CCC message size, use the procedure in sk66087 http://supportcontent.checkpoint.com/solutions?id=sk66087.

Transparent Portal Authentication fails for some users

This issue can occur for users that try to authenticate with Kerberos authentication with the transparent portal. The user sees a **400 Bad Request** page with this message:

```
Your browser sent a request that this server could not understand.
Size of a request header field exceeds server limit.
```

The authentication failure occurs because the HTTP request header is larger than the default maximum size. You increase the maximum HTTP request header to prevent this error.

To increase the maximum HTTP request header size, use the procedure in sk92802 http://supportcontent.checkpoint.com/solutions?id=sk92802 .

Configuring Terminal Servers

Deploying the Terminal Servers Identity Awareness Solution

To deploy Terminal Servers:

- **Install a Terminal Servers Identity Agent** - You install this agent on the application server that hosts the Terminal/Citrix services after you enable the Terminal Servers identity source and install policy. Go to the link https://<gateway_IP>/_IA_MU_Agent/download/muhAgent.exe. Make sure you open the link from a location defined in the Terminal Servers Accessibility setting (**Gateway Properties** > **Identity Awareness** > **Terminal Servers** > **Settings** > **Edit**).
- **Configure a shared secret** - You must configure the same password on the Terminal Servers Identity Agent and the gateway (the Security Gateway enabled with Identity Awareness). This password is used to secure the established trust between them.

Installing the Terminal Servers Endpoint Identity Agent

The Terminal Servers Endpoint Identity Agent installation installs the Terminal Servers driver and features. A user with administrator rights must run the Terminal Servers installation.

You can download the Terminal Servers Endpoint Identity Agent from a link in SmartConsole.

To download the Terminal Servers Endpoint Identity Agent:

1. On the **Identity Awareness** page, enable the **Terminal Servers** identity source.
2. Install policy.
3. Go back to the same page and click the download **Endpoint Identity Agent** link. Make sure you open the link from a location defined in the Accessibility setting (**Terminal Servers** > **Settings** > **Edit**).
4. Install the Endpoint Identity Agent on the Terminal Server.

Upgrading a Terminal Servers Endpoint Identity Agent

There is no option to upgrade the Terminal Servers Endpoint Identity Agent when you upgrade a Security Gateway to a newer version. You must manually install the new version of the Terminal Servers Endpoint Identity Agent on the Citrix or Terminal Server.

Configuring the Shared Secret

You must configure the same password as a shared secret in the Terminal Servers Endpoint Identity Agent on the application server that hosts the Terminal/Citrix services and on the Security Gateway enabled with Identity Awareness. The shared secret enables secure communication and lets the Security Gateway trust the application server with the Terminal Servers functionality.

The shared secret must contain at least 1 digit, 1 lowercase character, 1 uppercase character, no more than three consecutive digits, and must be eight characters long. In SmartConsole, you can automatically generate a shared secret that matches these conditions.

To configure the shared secret on the gateway:

1. Log in to SmartConsole.
2. From the **Gateways & Servers** view, double-click the Check Point Security Gateway that has Identity Awareness enabled.
3. Go to the Identity Awareness page.
4. In the **Identity Sources** section, select **Terminal Servers** and click **Settings**.
5. To automatically configure the shared secret:
   a) Click **Generate** to automatically get a shared secret that matches the string conditions.

      The generated password is shown in the Pre-shared secret field.
   b) Click **OK**.
6. To manually configure the shared secret:
   a) Enter a password that matches the conditions in the **Pre-shared secret** field. Note the strength of the password in the Indicator.
   b) Click **OK**.

To configure the shared secret on the application server:

1. Open the Terminal Servers Endpoint Identity Agent.

   The Check Point Endpoint Identity Agent - Terminal Servers main window opens.
2. In the **Advanced** section, click **Terminal Servers Settings**.
3. In **Identity Server Shared Secret**, enter the shared secret string.
4. Click **Save**.

Configuring Terminal Servers Accessibility

1. On the **Identity Awareness** page, click Terminal Servers - **Settings**.
2. In the **Accessibility** section, click **Edit** to select from where the Terminal Server Identity Agent can connect. The options are based on the topology configured for the gateway.
   - Through all interfaces
   - Through internal interfaces
     - Including undefined internal interfaces
     - Including DMZ internal interfaces
     - Including VPN encrypted interfaces
   - According to the Firewall policy - Select this if there is a rule that states who can access the portal.

Terminal Servers - Users Tab

The Users tab in the Terminal Servers Endpoint Identity Agent shows a table with information about all users that are actively connected to the application server that hosts the Terminal/Citrix services.

Table Field	Description
ID	The SID of the user.
User	The user and domain name. The format used: <domain>\<user>
TCP Ports	The ports allocated to the user for TCP traffic.
UDP Ports	The ports allocated to the user for TCP traffic.
Authentication Status	Indicates whether this user is authenticated on the gateway.

The ID and User field information is automatically updated from processes running on the application server. The Terminal Servers Endpoint Identity Agent assigns TCP and UDP port ranges for each connected user.

Terminal Servers Advanced Settings

From the **Advanced** section of the Multi User Host main window, you can access **Terminal Servers Settings**.

Advanced uses can change these settings when necessary. **Best Practice -** We highly recommend that you keep the default values if you are not an advanced user.

Changes are applied to new users that log in to the application server after the settings are saved. Users that are currently logged in, will stay with the older settings.

Advanced Setting	Description
Excluded TCP Ports	Ports included in this range will not be assigned to any user for TCP traffic. This field accepts a port range or list of ranges (separated with a semicolon).
Excluded UDP Ports	Ports included in this range will not be assigned to any user for UDP traffic. This field accepts a port range or list of ranges (separated with a semicolon).
Maximum Ports Per User	The maximum number of ports that can be assigned to a user in each of the TCP and UDP port ranges.
Ports Reuse Timeout (seconds)	The number of seconds the system waits until it assigns a port to a new user after it has been released by another user.
Errors History Size	N/A

Advanced Setting	Description
Gateway Shared Secret	The same password that is set on the gateway that enables trusted communication between the Security Gateway and the application server.

Configuring RADIUS Accounting

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 Gateways before they can work as a RADIUS Accounting server.

To enable RADIUS Accounting for a Security Gateway:

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.

To select gateway interfaces:

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** - Also accepts connections from internal interfaces without a defined IP address
      - **Including DMZ internal interfaces** - Also accepts connections from clients located in the DMZ
   c) **Firewall Policy** - Interface connections are allowed according to the Firewall policy.
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 Security Gateway accepts RADIUS Accounting requests only from authorized RADIUS Accounting clients. A Radius Accounting client is a host with a RADIUS client software installed.

To configure an authorized RADIUS client:

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 define a new host object for the RADIUS Accounting client. This host object is selected automatically.

   Click the **-** icon to remove an existing 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.

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 deployments.

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 define the 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 define the 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 define the 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 **+** icon and then select one or more LDAP account units.

Configuring Remote Access

To configure Remote Access:

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

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

Configuring the Identity Collector

This section explains how to configure the Identity Collector, both on the gateway and on the Windows server where it is installed.

Deploying the Identity Collector Solution

To deploy the Identity Collector:

- **Install an Identity Collector** - You install this agent on the Windows server that hosts the Identity Collector after you enable the Identity Collector identity source and install policy. Go to the link https://<gateway_IP>/_IA_IDC/download/CPIdentityCollector.msi. Make sure you open the link from a location defined in the Identity Collector Accessibility setting (**Gateway Properties** > **Identity Awareness** > **Identity Collector** > **Settings** > **Edit**).
- **Configure a shared secret** - You must configure the same password on the Identity Collector and the gateway (the Security Gateway enabled with Identity Awareness). This password is used to secure the established trust between them.

Installing the Identity Collector Endpoint Identity Agent

A user with administrator rights must run the Identity Collector installation. You can download the Identity Collector from a link in SmartConsole.

To download the Identity Collector:

1. On the **Identity Awareness** page, enable the **Identity Collector** identity source.
2. Install policy.
3. Go back to the same page and click the download **Identity Collector** link. Make sure you open the link from a location defined in the Accessibility setting (**Identity Collector** > **Settings** > **Edit**).
4. Install the Identity Collector.

Configuring the Identity Collector on the Gateway

To enable the Identity Collector solution, you must also configure it on the gateway.

To configure the Identity Collector on the gateway:

1. In the **Gateways & Servers** view, double-click the Security Gateway.
2. In the **Identity Sources** section of the Identity Awareness page, select **Identity Collector** and click **Settings**.
3. In the **Identity Collector Settings** window, configure:
   - **Client Access permissions** ("Identity Collector Accessibility" on page 49)
   - **Authorized Clients** and **Client Secret** ("Authorized Identity Collector Clients" on page 50)
   - **Authentication Settings** ("Identity Collector Authentication Settings" on page 50)
4. **Optional:** If you want to enforce the Cisco Security Group Tags (SGTs) on the gateway:
   a) In the **Objects** menu, click **Object Explorer** > **New** > **User** > **User Group**.
   b) Name the new group: CSGT-<*SGT_NAME*>.
   c) Assign the group to an Access Role.
5. **Install Policy**.

Identity Collector Accessibility

You must authorize Gateway interfaces that can accept connections from Identity Collector clients.

To select the gateway interfaces:

1. In the **Client Access Permissions** section, click **Edit**.
2. Select Security Gateway interfaces that can accept connections from Identity Collector clients. The options are based on the topology configured for the Security Gateway. Identity Collector clients can access the Security Gateway if they use networks connected to these interfaces. The options are:
   a) **All Interfaces** - All Security Gateway interfaces can accept connections from Identity Collector clients.
   b) **Internal Interfaces** - Only explicitly defined internal Security Gateway interfaces can accept connections from Identity Collector clients.

- **Including undefined internal interfaces** - Also accepts connections from internal interfaces without a defined IP address
- **Including DMZ internal interfaces** - Also accepts connections from clients located in the DMZ
- **Including VPN Encrypted interfaces** - Also accepts connections from clients located in the VPN

c) **According to the Firewall policy** - Select this if there is a rule that states which interfaces can accept connections from Identity Collector clients.

Important - The **All Interfaces** and **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 Identity Collector Clients

An Identity Awareness Security Gateway accepts connections only from authorized Identity Collector clients.

To configure an authorized Identity Collector client:

1. In the **Authorized Clients** section of the **Identity Collector Settings** window, click the **+** icon and select an Identity Collector client from the list.

   To define a new host object, go to the **Objects** pane or to the **Objects** menu, and click **New**.

   Click the **-** icon to remove an existing Identity Collector client from the list.
2. Click **Generate** to create a strong, client secret for client authentication. Each client has its own client secret.

   You can also create a client secret manually. To modify a client secret, change it manually.

Identity Collector Authentication Settings

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

- Authentication Settings **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:
    - **All Gateway's Directories** -Users from all LDAP servers.
    - **Specific** - Users from LDAP servers 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. You can 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.

Configuring the Identity Collector on the Windows Server

To add a new Active Directory with its Domain Controllers:

1. Go to **Domains** > **New Domain**.
2. Enter the Domain name and account credentials. There are 2 optional fields: **Comment** and **DC IP Address** to test connectivity.

   Note - The account must be a member of the **Event Log Readers** group.
3. Click **OK**.
4. Use one of these options to add the required Domain Controllers:
   a) Add Domain Controllers automatically by DNS and LDAP queries:
      (i) Go to **Identity Sources** > **New Source** > **Active Directory**.
      (ii) Select **Fetch Automatically**.
      (iii) Select the **Domain**.
      (iv) Enter the **DC IP Address** of one of the Domain Controllers you want to add.
      (v) Click **Fetch**. A list of the Domain Controllers show.
      (vi) Enable the Domain Controllers you want to add.
      (vii) Click **OK**.
   b) Add Domain Controllers manually one at a time:
      (i) Go to **Identity Sources** > **New Source** > **Active Directory**.
      (ii) Click **Add Manually**.
      (iii) Enter the **Domain Controller Name**.
      (iv) Select the **Domain**.
      (v) Enter the **IP Address** of the Domain Controller you want to add.
      (vi) **Optional:** Enter a **comment** and enter a **Site**'s name.
      (vii) If this server is not a domain controller but a server that the events are forwarded to, select this checkbox.
      (viii) **Optional:** Click **Test** to check the connectivity.
      (ix) Click **OK**.

To add a new Cisco ISE Server:

1. Go to **Identity Sources** > **New Source** > **ISE**.
2. Enter this information:
   - **Server name** - The Cisco ISE Server name shown in the Identity Collector.
   - **Primary Node** – The resolvable FQDN of the primary pxGrid node (or the stand-alone node).
   - **Secondary Node** - The resolvable FQDN of the secondary pxGrid node. Only requried in distributed pxGrid environment with more than one pxGrid nodes.
   - **Optional:** Enter a **comment** and enter a **Site**'s name
   - **Server Certificate File** - Certificate file (in jks format) for the ISE server, generated by the ISE Server. To create the JKS file, see the Cisco pxGrid documentation.
   - **Server Certificate Key** – key to the above JKS file.

- **Machine Name** - The resolvable FQDN of the Identity Collector computer. The ISE Server pxGrid client list will later show this FQDN (Administration > pxGrid Services > Client Name) and it must be approved.
- **Client certificate file** - Certificate file (in jks format) for the Identity Collector, generated by the ISE server. To create the JKS file, see the Cisco pxGrid documentation.
- **Client Certificate Key** – key to the above JKS file.

3. Click **OK**.

To add a new Query Pool:

Assign one Query Pool to each gateway.

1. Click **Query Pools** > **New Query Pool**.
2. Enter the **Query Pool Name** and select the **Identity Sources** from which to collect identities.
3. **Optional:** Enter a **Comment**.
4. Click **OK**.

Note – The Identity Collector queries only the AD Domain Controllers and ISE Servers that are in the Query Pool.

To connect the Identity Collector to a Check Point gateway:

1. Go to **Gateways** > **New Gateway**.
2. Enter the **Gateway Name**, **IP Address** and **Shared Secret** as configured in SmartConsole.
3. **Optional:** Enter a comment.
4. Select a **Query Pool** to assign to the gateway.

   Note - Assign one Query Pool to each gateway.
5. Click **Test**.
6. Make sure the certificate is correct and approve it.
7. Click **OK**.

Filtering

You can configure the Identity Collector to filter the login events. The Identity Collector sends to the gateway only events that match the filtering criteria.

To filter events:

1. Go to **Exclusion List**.
2. Select a filter:
   - **Network Filter** - Defines IP addresses and networks to include or exclude.
   - **Identity Filter** - Defines user names and computer names to include or exclude. You can filter by full names, names with wildcard or regular expression (select the checkbox).

Advanced Configuration

For advanced configuration options, go to the **Advanced** tab on the left pane of the Identity Collector.

Activity Log

Logs the date and time of activities done in the Identity Collector. This log is cleared every time the GUI restarts.

Settings > Identity Reporting

Association time-to-live – How long this association will live on the PDP Security Gateway. The default is 12 hours.

Cache time-to-live – The cache saves associations (user to IP) that the Identity Collector creates for a set period of time (the default is 5 minutes). If the event occurs again during that time period, the Identity Collector does not send the event to the gateway again.

Ignore machine identities – The Identity Collector does not send computer associations, only user associations. The default of this feature is off.

Ignore RDP events – When remote desktop login occurs, 2 login events occur in the domain controller with the same username but different IPs: the computer logged in from and the computer logged in to. Therefore, the IP of the computer logged in from is redundant and with this configuration the Identity Collector ignores it.

Clear Cache Button – Clears all the entries saved in the cache. The Identity Collector will create new cache entries when it receives new associations.

Settings > ISE Servers

Session Keep-alive – The Identity Collector goes over its internal ISE sessions database every configured period of time. If it finds expired sessions, it queries the ISE Server to see if the session is still alive. Then it updates the gateway accordingly. This value sets the interval during which this occurs.

Settings > Logins Monitor

Enable Logins Monitor – When selected, the Identity Collector records user logging events and shows them in the **Logins Monitor** tab.

Event expiration time – The maximum time that the **Logins Monitor** Table stores each login record.

Cache time-to-live – The maximum time between two different login events by the same user or same computer that are treated as one **Logins Monitor** record.

Auto refresh time – The interval of time during which the user interface of the Logins Monitor refreshes its view when it requests an update of the users logins records.

Ignore revoked events – When selected, the Logins Monitor tab only stores and displays the latest login event (both user and computer event) for each IP address.

Ports and protocols

Direction	Port	Protocol
Idc to gw	443	Proprietary Check Point protocol, over HTTPS. Used for ongoing communication between the agent and the gateway.
idc to dc	53	DNS
idc to dc	389	LDAP
idc to dc	135, and dynamically allocated ports	* DCOM protocol, which makes extensive use of DCE/RPC.
idc to ise	5222	Session subscribe. Gets notifications of new login/logout events.
idc to ise	8910	Bulk session download. Fetches all the active sessions from the ISE Server.

*DCOM uses DCE/RPC. If the DC uses Windows Firewall, you must configure it to allow Identity Collector traffic: enable **Remote Event Log Management** > Remote **Event Log Management (RPC)**.

Alias Feature

Sometimes, a Domain Controller sends events with domain names that are not the BIOS or the FQDN names. When this occurs, the gateway does not know the domain and drops the association. The Alias feature of the Identity Collector fixes this issue.

To enable this feature, create a new configuration file (DomainDictionaryAliases.cfg) and locate it in the configuration files directory: (C:\ProgramData\CheckPoint\IdentityCollector).

The structure of the file must be as follows:

<name to convert>=<name to convert to>

Each line shows one conversion.

For example, if the nickname of "something.com" is "someone", add this line to the file:

someone=something.com

This way, if an event contains the "someone" domain, the domain name will change to "something.com".

Notes:

- There is no space between the equal sign and the name of the domain or the nickname.
- After you add the file, restart the service.

Optimization

Exclude multi-user machines

After the Identity Collector works for a while, you can check how many multi-user computers there are, and add them to the Network Exclusion List. To do so, enter this command on the gateway CLI:

```
pdp idc muh show
```

Exclude service accounts

After the Identity Collector works for a while, you can see how many service accounts there are, and add them to the Identity Exclusion List. To do so, enter this command on the gateway CLI:

```
pdp idc service_accounts
```

Consolidate Groups

If the gateway receives the user groups from the Identity Collector (SGT), it does not try to fetch them from the user directory. If you enable group consolidation, the gateway fetches the group even if it receives groups from the Identity Collector:

```
pdp idc groups_consolidation show
```

Configuring Identity Awareness API

To configure the Identity Awareness Web API:

1. In the **Gateways & Servers** view, double-click the Security Gateway.
2. In the **Identity Sources** section of the Identity Awareness page, select **Identity Web API** and click **Settings**.
3. In the **Identity Web API Settings** window, configure:
   - **Client Access permissions** ("Identity Web API Access" on page 55)
   - **Authorized Clients** and **Client Secret** ("Authorized Web API Clients" on page 56)
   - **Authentication Settings** ("Web API Authentication Settings" on page 56)

Identity Web API Access

You must authorize Gateway interfaces that can accept connections from Web API clients.

To select the gateway interfaces:

1. In the **Client Access Permissions** section, click **Edit**.
2. 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 access the Security Gateway if they use networks connected to these interfaces. The options are:

   a) **All Interfaces** - All Security Gateway interfaces can accept connections from Web API clients.

   b) **Internal Interfaces** - Only explicitly defined internal Security Gateway interfaces can accept connections from Web API clients.

- **Including undefined internal interfaces** - Also accepts connections from internal interfaces without a defined IP address.
- **Including DMZ internal interfaces** - Also accepts connections from clients located in the DMZ.
- **Including VPN Encrypted interfaces** - Also accepts connections from clients located in the VPN.

c) **According to the Firewall policy** - Select this if there is a rule that states which interfaces can accept connections from Web API clients.

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

Authorized Web API Clients

An Identity Awareness Security Gateway accepts Web API requests only from authorized Web API clients.

To configure an authorized Identity Web API client:

1. In the **Authorized Clients** section, click the **+** icon and select an Identity Web API client from the list.

   To define a new host object, go to the **Objects** pane or to the **Objects** menu, and click **New**.

   Click the **-** icon to remove an existing Identity Web API client from the list.
2. Create a strong client secret for client authentication. You can do it manually, or automatically with the **Generate** button. Create a separate client secret for each client. To change a client secret, do it manually.

Web API Authentication Settings

In the **Authentication Settings** section, click Settings to open the **Authentication Settings** window. In this window you can configure:

- **User Directories** - Select one or more places where the Security Gateway searches to find users which the API reports.
  - **Internal users** - The directory of internal users.
  - **LDAP users** - The directory of LDAP users:
    - **All Gateway's Directories** -Users from all LDAP servers.
    - **Specific** - Users from LDAP servers that you select.
  - **External user profiles** - The directory of users who have external user profiles.

All user directory options are selected by default.

Best Practice - Select only one or two options if users are from a specified directory or directories.

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://<gw>/_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	Minimal Gateway Version
https://<gw>/_IA_API/idasdk/<command>	1.0	R80.10
https://<gw>/_IA_API/v1.0/<command>	1.0	R80.10
https://<gw>/_IA_API/ <command>	Latest	R80.10

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

Add Identity (v1.0)

Description

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

Syntax

POST https://<gateway-server>/_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)

Parameter	Type	Description	Default value
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
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

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. This ensures 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 such as user, domain and group names, must not contain curly brackets ("{", "}"), square brackets ("[", "]"), or angle brackets ("<", ">"). Requests containing such characters will fail.
- When you set `fetch-user-groups` or `fetch-machine-groups` or both to 1, you must also set `calculate-roles` to 1. Otherwise, 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 auditing information, but does not affect 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 request 1: Minimum request for user identity generation

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

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

Response 1

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

Example request 2: User-defined groups, calculate roles

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":43200,
 "fetch-user-groups":0,
 "calculate-roles":1,
 "identity-source":"ACME API Client"
}
```

Response 2

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

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

```
{
 "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 3

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

Delete Identity (v1.0)

Description

Delete Identity Awareness associations for one IP address, an IP range, or a subnet.

Syntax

POST https://<gateway-server>/_IA_API/v1.0/delete-identity

Parameter	Type	Description	Default value
shared-secret	String	Shared secret	N/A
ip-address	String (IP)	Association IP. Required when you revoke a single IP.	Empty
revoke-method	String	Type of revoke method. It can be empty for the deletion of a single association by an IP. Otherwise permitted values: **mask** – for the deletion of all associations in a subnet. **range** – for the deletion of all associations in a range.	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 in the range. Required when the revoke method is range.	Empty

Parameter	Type	Description	Default value
ip-address-last	String (IP)	Last IP 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 gateway deletes all identities associated with the given IP (or IPs) (see the client type table for a list of the permitted values). **Note -** When the `client-type` is set to vpn (remote access), the gateway deletes all the identities associated with the given IP (or IPs). This is because when you delete an identity associated with an office mode IP, this usually means that this office mode IP is no longer valid.	Any

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
if-map	IFMAP
multihost-agent	Terminal Servers (multi-user host agent)
radius	RADIUS Accounting
ida-api	Identity Web API
identity-collector	Identity Collector

Response

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 request 1: Delete by IP

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

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

Response 1

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

Example request 2: Delete by IP range

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 2

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

Example request 3: Delete by IP subnet

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 3

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

Query Identity (v1.0)

Description

Queries the Identity Awareness associations of a given IP.

Syntax

POST https://<gateway-server>/_IA_API/idasdk/show-identity

Parameter	Type	Description	Default Value
shared-secret	String	Shared secret	N/A

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

Response

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.

Examples

Request 1

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":"Identiy 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 show in the order of the requests.

Request 1: Adding multiple associations

```
{
 "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 1: Added multiple associations

```
{
 "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."
  }
```

```
 ]
}
```

Request 2: Adding multiple associations, one of which is incorrect

```
{
 "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 2: Corresponding return values

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

Request 3: Request multiple identities

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

Response 3: Returned identities

```
{
  "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

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 also on success. The `code` field implies that the action failed. For bulk requests, the HTTP status code is always 200. A granular error code is given for each of the requests.

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 access the gateway and that the gateway does not drop the traffic.

HTTP status	API response (`code` field)	Possible cause
404	N/A	This is the result of these causes: • IDA API is not enabled. • IDA API is enabled, but the API client is not authorized. • IDA 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
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 technical support for further assistance.

Selecting Identity Sources

Identity sources have different security and deployment considerations. Depending on your organization requirements, you can choose to set them separately or as combinations that supplement each other.

This section presents some examples of how to choose identity sources for different organizational requirements.

- For logging and auditing with basic enforcement - enable Identity Awareness on the Security Gateway and select AD Query as the identity source.
- For logging and auditing only - select the **Add** identity to logs received from Security Gateways without Identity Awareness (requires Active Directory Query).
- For Application Control - set the AD Query and Browser-Based Authentication identity sources. The AD Query finds all AD users and computers. The Browser-Based Authentication identity source is necessary to include all non-Windows users. It also 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.
- For Data Center/internal server protection - these are some identity source options:
  - AD Query and Browser-Based Authentication - When most users are desktop users (not remote users) and easy deployment is important.

  Note - You can add Endpoint Identity Agents if you have mobile users and also have users that are not identified by AD Query. Users that are not identified encounter redirects to the Captive Portal.

Endpoint Identity Agents and Browser-Based Authentication - When a high level of security is necessary. The Captive Portal is used for distributing the Endpoint Identity Agent. IP Spoofing protection can be set to prevent packets from being IP spoofed.

- For Terminal Servers and Citrix environments - Set the Terminal Servers identity source and install the Terminal Servers Endpoint Identity Agent on each Terminal Server.
- For users that access the organization through VPN - Set the Remote Access identity source to identify Mobile Access and IPsec VPN clients that work in Office Mode.
- For environments that use a RADIUS server for authentication, select the RADIUS Accounting identity source. 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

In this section:

Acquiring 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 will have seamless access to resources based on Firewall rules.

Scenario: Laptop Access

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 John's desktop which is assigned a static IP address 10.0.0.19.

He received a laptop and wants to access 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 access the HR Web Server from his laptop with a static IP (10.0.0.19).

Name	Source	Destination	VPN	Service	Action	Track
Jadams to HR Server	Jadams_PC	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 & Monitor** 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 access the HR Web Server from any computer and from any location.
4. Sees how the system tracks the actions of the access role in in the **Logs & Monitor** view of SmartConsole.

User Identification in the Logs

The logs in the **Logs & Monitor** 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 based on 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 access the HR Web Server from **any** computer, change the rule in the Access Control Policy Rule Base. Create an access role ("Working with Access Roles" on page 27) for James Wilson, 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 from the laptop of James Wilson and give it a dynamic IP. The Security Gateway James Wilson, defined in the HR_Partner access role, access the HR Web server from his laptop with a dynamic IP.

Acquiring 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 will attempt to identify users that are logged into the domain using SSO before it shows the Captive Portal.

Scenario: 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. However, 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 is based on rules in the Firewall Rule Base.

Required SmartConsole Configuration

To make this scenario work, the IT administrator must:

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

   The **Action Settings** window opens.
5. Select **Enable Identity Captive Portal**.
6. Click **OK**.
7. 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 Daniel David.
   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	Daniel David	Finance_Server	Any Traffic	http	Accept (Enable Identity Captive Portal)	Log

User Experience

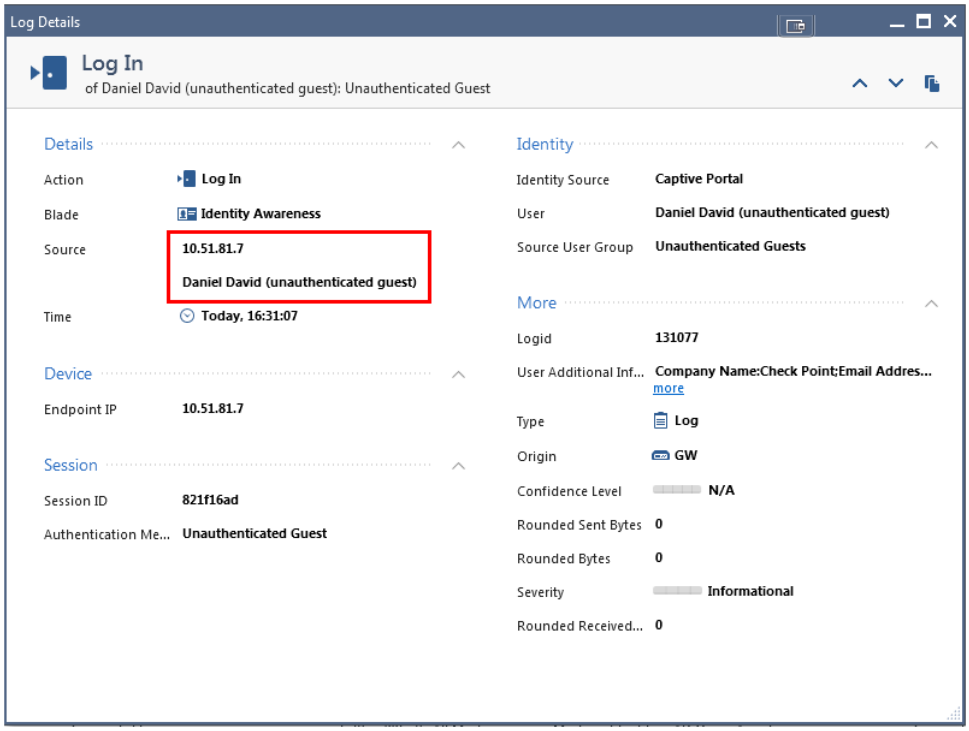
Jennifer McHanry does these steps:

1. Browses to the Finance server from her iPad.

   The Captive Portal opens because she is not identified and therefore cannot access the Finance Server.
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 & Monitor view shows how the system recognizes Daniel David from his iPad. This uses the identity acquired from Captive Portal.

Scenario: 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. Afterwards they are given access to the Internet for a specified period of time.

Required SmartConsole Configuration

To make this scenario work, the IT administrator must:

1. **Enable Identity Awareness** on a Security Gateway and select **Browser-Based Authentication** as one of the **Identity Sources**, and click **Settings**.
2. In the **Portal Settings** window in the **Users Access** section, make sure that **Unregistered guest login** is selected.
3. Click **Unregistered guest login - Settings.**
4. In the **Unregistered Guest Login Settings** window, configure:
   - The data guests must enter.
   - For how long users can access the network resources.
   - If a user agreement is required and its text.
5. 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**.

6. 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

From the perspective of a guest at ACME, she does these steps:

1. 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 to the Internet for a specified period of time.

Acquiring Identities with Endpoint Identity Agents

Scenario: Endpoint Identity Agent Deployment and User Group Access

The ACME organization wants to make sure that only the Finance department can access the Finance Web server. The current Rule Base uses static IP addresses to define access for the Finance department.

Amy, the IT administrator wants to leverage the use of Endpoint Identity Agents so:

- Finance users will automatically be authenticated one time with SSO when logging in (using Kerberos which is built-in into Microsoft Active Directory).
- Users that roam the organization will have continuous access to the Finance Web server.
- Access to the Finance Web server will be more secure by preventing IP spoofing attempts.

Amy wants Finance users to download the Endpoint Identity Agent from the Captive Portal. She needs to configure:

- **Endpoint Identity Agents** as an identity source for Identity Awareness.
- Endpoint Identity Agent deployment for the Finance department group from the Captive Portal. She needs to deploy the Full Endpoint Identity Agent so she can set the IP spoofing protection. No configuration is necessary on the client for IP spoofing protection.

- A rule in the Rule Base with an access role for Finance users, from all managed computers and from all locations with IP spoofing protection enabled.

After configuration and policy install, users that browse to the Finance Web server will get the Captive Portal and can download the Endpoint Identity Agent.

User Experience

A Finance department user does this:

1. Browses to the Finance Web server.

   The Captive Portal opens because the user is not identified and cannot access the server. A link to download the Endpoint Identity Agent is shown.
2. The user clicks the link to download the Endpoint Identity Agent.

   The user automatically connects to the Security Gateway. A window opens asking the user to trust the server.

   Note - The trust window opens because the user connects to the Security Gateway with Identity Awareness, with the **File name based server** discovery option. There are other server discovery methods that do not require user trust confirmation.
3. Click **OK**. The user automatically connects to the Finance Web server.

   The user can successfully browse to the internet for a specified period of time.

Required SmartConsole Configuration

To make this scenario work, the IT administrator must:

1. **Enable Identity Awareness** on a Security Gateway and select **Endpoint Identity Agents** and **Browser-Based Authentication** as **Identity Sources**.
2. Click the Browser-Based Authentication **Settings** button.
3. In the Portal Settings window in the **Users Access** section, select **Name and password login**.
4. In the Endpoint Identity Agent Deployment from the Portal, select **Require users to download** and select **Endpoint Identity Agent - Full** option.

   Note - This configures Endpoint Identity Agent for all users. Alternatively, you can set Endpoint Identity Agent download for a specific group ("Configuring Endpoint Identity Agent Deployment for User Groups" on page 41).
5. Configure Kerberos SSO.
6. Create a rule in the Firewall Rule Base that lets only Finance department users access the Finance Web server and install policy:

   a) From the **Source** of the rule, right-click to create an **Access Role**.

   b) Enter a **Name** for the Access Role.

   c) In the Networks tab, select **Specific users** and add the Active Directory Finance user group.

   d) In the Users tab, select **All identified users**.

   e) In the **Machines** tab, select **All identified machines** and select **Enforce IP spoofing protection (requires Full Endpoint Identity Agent)**.

   f) Click **OK**.

   The Access Role is added to the rule.
7. Install policy.

What's Next

Other options that can be configured for Endpoint Identity Agents:

- A method that determines how Endpoint Identity Agents connect to a Security Gateway enabled with Identity Awareness and trusts it. In this scenario, the File Name server discovery method is used.
- Access roles ("Working with Access Roles" on page 27) to leverage computer awareness.
- End user interface protection so users cannot access the client settings.
- Let users defer client installation for a set time and ask for user agreement confirmation. See User Access (on page 39).

User Identification in the Logs

The log in the **Logs & Monitor** > **Logs** tab shows how the system recognizes a guest.

The log entry shows that the system maps the source IP address with the user identity. In this case, the identity is "guest" because that is how the user is identified in the Captive Portal.

Acquiring Identities in a Terminal Server Environment

Scenario: Identifying Users Accessing the Internet through Terminal Servers

The ACME organization defined a new policy that only allows users to access the internet through Terminal Servers. The ACME organization wants to make sure that only the Sales department will be able to access Facebook. The current Rule Base uses static IP addresses to define access for Facebook, but now all connections are initiated from Terminal Server IP addresses.

Amy, the IT administrator wants to leverage the use of the Terminal Servers solution so that:

- Sales users will automatically be authenticated with Identity Awareness when logging in to the Terminal Servers.
- All connections to the internet will be identified and logged.
- Access to Facebook will be restricted to the Sales department users.

To enable the Terminal Servers solution, Amy must:

- Configure Terminal Server/Citrix Identity Agents as an identity source for Identity Awareness.
- Install a Terminal Servers Identity Agent on each of the Terminal Servers.
- Configure a shared secret between the Terminal Servers Identity Agents and the gateway.
- After configuration and installation of the policy, users that log in to Terminal Servers and browse to the internet will be identified and only Sales department users will be able to access Facebook.

Acquiring Identities in Application Control

You can use the Identity Awareness and Application Control and 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 Control and 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 to access applications.
- In logs and events, you can see which user and IP address accesses which applications.

Scenario: Identifying Users in Application Control Logs

The ACME organization wants to use Identity Awareness to monitor outbound application traffic and learn what their employees are doing. To do this, the IT administrator must enable Application Control and Identity Awareness. Identity information for the traffic then shows in the logs and events. See the logs in the **Logs & Monitor** > **Logs** tab. See the events in the **Logs & Monitor** views, in the Access Control categories.

Next, the IT department can add rules to block specific applications or track them differently in the Application Control and URL Filtering Layer of the policy to make it even more effective. See the *R80.10 Application Control and URL Filtering Administration Guide* http://supportcontent.checkpoint.com/documentation_download?ID=46526.

Required SmartConsole Configuration

To make this scenario work, the IT administrator:

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. Enables Identity Awareness on a Security Gateway, selects **AD Query** as one of the **Identity Sources**.
3. Installs the policy.

User Identification in the Logs

You can see data for identified users in the Logs and Events that relate to application traffic. See Logs in the **Logs & Monitor** view **Logs** tab. See Events in the **Logs & Monitor** Access Control views.

The log entry shows that the system maps the source IP address with the user identity. It also shows Application Control data.

Configuring Identity Logging for a Log Server

In This Section:

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 Gateways 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

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 logging:

1. Log in to SmartConsole.
2. From the **Gateways & Servers** view, select the **Log Server**.
3. In the **General Properties** page, in the **Management** section, select **Logging & Status** and **Identity Awareness** .

   The Identity Awareness Configuration wizard opens.
4. Click **Next**.

   The Integration With Active Directory window opens.

   When SmartConsole is part of the 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.

   Best practice - In the LDAP Account Unit, make sure that only necessary domain controllers are in the list. Delete the domain controllers that are not required to operate with the AD Query from the LDAP Servers list.

   With the Identity Awareness configuration wizard you can use existing LDAP Account units or create a new one for an AD domain. If you create a new 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 at a later time manually to the LDAP Servers list after you complete the wizard.

To view/edit the LDAP Account Unit object, select **Servers and OPSEC** in the objects tree > **LDAP Account Unit**.

The LDAP Account Unit name syntax is: <domain name>_ _ AD

For example, CORP.ACME.COM_ _ AD.

5. 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 did not set up Active Directory, enter a **domain name**, **username, password** and **domain controller** credentials.
6. Enter the Active Directory credentials and click **Connect** to make sure the credentials are correct.

   Important - For AD Query you must enter domain administrator credentials or do the steps in sk43874 http://supportcontent.checkpoint.com/solutions?id=sk43874.
7. Click **Finish**.

Install Database for a Log Server

If you have configured Identity Awareness for a log server, but do not see identities in logs, make sure you installed the database.

To install the database:

1. From **SmartConsole**, click **Menu** > **Install Database**.

   The **Install Database** window appears.
2. Select the computers to install the database on.
3. Click **OK**.
4. Click **Close** when done.

WMI Performance

Bandwidth between the Log server and Active Directory Domain Controllers

The amount of data transferred between the Log server and domain controllers depends on the amount of events generated. The generated events include event logs and authentication events. The amounts vary according to the applications running in the network. Programs that have many authentication requests result in a larger amount of logs. The observed bandwidth range varies between 0.1 to 0.25 Mbps per each 1000 users.

CPU Impact

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

Identity Awareness Deployment

In This Section:

Identity Sharing

Best Practice - In environments that use many Security Gateways and AD Query, we recommend that you set only one Security Gateway to acquire identities from a given Active Directory domain controller for each physical site. If more than one Security Gateway gets identities from the same AD server, the AD server can become overloaded with WMI queries.

Set these options on the **Identity Awareness** > **Identity Sharing** page of the Security Gateway object:

- One Security Gateway to *share* identities with other Security Gateways. This is the Security Gateway that gets identities from a given domain controller.
- All other Security Gateways to *get* identities from the Security Gateway that acquires identities from the given domain controller.

The *Deployment Scenarios* (on page 85) section has more details.

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 account unit.

You can use the Identity Awareness Configuration Wizard to define **one** subdomain. This automatically creates an LDAP Account Unit that you can easily configure for more settings. You must manually create all other domains that you want Identity Awareness to relate to, from **Servers and OPSEC** in the **Objects** tree > **Servers** > **New** > **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 a Security Gateway enabled with Identity Awareness, 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 set 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 supports the use of LDAP nested groups. When a group is nested in another group, users in the nested group are identified as part of the parent group. For example, if you make Group_B a member of Group_A, Group_B members will be identified by Identity Awareness as being part of Group A.

There are three ways to configure nested group queries:

- **Recursive nested groups -** The gateway sends a query with the user name to the LDAP server. The server finds the groups that the user is a member of and sends it to the gateway. To know if a group is nested in another group, and for each nesting level, you must send a new query. This feature is enabled by default. The default nesting depth is configured to 20. For details, see sk66561 http://supportcontent.checkpoint.com/solutions?id=sk66561.
- **Per-user nested groups -** With one LDAP query, the response includes all groups for the given user, with all nesting levels. The server sends the groups of a given user as a flat list.
- **Multi per-group nested groups -** The gateway sends one LDAP query, which includes the user name and the group. The server responds if the user is in this group or not. **Best Practice -** Use this configuration for Microsoft Active Directory environment with many defined users and groups, and less groups defined in SmartConsole.

Configuring Nested Groups Query Options

You configure the nested group query options through the Security Gateway CLI:

Command	Description
`pdp nested_groups status`	Show status
`pdp nested_groups_set_state 1`	Set recursive nested groups (like R.77x)
`pdp nested_groups_set_state 2`	Set per-user nested groups
`pdp nested_groups_set_state 2`	Set multi per-group nested groups

Advanced Identity Awareness Deployment

In This Section:

Introduction to Advanced Identity AwarenessDeployment

Deploy Check Point Identity Awareness enabled Security Gateways for better security for your network environment and corporate data. This section describes recommended deployments with Identity Awareness.

Important - NAT between two Identity Awareness Security Gateways that share data with each other is not supported.

- Perimeter Security Gateway with Identity Awareness – This deployment is the most common scenario. Deploy the Security Gateway at the perimeter where it protects access to the DMZ and the internal network. The perimeter Security Gateway also controls and inspects internal traffic going to the Internet. In this deployment, create an identity-based Access Control Policy.
- Data Center protection – If you have a Data Center or server farm separated from the users' network, protect access to the servers with the Security Gateway. Deploy the Security Gateway in front of the Data Center. All traffic is inspected by the Security Gateway. Control access to resources and applications with an identity-based access policy. Deploy the Security Gateway in bridge mode to protect the Data Center without significant changes to the existing network infrastructure.
- Large scale enterprise deployment – In large networks, deploy multiple Security Gateways. For example: deploy a perimeter Firewall and multiple Data Centers. Install an identity-based policy on all Identity Awareness Security Gateways. The Security Gateways share user and computer data of the complete environment.
- Network segregation – The Security Gateway helps you migrate or design internal network segregation. Identity Awareness lets you control access between different segments in the network with an identity-based policy. Deploy the Security Gateway close to the access network to avoid malware threats and unauthorized access 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, deploy the Security Gateway at the remote branch offices. When you enable Identity Awareness on the branch office Security Gateway, users are authenticated before they reach internal resources. The identity data on the branch office Security Gateway is shared with other Security Gateways to avoid unnecessary authentication.

- Wireless campus – Wireless networks have built-in security challenges. To give access to wireless-enabled corporate devices and guests, deploy Identity Awareness Security Gateways in front of the wireless switch. Install an Identity Awareness policy. The Security Gateways give guest access after authentication in the web Captive Portal, and then they inspect the traffic from WLAN users.

Deployment Options

You can deploy a Security Gateway enabled with Identity Awareness in two different network options:

- IP routing mode
- Transparent mode (bridge mode)

IP routing mode – This is a regular and standard method used to deploy Security Gateways. You usually use this mode when you deploy the Security Gateway at the perimeter. In this case, the Security Gateway behaves as an IP router that inspects and forwards traffic from the internal interface to the external interface and vice versa. Both interfaces should be located and configured using different network subnets and ranges.

Transparent mode – Known also as a "bridge mode". This deployment method lets you install the Security Gateway as a Layer 2 device, rather than an IP router. The benefit of this method is that it does not require any changes in the network infrastructure. It lets you deploy the Security Gateway inline in the same subnet. This deployment option is mostly suitable when you must deploy a Security Gateway for network segregation and Data Center protection purposes.

Deploying a Test Environment

Best Practice - If you want to evaluate how Identity Awareness operates in a Security Gateway, we recommend that you deploy it in a simple environment. The recommended test setup below gives you the ability to test all identity sources and create an identity-based Policy.

The recommendation is to install 3 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)

Deploy the Security Gateway in front of the protected resource, the Windows server that runs IIS (web server). The user host computer will access the protected resource via the Security Gateway.

Testing Endpoint Identity Agents

Enable and configure Identity Agents, and configure Identity Agents self-provisioning through Captive Portal ("Configuring Endpoint Identity Agent Deployment from Captive Portal" on page 41).

1. Open a browser and connect to the web resource.

   You are redirected to the Captive Portal.
2. Enter user credentials.
3. Install the client as requested by the Captive Portal.

   When the client is installed wait for an authentication pop-up to enter the user credentials through the client.

4. Test connectivity.

Deployment Scenarios

Perimeter Security Gateway with Identity Awareness

Security Challenge

The Security Gateway at the perimeter behaves as a main gate for all incoming and outgoing traffic to and from your corporate network. Users in internal networks access the Internet resource and applications daily. Not all Internet applications and web sites are secure and some are restricted according to corporate policy. If you block all internal access, it will impact 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 require a more granular access policy for user and computer identity.

Access roles let you configure an identity aware policy with Application Control, to allow access only to specified user groups to the applications on the Internet.

Enable Identity Awareness on the perimeter Security Gateway.

Deployment scenario

1. Deploy the Security Gateway at the perimeter in routing mode and define an external interface towards the ISP (the Internet) and an internal interface points to the internal corporate network LAN.

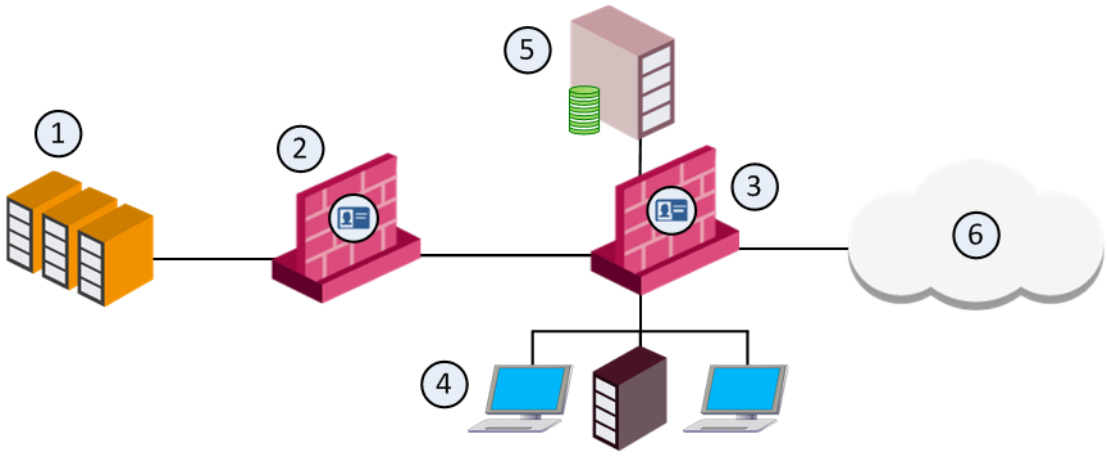
   Optional: you can define another internal interface which protects DMZ servers.
2. Make sure there are no NAT or Proxy servers between the gateway and your network.

   Best Practice - We recommend that the Proxy server be in the DMZ network.
3. Check that the Security Gateway has connectivity to the internal AD domain controllers.
4. Make sure that users can reach the internal interface of the Security Gateway.
5. Configure the Application Control blade.
6. If you have several perimeter Security Gateways leading to the Internet, we recommend that you manage these Security Gateways with one Security Management Server and SmartConsole to deploy the relevant security policy.

Configuration

1. Enable Identity Awareness and select the appropriate identity sources.
2. Create access roles based on users and computers. You can create multiple access roles that represent different departments, user and computer groups and their location in the network.
3. Add the access roles to the source column of the relevant Firewall and application control policies.

This is a sample diagram for a small to medium corporate headquarters.



Item	Description
1	Corporate data center
2	Security Gateway with Identity Awareness protects the data center
3	Perimeter Security Gateway with Identity Awareness User IDs are sent 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 securely protect from unauthorized access. You must also protect it from malwares and viruses that can harm databases and steal corporate information. Access to the Data Center and particularly to certain applications must be granted only to compliant users and computers.

Deployment Scenario

1. Deploy the Security Gateway inline in front of the Date Center core switch, protecting access to the Data Center from the LAN.
2. **Best Practice -** We recommend that you deploy the Security Gateway in the bridge mode, to avoid any changes in the network. However, IP routing mode is also supported.
3. Define at least two interfaces on the Security Gateway and configure them to be internal or bridged.
4. Make sure that the Security Gateway has connectivity to the Active Directory and all relevant internal domain controllers in the network (LAN).
5. Make sure that users from the LAN can connect to the Data Center through the Security Gateway with an ANY ANY Accept policy.

6. Make sure that you do not have a proxy or NAT device between the Security Gateway and users or the LAN.

Configuration

1. Enable Identity Awareness on the Security Gateway and select identity sources.
2. Create access roles for users and apply the access roles to relevant Access Control Policy rules.

Large Scale Enterprise Deployment

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 will impact 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 policy based on user and computer identity, use access roles with Application Control.

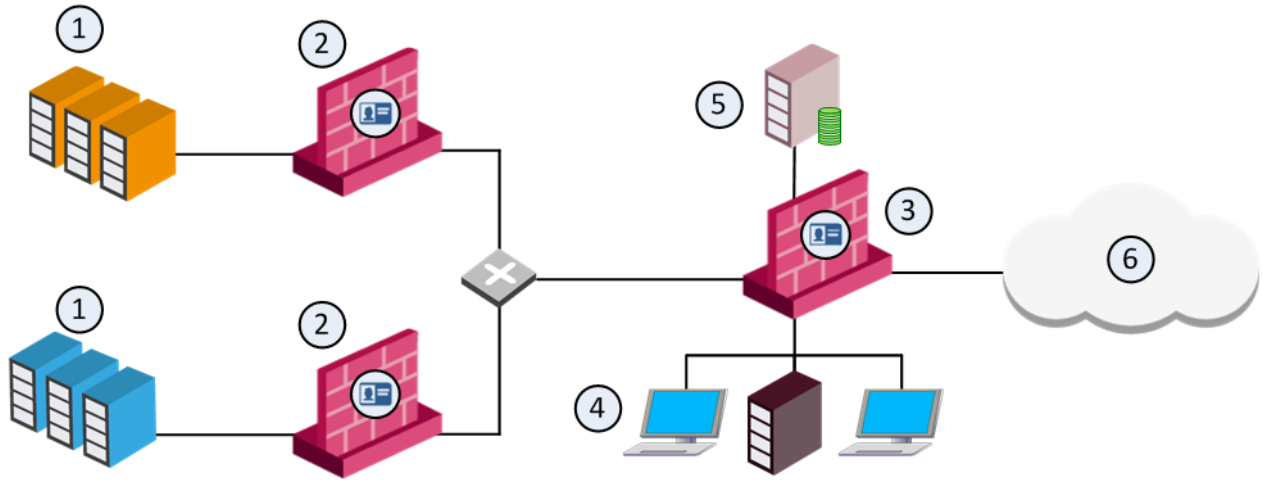
Deployment Scenario

1. Deploy or use existing Security Gateways 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 (define it as an internal interface).
3. Deploy the Security Gateway as an inline device in front of the Data Center in bridge mode to avoid network changes. This is not required, but is recommended. Nonetheless, IP routing mode is also supported.
4. Make sure that all Security Gateways in the Data Centers and perimeter can communicate directly with each other.
5. **Best Practice -** We recommend that you manage the Security Gateway from one Security Management Server and SmartConsole.
6. Make sure that there is connectivity from each Security Gateway to the Active Directory internal domain controllers.
7. Make sure that in an "Any Any Accept" Policy, users from the LAN can connect to the desired resources.
8. 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

1. Enable Identity Awareness on the Security Gateway.
2. Choose 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. In 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	Security Gateway with Identity Awareness protects the data center
3	Perimeter Security Gateway with Identity Awareness User IDs are sent 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 obtain user and computer identity, we recommend that you enable the feature on all Security Gateways that participate in the network environment. All Security Gateways should have the Active Directory domain defined with the list of all applicable domain controllers in the internal network.

Best Practice - Endpoint Identity Agents Recommended Configuration

If you choose to use Endpoint Identity Agents to authenticate users and computers, you have to select the Security Gateway that will be used to maintain Endpoint Identity Agents.

For a single Data Center and perimeter Security Gateway it is recommended to define Endpoint Identity Agents that connect to a single Security Gateway. Then the identity obtained by the Security Gateway is shared with the other Security Gateways in the network. Select a high capacity / performance Security Gateway, which can also behave as an authentication server, and configure this Security Gateway's IP / DNS on the Endpoint Identity Agents (see Endpoint Identity Agents section).

For complex multi Data Center environments where there are several Security Gateways that protect different Data Centers and the perimeter, we recommend that you balance Endpoint

Identity Agents authentication using different Security Gateways. You can configure a list of Security Gateways in the Endpoint Identity Agent settings, where the Endpoint Identity Agent will connect to different Security Gateways. This provides load balancing across the Security Gateways. Identities learned from the agents are shared between all Security Gateways in the network.

To define a list of Security Gateways between which identity information is shared:

1. Open **Gateway properties** > **Identity Awareness**.
2. Select **Get identities from other gateways**.
3. Select the Security Gateways 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 malwares across the network that can infect other computers and servers on the network. You want to make sure that only compliant users and computers can pass and connect across multiple network segments, as well as authenticate users connecting to the servers and the Internet.

Deployment scenario

- **Best Practice -** We recommend that you deploy Security Gateways close to 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 Gateways either at each segment or at the perimeter Security Gateway.
- **Best Practice -** We recommend that you deploy 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.
- Share identities learned from the segment Security Gateways with the perimeter Firewall to create an outgoing traffic Firewall policy or use an Application Control policy as well.

Configuration

1. Deploy Security Gateways in each segment in bridge mode.
2. Make sure that there is no proxy or NAT device between the Security Gateways and the LAN.
3. Make sure that the Security Gateways can communicate with the Active Directory domain controller deployed 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 Gateways 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 Endpoint Identity Agents, then define the particular Security Gateway DNS/IP in the agent Security Gateway configuration per access segment.

Distributed Enterprise with Branch Offices

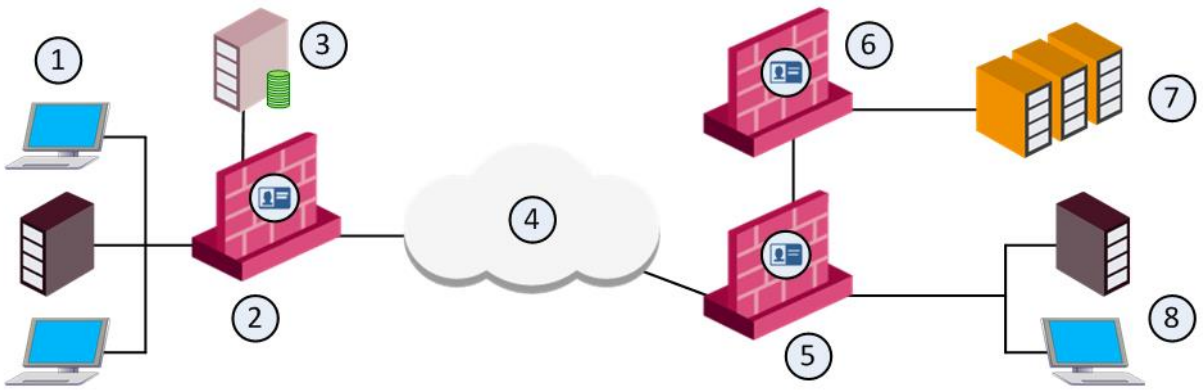
Security Challenge

In distributed enterprises there is a potential risk of malware and viruses spreading from remote branch offices over VPN links to the corporate internal networks. There is also a challenge of how to provide authorized access to users that come from remote branch offices that request and want to access the Data Center and the Internet.

Deployment Scenario

1. **Best Practice -** We recommend that you deploy Security Gateways at the remote branch offices and at headquarters in front of the Data Center and at the perimeter.
2. At remote branch offices, you can deploy low capacity Security Gateways due to a relatively low number of users.

   Deploy the remote branch Security Gateways in IP routing mode and have them function as a perimeter Firewall and VPN gateway, establishing a VPN link to the corporate Security Gateways.
3. **Best Practice -** At the corporate headquarters, we recommend that you deploy Data Center Security Gateways to protect access to Data Center resources and applications, as well as a perimeter Security Gateway. You can install the Data Center Security Gateway in bridge mode to avoid changes to the existing network.
4. In this scenario, users from the branch office are identified by the local branch office Security Gateway before connecting to the corporate network over VPN.
5. The identities learned by the branch office Security Gateways are then shared with the headquarters' internal and perimeter Security Gateways. When a user from a branch office attempts to connect to the Data Center, the user is identified by the Security Gateway at the headquarters Data Center without the need for additional authentication.



Item	Description
1	Internal network resources - branch office
2	Branch Security Gateway with Identity Awareness User IDs are sent to the corporate gateways

Item	Description
3	LDAP server (for example Active Directory)
4	Internet
5	Perimeter corporate Security Gateway with Identity Awareness
6	Security Gateway with Identity Awareness that protects the data center
7	Corporate data center
8	Internal network resources - corporate office

Configuration

1. Select a Security Gateway according to a performance guideline for your remote branch offices.
2. Deploy the Security Gateways at the branch offices in routing mode. Define VPN site-to-site if necessary.
3. Deploy Security Gateways inline at the Data Center. We recommend using bridge mode.
4. Deploy a Security Gateway at the perimeter that protects the internal network in routing mode. The perimeter Security Gateway can serve as a VPN Security Gateway for branch offices as well.
5. If you have Active Directory domain controllers replicated across your branch offices make sure that local Security Gateways can communicate with the domain controller. In case you do not have a local domain controller, make sure that the Security Gateways can access the headquarters' internal domain controller over VPN.
6. Enable Identity Awareness and select the appropriate methods to get identity.
7. Create an access role and apply the roles in the security policy on the branch office Security Gateways, perimeter and Data Center Security Gateway.
8. Share identities between the branch offices with the headquarter and Data Center Security Gateways. In the Identity Awareness tab, select **Get identities from other gateways** and **Share local identities with other gateways**.

Best Practice - AD Query Recommended Configuration

When you use AD Query to authenticate users from the local and branch offices, we recommend that you only configure a local domain controller list per site in the relevant Security Gateways. For example, if you have a branch office Security Gateway and a Data Center Security Gateway, enable AD Query on all Security Gateways. On the branch office Security Gateway, select the Active Directory domain controllers replications installed in the branch office only. 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, since the identity information is shared between branch and internal Security Gateways accordingly.

Best Practice - Endpoint Identity Agents Recommended Configuration

When using Endpoint Identity Agents, we recommend that you configure the local branch office Security Gateway DNS/IP on the agent. The agents connect to the local Security Gateway and the user is authenticated, identities are shared with the internal headquarter Security Gateways.

Wireless Campus

Security Challenge

You use wireless networks to grant access to employees that use Wi-Fi enabled devices, guests and contractors. Guests and contractors in some cases cannot use the corporate wired network connection and must connect through WLAN. Furthermore, it is not intended for guests and contractors to install any endpoint agents on their devices.

Wireless access is also intensively used to connect mobile devices such as smartphones where agents can be installed. These devices are not part of the Active Directory domain. Wireless networks do not give a desired level of security in terms of network access.

Deployment Scenario

1. Deploy the Security Gateway in bridge mode in front of the Wireless Switch.
2. Make sure that the Security Gateway can access the Internet or any other required resource in the network.
3. Make sure that the Security Gateway can communicate with the authentication server, such as Active Directory or RADIUS.
4. Check that there is no NAT or proxy device between the Security Gateway and the WLAN network.

Configuration

1. Enable Identity Awareness on the Security Gateway.
2. Select Browser-Based Authentication as an identity source.
3. In the Gateway properties > Identity Awareness tab > Browser-Based Authentication Settings, select **Unregistered guests login** and in Settings, select the fields you want guests to fill when they register.
4. Select **Log out users when they close the portal browser**.

Dedicated Identity Acquisition Security Gateway

Security Challenge

You have several Security Gateways that protect the Data Center or Internet access where access is based on identity acquisition. The Security Gateways run different blades and deal with heavy traffic inspection.

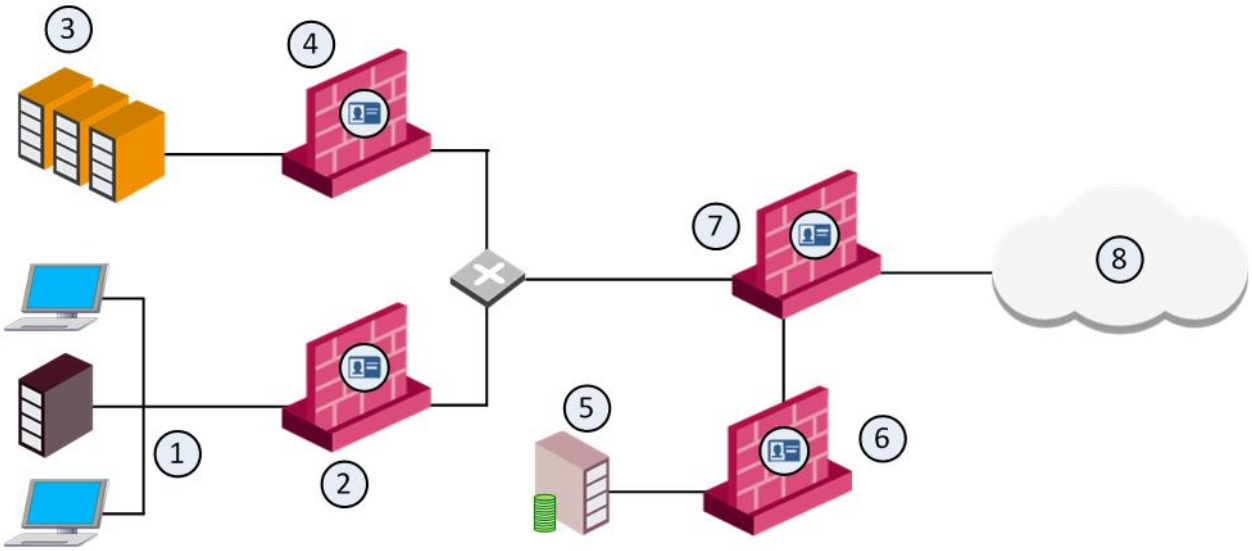
To avoid an impact on performance of the Security Gateways in terms of user identity acquisition and authentication, it is possible to offload this functionality to a separate Security Gateway. The dedicated Security Gateway is responsible for acquiring user identity, performing authentication and sharing learned identities with all Security Gateways in the network.

Deployment Scenario

In this deployment scenario, you have to choose an appropriate appliance to deploy as the dedicated Identity Awareness enabled Security Gateway. All users authenticate with this Security Gateway.

If you enable AD Query, the dedicated Security Gateway should communicate with all Active Directory domain controllers over WMI.

1. On the dedicated identity acquisition Security Gateway, enable the Identity Awareness feature and select the identity method.
2. On the Security Gateways, enable Identity Awareness and select **Get identities from other gateways** and **Share local identities with other gateways**.



Item	Description
1	Internal network resources
2	Security Gateway with Identity Awareness that protects the internal network User IDs are sent to the corporate gateways
3	Corporate data center
4	Security Gateway with Identity Awareness that protects the data center
5	LDAP server (for example Active Directory)
6	Dedicated Identity Awareness Security Gateway
7	Perimeter corporate Security Gateway with Identity Awareness
8	Internet

Advanced Browser-Based Authentication Configuration

In This Section:

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

To set the 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 that you see 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`. See the highlighted text in step number 2 above.

Changing Portal Text in SmartConsole

To change the text that shows in SmartConsole:

1. Go to **Menu > Global Properties > Advanced**.
2. Click **Configure**.
3. Go to **Identity Awareness** > **Portal Texts**.

4. Delete the word `DEFAULT` and type the new English text in the required 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:

1. Edit the language array for the new language locale.
2. Use the English language file as a template to create new language files. Then translate the strings in the new language file.
3. Save the files with UTF-8 encoding and move them to the correct location.
4. Set the language selection list to show on the Network Login page.
5. Make sure the text strings are shown correctly.

Editing the Language Array

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.

To create a new language, add an entry to the supported languages file:

1. Open the file:
   `/opt/CPNacPortal/phpincs/conf/L10N/supportedLanguages.php`
2. In the `$arLanguages` array, create a new locale entry with the syntax: `"xx_XX" => "XName"`.
   For example: "de_DE" => "German".

To disable a language:

Comment out the line of the specific language or delete the line.

Creating New Language Files

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 `  / < / >` in the translated strings.

To create a new language file:

1. Make a copy of the English language file:
   `/opt/CPNacPortal/phpincs/conf/L10N/portal_en_US.php`
2. Rename it to the new language using the syntax `portal_xx_XX.php`.
   For example, `portal_de_DE.php`
3. Translate the strings in the new language file.
4. 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>`.

Saving New Language Files

You must save the language file with UTF-8 encoding.

To save a file with UTF-8 encoding:

1. Use Notepad, Microsoft Word or a different editor to save the file with UTF-8 encoding. When using 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`.
2. Move the file to `/opt/CPNacPortal/phpincs/conf/L10N` if it is not already there.

Showing the Language Selection List

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.

To see the language list on the Network Login page:

1. On the Security Gateway, open the file:
   `/opt/CPNacPortal/phpincs/view/html/Authentication.php`
2. Back up the file (for possible future revert).
3. In `<label for="language_selection">`, remove the lines that start with `<?PHP /*` and end with `*/ ?>`

The lines to remove are in the square:

```
</table>

<!-- Separator and login button -->
            <?PHP if ($isPasswordLoginEnabled || $isUnauthLoginEnabled) { ?>
        <div class="contentFooter">
            <hr size="1" class="hr_footer">
            <table class="fullyExpanded" cellspacing="0" cellpadding="0">
                <tr>
<?PHP /*
                                        <td  align="left" >
                        <label for="language_selection">
                        <select NAME='LangSelect' class="languageSelection" onchange='oAuthent
                        <?PHP
                            foreach ($arLanguages as $sLangCode => $sLang)
                            {
                        ?>
                        <option class="languageOption" value='<?PHP echo $sLangCode?>'
                            <?PHP if ($sLangCode == $locale){
                                echo "selected";
                            }
                                                    ?>
                                ><?PHP if($UTILS->isIpad()){?>   <?PHP } echo $sLang
                        <?PHP
                                                    }
                                                ?>
                        </select>
                        </label>
                    </td>
*/ ?>
                    <td align="right">
                        <input class="footerButton"
                               type="button"
                               id="authn_form_submitButt"
                               tabindex=99
                               value="<?PHP echo $REQUEST->getL10N()->getStr("LOGIN");?>"
                               onclick="oAuthentication.submitActiveForm();">
                    </td>
                </tr>
            </table>
        </div>
                <?PHP   }  ?>
```

4. Save the file.

   The language selection list will show on the Network Login page.

To revert back to not showing the language selection list, replace the current file with the backup of the original file.

Making Sure the Strings Show Correctly

To make sure the strings show correctly:

1. Browse to the Captive Portal and select the new language.
2. Browse from different operating systems with different locale setups.
3. Make sure that the text is shown correctly on the Captive Portal pages.
4. Browse to the Captive Portal from a different browser and use a different font size.

Server Certificates

For secure SSL communication, 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).

The next sections describe how 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 acts 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 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. You see this output:

   ```
   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 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

To install the certificate:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click the appropriate 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**.
3. **Install 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 access 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 Endpoint 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 Security Gateway enabled with Identity Awareness).
4. The gateway decrypts the ticket, extracts the user's identity, and publishes it to all Security Gateways 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 Endpoint Identity Agents use to present the Kerberos ticket ("How SSO Works" on page 106).

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.

For more about Kerberos SSO, we recommend the MIT Kerberos web site http://web.mit.edu/Kerberos/ and the Microsoft TechNet Library http://technet.microsoft.com/en-us/library/bb742433.aspx.

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 Security Gateway configured with Identity Awareness.
- 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 choose any username and password. For example: a user account named `ckpsso` with the password `qwe123!@#` to the domain `corp.acme.com`.
3. Clear **User must change password at next logon** 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. The `setspn.exe` utility is not installed by default in Windows 2003.

To get the correct executable:

On Windows 2003:

1. Get the correct executable for your service pack from the Microsoft Support site http://support.microsoft.com/ before installation. It is part of the Windows 2003 support tools. For example, AD 2003 SP2 requires support tools for 2003 sp2 http://www.microsoft.com/downloads/details.aspx?familyid=96A35011-FD83-419D-939B-9A772EA2DF90&displaylang=en.
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 higher, the `setspn` utility is installed on your server in the `Windows\System32` folder. Run the command prompt as an Administrator.

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 will fail.

To use setspn:

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>
   ```

   For HTTPS connections:

   ```
   > setspn -A HTTPS/<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 steps. Start with: "Click **Active Directory SSO configuration** and configure the values".

To configure an account unit:

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** > **Server** > **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 101).
   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, select **Use Encryption (SSL)**. Fetch the fingerprint and click **OK**.

      Note - LDAP over SSL is not supported by default. If you did not configure your domain controller to support LDAP over SSL, configure it, or make sure **Use Encryption (SSL)** is not selected.
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. In SmartConsole, go to the **Gateways & Servers** view
2. Double-click the Security Gateway with **Identity Awareness** enabled.
3. Click **Identity Awareness** > **Browser-Based Authentication** > **Settings**.
   The **Portal Settings** window opens.
4. Select **Authentication Settings** - **Edit**.
   The **Authentication Settings** window opens.
5. Select **Automatically authenticate users from machines in the domain**.
   - **Main URL:** The URL used to begin the SSO process. If transparent authentication fails, users are redirected to the configured Captive Portal.
   - **IP Address:** The IP address to which the Portal URL is resolved if DNS resolution fails.

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 also enter the URL in the **Local Internet** field using 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 you have already configured Internet Explorer for Transparent Kerberos Authentication, that configuration also 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.

Advanced Endpoint Identity Agents Configuration

In This Section:

Customizing Parameters

You can change settings for Endpoint Identity Agent parameters to control Endpoint Identity Agent behavior. You can change some of the settings in SmartConsole and others using the Endpoint Identity Agent Configuration tool ("Creating Custom Endpoint Identity Agents" on page 113).

To change Endpoint Identity Agents parameters in SmartConsole:

1. Go to **Menu > Global Properties > Advanced**.
2. Click **Configure**.
3. Go to **Identity Awareness > Agent**.
4. Change the Endpoint Identity Agents parameters.
5. Click **OK**.

This is a sample list of parameters that you can change:

Parameter	Description
Nac_agent_disable_settings	Whether users can right click the Endpoint Identity Agent client (umbrella icon on their desktops) and change settings.
Nac_agent_email_for_sending_logs	You can add a default email address for to which to send client troubleshooting information.
Nac_agent_disable_quit	Whether users can right click the Endpoint Identity Agent client (umbrella icon on their desktops) and close the agent.
Nac_agent_disable_tagging	Whether to disable the packet tagging feature that prevents IP Spoofing.
Nac_agent_hide_client	Whether to hide the client (the umbrella icon does not show on users' desktops).

Advanced Endpoint Identity Agent Options

Kerberos SSO Compliance

The Identity Awareness Single Sign-On (SSO) solution for Endpoint Identity Agents gives the ability to transparently authenticate users that are logged in to the domain. This means that a user authenticates to the domain one time and has access to all authorized network resources without additional authentication.

Using Endpoint Identity Agents gives you:

- **User and computer identity**
- **Minimal user intervention** - The administrators do all the necessary configuration steps and no user input is required user.
- **Seamless connectivity** - Transparent authentication when users are logged in to the domain. If you do not want to use SSO, users enter their credentials manually. You can let them save these credentials.
- **Connectivity through roaming** - Users stay automatically identified when they move between networks, while the client detects the movement and reconnects.
- **Added security** - You can use the patented *packet tagging* technology to prevent IP Spoofing. Endpoint Identity Agents also gives you strong (Kerberos based) user and computer authentication.

You get SSO in Windows domains with the Kerberos authentication protocol. Kerberos is the default authentication protocol used in Windows 2000 and above.

The Kerberos protocol is based on the idea of *tickets*, encrypted data packets issued by a trusted authority which in this case is the Active Directory (AD). When a user logs in, the user authenticates to a domain controller that provides an initial *ticket granting ticket* (TGT). This ticket vouches for the user's identity. When the user needs to authenticate against the Security Gateway with Identity Awareness, the Endpoint Identity Agent presents this ticket to the domain controller and requests a *service ticket* (SR) for a specific resource (Security Gateway that Endpoint Identity Agents connect to). The Endpoint Identity Agent then presents this service ticket to the Security Gateway that grants access.

How SSO Works

This is the workflow for SSO (Single Sign On):

1. The user logs in to the computer and authenticates to the AD server.
2. The AD send an initial ticket (TGT) to the computer.
3. The Endpoint Identity Agent connects to the Security Gateway, which then requests the identity.
4. The Endpoint Identity Agent requests an SR (service ticket) for the Security Gateway and presents the TGT to the AD server.
5. The AD server sends the SR to the computer.

   The user name is encrypted with the shared secret between the Security Gateway and the AD server.
6. The Endpoint Identity Agent sends the SR to the Security Gateway.
7. The Security Gateway uses the shared secret to decrypt the ticket and confirms the user identity.

8. The user can access the Data Center.

Item	Description
1	Computer for the user
2	Active Directory Domain Controller server
3	Security Gateway with Identity Awareness
4	Data Center servers

SSO Configuration

SSO configuration includes two steps:

- AD Configuration - Creating a user account and mapping it to a Kerberos principal name.
- SmartConsole Configuration - Creating an LDAP Account Unit and configuring it with SSO.

AD Configuration

To use Kerberos with AD, make a Kerberos principal name with the Check Point Security Gateway service. Map this new account to the domain name.

Use the `setspn.exe` utility. Make sure you have the correct version ("Installing setspn.exe" on page 101).

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 ckp_pdp/<domain_full_dns_name> <old_account name>`

If you do not do this, authentication will fail.

To configure AD for Kerberos:

1. Make a new user account ("Creating a New User Account" on page 101).
2. Open the command line (**Start** > **Run** > **cmd**).
3. Run: `setspn -A ckp_pdp/<domain_full_dns_name> <username>`

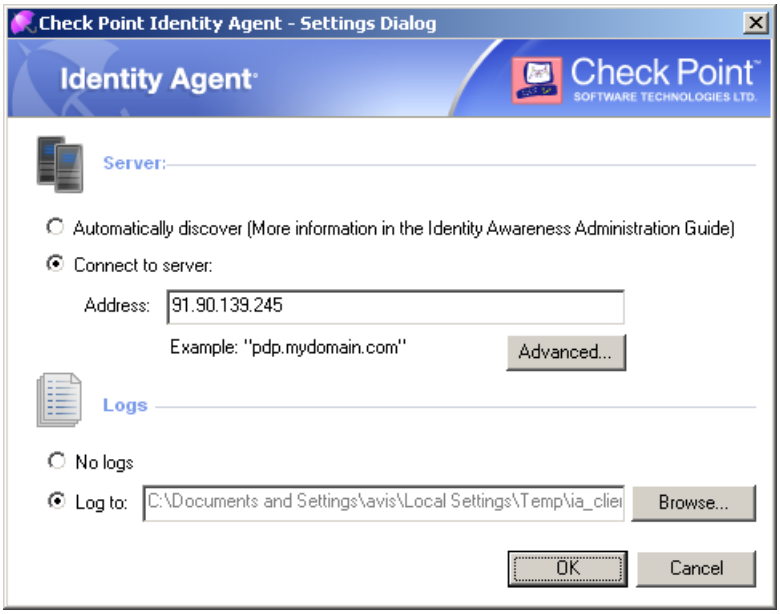
To see users associated with the principle name, run: `setspn -Q ckp_pdp*/*`

When done, make an Account Unit ("Configuring an Account Unit" on page 102) on the SmartConsole, to use this account.

Server Discovery and Trust

Introduction

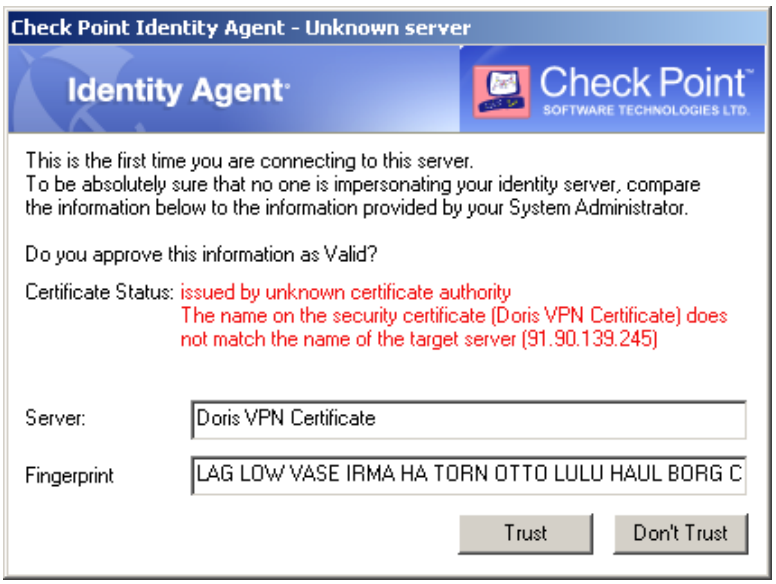
The Endpoint Identity Agent client needs to be connected to a Security Gateway with Identity Awareness. For this to happen, it must *discover* the server and *trust* it.



Server *discovery* refers to the process of deciding which server the client should connect to. We offer several methods for configuring server discovery – from a very basic method of simply configuring one server to a method of deploying a domain wide policy of connecting to a server based on your current location. This section describes these options.

Server *trust* refers to the process of validating that the server the end user connects to is indeed a genuine one. It also makes sure that communication between the client and the server was not tampered with by a Man In The Middle (MITM) attack.

The trust process compares the server fingerprint calculated during the SSL handshake with the expected fingerprint. If the client does not have the expected fingerprint configured, it will ask the user to verify that it is correct manually. This section describes the methods that allow the expected fingerprint to be known, without user intervention.



Discovery and Trust Options

These are the options that the client has for discovering a server and creating trust with it:

- **File name based server configuration** – If no other method is configured (default, out-of-the-box situation), any Endpoint Identity Agent downloaded from the portal will be renamed to have the portal computer IP in it. During installation, the client uses this IP to represent the Security Gateway with Identity Awareness. Note that the user has to trust the server by himself (the trust dialog box opens).
- **AD based configuration** – If client computers are members of an Active Directory domain, you can deploy the server addresses and trust data using a dedicated tool.
- **DNS SRV record based server discovery** – It is possible to configure the server addresses in the DNS server. Because the DNS is not secure, we recommend that you do not configure trust this way. Users can authorize the server manually in a trust dialog box that opens. This is the only server discovery method that is applicable for the MAC OS Endpoint Identity Agent.
- **Remote registry** – All client configuration, including the server addresses and trust data are in the registry. You can deploy the values before installing the client (by GPO, or any other system that lets you control the registry remotely). This lets you use the configuration from first run.
- **Custom Endpoint Identity Agents** – You can create a custom version of the Endpoint Identity Agent installation package that includes the server IP and trust data.

Comparing Options

	Requires AD	Manual User Trust Required?	Multi-Site	Client Remains Signed?	Allows Ongoing Changes	Level	Recommended for...
File name based	No	Yes	No	Yes	No	Very Simple	Single Security Gateway deployments
AD based	Yes	No	Yes	Yes	Yes	Simple	Deployments with AD that you can modify
DNS based	No	Yes	Partially (per DNS server)	Yes	Yes	Simple	Deployments without AD or with an AD you cannot modify, but the DNS can be changed
Remote registry	No	No	Yes	Yes	Yes	Moderate	Where remote registry is used for other purposes

	Requires AD	Manual User Trust Required?	Multi-Site	Client Remains Signed?	Allows Ongoing Changes	Level	Recommended for...
Pre-packaging	No	No	Yes	No	No	Advanced	When both DNS and AD cannot be changed, and there is more than one Security Gateway

File Name Based Server Discovery

This option is the easiest to deploy, and works out-of-the-box if the Captive Portal is also the Security Gateway with Identity Awareness. If your deployment consists of one Security Gateway with Identity Awareness and a Captive Portal running on the same Security Gateway and it is OK with you that the user needs to verify the server fingerprint and trust it once, you can use this option, which works with no configuration.

How does it work?

When a user downloads the Endpoint Identity Agent client from the Captive Portal, the address of the Security Gateway with Identity Awareness is embedded into the file name. During the installation sequence, the client checks if there is any other discovery method configured (prepackaged, AD based, DNS based or local registry). If no method is configured and the server can be reached, it will be used as the Security Gateway with Identity Awareness. You can make sure that this is the case by looking at the client settings and seeing that the server that is shown in the file name is present in the Endpoint Identity Agent dialog box.

Why can't we use this for trust data?

As the file name can be changed, we cannot be sure that the file name wasn't modified by an attacker along the way. Therefore, we cannot trust data passed in the file name as authentic, and we need to verify the trust data by another means.

AD Based Configuration

If your endpoint computers are members of an Active Directory domain and you have administrative access to this domain, you can use the Distributed Configuration tool to configure connectivity and trust rules.

The Distributed Configuration tool has three windows:

- **Welcome** - This window describes the tool and lets you to enter alternate credentials that are used to access the AD.
- **Server configuration** – This window lets you configure which Security Gateway with Identity Awareness the client should use, depending on its source location.
- **Trusted Gateways** – This window lets you view and change the list of fingerprints that the Security Gateways with Identity Awareness consider secure.

Server Configuration Rules

If you use the Distributed Configuration tool and you configure 'Automatically discover' the server, the client fetches the rule lists and each time it needs to connect to a server, it tries to match itself against a rule, from top to bottom.

When it matches a rule, it uses the servers shown in this rule, according to the priority specified.

Trusted Gateways

The Trusted Gateways window shows the list of servers considered trusted – no popups will open when trying to connect to them.

You can add, edit or delete a server. If you have connectivity to the server, you can get the name and fingerprint by entering its address and clicking 'Fetch Fingerprint'. Otherwise, you should enter the same name and fingerprint that is shown when connecting to that server.

The complete configuration is written in a hive named **Check Point**, under the **Program Data** branch in the AD database, added in the first run of the tool. Adding this hive will not have an effect on other AD based applications or features.

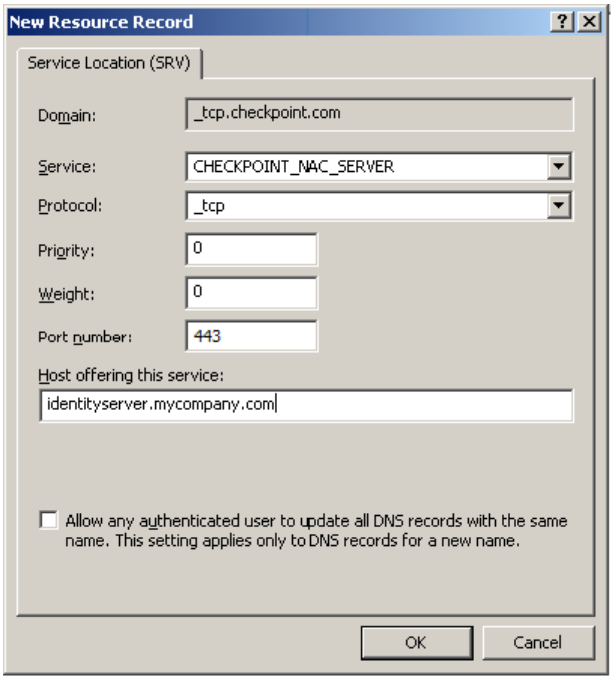
DNS Based Configuration

If you configure the client to 'Automatic Discovery' (the default), it looks for a server by issuing a DNS SRV query for the address 'CHECKPOINT_NAC_SERVER._tcp' (the DNS suffix is added automatically). You can configure the address in your DNS server.

To configure the automatic discovery address on the DNS server:

1. Go to **Start** > **All Programs** > **Administrative Tools** > **DNS**.
2. Go to **Forward lookup zones** and select the applicable domain.
3. Right click and select **Other new record**.
4. Select **Service Location** > **Create Record**.
5. In the **Service** field, enter CHECKPOINT_NAC_SERVER.
6. Set the **Port number** to `443`.
7. In the **Protocol** field, select `_tcp`.
8. In the **Host offering this service** field, enter the Security Gateway (with Identity Awareness) IP address.
9. Click **OK**.

Note - Security Gateway with Identity Awareness Load Sharing can be achieved by creating several SRV records with the same priority and High Availability can be achieved by creating several SRV records with different priorities.



Note - If you configure AD based and DNS based configuration, the results are combined according to the specified priority (from the lowest to highest).

Troubleshooting - See SRV Record Stored in the DNS Server

Run: `nslookup`

```
C:\> nslookup
> set type=srv
> checkpoint_nac_server._tcp

Server:  dns.company.com
Address:  192.168.0.17

checkpoint_nac_server._tcp.ad.company.com    SRV service location:
          priority              = 0
          weight                = 0
          port                = 443
          svr hostname   = idserver.company.com

idserver.company.com internet address = 192.168.1.212
```

Remote Registry

If you have another way to deploy registry entries to your client computers (such as Active Directory GPO updates), you can deploy the Security Gateway with Identity Awareness addresses and trust parameters before you install the clients. Clients will use the already-deployed settings immediately after installation.

To use the remote registry option:

1. Install the client on a computer. Make sure it is installed in the same mode that will be installed on the other computers.

   The *full agent* installs itself to your program files directory and saves its configuration to HKEY_LOCAL_MACHINE.

   The *light Endpoint Identity Agent* installs itself to the users directory and saves its configuration to HKEY_CURRENT_USER.

2. Connect manually to all of the servers that are configured, verify their fingerprints, and click **Trust** in the fingerprint verification window.
3. In the client **Settings** window, configure it to connect to the requested servers.

   If let the client choose a server based on location, click **Advanced** ("AD Based Configuration" on page 110).
4. Export these registry keys (from HKEY_LOCAL_MACHINE or HKEY_CURRENT_USER, according to the client type installed):

   a) SOFTWARE\CheckPoint\IA\TrustedGateways (the whole tree)

   b) SOFTWARE\CheckPoint\IA\ (32 bit) or SOFTWARE > Wow6432Node > Checkpoint > IA (64 bit)

   - DefaultGateway
   - DefaultGatewayEnabled
   - PredefinedPDPConnRBUsed
   - PredefinedPDPConnectRuleBase
5. Deploy the exported keys to the workstations before you install the client on them.

Creating Custom Endpoint Identity Agents

Custom Endpoint Identity Agents

You can use the IA Configuration Utility to create custom Endpoint Identity Agent installation packages. Endpoint Identity Agents have many advanced configuration parameters. Some of these parameters are related to the installation process, while others are related to Endpoint Identity Agent functionality. All of the configuration parameters have default values that are deployed with the product and can remain unchanged.

- **Full** – Predefined Endpoint Identity Agent includes packet tagging and computer authentication. It applies to all users of the computer that it is installed on. Administrator permissions are required to use the Full Endpoint Identity Agent type.
- **Light** – Predefined Endpoint Identity Agent that does not include packet tagging and computer authentication. You can install this Endpoint Identity Agent individually for each user on the target computer. Administrator permissions are not required.
- **Terminal Servers** - Predefined Endpoint Identity Agent that installs MAD services and the Multi-user host driver on Citrix and Terminal Servers. This Endpoint Identity Agent type cannot be used for endpoint computers.
- **Custom** - Configure custom features for all computers that use this agent, such as MAD services and packet tagging.

Installing Microsoft .NET Framework

You must install Microsoft .NET framework 4.0 or higher before you install and run the **Endpoint Identity Agent Configuration Tool**.

To install the .NET framework:

1. Download the installation package http://www.microsoft.com/en-us/download/details.aspx?id=17718.
2. When prompted to start the installation immediately, click **Run**.
3. Do the instructions on the screen.

Working with the Endpoint Identity Agent Configuration Tool

Getting the source MSI File

To create a custom Endpoint Identity Agent installation package, you must first copy the customizable MSI file from the Security Gateway to your management computer. This is the computer on which you use the Endpoint Identity Agent Configuration Tool.

To get the customizable MSI file:

1. Copy this file from the Security Gateway to your management computer:
   Gaia or Linux:
   `/opt/CPNacPortal/htdocs/nac/nacclients/customAgent.msi`
2. Make a backup copy of this file on your management computer with a different name.
   You must use the **original** copy of the MSI file when you work with the **Endpoint Identity Agent Configuration Tool**.

Running the Endpoint Identity Agent Configuration Tool

You must install Endpoint Identity Agent v2.0 (R77) or higher on your management client computer. The Configuration Tool is installed in the Endpoint Identity Agent installation directory.

To install the Endpoint Identity Agent on your client computer:

1. Copy these agents from the Security Gateway to your management computer:
   - Full Endpoint Identity Agent -
     `opt/CPNacPortal/htdocs/nac/nacclients/fullAgent.exe`
   - Light Endpoint Identity Agent -
     `opt/CPNacPortal/htdocs/nac/nacclients/lightAgent.exe`
2. Run one of these executable files as applicable for your environment.
3. Do the instructions on the screen.

To run the Endpoint Identity Agent Configuration Tool:

1. Go to the Endpoint Identity Agent installation directory.
   a) Click **Start > All Programs > Check Point > Endpoint Identity Agent**.
   b) Right click the Endpoint Identity Agent shortcut and select Properties from the menu.
   c) Click **Open File Location** (**Find Target** in some Windows versions).
2. Double-click **IAConfigTool.exe**.
   The Endpoint Identity Agent Configuration Tool opens.

Configuring the Endpoint Identity Agent

You configure all features and options in the Endp**oint Identity Agent Configuration Tool** window.

MSI Package Path

Enter or browse to the source installation package. You must use a Check Point customizable MSI file as the source for the configuration tool.

Installation Type

Select whether the Endpoint Identity Agent applies to one user or to all users of the computer on which it is installed.

- **Per-User** - Install the Light Endpoint Identity Agent only for the user who does the installation. Administrator permissions are **not** required for this installation.
- **Per Computer** - Install any Endpoint Identity Agent type for all users on the computer. Administrator permissions are required for this installation type, even for the **Light Endpoint Identity Agent** type.

Installation UI

Select one of these end user interaction options:

- **FULL** (Default) - Interactive installation where the end user sees the full installation interface and can select options.
- **BASIC** - Non-interactive installation where the end user only sees a progress bar and a **Cancel** button.

Endpoint Identity Agent Type

Select the type of Endpoint Identity Agent to install:

- **Full** – Predefined Endpoint Identity Agent includes packet tagging and computer authentication. It applies to all users of the computer that it is installed on. Administrator permissions are required to use the Full Endpoint Identity Agent type.
- **Light** – Predefined Endpoint Identity Agent that does not include packet tagging and computer authentication. You can install this Endpoint Identity Agent individually for each user on the target computer. Administrator permissions are not required. You must select the **Per-Computer installation** type for this agent type.
- **Terminal Servers** - Predefined Endpoint Identity Agent that installs MAD services and the Multi-user host driver on Citrix and Terminal Servers. This Endpoint Identity Agent type cannot be used for endpoint computers.
- **Custom** - Configure custom features for all computers that use this agent, such as MAD services and packet tagging.

Custom Features

Select these features for the Custom Endpoint Identity Agent type:

- **MAD** Service - Install MAD (Managed Asset Detection) services for Kerberos SSO and computer authentication.
- **Packet Tagging** - Install the packet tagging driver to enable anti-spoofing protection. The driver signs every packet that is sent from the computer. This setting is required if you have Firewall rules that use **Access Roles** and IP Spoofing is enabled.

Copy configuration

- **Copy configuration from this computer** - Copy Endpoint Identity Agent configuration settings from this computer to other computers running a custom MSI file.

Save

Click to save this configuration to a custom MSI file. Enter a name for the MSI file.

Deploying a Custom Endpoint Identity Agent with the Captive Portal

To deploy a custom Endpoint Identity Agent with the Captive Portal:

1. Upload the custom `customAgent.msi` to `/opt/CPNacPortal/htdocs/nacclients`.
2. Configure the Captive Portal to distribute the custom agent.
   a) In SmartConsole, go to the Security Gateway with Identity Awareness.
   b) Go to the Identity Awareness page.
   c) Click on the Browser-Based Authentication **Settings** button.
   d) Change the **Require users to download** value to **Identity Agent - Custom**.

Identity Awareness Commands

In This Section:

Introduction

These terms are used in the CLI commands:

- **PDP** - The process on the Security Gateway responsible for collecting and sharing identities.
- **PEP** - The process on the Security Gateway responsible for enforcing network access restrictions. Decisions are made according to identity data collected from the PDP.
- **AD Query** - AD Query is the module responsible for acquiring identities of entities (users or computers) from the AD (Active Directory). AD Query was called Identity Logging in previous versions and in some cases is also referenced as AD Log. The adlog is the command line process used to control and monitor the AD Query feature.

The PEP and PDP processes are key components of the system. Through them, administrators control user access and network protection.

AD Query can run either on a Security Gateway that has been enabled with Identity Awareness or on a Log Server. When it runs on a Security Gateway, AD Query serves the Identity Awareness feature, and gives logging and policy enforcement. When it runs on a Log Server, AD Query gives identity logging. The command line tool helps control users' statuses as well as troubleshoot and monitor the system.

pdp

Description These commands control and monitor the PDP process.

Syntax `# pdp [command]... <parameter>`

Parameter	Description
`<none>`	Display available options for this command and exit
`debug`	Control debug messages
`tracker`	Tracker options
`connections`	pdp connections information
`network`	pdp network information
`status`	pdp status information

Parameter	Description
`control`	pdp control commands
`monitor`	Display monitoring data
`update`	Recalculate users and computers group membership (deleted accounts will not be updated)
`ad`	Operations related to AD Query
`timers`	Show pdp timers information
`nested_groups`	Nested groups configuration
`auth`	Authentication or authorization options
`ifmap`	Monitor or control IFMAP
`vpn`	Display connected vpn gateways that send vpn client identity data
`radius`	RADIUS accounting options
`idc`	Operations related to Identity Collector
`tasks_manager`	The task manager menu

pdp monitor

Description Lets you monitor the status of connected sessions. You may perform varied queries according to the usage below to get the output you are interested in.

Syntax `# pdp monitor <parameter> <option>`

Parameter	Description
`all`	Display information for all connected sessions
`user <user name>`	Display session information for the given user name
`ip <IP address>`	Display session information for the given IP address
`machine <computer name>`	Display session information for the given computer name
`mad`	Display all sessions that relate to a managed asset (i.e. all sessions that successfully performed computer authentication)

Parameter	Description
`client_type [unknown|portal|"Identity Agent"|"AD Query"]`	Display all sessions connecting via the given client type Possible client types are: • Unknown - User was identified by an unknown source • Portal - User was identified by the Captive Portal • Identity Agent - User/computer was identified by an Identity Awareness Agent • AD Query - User was identified by AD Query
`groups <group name>`	Display all sessions of users / computers that are members of the given group name
`cv_ge <version>`	Display all sessions that are connected with a client version that is higher than (or equal to) the given version
`cv_le <version>`	Display all sessions that are connected via a client version that is lower than (or equal to) the given version.
`s_port`	Print sessions filtered by assigned source port (MUH sessions only)
`network`	Print sessions filtered by a network wild card (example: 192.168.72.*)
`user_exact`	Print sessions filtered by the exact user
`machine_exact`	Print sessions filtered by the exact machine name

Example

```
pdp monitor ip 192.0.2.1
```

Shows the connected user behind the given IP address (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 connections

Description These commands assist in monitoring and synchronizing the communication between the PDP and the PEP.

Syntax `pdp connections <argument>`

Argument	Description
`pep`	Shows the connection status of all the PEPs that should be updated by the current PDP
`ts`	Shows a list of terminal servers that are connected
`ifmap`	Shows a list of the active IFMAP sessions

pdp control

Description Provides commands to control the PDP process.

Syntax `# pdp control <parameter> <option>`

Parameter	Description
`revoke_ip <IP address>`	Log out the session that is related to the given IP.
`revoke_pt_key <session id.>`	Revoke the packet tagging key if one exists.
`sync`	Force an initiated synchronization operation between the PDPs and the PEPs. When running this command, the PDP will inform its related PEPs the up-to-date information of all connected sessions. At the end of this operation, the PDP and the PEPs will contain the same and latest session information.

pdp network

Description Shows information about network related features.

Syntax `# pdp network <parameter>`

Parameter	Description
`info`	Display a list of networks known by the PDP.
`registered`	Display the mapping of a network address to registered gateways (PEP module).

pdp debug

Description Activates and deactivates the debug logs of the PDP daemon.

Syntax `# pdp debug <parameter> <option>`

Parameter	Description
`on`	Turn on the debug logs (should be followed by the command "set" to determine the required filter).
`off`	Turn off the debug logs.
`set <topic name> [critical|surprise| important|events| all]…`	Filter the debug logs that would be written to the debug file according to the given topic and severity **Best Practice -** For debug it is recommended to run: `pdp debug set all all` Note that you can place a number of topics and severity pairs. For example: `topicA severityA topicB severityB ...`
`unset <topic name>…`	Unset a specific topic or topics.

Parameter	Description
`stat`	Show the status of the debug option.
`reset`	Reset the debug options of severity and topic. The debug is still activated after running this command.
`rotate`	Rotate the log files (increase the index of each log file) so that the current log file that will be written is the PDP log. For example, pdpd.elg becomes pdpd.elg.0 and so on.
`ccc [on|off]`	Allows enabling or disabling writing of the CCC debug logs into the PDP log file.

Important - Activating the debug logs affects the performance of the daemon. Make sure to turn off the debug after you complete troubleshooting.

pdp tracker

Description Adds the TRACKER topic to the PDP logs (on by default). This is very useful when monitoring the PDP-PEP identity sharing and other communication on distributed environments. This can be set manually by adding the TRACKER topic to the debug logs.

Syntax `# pdp tracker <parameter>`

Parameter	Description
`on`	Turns on logging of TRACKER events in the PDP log.
`off`	Turns off the logging of TRACKER events in the PDP log.

pdp status

Description Displays PDP status information such as start time or configuration time.

Syntax `# pdp status <parameter>`

Parameter	Description
`show`	Display PDP information.

pdp update

Description Initiates a recalculation of group membership for all users and computers. Note that deleted accounts will not be updated.

Syntax `# pdp update <parameter>`

Parameter	Description
`all`	Recalculate group membership for all users and computers.

pdp ad associate

Description For 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> u <username> d <domain> [m <machine>] [t <timeout>] [s]`

Parameter	Description
`ip <ip>`	IP address for the identity.
`u <username>`	Username for the identity.
`m <machine>`	Computer that is defined for the identity.
`d <domain>`	Domain of the ID server.
`t <timeout>`	Timeout setting for the AD Query (default is 5 hours).
`s`	Associates `u <username>` and `m <machine>` parameters sequentially. First the `<machine>` is added to the database and then the `<username>`.

pdp ad disassociate

Description 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> {u <username>|m <machine>} [r {probed|override|timeout}]`

Parameter	Description
`ip <ip>`	IP address for the identity
`u <username>`	Username for the identity
`m <machine>`	Computer that is defined for the identity
`t <timeout>`	Timeout setting for the AD Query (default is 5 hours)
`r {probed|override|timeout}`	Reason that is shown in the **Logs & Monitor** > **Logs** tab

pep

Description Provides commands to control and monitor the PEP process.

Syntax `# pep [command]... <parameter>`

Parameter	Description
`tracker`	Tracker options.
`show`	Display PEP information.

Parameter	Description
`debug`	Control debug messages.
`control`	Control and set PEP parameters.

pep show

Description Displays information regarding pep status.

Syntax `# pep show <parameter> <option>`

pep show user

Description Enables monitoring the status of sessions that are known to the PEP. You can perform varied queries according to the usage below to get the output you are interested in.

Syntax `# pep show user all`

Parameter	Description
`all`	Display all sessions with information summary.

Query Syntax `# pep show user query <parameter>`

Parameter	Description
`usr <username>`	Display session information for the given user name.
`mchn <computer name>`	Display session information for the given computer name.
`cid <IP>`	Display session information for the given IP.
`uid <uidString>`	Display session information for the given session ID.
`pdp <IP>`	Display all session information that was published from the given PDP IP.
`ugrp <group>`	Display all sessions of users that are members of the given user group name.
`mgrp <group>`	Display all sessions of computers that are members of the given computer group name.

Note - You can use multiple query tokens (parameters) at once to create a logical "AND" correlation between them. For example, to display all users that have a sub string of "jo" AND are part of the user group "Employees" then you can use:

```
# pep show user query usr jo ugrp Employees
```

pep show pdp

Description Enables monitoring the communication channel between the PEP and the PDP. The output displays the connect time and the number of users that were shared through the connection.

Syntax `# pep show pdp <parameter>`

Parameter	Description
`all`	List all the PDPs that are connected to the current PEP with the relevant information.
`id <IP>`	Display connection information of the given PDP IP.

pep show stat

Description Shows the last time the daemon was started and the last time a policy was received.

Important - Each time the daemon starts, it loads the policy and the two timers (Daemon start time and Policy fetched at) will be very close.

Syntax `# pep show stat`

pep show network

Description Shows network related information.

Syntax `# pep show network <parameter>`

Parameter	Description
`pdp`	Shows information about mapping between the network and PDPs.
`registration`	Shows which networks this PEP is registered to.

pep debug

Description See pdp debug (on page 120).

adlog

Description Provides commands to control and monitor the AD Query process.

When AD Query runs on a Security Gateway, AD Query serves the Identity Awareness feature that gives logging and policy-enforcement. In this case the command line is: `adlog a <argument>` (see below for options)

When it runs on a Log Server, AD Query gives identity logging. In this case, the command line is: `adlog l <argument>`. Note: the `l` in `adlog l` is a lowercase L.

Options for `adlog a` and `adlog l` are identical.

Syntax `# adlog {a|l} <command>... <argument>`

Parameter	Description
`<none>`	Display available options for this command and exit.

Parameter	Description
`{a|l}`	Set the working mode: `adlog a` - if you are using AD Query for Identity Awareness. `adlog l` - if you are using a Log Server (identity logging)
`query`	See sections below.
`debug`	
`dc`	
`statistics`	
`control`	
`control muh`	
`control srv_account`	

adlog query

Description Shows the database of identities acquired by AD Query, according to the given filter.

Usage `adlog [a|l] query <argument>`

Syntax

Parameter	Description
`ip <IP address>`	Filters identities relating to the given IP.
`string <string>`	Filters identity mappings according to the given string.
`user <user name>`	Filters identity mappings according to a specific user.
`machine <computer name>`	Filters identity mappings according to a specific computer.
`all`	No filtering, shows the entire identity database.

Example

```
adlog a query user jo
```

Shows the entry that contains the string "jo" in the user name.

adlog debug

Description Turns on/off debug flags for controlling the debug file. The debug file is located at $FWDIR/log/pdpd.elg (for Identity Awareness on a Security Gateway) or $FWDIR/log/fwd.elg (for identity logging on a log server).

Usage `adlog [a|l] debug <parameter>`

Syntax

Parameter	Description
`on`	Turn on debug.
`off`	Turn off debug.
`mode`	Show debug status (on/off).
`extended`	Turn on debug and add extended debug topics.

adlog dc

Description Shows status of connection to the AD domain controller.

Usage `adlog [a|l] dc`

Syntax None

adlog statistics

Description Displays statistics regarding NT Event Logs received by adlog, per IP and by total. It also shows the number of identified IPs.

Usage `adlog [a|l] statistics`

Syntax None

adlog control

Description Sends control commands to AD Query.

Usage `adlog {a|l} control <parameter>`

Syntax

Parameter	Description
`stop`	Stop AD Query. New identities are not acquired via AD Query.
`reconf`	Send a reconfiguration command to AD Query, which means it resets to policy configuration as was set in SmartConsole.

adlog control muh

Description Manages the list of Multi-User Hosts.

Usage `adlog {a|l} control muh <parameter>`

Syntax

Parameter	Description
`mark`	Adds an IP address as a Multi-User Host

Parameter	Description
`unmark`	Remove an IP address from the list of Multi-User Hosts
`show`	Show all known Multi-User Hosts

adlog control srv_accounts

Description Manages service accounts. Service accounts are accounts that don't belong to actual users, rather they belong to services running on a computer. They are suspected as such if they are logged in more than a certain number of times.

Usage `adlog {a|l} control srv_accounts <parameter>`

Syntax

Parameter	Description
`show`	Show all known service accounts
`find`	Manually updates the list of service accounts
`unmark`	Remove an account name from the list of service accounts
`clear`	Clears all the accounts from the list of service accounts

References

For more about Kerberos SSO, see:

- http://web.mit.edu/Kerberos/ http://web.mit.edu/Kerberos/
- http://technet.microsoft.com/en-us/library/bb742433.aspx
  http://technet.microsoft.com/en-us/library/bb742433.aspx

Appendix: Regular Expressions

In This Section:

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 07)
\cx	"control-x", where x is any character
\e	escape (hex 1B)
\f	formfeed (hex 0C)
\n	newline (hex 0A)
\r	carriage return (hex 0D)
\t	tab (hex 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)