QUANTUM

16 March 2026

IDENTITY AWARENESS CLIENTS

Administration Guide

CHECK POINT™

Check Point Copyright Notice

Important Information

Latest Software

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

Certifications

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

Check Point Identity Awareness Clients Administration Guide

For more about this release, see the home page.

Latest Version of this Document in English

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

Feedback

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

Revision History

Date	Description
18 December 2025	Updated: ■ *"Identity Collector - Requirements" on page 68*
11 December 2025	Updated: ■ *"Identity Agent for a Terminal Server" on page 45*
11 May 2025	Updated: ■ *"Identity Collector - Connecting to an Identity Awareness Gateway" on page 78* ■ *"Identity Collector - Working with a Cisco Identity Services Engine (ISE) Server" on page 89* ■ *"Identity Collector - Advanced Configuration" on page 113*
15 April 2025	Updated: ■ *"Identity Agent for a Terminal Server" on page 45* ■ *"Identity Collector - Working with Active Directory" on page 80* ■ *"Identity Agent for a User Endpoint Computer" on page 14*
07 December 2023	Updated: ■ *"Identity Collector - Working with Active Directory" on page 80*
22 August 2023	Added: ■ *"Identity Collector - Updating" on page 76* ■ *"Identity Collector - Forwarding Identities to an Event Log Collector" on page 112* ■ *"Identity Collector - Debug" on page 119* ■ *"How to increase number and size of logs in Identity Collector" on page 118* ■ *"Identity Collector" on page 65*
24 May 2023	Updated: ■ *"Introduction to Identity Awareness" on page 10* ■ *"Identity Agent for a User Endpoint Computer" on page 14*
27 April 2023	Updated: ■ *"Identity Agent for a Terminal Server" on page 45* ■ *"Identity Collector - Requirements" on page 68*

Date	Description
26 March 2023	Added: ■ *"Identity Collector - Service Account Exclusion" on page 104* Updated: ■ *"Identity Collector - Connecting to an Identity Awareness Gateway" on page 78* ■ *"Identity Agent for a Terminal Server" on page 45* ■ *"Identity Collector" on page 65*
22 January 2023	Updated: ■ *"Identity Agent for a Terminal Server" on page 45* ■ *"Identity Collector - Working with Syslog Messages" on page 92*
27 December 2022	Updated: ■ *"Identity Collector" on page 65* ■ *"Identity Collector - Requirements" on page 68*
15 December 2022	First release of this document

Table of Contents

Introduction to Identity Awareness

Firewalls traditionally monitor traffic based on IP addresses, without recognizing the user or device identities linked to those addresses. Identity Awareness enables enforcement of access control policies based on user and device identities for enhanced security.

Check Point provides a scalable solution for both Active Directory and non-Active Directory networks, supporting employees and guest users.

The solution identifies users and devices using the source and destination IP addresses of network traffic. These identities can be used in the Source and Destination fields of Access Control policy rules:

- User or user group identities
- Computer or computer group identities

Identity Awareness retrieves identities from configured identity sources. At least one Identity Source must be enabled and configured in the Identity Awareness Security Gateway object. Refer to *"Identity Sources" on page 11* for configuration details.

To start working with Identity Clients, see *"Getting Started with Identity Clients" on page 13*.

Known Limitations

- Identity Awareness does not support NAT.

Identity Sources

An Identity Awareness Gateway retrieves user and device identities from multiple sources.

Some identity sources provide information directly to the Gateway. For others, Identity Clients installed on endpoint devices or Windows servers collect identities and transmit them to the Gateway.

Note - Identity Client versions are separate and may differ from Identity Awareness Gateway versions.

To download the latest Identity Clients, see sk134312.

Identity Source	Documentation	Description
Browser-Based Authentication	See the *Identity Awareness Administration Guide* for your version.	The Identity Awareness Gateway gets identities from one of these: ■ The authentication web portal on the Identity Awareness Gateway (Captive Portal) ■ Transparent Kerberos Authentication
Active Directory Query	See the *Identity Awareness Administration Guide* for your version.	The Identity Awareness Gateway gets identities seamlessly from Microsoft Active Directory. This is a clientless identity acquisition tool (AD Query).
Identity Agents	See *"Identity Agent for a User Endpoint Computer" on page 14*	The Identity Awareness Gateway gets identities from Identity Agents that are installed on the user endpoint computers.
Terminal Servers	See *"Identity Agent for a Terminal Server" on page 45*	The Identity Awareness Gateway gets identities from Identity Agents that are installed on a Windows-based application server that hosts Terminal Servers, Citrix XenApp, and Citrix XenDesktop services. These Identity Agents identify individual users.
RADIUS Accounting	See the *Identity Awareness Administration Guide* for your version.	The Identity Awareness Gateway gets identities through RADIUS Accounting directly from a RADIUS Accounting client.

Identity Source	Documentation	Description
Identity Collector	See *"Identity Collector" on page 65*	The Identity Awareness Gateway gets identities from Identity Collectors that are installed on these: ■ Microsoft Active Directory Domain Controllers ■ Cisco Identity Services Engine (ISE) Servers ■ NetIQ eDirectory Servers ■ Syslog
Identity Web API	See the *Identity Awareness Administration Guide* for your version.	Gives you a flexible method to create identities.
Remote Access	See these: ■ *Identity Awareness Administration Guide* for your version ■ *Mobile Access Administration Guide* for your version ■ *Remote Access VPN Administration Guide* for your version	The Identity Awareness Gateway gets identities from Mobile Access clients and IPsec VPN clients configured to work in Office Mode when they connect to the Security Gateway.

Getting Started with Identity Clients

1. Install the Management Server.

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

2. Install the Security Gateway.

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

3. Install the applicable Identity Clients.

   See sk134312.

4. In SmartConsole, configure the Security Gateway:

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

   b. Open the Security Gateway object.

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

      See the *Identity Awareness Administration Guide* for your version.

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

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

      See:

      - *"Identity Agent for a User Endpoint Computer" on page 14*
      - *"Identity Agent for a Terminal Server" on page 45*
      - *"Identity Collector" on page 65*

   f. Click **OK**.

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

   See the *Identity Awareness Administration Guide* for your version.

6. In SmartConsole, install the Access Control policy.

7. In SmartConsole or SmartView, examine the logs in the **Logs & Monitor** view > on the **Logs** tab.

Identity Agent for a User Endpoint Computer

This section describes how to configure an Identity Agent (a type of Identity Client) for a user endpoint computer.

Introduction

An administrator installs these Identity Agents on user endpoint computers that acquire and report user identities to the Identity Awareness Gateway.

The administrator, not the users, configures these Identity Agents.

The Capabilities of Identity Agents

Item	Description
User identification	SSO transparently authenticates users that log in to the Active Directory domain, and then an Identity Agent identifies them as they use the Identity Agent. If you do not configure SSO, or you disable it, the Identity Agent uses username and password authentication with a standard LDAP server. The system opens a window for you to enter credentials. **Known Limitation** - RADIUS challenge-response authentication is **not** supported for Identity Agent for a user endpoint computer.
Computer identification	You get computer identification only when you use the Full Identity Agent, because it requires a service installation.
Seamless connectivity	Transparent authentication when users use Kerberos Single Sign-On (SSO), when they are logged in to the domain. Users who do not want to use SSO enter their credentials manually. You can let users keep these credentials.
Detection of IP address change	When an endpoint IP address changes (interface roaming, or DHCP assigns a new IP address), the Identity Agent automatically detects the change and reconnects.

Item	Description
Added security	You can use the patented *packet tagging* technology to prevent IP Spoofing. Packet tagging is available only for the Full Identity Agent, because it requires a driver. In addition, Identity Agent gives you strong (Kerberos-based) user and computer authentication.
Packet tagging	Packet Tagging for Anti-Spoofing is a technology that prevents IP Spoofing. **Note** - Available only for the Full Identity Agent, because it requires installation of a driver. IP Spoofing occurs when a user who is not approved assigns an IP address of an authenticated user to an endpoint computer. In this procedure, the user bypasses identity access enforcement rules. To protect packets from IP Spoofing attempts, enable **Packet Tagging**. Packet Tagging is a technology that forbids spoofed connections to go through the Identity Awareness Gateway. In packet tagging, the Identity Agent and the Identity Awareness Gateway sign packets with a shared key. **To see Packet Tagging logs in SmartConsole** 1. From the left navigation panel, click **Logs & Monitor** > **Logs**. 2. At the top, click the **Logs** tab. 3. In the **Query** field, enter: `blade:"Identity Awareness"` In addition, you can click **Queries > Predefined > Access > Identity Awareness Blade > All**. The **Successful** status indicates that a successful key exchange happened. **To enable IP Spoofing protection** 1. Make sure to install the Full Identity Agent. 2. Create an Access Role (see the *Identity Awareness Administration Guide* for your version > section *Creating Access Roles*). 3. On the **Machines** tab, select **Enforce IP spoofing protection (requires full Identity Client)**. 4. Click **OK**. 5. Install the Access Control Policy on the Identity Awareness Gateway.

Types of Identity Agents for a User Endpoint Computer

Important - For more information, see sk134312.

Type of Identity Agent	Description
Full	This is a predefined client that includes packet tagging and computer authentication. The Windows administrator installs this client one time on a computer, and it applies to all users who log on to this computer. Windows administrator permissions are required to use the Full Identity Agent. The Full Identity Agent supports: ■ IP spoofing protection ■ Computer authentication if you define computers in Access Roles in SmartConsole
Light	This is a predefined client that does **not** include packet tagging and computer authentication. The Windows administrator installs this client for each user who logs on to this computer. Windows administrator permissions are **not** required to use the Light Identity Agent.

Comparison of the Light and Full Identity Agent Types

Category	Item	Full Identity Agent	Light Identity Agent
Installation Elements	Installed component	Application, Windows Service, Windows Driver	Application only
	Required installation permissions	Administrator	None
	Required upgrade permissions	None	None
Security Features	User identification	Single Sign-On	Single Sign-On
	Computer identification	Yes	No
	Detection of an IP address change on the client computer	Yes	Yes
	Packet Tagging for Anti-Spoofing	Yes	No

Downloading Identity Agents

It is a Best Practice to download the latest Identity Agents to endpoint computers from sk134312.

File Paths for Identity Agents

Identity Agent	Path

Full Identity Agent (Multi-User Host (MUH) Identity Agent	`$FWDIR/nac/proxyis/html/_IA_MU_Agent/download/`
	Example for R81.10:
	`/opt/CPsuite-R81.10/fw1/nac/proxyis/html/_IA_MU_Agent/download/`

Light Identity Agent	`$FWDIR/nac/proxyis/html/_IAAgent/download/`
	Example for R81.10:
	`/opt/CPsuite-R81.10/fw1/nac/proxyis/html/_IAAgent/download/`

An administrator of an Identity Awareness Gateway can require end users to download an Identity Agent from the Identity Awareness Captive Portal so that they can access the Identity Awareness Gateway.

To require end users to download an Identity Agent

1. Connect with SmartConsole to the Management Server that manages the Identity Awareness Gateway.
2. From the left navigation panel, click **Gateways & Servers**.
3. Open the Identity Awareness Gateway object.
4. From the left, click the **Identity Awareness** page.
5. Enable the **Browser-Based Authentication** and click **Settings**.
6. In the section **Identity Agent Deployment from the Portal**:
    a. Select **Require users to download**.
    b. Select the required Identity Agent type.
7. Click **OK**.
8. Install the Access Control Policy on the Identity Awareness Gateway.

By default, the version of the Identity Agent that end users download from the Identity Awareness Captive Portal is current to the General Availability release date of the Identity Awareness Gateway. Identity Agent is **not** updated in Jumbo Hotfix Accumulators. An administrator can replace the default Identity Agent file on the Identity Awareness Gateway with a newer version of Identity Agent.

To replace the Identity Agent file on the Identity Awareness Gateway with a different version of Identity Agent

1. Download the new version of Identity Agent from sk134312 to your computer.
2. Transfer the downloaded Identity Agent from your computer to the Identity Awareness Gateway to some directory (for example: `/var/log`).
3. Connect to the command line of the Identity Awareness Gateway.
4. Log in to the Expert mode.
5. Go to the required directory:

   ```
   cd /opt/CPNacPortal/htdocs/nac/nacclients ; pwd
   ```

6. Back up the current Identity Agent that you need to replace:
   - To back up the Full Identity Agent for Windows OS, run:

     ```
     mv -v fullAgent.exe{,_BKP}
     ```

   - To back up the Light Identity Agent for Windows OS, run:

     ```
     mv -v lightAgent.exe{,_BKP}
     ```

   - To back up the Custom Identity Agent for Windows OS, run:

     ```
     mv -v customAgent.msi{,_BKP}
     ```

   - To back up the Identity Agent for macOS, run:

     ```
     mv -v Identity_Agent_Installer.dmg{,_BKP}
     ```

7. Move the new Identity Agent package to the required directory and give it the required name.

   Note - In our example, we uploaded the Identity Agent package to the `/var/log/` directory.

- To replace the Full Identity Agent for Windows OS, run:

```
mv -v /var/log/<File_Name>.exe
/opt/CPNacPortal/htdocs/nac/nacclients/fullAgent.exe
```

- To replace the Light Identity Agent for Windows OS, run:

```
mv -v /var/log/<File_Name>.exe
/opt/CPNacPortal/htdocs/nac/nacclients/lightAgent.exe
```

- To replace the Custom Identity Agent for Windows OS, run:

```
mv -v /var/log/<File_Name>.msi
/opt/CPNacPortal/htdocs/nac/nacclients/customAgent.msi
```

To replace the Identity Agent for macOS, run:

```
mv -v /var/log/<File_Name>.dmg
/opt/CPNacPortal/htdocs/nac/nacclients/Identity_Agent_
Installer.dmg
```

8. Assign the required ownership to the new Identity Agents package:

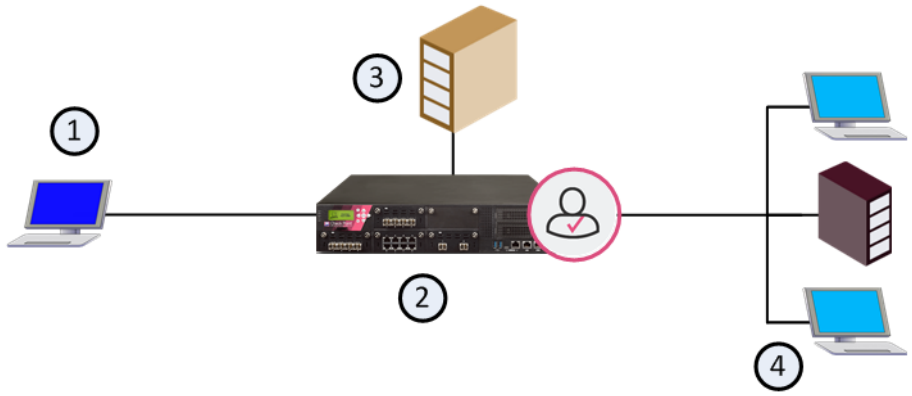
```
chown -v admin:root
/opt/CPNacPortal/htdocs/nac/nacclients/<File_Name>.<File_
Extension>
```

9. Assign the required permissions to the new Identity Agent package:

```
chmod -v 644 /opt/CPNacPortal/htdocs/nac/nacclients/<File_
Name>.<File_Extension>
```

10. Connect to the Captive Portal.
11. Make sure you can download thew new Identity Agent.

Authentication with an Identity Agent



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

High-level overview of the Identity Awareness authentication process

1. A user logs in to a computer with credentials and requests access to the Internal Data Center.
2. The Identity Agent connects to the Identity Awareness Gateway:
   - If the Identity Agent is already installed, then it connects to the Identity Awareness Gateway.
   - If the Identity Agent is not installed yet:
     a. The Identity Awareness Gateway does not recognize the user and redirects the user to the Identity Awareness Captive Portal.
     b. The user logs in to Captive Portal.
     c. The Captive Portal shows a link to download the Identity Agent (if the Identity Awareness Gateway administrator configured so).
     d. The user downloads the Identity Agent from the Captive Portal and installs it.
     e. The Identity Agent connects to the Identity Awareness Gateway.

   Note - If SSO with Kerberos is configured, the user is automatically connected.
3. The Identity Awareness Gateway authenticates the user.
4. The Identity Awareness Gateway sends the connection to its destination, based on the Access Control Policy.

Identity Agent for a User Endpoint Computer - Configuring as Identity Source

Configuring the Identity Agent Settings on the Identity Awareness Gateway

1. Connect with SmartConsole to the Security Management Server / Multi-Domain Server that manages the Identity Awareness Gateway.
2. From the left navigation panel, click **Gateways & Servers**.
3. Double-click the Identity Awareness Gateway object.
4. From the left tree, click the **Identity Awareness** page.
5. In the **Identity Sources** section, select **Identity Agents** and click **Settings**.

   The **Identity Agents Settings** window opens.
6. In the **Identity Agents Settings** window, configure the applicable settings:

   Agent Access

   In the **Agent Access** section, click **Edit**.

   The **Accessibility** window opens.

   Select to which interfaces on the Identity Awareness Gateway the Identity Agent can connect.

   Available options are based on the topology configured for the Identity Awareness Gateway interfaces:

   - **Through all interfaces**

     Identity Clients can connect to the Identity Awareness Gateway through all interfaces that an administrator configured in the Identity Awareness Gateway object (regardless of their **Topology** settings).
   - **Through internal interfaces**

     Identity Clients can connect to the Identity Awareness Gateway through internal interfaces only.

- **Including undefined internal interfaces**

  Identity Clients can connect to the Identity Awareness Gateway through all interfaces that the administrator configured in this way in the Identity Awareness Gateway object:

  a. From the left tree, click **Network Management**.

  b. Right-click an interface and click **Edit**.

  c. In the **Topology** section, click **Modify**.

  d. In the Leads To section, select **Override** > select **This Network (Internal)** > select **Not defined**.

  e. Click **OK**.

- **Including DMZ internal interfaces**

  Identity Clients can connect to the Identity Awareness Gateway through interfaces that the administrator configured in this way in the Identity Awareness Gateway object:

  a. From the left tree, click **Network Management**.

  b. Right-click an interface and click **Edit**.

  c. In the **Topology** section, click **Modify**.

  d. In the Leads To section, select **Override** > select the applicable option > select **Interface leads to DMZ**.

  e. Click **OK**.

- **Including VPN encrypted interfaces**

  Identity Clients can connect to the Identity Awareness Gateway through interfaces used for establishing route-based VPN tunnels (VTIs).

- **According to the Firewall policy**

  Select this option to control the access with Access Control rules.

Authentication Settings

In the **Authentication Settings** section, click **Settings**.

The Identity Awareness Gateway separately saves the authentication settings for different Identity Clients. This lets the administrator configure different authentication settings for different Identity Clients.

The configuration options are:

- **Authentication Method**

  This section controls how the Identity Awareness Gateway must authenticate users.

  - **Defined on user record (Legacy Authentication)**

    The Identity Awareness Gateway takes the authentication method from **Gateway Object Properties** > **Other** > **Legacy Authentication**.

  - **Username and password**

    You can configure this internally or on an LDAP server.

    To get usernames and passwords from a Terminal Server, see the *Identity Awareness Administration Guide* for your version > Chapter "Identity Awareness Use Cases" > Section "Getting Identities in a Terminal Server Environment".

    To get usernames and passwords from an LDAP server, see the *Identity Awareness Administration Guide* for your version > Chapter "Configuring Identity Sources" > Section "Configuring AD Query".

  - **RADIUS**

    The Identity Awareness Gateway gets the authentication information from a configured RADIUS server.

    Select the server from the list.

    To configure a RADIUS server, see the *Identity Awareness Administration Guide* for your version > Chapter "Configuring Identity Sources" > Section "Configuring RADIUS Accounting".

- **Users Directories**

  This section controls where the Identity Awareness Gateway searches for users when they begin to authenticate.

  All user directory options are selected by default. To improve Identity Awareness Gateway performance, select only those directories, from which the users authenticate.

  Users with the same username must log in with domain / user.

  - **Internal users**

    The directory of internal users.

  - **Users from external directories**

    - **All Gateway's Directories**

      All external directories from which the Identity Awareness Gateway pulls identities.

    - **Specific**

      Users from one or more external directories. To add an external directory, click the **+** button. In the window that opens, search for and select the external directory and click **OK**.

  - **External user profiles**

    The directory of users who have external user profiles.

Session

This section controls the Identity Agent session.

- **Agents send keepalive every X minutes**

  The interval when the Identity Client sends a keepalive signal to the Identity Awareness Gateway.

  The keepalive signal is a message to the server that the user is not logged out.

  Lower values increase the number of these keepalive packets on your network.

- **Users should re-authenticate every XYZ minutes**

  The interval when users have access to the network resources before they must to authenticate again.

  Not applicable if you use SSO.

- **Allow user to save password**

  When SSO is disabled, you can let users save the passwords they enter in the Identity Agent login window.

Agent Upgrades

This section controls how the Identity Awareness Gateway enforces the upgrade of Identity Agents.

Note -When you install or upgrade the Full Identity Agent version, the user loses connectivity for a moment.

- **Check agent upgrades for**

  You can select **All Users** or select specific user groups.

  To select specific user groups click the **+** button and select the specific group object. You can search for configured user groups.

- **Upgrade only non-compatible versions**

  The Identity Agent only checks for upgrades when its version is no longer compatible with the Identity Awareness Gateway.

- **Keep agents settings after upgrade**

  Keeps settings that users made in the Identity Agent before the upgrade.

- **Upgrade agents silently (without user intervention)**

  The Identity Agent automatically updates in the background, with no user confirmation for the upgrade.

7. Click **OK** to close the **Check Point Gateway** window.
8. Install the Access Control Policy on the Identity Awareness Gateway.

Configuring an Identity Agent Environment

It is possible to configure an Identity Agent environment in these ways:

- **From Captive Portal**

  You can tell users to download the Identity Agent from the Captive Portal. In addition, you can let users install the Identity Agent on a specified later date . During installation, the Identity Agent automatically detects if there are administrator permissions on the computer , and installs itself accordingly.

  Notes:
  - When you configure the Full Identity Agent, the user that installs the client must have administrator privileges on the computer. If the user does not have administrator privileges, the Light Identity Agent is installed instead.
  - When users authenticate with the transparent portal, the download link does not show. Users must install the agent from the distribution media.

  Procedures:

  Configuring an Identity Agent Environment from Captive Portal

  1. Connect with SmartConsole to the Security Management Server / Multi-Domain Server that manages the Identity Awareness Gateway.
  2. From the left navigation panel, click **Gateways & Servers**.
  3. Double-click the Identity Awareness Gateway object.
  4. From the left tree, click the **Identity Awareness** page.
  5. Select **Browser-Based Authentication** and click **Settings**.

     The **Portal Settings** window opens.
  6. In the **Captive Portal Settings** window, below **Identity Agent Deployment from the Portal**, select **Require users to download** to make users install the Identity Agent.

     Select a type of Identity Agent for users to install:

     - **Identity Agent - Full**
     - **Identity Agent - Custom**
     - **Identity Agent - Light**
  7. **Optional:** To give users flexibility to choose when they install the Identity Client, select **Users may defer installation until** and select the latest date before users must install the Identity Client to continue to connect to the Identity Awareness Gateway. Until the selected date, the user sees a **Skip Identity Client** installation option in the Captive Portal.

8. Click **OK** to close the Security Gateway object.
9. Install the Access Control Policy.

Configuring an Identity Agent Environment for a User Group

When necessary, you can configure specific groups of users to download the Identity Agent.

Use Case: A group of mobile users need to stay connected as they move between mobile networks.

1. Connect with SmartConsole to the Security Management Server / Multi-Domain Server that manages the Identity Awareness Gateway.
2. From the left navigation panel, click **Gateways & Servers**.
3. Double-click the Identity Awareness Gateway object.
4. From the left tree, click the **Identity Awareness** page.
5. Select **Browser-Based Authentication** and click **Settings**.

   The **Portal Settings** window opens.
6. In the **Users Access** section, select **Name and password login** and click **Settings**.

   The **Name And Password Login Settings** window opens.
7. Select **Adjust portal settings for specific user groups**.

   You can add user groups and configure the settings that are different from other users.

   Settings you configure here for a user group, override the settings you configure elsewhere in the **Portal Settings** window.

   You can configure these options for each user group:

   - If they must accept a user agreement.
   - If they must download the Identity Client and which one.
   - If they can defer the Identity Client installation and until when.
8. Click **OK** to close the Security Gateway object.
9. Install the Access Control Policy.

- **With the Identity Agent Distributed Configuration Tool**

  You can configure the Identity Agent with distribution software. You can download Identity Agent (Full Agent and Light Agent) from sk134312.

Identity Agent for a User Endpoint Computer - Downloading

There are the ways to download Identity Agents for a user endpoint computer:

It is a Best Practice to download the latest Identity Agents from sk134312.

An administrator of an Identity Awareness Gateway can force the endpoint users to download an Identity Agent from the Identity Awareness Captive Portal.

Note - To force endpoint users to download a newer version of the Identity Agent, an administrator can change the file path in the Identity Awareness Gateway to the path for the new version of the Identity Agent.

Procedure

1. Connect with SmartConsole to the Management Server that manages the Identity Awareness Gateway.
2. From the left navigation panel, click **Gateways & Servers**.
3. Double-click the Identity Awareness Gateway object.
4. From the left, click the **Identity Awareness** page.
5. Enable the **Browser-Based Authentication** and click **Settings**.
6. In the section **Identity Agent Deployment from the Portal**:
    a. Select **Require users to download**.
    b. Select the required Identity Agent type.
        - **Identity Agent - Light**
        - **Identity Agent - Full**
        - **Identity Agent - Custom**

          This is a custom configuration created in the Identity Agent Configuration Utility.

          For more information, see *"Creating Custom Identity Clients" on page 147*
7. Click **OK** to close the Security Gateway object.
8. Install the Access Control Policy on the Identity Awareness Gateway.

The version of the Identity Agent that end users download from the Identity Awareness Captive Portal is current to the General Availability release date of the Identity Awareness Gateway.

This version is **not** updated.

To update the version of Identity Agent that end users download

1. Download the new version of Identity Agent from sk134312 to your computer.
2. Copy the downloaded Identity Agent from your computer to the Identity Awareness Gateway to this directory:

   ```
   /opt/CPNacPortal/htdocs/nac/nacclients
   ```

3. Connect to the command line of the Identity Awareness Gateway.
4. Log in to the Expert mode.
5. To make sure the file has permissions configured to allow end users to download it, run:

   ```
   chmod -v 644
   /opt/CPNacPortal/htdocs/nac/nacclients/<Identity Agent
   Package>
   ```

6. Make sure that users are required to download the same type of Identity Agent that you downloaded to the Security Gateway.

   For example, if you downloaded the Full Identity Agent package, then:

   a. Connect with SmartConsole to the Security Management Server / Domain Management Server that manages the Identity Awareness Gateway.

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

   c. Double-click the Identity Awareness Gateway object.

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

   e. Select **Browser-Based Authentication** and click **Settings**.

      The **Portal Settings** window opens.

f. In the **Captive Portal Settings** window, below **Identity Agent Deployment from the Portal**, select **Require users to download** to make users install the Identity Agent.

   Make sure the selected a type of Identity Agent matches the type of Identity Agent you downloaded to the Security Gateway:

   - **Identity Agent - Full**
   - **Identity Agent - Custom**
   - **Identity Agent - Light**

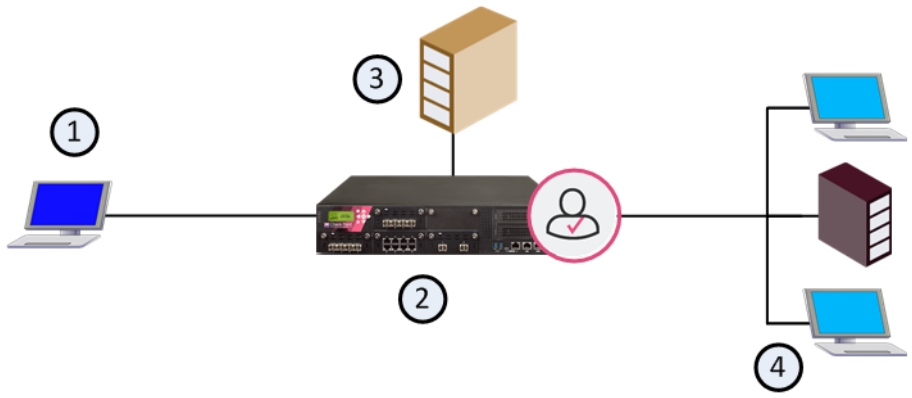
g. **Optional:** To give users flexibility to choose when they install the Identity Client, select **Users may defer installation until** and select the latest date before users must install the Identity Client to continue to connect to the Identity Awareness Gateway. Until the selected date, the user sees a **Skip Identity Client** installation option in the Captive Portal.

h. If you selected a new kind of Identity Agent or made changes to **Users may defer installation until**:

   i. Click **OK** to close the Security Gateway object.

   ii. Install the Access Control Policy.

Authentication with an Identity Agent



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

High-level overview of the Identity Awareness authentication process

1. A user logs in to a computer with credentials and requests access to the Internal Data Center.
2. The Identity Agent connects to the Identity Awareness Gateway:
   - If the Identity Agent is already installed, then it connects to the Identity Awareness Gateway.
   - If the Identity Agent is not installed yet:
     a. The Identity Awareness Gateway does not recognize the user and redirects the user to the Identity Awareness Captive Portal.
     b. The user logs in to Captive Portal.
     c. The Captive Portal shows a link to download the Identity Agent (if the Identity Awareness Gateway administrator configured so).
     d. The user downloads the Identity Agent from the Captive Portal and installs it.
     e. The Identity Agent connects to the Identity Awareness Gateway.

   Note - If SSO with Kerberos is configured, the user is connected automatically.
3. The Identity Awareness Gateway authenticates the user.
4. The Identity Awareness Gateway sends the connection to its destination, based on the Access Control Policy.

Identity Agent for a User Endpoint Computer - Server Discovery and Server Trust

To connect to an Identity Awareness Gateway, the Identity Agent must *discover* it and *trust* it.

The *discovery* is the process the Identity Agent uses when it decides to connect to an Identity Awareness Gateway (server).

Server *trust* is the process the Identity Agent uses to validate that the end user connects to a genuine server. In addition, it makes sure that the connection between the client and the server is not breached 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, the trust process asks the user to verify the fingerprint manually. This section describes how the trust process can recognize the fingerprint without user intervention.

Discovery and Trust Options

These are the configuration options for the client to discover and trust a server:

Discovery and Trust Method	Description
Based on Identity Agent File Name	If no other method is configured (out of the box situation), the Identity Agent downloaded from the Captive Portal is renamed to include the Captive Portal computer IP address in its name. During installation, the Identity Agent uses this IP address for the Identity Awareness Gateway. Users manually accept the server in the **Trust** window.
Based on Active Directory Membership	If the Identity Agent computers are members of an Active Directory domain, configure the server IP addresses and trust data with the Identity Agent Distributed Configuration Tool (installed as a part of the Identity Agent).
Based on DNS SRV record	Configure the Identity Awareness Gateway's addresses on the DNS server. Users manually accept the server in the **Trust** window. **Note** - This is the only server discovery method for the macOS Identity Agent.
Based on Remote Registry	All client configurations, including Identity Server IP addresses and trust data, are in the Windows OS Registry. Configure these values before installing the client (by GPO, or other method that lets you remotely control the Windows registry). The Identity Agent uses the data immediately.
Prepackaging Custom Identity Agents (see *"Creating Custom Identity Clients" on page 147*)	Create a custom version of the Identity Agent installation that comes with the Identity Awareness Gateway.

General Overview

Server Discovery	Must Have AD	Manual User Trust Necessary?	Multi-Site	Client Remains Signed?	Allows Ongoing Changes	Level	Recommended for...
Based on Identity Agent File Name	No	Yes	No	Yes	No	Very Simple	Environment with single Security Gateway
Based on Active Directory Membership	Yes	No	Yes	Yes	Yes	Simple	Environment where you can change AD settings
Based on DNS SRV record	No	Yes	Partially (per DNS server)	Yes	Yes	Simple	Environment with AD where you cannot change AD settings (or without AD), but can change the DNS settings
Based on Remote Registry	No	No	Yes	Yes	Yes	Moderate	Environment where remote registry is used for other purposes

Server Discovery	Must Have AD	Manual User Trust Necessary?	Multi-Site	Client Remains Signed?	Allows Ongoing Changes	Level	Recommended for...
Pre-packaging	No	No	Yes	No	No	Advanced	Environment where you cannot change AD and DNS settings, with more than one Security Gateway

Server Discovery Based on an Identity Agent File Name

This option is the easiest to configure, and works by default if Captive Portal is configured in addition the Identity Awareness Gateway. This configuration is suitable for an environment that meets these criteria:

- There is one Identity Awareness Gateway.
- Captive Portal and Identity Awareness run on the same Security Gateway
- It is acceptable for new users to verify the server fingerprint once to establish trust.

How does it work?

When a user downloads the Identity Agent client from the Captive Portal, the address of the Identity Awareness Gateway is added to the file name. During the installation sequence, the client checks if there is any other discovery method configured (Pre-packaged, AD-based, DNS-based or local registry). If no discovery method is configured, the Identity Agent connects to the Identity Awareness Gateway.

Why cannot we use this for data trust?

As the file name can be changed, we cannot be sure that the file name was not 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.

Server Discovery Based on Active Directory Membership

If endpoint computers are members of an Active Directory domain, and you have administrative access to this domain, you can use the Identity Agent Distributed Configuration Tool to configure connectivity and trust rules for Identity Agent. This tool is installed a part of the Identity Agent.

Notes:

- You must have administrative access to this Active Directory domain to allow automatic creation of new LDAP keys and writing information into these keys.
- The credentials are not saved anywhere. The access is only necessary to modify the distributed configuration. The Identity Agent Distributed Configuration Tool only writes to this Active Directory domain when it saves configuration.
- All users are allowed to view the configuration (without this permission, the Identity Agents cannot fetch it).
- The LDAP keys are:

```
LDAP://CN=PDP,CN=Check Point,CN=Program Data,DC=...<
Domain Name>...
LDAP://CN=PDPconnRB,CN=Check Point,CN=Program
Data,DC=...< Domain Name>...
```

The Identity Agent Distributed Configuration Tool has three panes:

- **Welcome**

  This pane describes the tool and lets you enter alternate credentials that you use to get an access to the AD.

- **Server Configuration**

  This pane lets you configure, to which Identity Awareness Gateway the Identity Agent should connect, depending on the IPv4 / IPv6 address that is configured on the endpoint computer, or its AD Site.

- **Trusted Gateways**

  This pane lets you view and change the list of fingerprints of Identity Awareness Gateways, which the Identity Agent considers secure.

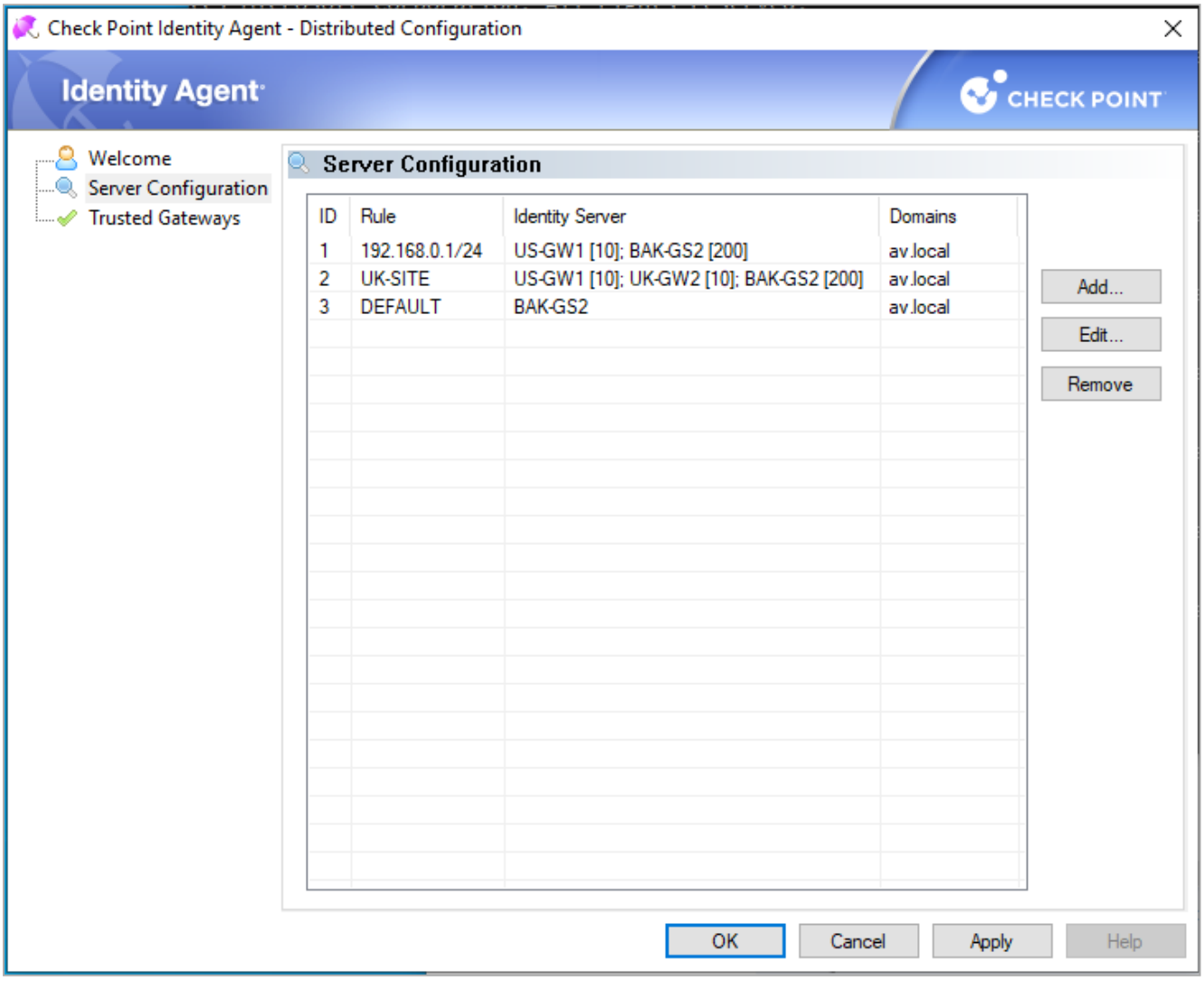
Note - The complete configuration is in the Active Directory database, under the **Program Data** branch in a hive named Check Point. The first run of the tool adds this hive. This hive has no effect on other AD-based applications or features.

Server Configuration Rules

The Identity Agent fetches the configured rule lists from the Active Directory database. When the Identity Agent connects to an Identity Awareness Gateway, it matches against the rules, from top to bottom.

When the Identity Agent matches a rule, it uses the Identity Awareness Gateways configured in this rule based on the specified priority.

For example:



This configuration means:

- If the user's computer is configured with the IPv4 address `192.168.0.1 / 24`, then the Identity Agent needs to connect to the Identity Awareness Gateway "`US-GW1`".

  If the gateway "`US-GW1`" is not available, then the Identity Agent needs to connect to the Identity Awareness Gateway "`BAK-GS2`" (applies only if gateway "`US-GW1`" is not available, because its priority is higher).

- If the user connects from the Active Directory site "UK-SITE", then the Identity Agent needs to connect to Identity Awareness Gateway "US-GW1", or to Identity Awareness Gateway "UK-GW2". The Identity Agent selects between these gateways randomly, because they both have the same priority).

  If both of these gateways are not available, then the Identity Agent needs to connect to the Identity Awareness Gateway "BAK-GS2".

- The default rule is that the Identity Agent needs to connect to Identity Awareness Gateway "BAK-GS2" (the default rule is always matched when it is encountered).

Trusted Gateways

The Trusted Gateways pane shows the list of Identity Awareness Security Gateways considered trusted. When the Identity Agent starts to connect to these Identity Awareness Security Gateways, no pop-up windows open.

You can add, edit or delete a server. If you get a connection to the Identity Awareness Security Gateway, enter its address and click **Fetch Fingerprint** to get the name and fingerprint. If not, enter the same name and fingerprint that appear when you connect to this Identity Awareness Security Gateway.

Server Discovery Based on a DNS SRV Record

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 the DNS server.

On the DNS server (Example is for Windows 2003. For more information, see official Microsoft documentation):

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

Notes

- To create a specified Identity Awareness Load Sharing, make some SRV records with the same priority. To create a specified Identity Awareness High Availability, make some SRV records with different priorities.
- If you configure AD based and DNS based configuration, the results are combined based on the specified priority (from the lowest to highest).

Troubleshooting - Viewing the SRV Record Stored in the DNS Server

1. In Windows Command Prompt, run:

   ```
   nslookup
   ```

2. Set query type to *SERVER*:

   ```
   set type=SRV
   ```

3. Query for the *checkpoint_nac_server*:

   ```
   checkpoint_nac_server._tcp
   ```

   Example output:

   ```
   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
   ```

4. Exit:

   ```
   exit
   ```

Server Discovery Based on Remote Registry

If you have another way to configure registry entries to your client computers (such as Active Directory GPO updates), you can configure the Identity Awareness Gateway addresses and trust parameters before you install the clients. Clients use the new 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 in all computers.

   The *Full Identity Agent* installs itself to your `Program Files` directory and saves its configuration to `HKEY_LOCAL_MACHINE`.

   The *lLght 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 you let the client select a server in dependence to location, click **Advanced** (see *"Server Discovery Based on Active Directory Membership" on page 38*).

4. Export these registry keys (from `HKEY_LOCAL_MACHINE` or `HKEY_CURRENT_USER`, based on the client type installed):

a. The whole tree:

`SOFTWARE\CheckPoint\IA\TrustedGateway`.

b. The "IA" branch:

- 64-bit:

  `SOFTWARE\Wow6432Node\Checkpoint\IA`

- 32-bit:

  `SOFTWARE\CheckPoint\IA\`

Parameters:

- `Default Gateway`
- `DefaultGatewayEnabled`
- `PredefinedPDPConnRBUsed`
- `PredefinedPDPConnectRuleBase`

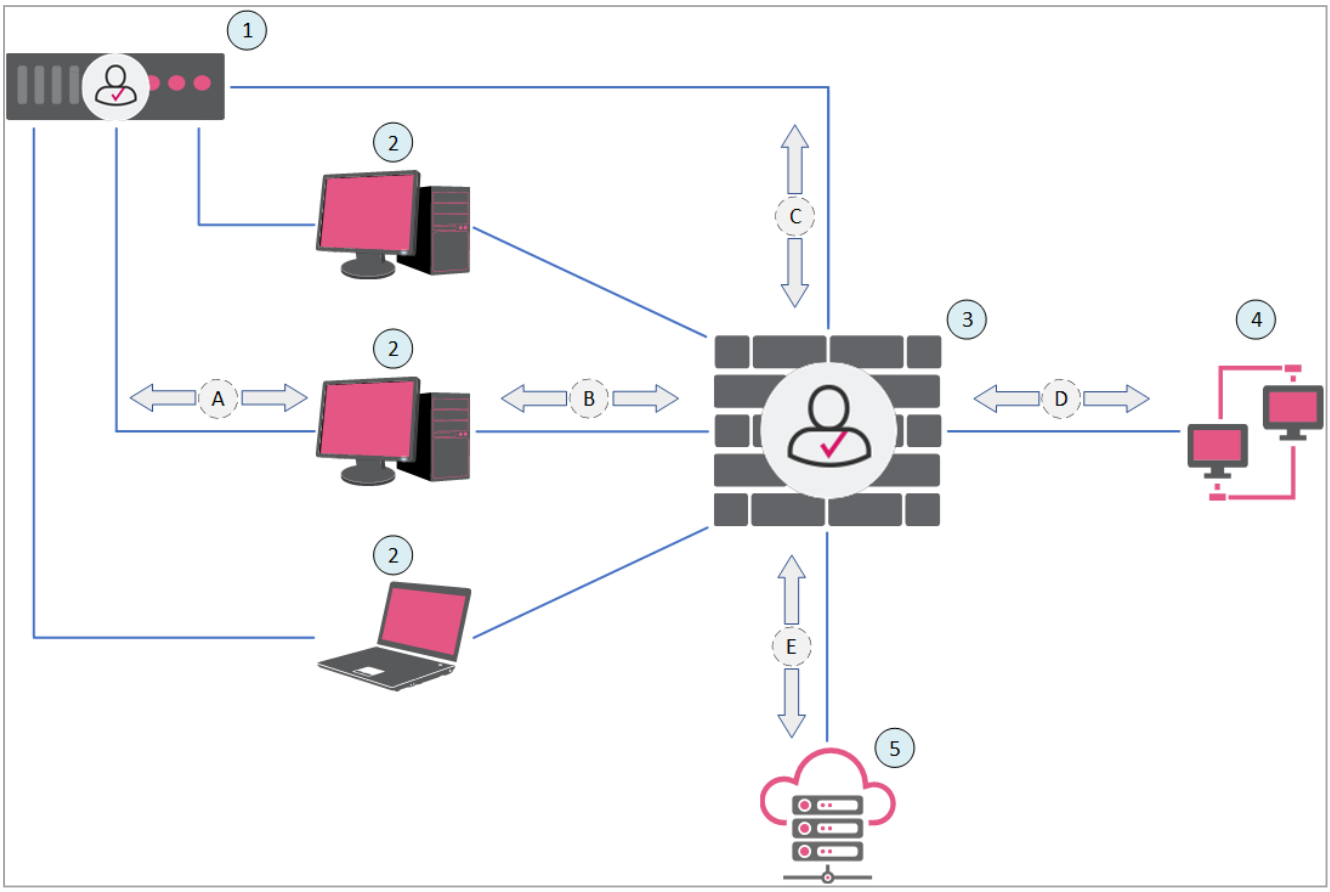
5. Configure the exported keys on the workstations before you install the client on them.

Identity Agent for a Terminal Server

This section is an introduction to Identity Agent (a type of Identity Client) for a Microsoft Terminal Server (also known as Multi-User Host (MUH).

Identity Agent for a Terminal Server can identify user accounts that belong to an Active Directory domain, including service accounts. Identity Agent for a Terminal Server communicates with the Identity Awareness Gateway over SSL (by default, port 443).

Example Topology and Traffic Flow:



Item	Description
1	Windows Server with Identity Agent for a Terminal Server installed
2	User endpoint computers
3	Identity Awareness Gateway
4	Internal resources
5	Security Management Server
A	Endpoint users authenticate on the Windows Server (1)
B	Endpoint user computers (2) communicate with the Identity Awareness Gateway (3)
C	Identity Agent for a Terminal Server on the Windows Server sends user and machine identities to the Identity Awareness Gateway (3)
D	Identity Awareness Gateway (3) grants or denies users access to internal resources according to the Access Control Policy

Item	Description
E	Security Management Server (5) manages the Identity Awareness Gateway (3)

Comparing Versions of Identity Agent for a Terminal Server

There are different versions of Identity Agent for Terminal Servers:

- Terminal Server Identity Agent Version 1 (MUH v1) - Based on source ports. Supports older versions of Windows Server that MUH v2 does not support.
- Terminal Server Identity Agent Version 2 (MUH v2) - Based on packet tagging. Supports more simultaneous users and more features than MUH v1. MUH v2 is a new installation, and is **not** an upgrade for MUH v1.

Aspect	Terminal Server Identity Agent Version 1 (MUH v1)	Terminal Server Identity Agent Version 2 (MUH v2)
How it Works	Based on source ports. Workflow: 1. MUH v1 installs a TDI driver on the Terminal Server that intercepts all requests from any process that requests a new connection. 2. When a request reaches the TDI driver, the TDI driver: a. Sends a query to the Terminal Server to fetch the requesting user behind this new connection b. Selects a source port from a pool of port ranges that MUH v1 allocates for this specific use 3. MUH v1 communicates to the Identity Awareness Gateway how it controls the connections for each user. 4. The Identity Awareness Gateway distinguishes between the different connection owners. Two different users have two different port range pools.	Based on packet tagging. Workflow: 1. MUH v2 installs a WFP driver on the Terminal Server that intercepts all traffic originated by a user. 2. When a request reaches the WFP driver, the WFP driver tags the packet from a pool of ID ranges that MUH v2 allocates this specific user. 3. MUH v2 communicates to the Identity Awareness Gateway how it tags the packets for each user. 4. The Identity Awareness Gateway distinguishes between the different packets. Two different users have two different packet tag pools.
Available Check Point Versions	R77 and higher.	▪ Check Point R80.40 and higher. ▪ R80.30 Jumbo Hotfix Accumulator starting from Take 210 (on the Security Gateway and the Management Server / Multi-Domain Server).

Aspect	Terminal Server Identity Agent Version 1 (MUH v1)	Terminal Server Identity Agent Version 2 (MUH v2)
Supported Windows Server Versions (32-bit and 64-bit)	■ Windows Server 2022 ■ Windows Server 2019 ■ Windows Server 2016 ■ Windows Server 2012 R2 ■ Windows Server 2012 ■ Windows Server 2008 R2	■ Windows Server 2025 ■ Windows Server 2022 ■ Windows Server 2019 ■ Windows Server 2016 ■ Windows 10 Enterprise multi-session (see sk177024) ■ Windows 10 ■ Windows 11 Enterprise multi-session (see sk177024)
Supported Windows Desktop Operating System Versions	■ Windows 8 ■ Windows 7 ■ Windows Vista	■ Windows 10 Enterprise multi-session (see sk177024) ■ Windows 10 ■ Windows 11 Enterprise multi-session (see sk177024)
Supported Number of Simultaneous Users	Supports a maximum of 20 simultaneous users per MUH v1 instance.	Supports a maximum of 256 simultaneous users per MUH v2 instance.
Support for Windows Secure Boot (Windows security feature)	Does **not** support Windows Secure Boot.	Supports Windows Secure Boot.
SYSTEM and other local user accounts	Assigns source ports in a special port range to processes that run in SYSTEM and other local user account. Ports in this special range are not assigned to any user identity authentication.	Does not identity and does not assign an ID range to SYSTEM and other local user accounts. To enforce machine identities for these users, use Kerberos SSO authentication.

Best Practice - If you decide to use AD Query for end user computers, exclude the IP addresses of the Terminal Servers from AD Query. This prevents unexpected disconnections of agents and high CPU utilization by the PDP daemon. See sk86560 for instructions.

Known Limitations

- IPv6 is not supported for Terminal Server Identity Agent (Version 1 or Version 2).
- Terminal Server Identity Agent Version 2 (MUH v2) supports only TCP and UDP protocols.
- Terminal ServerIdentity Agent (Version 1 and Version 2) does not support other protocols such as ICMP. For unsupported protocols, such as ICMP, the Terminal Server Identity Agent cannot control the network connections. The Identity Server is not aware of the user that initiates these connections.
- A Policy Decision Point (PDP) Security Gateway can support a maximum of 1000 MUH v2 agents connected to it directly. Check Point QA certified this with 20 users per MUH v2 client.
- Upgrade from Terminal Server Identity Agent Version 1 (MUH v1) to Terminal Server Identity Agent Version 2 (MUH v2) is not supported.
- Terminal Server Identity Agent Version 1 (MUH v1) does not support applications that do port tunneling on the Terminal Server.
- When Terminal Server Identity Agent Version 2 (MUH v2) is configured, it is not supported for an application to make decisions based on user context (example: Windows Firewall). This is because when MUH v2 tags traffic, it changes the user context to SYSTEM context.
- Terminal ServerIdentity Agent (Version 1 and Version 2) ignores traffic generated by a Windows system user. To allow users to browse to a network drive from Terminal ServerIdentity Agent, do one of these workarounds in the Access Control Policy for the Security Gateway:

  - Add a regular IP address / network based rule to accept this traffic between the Terminal Server/Citrix and Security Gateway.
  - Add an access role based on Machine Identity of Terminal Server/Citrix (if you have this identity).

  For more information, see the *Quantum Security Management Administration Guide* for your version.
- Terminal Server Identity Agent (Version 1 and Version 2) is not supported on a Terminal/Citrix server that runs proxy software that tunnels network activity through its own process, such as TrendMicro Proxy Service Controller.

Identity Agent for a Terminal Server - Installing

To download Identity Agent for a Terminal Server Version 1 (MUH v1) or Identity Agent for a Terminal Server Version 2 (MUH v2), see sk134312.

Installation of Identity Agent for a Terminal Server requires administrative privileges on the Terminal Server.

No installation is required on the endpoint clients that connect to the Terminal Server.

You can use a terminal session to install Identity Agent for a Terminal Server.

Identity Agent for a Terminal Server - Configuring as Identity Source

Configuring an Identity Agent for a Terminal Server

1. Install an Identity Agent for Terminal Servers.

   Steps

   Install this agent on the application server that hosts the Terminal/Citrix services after you enable the **Terminal Servers** identity source in the Identity Awareness Gateway object and install the Access Control Policy.

   Note - To install an Identity Agent for a Terminal Server, you must have administrator privileges for the Terminal Server.
   After the agent is installed, non-admin users can access the Controller of the agent, but only in read-only mode.

   a. Download the Terminal Server Identity Agent from sk134312.

      Important - Terminal Server Identity Agent Version 2 (Multi-User Host (MUH) v2) is a new installation. It is **not** an upgrade.

      To uninstall Terminal Server Identity Agent Version 1 and install Terminal Server Identity Agent Version 2 (MUH v2):
      i. Uninstall Terminal Server Identity Agent (Version 1).
      ii. Reboot your computer.
      iii. Enter the new preshared key for the new Terminal Server Identity Agent (Version 2).
      iv. Reboot your computer.

   b. Make sure you open the link from a location defined in the **Accessibility** section:

      Identity Awareness Gateway object properties > **Identity Awareness** page > near **Terminal Servers**, click **Settings** > in the **Accessibility** section, click **Edit**.

2. Configure the Shared Secret.

   Steps

   You must configure the same password as a shared secret in the Terminal Servers Identity Agent in these places:

   - The application server that hosts the Terminal/Citrix services
   - The Identity Awareness Gateway

The shared secret enables secure connection, so that the Identity Awareness Gateway trusts the application server with the Terminal Servers functionality.

The shared secret must be eight characters long and contain each of these:

- at least one digit
- at least one lowercase character
- at least one uppercase character
- no more than three consecutive digits

In SmartConsole, you can automatically generate a shared secret that matches these conditions.

On the Identity Awareness Gateway

a. Connect with SmartConsole to the Management Server that manages this Identity Awareness Gateway.

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

c. Double-click the Identity Awareness Gateway object.

d. In the left tree, click the **Identity Awareness** page.

e. Select **Terminal Servers** and click **Settings**.

   The **Terminal Servers** window opens.

f. Configure the shared secret automatically or manually.

   - To configure the shared secret automatically:

     Click **Generate** to get a shared secret automatically that matches the string conditions.

     The generated password appears in the **Pre-shared secret** file.

   - To configure the shared secret manually:

     Enter a password that matches the conditions in the **Pre-shared secret** field.

     Note the strength of the password in the Indicator.

On the Terminal Server

a. Open the Identity Agent.

b. In the **Overview** section, click **Multi User Host Settings**.

c. In **Identity Server Shared Secret**, enter the shared secret string.

d. Click **Save**.

3. Configure Identity Agent Accessibility in the Identity Awareness Gateway object.

Steps

a. The **Terminal Servers** window is still open.

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

The **Accessibility** window opens.

Select to which interfaces on the Identity Awareness Gateway the Identity Agent can connect.

Available options are based on the topology configured for the Identity Awareness Gateway interfaces:

Available options are based on the topology configured for the Identity Awareness Gateway interfaces:

- **Through all interfaces**

  Identity Clients can connect to the Identity Awareness Gateway through all interfaces that an administrator configured in the Identity Awareness Gateway object (regardless of their **Topology** settings).

- **Through internal interfaces**

  Identity Clients can connect to the Identity Awareness Gateway through internal interfaces only.

  - **Including undefined internal interfaces**

    Identity Clients can connect to the Identity Awareness Gateway through all interfaces that the administrator configured in this way in the Identity Awareness Gateway object:

    i. From the left tree, click **Network Management**.

    ii. Right-click an interface and click **Edit**.

    iii. In the **Topology** section, click **Modify**.

    iv. In the Leads To section, select **Override** > select **This Network (Internal)** > select **Not defined**.

    v. Click **OK**.

- **Including DMZ internal interfaces**

  Identity Clients can connect to the Identity Awareness Gateway through interfaces that the administrator configured in this way in the Identity Awareness Gateway object:

  i. From the left tree, click **Network Management**.

  ii. Right-click an interface and click **Edit**.

  iii. In the **Topology** section, click **Modify**.

  iv. In the Leads To section, select **Override** > select the applicable option > select **Interface leads to DMZ**.

  v. Click **OK**.

- **Including VPN encrypted interfaces**

  Identity Clients can connect to the Identity Awareness Gateway through interfaces used for establishing route-based VPN tunnels (VTIs).

- **According to the Firewall policy**

  Select this option to control the access with Access Control rules.

c. Click **OK** to close the **Accessibility** window.

4. Configure Identity Agent Authentication Settings.

Steps

The Identity Awareness Gateway separately saves the authentication settings for different Identity Clients. This lets the administrator configure different authentication settings for different Identity Clients.

a. In the **Terminal Servers** window > **Authentication Settings** section, click **Edit**.

The **User Directories** window opens.

b. Select the applicable option.

Note - Terminal Server Identity Agent (MUH) works only with Microsoft Active Directory as a user-directory server.

To work with all Active Directory servers

i. Select **All Gateway's Active Directories (Security Gateway > Other > User Directory)**.

ii. Click **OK** to close the **User Directories** window.

iii. Click **OK** to close the **Terminal Servers** window.

iv. Click **OK** to close the **Check Point Gateway** window.

v. Configure the Account Units Query settings:

i. In the left tree of the Security Gateway object, click the **[+]** icon near the **Other** pane.

ii. Click the User Directory pane.

iii. In the **Account Units Query** section, select **All**.

vi. Configure the Account Units Query settings in the Identity Awareness Gateway object:

i. In the left tree, expand **Other**.

ii. Click the **User Directory** page.

iii. In the **User Directories** section, select **All**.

To work with a specific Active Directory server

i. Select **Specific**.

ii. Click the green **[+]** icon > select the applicable existing **LDAP Account Unit** object.

iii. Click **OK** to close the **User Directories** window.

iv. Click **OK** to close the **Terminal Servers** window.

v. Configure the Account Units Query settings in the Identity Awareness Gateway object:

i. In the left tree, expand **Other**.

ii. Click the **User Directory** page.

iii. In the **User Directories** section, select **Selected User Directories list**.

iv. Click **Add**.

v. Select the same LDAP Account Unit object that you selected earlier the **Terminal Servers** > **User Directories** window.

5. Click **OK** to close the **Check Point Gateway** window.
6. Install the Access Control Policy on the Identity Awareness Gateway.

Best Practice - After you finish the configuration procedure, it is highly recommended to reboot the Terminal Server. After you finish installation, Identity Agent for a Terminal Server identifies and enforces policy for all new connections. When you reboot the Terminal Server, you terminate all connections that started before Identity Agent for a Terminal Server was installed. After the reboot, Identity Agent for a Terminal Server identifies and enforces policy for all connections.

Identity Agent for a Terminal Server - User Interface

The "Advanced" Page

In the Identity Agent main window, click the **Advanced** page > in the **Troubleshooting** section, click **Change settings**.

Advanced uses can change these settings when necessary.

Best Practice - If you are not an advanced user, we recommend to keep the default values.

Changes are applied to new users that log in to the application server after the Identity Agent saves the settings. Users that are logged in keep their current settings.

For Identity Agent Version 1 (MUH v1)

Advanced Setting	Description
Excluded TCP Ports	Ports included in this range do not get 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 do not get 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	The number of errors to keep in the history.

For Identity Agent Version 1 (MUH v1)and Identity Agent Version 2 (MUH v2):

Advanced Setting	Description
Gateway Shared Secret	This field is available only in Identity Agent Version 2 (MUH2). The same password that is set on the Identity Awareness Gateway enables trusted connection between the Identity Awareness Gateway and the application server.

Important - Identity Agent Version 2 (MUH2) is supported in:

- R80.40 and higher.
- R80.30 Jumbo Hotfix Accumulator Take 210 and higher.

The "Users" Page

The **Users** page in the main window shows a table with information about all users that are actively connected to the application server that hosts the Terminal/Citrix services.

For Identity Agent Version 1 (MUH v1):

The **ID** and **User** field information is automatically updated from processes running on the application server.

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 UDP traffic.
Authentication Status	Indicates whether this user is authenticated on the Identity Awareness Gateway.

The Identity Agent assigns TCP and UDP ports ranges for each connected user.

For Identity Agent Version (MUH v2):

The **ID** and **User** field information is automatically updated from the login and logout events.

Table Field	Description
ID	The SID of the user.
User	The user and domain name. The format used: `<domain>\<user>`
ID Range	The ID's allocated to the users.
Authentication Status	Indicates whether this user is authenticated on the Identity Awareness Gateway.

The Identity Agent dynamically assigns an ID to connected each user from the range of IDs.

Important - Supported in:

- R80.40 and higher.
- R80.30 Jumbo Hotfix Accumulator Take 210 and higher.

Identity Agent for a Terminal Server - Login Tracking

A computer with Identity Agent (MUH Agent) installed tracks user logins during a one-hour period. You can change this timeout period.

Note - The interval configured in this procedure applies to the Identity Collector Service Account Exclusion feature on Identity Awareness Gateways that support this feature. Starting from R80.40, you can configure Service Account Exclusion on an Identity Awareness Gateway. For more information, see *"Identity Collector - Service Account Exclusion" on page 104*.

To change the detection interval for Identity Agent (MUH) Login Tracking

1. Connect to the command line on the Identity Awareness Gateway/ each Cluster Member.
2. Log in to the Expert mode.
3. Back up the current `$FWDIR/conf/pdp_overriding_attrs.C` file, if it exists:

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

4. Edit the current `$FWDIR/conf/pdp_overriding_attrs.C` file:

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

5. Configure the applicable value for the `idc_muh_interval` attribute:

   ```
   (
       :idc_muh_serviceaccount_interval (<NUMBER OF SECONDS>)
   )
   ```

   The default value is `3600` seconds.

   The acceptable values are from `1` to `86400` seconds.

6. Save the changes in the file and exit the editor.
7. In SmartConsole, install the Access Control Policy on the Identity Awareness Gateway/ Cluster.

Identity Agent for a Terminal Server - Monitoring

Identity Agent for a Terminal Server sends monitoring information to the Identity Awareness Gateway.

Monitoring information includes:

- IP address
- Terminal Server version
- Next keep-alive message
- Number of connected users
- Number of assigned port ranges (Identity Agent for a Terminal Server Version 1 (MUH v1)

Monitoring is **disabled** by default. After you enable monitoring, by default Identity Agent sends logs at an interval of `15` seconds.

To enable monitoring of Identity Agent for a Terminal Server:

1. In the Registry Editor, go to the relevant Check Point key:
   - Location of the registry key on 64-bit Terminal Servers:

     ```
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\CheckPoint\IA\
     ```

   - Location of the registry key on 32-bit Terminal Servers:

     ```
     HKEY_LOCAL_MACHINE\SOFTWARE\CheckPoint\IA\
     ```

2. If the key `MUHMonitoringEnabled` does not exist, create it as DWORD.
3. To enable the monitoring, configure the value `1` (one).

   To disable the monitoring later, configure the value `0` (zero).
4. Close the Registry Editor.
5. Do **one** of these:
   - Reboot the Terminal Server.
   - Restart the Check Point Managed Asset Detection service.

To view logs on the Identity Awareness Gateway:

- Use SNMP

  The file `$FWDIR/conf/identity_server.cps` file contains the applicable SNMP Object Identifiers (OIDs).

- Use these CLI commands:

  - The `cpstat` command:

    ```
    cpstat identityServer -f muh
    ```

  - The `pdp` command (available from R80.30):

    ```
    pdp muh status
    ```

Identity Agent for a Terminal Server - Active Directory Cross-Forest Trust

Terminal Server Identity Agent (MUH) supports Microsoft Active Directory cross-forest trust.

This lets you associate users from foreign domains, if these users are members of groups in the local domain.

This feature is enabled by default.

Note - Terminal Server Identity Agent (MUH) works only with Microsoft Active Directory as a user-directory server.

Identity Collector

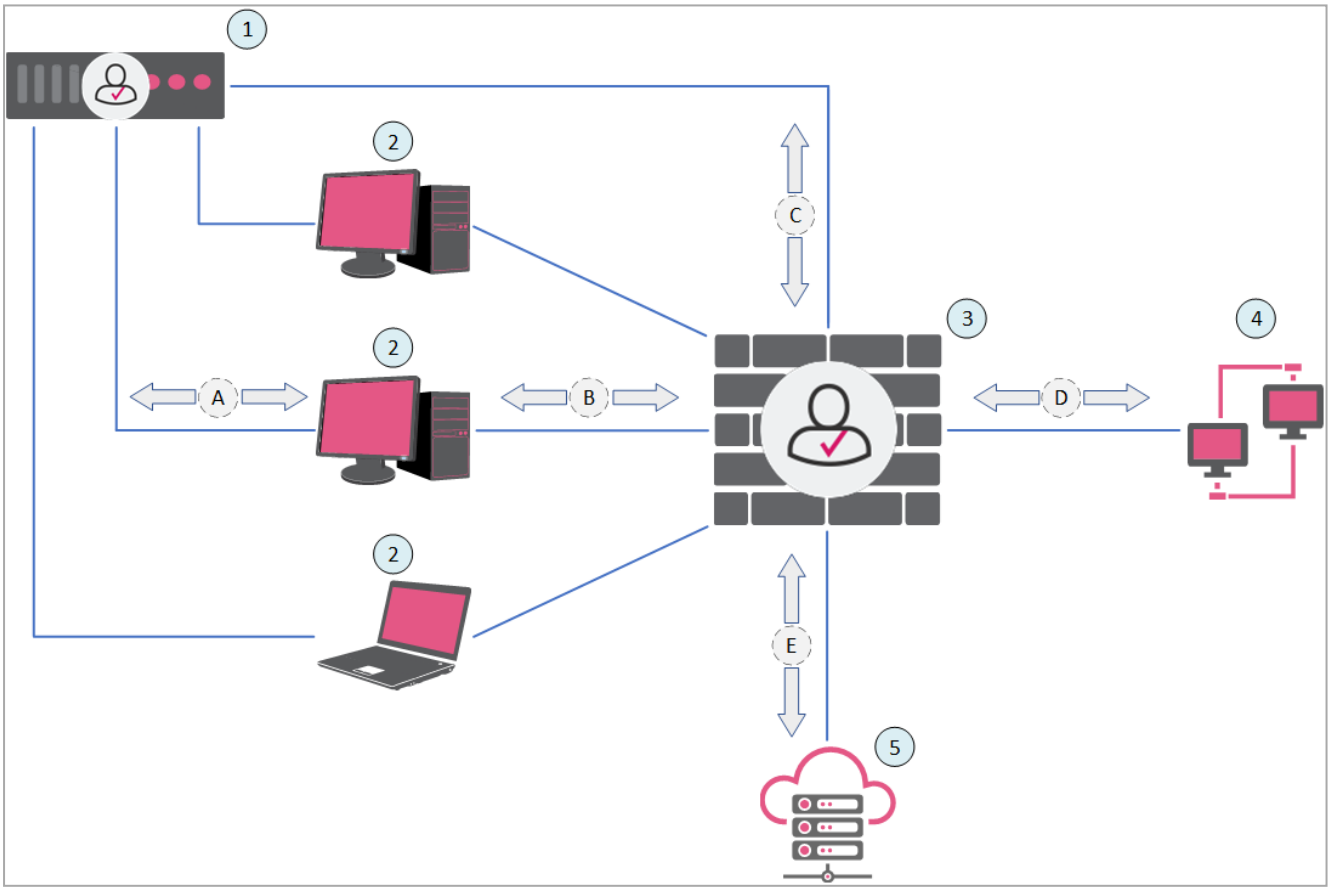
This section describes how to configure an Identity Collector (a type of Identity Client) for a Microsoft Server.

The Check Point Identity Collector serves as a specialized client agent that is deployed on Windows Servers within your network infrastructure.

Functionally, the Identity Collector is responsible for gathering identity-related data, which includes corresponding IP addresses, and subsequently transmits this information to the Check Point Identity Server. This exchange of data facilitates identity-driven enforcement measures.

To facilitate its operation, the Identity Collector leverages the Windows Event Log mechanism to retrieve security logs from the Domain Controller. The Windows Event Log functionality is an integral part of the operating system, available both for client systems (starting from Windows Vista) and server systems (starting from Windows Server 2008).

Example Topology and Traffic Flow with



Item	Description
1	Windows Server with Identity Collector installed
2	User endpoint computers
3	Identity Awareness Gateway
4	Internal resources
5	Security Management Server
A	Endpoint users authenticate on the Windows Server (1)
B	User endpoint computers (2) communicate with the Identity Awareness Gateway
C	Identity Collector on the Windows Server (1) sends user and machine identities to the Identity Awareness Gateway
D	Identity Awareness Gateway grants or denies access to internal resources (4) based on the Access Control Policy
E	Security Management Server manages the Identity Awareness Gateway

These are the benefits of using Identity Collector instead of a standard AD Query:

- Reduced load on the Security Gateway - Identity Collector does the queries instead of the Security Gateway
- Reduced load on the Domain Controller (DC) - the native Windows API consumes fewer resources
- Lower permissions required - Identity Collector requires read-only access to the domain security logs
- No changes are required in the Active Directory (AD) schema.
- One Identity Collector can serve multiple Security Gateways, even from a different Domain Management Servers on a Multi-Domain Server.
- Identity Collector can communicate with a maximum of up to 35 Active Directory (AD) servers.
- Identity Collector can process a maximum of 1900 Active Directory (AD) events per second.

Note - For the support of Identity Collector on Quantum Spark Appliances, see sk159772 and sk178604.

To set up the Identity Collector in High Availability mode, follow these steps:

1. Install the Identity Collector on two separate Windows servers.
2. Make sure that both Windows servers have identical configurations.

   After installed, the Identity Collector performs the following tasks on each Windows server:

   - Collects events from AD/ISE Servers.
   - Forwards the collected events to the Identity Server.

Note - If there are any duplicate events, the Identity Server automatically disregards them.

Identity Collector - Requirements

Supported Identity Sources

The Identity Collector supports these Identity Sources:

Identity Source	Requirements	Reference
Microsoft Active Directory Domain Controllers	No additional requirements specified	*"Identity Collector - Working with Active Directory" on page 80*)
Cisco Identity Services Engine (ISE) Servers	Supports Cisco ISE versions 2.0, 2.1, 2.2, 2.3, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, 3.3, 3.4	*"Identity Collector - Working with a Cisco Identity Services Engine (ISE) Server" on page 89*
NetIQ eDirectory Servers	Requires Identity Awareness Gateway R80.20 or higher	*"Identity Collector - Working with NetIQ eDirectory LDAP Servers" on page 84*
Syslog Messages	Requires Identity Awareness Gateway R80.20 or higher	*"Identity Collector - Working with Syslog Messages" on page 92*

Requirements for the Windows Server

These are minimum requirements for the Windows Server on which Identity Collector is installed:

Requirement	Details
Supported Versions	Windows Server 2025, 2022, 2019, 2016, 2012 R2, 2012, 2008 R2, 2008
RAM	Minimum: 8 GB
Disk Space	Minimum: 10 GB
.NET Framework	Version 4 required
Administrative Access	Administrator account required for installation and operation
Network Configuration	TCP port 443 must connect to Identity Server

Requirement	Details
Firewall Rules	■ Allow DNS, LDAP, and DCOM traffic if installed on Domain Controllers (including Windows Firewall). ■ Add "Allow" rule: Remote Event Log Management > Remote Event Log Management (RPC)
Processed Events	■ Authentication Events: 4624, 4768, 4769, 4770 ■ Group Update Events: 4728, 4729, 4732, 4733, 4756, 4757 ■ Group Deletion Events: 4730, 4734, 4758

Best Practices

Best Practice - For best performance, use a Windows Server with:

Specification	Recommended Value
CPU Cores	12 or more
RAM	16 GB or more
Disk Space	60 GB or more

Requirements for Integration with Active Directory

Requirement	Details
Connection to AD Domain Controllers	Windows Server must connect to AD Domain Controllers using DNS, LDAP, and DCOM protocols. **Note** - A connection between an Identity Awareness Gateway and Active Directory 2025 must use LDAP Account Units with SSL Encryption (LDAPS). Configure LDAPS in SmartConsole for the Management Server(s) that manages the Identity Awareness Gateway(s). For configuration instructions, see the Security Management Administration Guide for your version, search for "Account Units", and open the "Account Units" chapter.
Identity Collector User	Use an AD user account that is a member of the default Event Log Readers group.

Note - For the **Administrative Role**, the AD user account does **not** require administrative privileges..

Requirements for Integration with Cisco ISE PxGrid

The Identity Collector supports these versions of Cisco ISE:

Cisco ISE PxGrid Version	Supported Cisco ISE Versions	Required Java Version	Java Runtime Environment
1.0	2.0, 2.1, 2.2, 2.3, 2.4, 2.6, 2.7, 3.0, 3.1	Oracle Java JRE 1.8	Java SE Runtime Environment 8
2.0	2.0, 2.1, 2.2, 2.3, 2.4, 2.6, 2.7, 3.0, 3.1	Oracle Java SE Runtime Environment	Java SE Runtime Environment 8 or newer

Additional Requirements

Configure LDAP Account Unit(s) to enable PDP Identity Awareness Gateways to perform group lookups for user and machine identities. This setup ensures that theIdentity Awareness Gateways can accurately map users and machines to their respective groups, providing enhanced security and access control.

Identity Collector - Configuring as Identity Source

To enable the Identity Collector solution, you must configure it in the Identity Awareness Gateway object in SmartConsole:

1. Open SmartConsole and from the left panel, click **Gateways & Servers**.
2. Open the Identity Awareness Gateway object.
3. From the left menu, click the **Identity Awareness** pane.
4. Select **Identity Collector** and click **Settings**.
5. In the **Identity Collector Settings** window, configure these:

   Client Access Permissions

   Select to which interfaces on the Identity Awareness Gateway the Identity Collector can connect.

   Available options are based on the topology configured for the Identity Awareness Gateway interfaces:

   - **Through all interfaces**

     Identity Clients can connect to the Identity Awareness Gateway through all interfaces that an administrator configured in the Identity Awareness Gateway object (regardless of their **Topology** settings).

   - **Through internal interfaces**

     Identity Clients can connect to the Identity Awareness Gateway through internal interfaces only.

- **Including undefined internal interfaces**

  Identity Clients can connect to the Identity Awareness Gateway through all interfaces that the administrator configured in this way in the Identity Awareness Gateway object:

  a. From the left tree, click **Network Management**.

  b. Right-click an interface and click **Edit**.

  c. In the **Topology** section, click **Modify**.

  d. In the Leads To section, select **Override** > select **This Network (Internal)** > select **Not defined**.

  e. Click **OK**.

- **Including DMZ internal interfaces**

  Identity Clients can connect to the Identity Awareness Gateway through interfaces that the administrator configured in this way in the Identity Awareness Gateway object:

  a. From the left tree, click **Network Management**.

  b. Right-click an interface and click **Edit**.

  c. In the **Topology** section, click **Modify**.

  d. In the Leads To section, select **Override** > select the applicable option > select **Interface leads to DMZ**.

  e. Click **OK**.

- **Including VPN encrypted interfaces**

  Identity Clients can connect to the Identity Awareness Gateway through interfaces used for establishing route-based VPN tunnels (VTIs).

- **According to the Firewall policy**

  Select this option to control the access with Access Control rules.

Important - The **Through all interfaces** and **Through internal interfaces** options have priority over Access Control Policy rules. If an Access Control rule is configured to block connections from Identity Collector clients, the Identity Awareness Gateway continues to allow these connections.

Authorized Clients

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

To configure authorized Identity Collector client computers:

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

Notes:

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

To create an authentication secret for a selected Identity Collector client:

a. Select the Identity Collector client in the list.

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

Notes:

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

Authentication Settings

The Identity Awareness Gateway separately saves the authentication settings for different Identity Clients. This lets the administrator configure different authentication settings for different Identity Clients.

a. In the **Authentication Settings** section, click **Settings**.

The **User Directories** window opens.

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

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

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

c. Click **OK** to close the **User Directories** window.

6. Click **OK** to close the **Identity Collector Settings** window.
7. Click **OK** to close the **Check Point Gateway** window.
8. **Optional:** To enforce the Cisco Security Group Tags (SGTs) on the Identity Awareness Gateway:
   a. In SmartConsole, click the **Objects** menu > click **Object Explorer**.
   b. In the **Object Explorer**, click **New** > **User** > **User Group**.
   c. Name the new group: **CSGT-*<SGT_NAME>***.
   d. Assign this group to an Access Role.
9. Install the Access Control Policy.

Identity Collector - Downloading

You can download the Identity Collector from:

- sk134312.
- Identity Awareness Gateway object:

  1. Make sure you configured the Identity Collector in the Identity Awareness Gateway object.

     See *"Identity Collector - Configuring as Identity Source" on page 71*.

     Note - SmartConsole uses your web browser to download the package from the Identity Awareness Gateway. You web browser connects to the main IP address configured in the Identity Awareness Gateway object. You control the access to the Identity Awareness Gateway in the **Identity Collector Settings** window > **Client Access Permissions** section. If you change these settings, you must install the Access Control Policy.

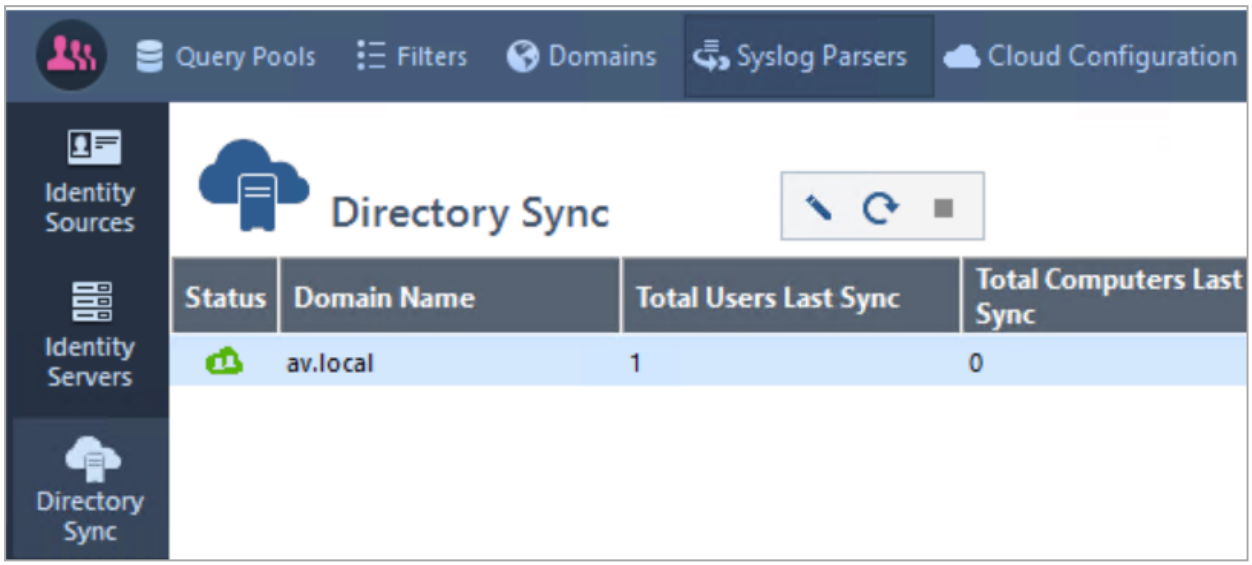
  2. From the left navigation panel, click **Gateways & Servers**.
  3. Open the Identity Awareness Gateway object.
  4. From the left tree, click the **Identity Awareness** pane.
  5. Below **Identity Collector**, click **Download agent**.
  6. You web browser starts the download.

     Note - If the **Client Access Permissions** in the Identity Awareness Gateway object do not allow this access, then the Identity Awareness Gateway redirects your web browser to Gaia Portal. Your browser shows that this HTTPS connection is not secure because the Identity Awareness Gateway uses a self-signed certificate.

  7. Click **Cancel** in Identity Awareness Gateway object.

Identity Collector - Updating

1. In the Identity Collector application, click the icon in the upper left corner and select **Export Configuration**.



2. As a backup, save the Identity Collector configuration file on your computer.
3. Download and install the Identity Collector application. See sk134312.

   The installation process runs an in-place upgrade for Identity Collector and keeps all configurations.

Identity Collector - User Interface

The elements of the Identity Collector GUI:

Location in GUI	Element in GUI	Description
Upper left corner	**Icon with pink people silhouettes**	Opens a menu with these options: ■ **Import Configuration** ■ **Export Configuration** ■ **About** ■ **Exit**
Top toolbar	**Query Pools**	Configuration of Query Pools
	Filters	Configuration of Filters for login events
	Domains	Configuration of Domains
	Syslog Parses	Configuration of Syslog Parses
	Cloud Configuration	Configuration of cloud connectivity
Left navigation toolbar	**Identity Sources**	Configuration of Identity Sources
	Identity Servers	Configuration of Identity Awareness Gateways
	Directory Sync	Configuration of AD Directory sync
	Logins Monitor	View of login events
	Settings	Configuration of advanced settings

Identity Collector - Connecting to an Identity Awareness Gateway

You can connect the Identity Collector to Identity Awareness Gateway and configure the Identity Collector to send logs to the Identity Awareness Gateway.

To connect the Identity Collector to Identity Awareness Gateway:

1. Open the Identity Collector application.
2. From the left navigation toolbar, click **Identity Servers**.
3. From the top toolbar, click the **Add** icon () and then select Security Gateway.
4. Configure the Identity Awareness Gateway:
   - **IP Address** - Enter the IPv4 address as configured in the Identity Awareness Gateway object in SmartConsole.
   - **Shared Secret** - Enter the shared secret as configured in the Identity Awareness Gateway object (**Identity Awareness** pane > **Identity Collector > Settings**).
   - **Query Pool** - Select the applicable query pool.
   - **Filter** - Select the applicable filter for the login events (if this field is empty, the default **Global** filter is used).
   - **Pre R80.10 Gateway** - Select this option if you connect to an Identity Awareness Gateway R77.30 or lower.
5. Click **Test**.
6. Examine and approve the **Certificate Info**.

   Note - Identity Collector does not trust a wildcard certificate from a Security Gateway.
7. Click **OK**.
8. Install the Access Control Policy on the Identity Awareness Gateway.

Note - Starting from R80.40, you can configure Service Account Exclusion on an Identity Awareness Gateway. For more information, see *"Identity Collector - Service Account Exclusion" on page 104*.

Designating the Main IP Address for Identity Collector on a Windows Server

When Identity Collector is installed on a Windows server that has more than one IP address on the external interface, you can designate one of the Windows server's IP addresses to use for communication between Identity Collector and an Identity Awareness Gateway. This feature is available starting from Identity Collector version R82.120.0000.

1. On the Windows server where Identity Collector is installed, stop the Identity Collector service.
2. In the Windows registry, go to: `HKLM\SOFTWARE\WOW6432Node\CheckPoint\IdentityCollector\`.
3. Set the value of the "`MainIP`" registry key as the IP address for the Windows Server to use for Identity Collector communication. The IP address must be in quad dotted format. For example: 192.168.1.1
4. Start the Identity Collector service.

Identity Collector - Working with Active Directory

To configure the Identity Collector to work with Active Directory:

1. In Identity Collector, add a new Active Directory Domain.

   To add a new Active Directory Domain

   a. Open the Identity Collector application.

   b. At the top, click **Domains**.

   c. From the top toolbar, click **New Domain** ().

   d. Enter the Domain name to show in the Identity Collector.

   The domain name must exactly match the actual domain name to ensure all features function correctly.

   e. **Optional:** Enter the comment.

   f. In the **Username** and **Password** fields, enter the Domain account credentials.

   Important:
   - The account must be a member of the **Event Log Readers** group.
   - To enable the configuration of Domain Controllers automatically by DNS and LDAP queries, as well as the periodic AD discovery flows to function seamlessly with Kerberos authentication, it is imperative that domain credentials be formatted in the User Principal Name (UPN) format. It is crucial to note that the use of a combination of User Principal Name format and DC IP address is not compatible.

   g. In the **DC Host name / IP Address** field, enter the host name or the IP address of one of the Domain Controllers that you want to add.

   h. Click **OK**.

   To edit a current Active Directory Domain

   a. Open the Identity Collector application.

   b. At the top, click Domains.

   c. Select the applicable Domain.

d. From the top toolbar, click **Edit Domain** ().

e. Configure the Domain.

f. Click **OK**.

To delete a current Active Directory Domain

a. Open the Identity Collector application.

b. At the top, click Domains.

c. Select the applicable Domain.

d. From the top toolbar, click **Delete Domain** ().

e. Click **Yes** to confirm.

f. Click **OK**.

2. In Identity Collector, add new Active Directory Domain Controllers.

   Follow one of these procedures to add the necessary Domain Controllers.

   Add Domain Controllers automatically by DNS and LDAP queries

   a. Open the Identity Collector application.

   b. From the left navigation toolbar, click **Identity Sources**.

   c. Click **New Source (**) **> Active Directory > Fetch Automatically**.

      The **Add Domain Controllers** window opens.

   d. Enter the Domain Controller information:

      - **Domain** - Select the Active Directory Domain that contains the Domain Controllers, or click and add this Domain to Identity Collector.
      - **DC Host name / IP Address** - Enter the host name or the IP address of one of the Domain Controllers you want to add.

        Note - To work with Kerberos authentication, you must use the host name.

   e. **Optional:** To configure the Identity Collector to fetch Active Directory Domain Controllers from LDAP over SSL, select **LDAP over SSL**.

   f. Click **Fetch**.

      A list of the Domain Controllers appears.

   g. Enable the Domain Controllers you want to add.

h. Click **OK**.

The enabled Domain Controllers are added.

Add Domain Controllers manually one at a time

a. Open the Identity Collector application.

b. From the left navigation toolbar, click **Identity Sources**.

c. Click **New Source ( )> Active Directory > Add Manually**.

d. Enter the **Domain Controller Name** to appear in the Identity Collector.

e. **Optional:** Enter your comment.

f. Enter the Domain Controller information:

- **Domain**

  Select the Active Directory Domain, or configure a new one.

- **DC Host name / IP Address**

  Enter the host name or the IP address of one of the Domain Controllers you want to add.

  Note - To work with Kerberos authentication, you must use the host name.

- **Site**

  Optional. Enter the Domain Controller site name.

- **Is Forwarded Event Log Collector**

  Select this option, if this server is not a Domain Controller, but a server, to which the login events are forwarded.

g. Click **Test**.

h. Click **OK**.

The Domain Controller is added.

3. In the Identity Collector, add a new Query Pool, or edit a current Query Pool.

   See *"Identity Collector - Query Pools" on page 96*.

4. In the Identity Collector, add a new Filter for the login events, or edit a current Filter.

   See *"Identity Collector - Filters for Login Events" on page 98*.

5. Connect the Identity Collector to the Check Point Identity Server.

See *"Identity Collector - Connecting to an Identity Awareness Gateway" on page 78*

Notes:

- Identity Collector uses the Windows Event Log API for fetching the security logs from Domain Controllers.
- Identity Collector can communicate with up to `35` Active Directory servers.
- Identity Collector can process up to `1900` Active Directory events per second.
- Domain Controllers configured with IP address must be changed to FQDN to work with Kerberos authentication.

Identity Collector - Working with NetIQ eDirectory LDAP Servers

Note - Check Point only supports user authentication for NetIQ eDirectory.

Configuration Procedure:

1. In SmartConsole, configure the Identity Awareness Gateway to work with a NetIQ eDirectory LDAP server.
   a. Configure the Identity Awareness Gateway object.

      Procedure

      i. Open the Identity Awareness Gateway object.

      ii. Enable the Identity Awareness Software Blade.

      The Identity Awareness Configuration Wizard opens.

      iii. On the **Methods For Acquiring Identity** page, select **Browser-Based Authentication** or **Terminal Servers** and click **Next**.

      You can disable this Identity Source later.

      iv. On the **Integration With Active Directory** page, select **I do not wish to configure the Active Directory at this time** and click **Next**.

      v. Click **Finish**.

      The Identity Awareness Configuration Wizard closes.

      vi. From the left navigation tree, go to the Identity Awareness page.

      vii. Select **Identity Collector** and click **Settings**.

      viii. Configure these settings:

      - **Client Access Permissions** - though which interfaces Identity Collector client can connect to Security Gateway
      - **Authorized Clients** - which computers with installed Identity Collector can connect to Security Gateway
      - **Selected Shared Secret** - to configure in Identity Collector for this Security Gateway
      - **Authentication Settings** - how to authenticate users

      ix. Click **OK** to close the **Identity Collector Settings** window.

x. Click **OK** to close the **Check Point Gateway** window.

b. Create a new **Host** object to represent your NetIQ eDirectory LDAP server.

Procedure

i. In the top left corner, click **Objects** > **New Host**.

ii. Configure the object name and IP address.

iii. Click **OK**.

c. Create a new LDAP Account Unit object to represent the NetIQ eDirectory LDAP server, which manages the identities.

Procedure

i. In the top left corner, click **Objects** menu > **Object Explorer**.

ii. In the left navigation tree, click **Servers**.

iii. From the top toolbar, click **New** > **More** > **User/Identity** > **LDAP Account Unit**.

The **LDAP Account Unit Properties** window opens.

d. Configure the new LDAP Account Unit object that represents the NetIQ eDirectory LDAP server.

- **The 'General' tab**

i. In the **Name** field, enter the applicable object name (for example, `mycompany.com_LDAP_ACC_UNIT`).

ii. In the **Profile** field, select **Novell_DS**.

iii. In the **Prefix** field, enter your domain name (for example, `mycompany.com`).

iv. In the **Account Unit usage** section, select all the options.

v. In the **Additional configuration** section, select **Enable Unicode support**.

- **The 'Servers' tab**

  i. Click **Add**.

  ii. The LDAP Server Properties window opens.

  iii. Go to the **General** tab.

  iv. In the **Host** field, select the host object you created for this LDAP server in **Step 2** above.

  v. In the **Username** field, enter the username for this LDAP server (for example, `John.Smith`).

  vi. In the **Login DN** field, enter the user's distinguished name (DN) for this LDAP server (see RFC1779).

  Note - Refer to the official NetIQ documentation. For example, use the `ldapsearch` command.

  vii. In the **Password** field, enter the password for this LDAP server.

  viii. In the **Confirm password** field, enter the password again.

  ix. Click **OK** to close the LDAP Server Properties window.

  Note - The order in which these LDAP Servers come to the view, is the default order in which they are queried. You can configure the applicable priority for these LDAP Servers.

- **The 'Objects Management' tab**

  i. In the **Server to connect** field, select the host object you created for this LDAP server in **Step 2** above.

  ii. Fetch or manually add the branch(es).

  The branch name is the suffix of the Login DN that begins with `DC=`.

  For example, if the Login DN is

  `CN=John.Smith,CN=Users,DC=mycompany,DC=com`

  then the branch name is

  `DC=mycompany,DC=com`

- **The 'Authentication' tab (Optional)**

  i. Clear **Use common group path for queries**.

  ii. In the **Allowed authentication schemes** section, select all the options.

  iii. In the **Users' default values** section:

  - Clear **Use user template**.
  - Select **Default authentication scheme** > **Check Point Password**.

e. Click **OK** to close the **LDAP Account Unit Properties** window.

f. In SmartConsole, install the Access Control Policy on the Identity Awareness Gateway that works as Identity Server.

2. In the Identity Collector, add a new NetIQ eDirectory LDAP Server.

   Procedure

   a. Open the Identity Collector application.

   b. From the left navigation toolbar, click **Identity Sources**.

   c. From the top toolbar, click **New Source > eDirectory**.

   d. Enter the eDirectory Server information:

   - **Object Name** - Enter the NetIQ eDirectory Server name to show in the Identity Collector.
   - Domain - Select the NetIQ eDirectory domain, or click **New Domain** to configure a New Domain:

     i. **Domain Name** - Enter the NetIQ eDirectory Domain name to show in the Identity Collector.

     ii. (Optional) Enter your comment.

     iii. **Username** - Enter the NetIQ eDirectory username DN.

     iv. **Password** - Enter the password for the given NetIQ eDirectory username.

     v. Click **OK** to close the **New Domain** window.

   - **IP address** - Enter the NetIQ eDirectory Server IP address.

- **Port** - Enter the NetIQ eDirectory LDAP port (default is 389, SSL default is 636).
- **Site** - (Optional) Enter the NetIQ eDirectory site.
- **Base DN** - (Optional) Enter the queried base DN (for example, `o=corp`).
- **LDAP over SSL** - (Optional) Select for using LDAP over SSL.

e. Click **OK** to close the **New eDirectory Server** window.

3. In the Identity Collector, add a new Query Pool, or edit a current Query Pool

   See *"Identity Collector - Query Pools" on page 96*

4. In the Identity Collector, add a new Filter for the login events, or edit a current Filter

   See *"Identity Collector - Filters for Login Events" on page 98*.

5. Connect the Identity Collector to the Check Point Identity Server.

   See *"Identity Collector - Connecting to an Identity Awareness Gateway" on page 78*.

Identity Collector - Working with a Cisco Identity Services Engine (ISE) Server

You can configure Identity Collector to take identity information from Cisco ISE servers over Platform Exchange Grid (PXGrid) send it to Identity Servers for identity-based enforcement.

To configure the Identity Collector to work with Cisco ISE:

1. In the Identity Collector, add a new Cisco ISE Server as an Identity Source.

   Procedure

   a. Open the Identity Collector application.

   b. From the left navigation toolbar, click **Identity Sources**.

   c. From the top toolbar, click **New Source > Cisco ISE**.

   d. Enter the **ISE Server Name** to appear in the Identity Collector.

   e. Enter the Server Settings:

   - **Primary Node** - Enter the resolvable FQDN of the primary pxGrid node (or the standalone node).
   - **Secondary Node** - Enter the resolvable FQDN of the secondary pxGrid node. Only necessary in distributed pxGrid environment with more than one pxGrid node.
   - **Site** - (Optional) Enter a Site name.
   - **Certificate File** - Select the ISE Server certificate file (in `jks` format). This file contains certificates of primary PxGrid, secondary PxGrid, and MnT nodes. See Cisco pxGrid documentation for instructions to export Cisco ISE certificates to the `jks` file.
   - **Certificate Key** - Enter the key for the ISE Server certificate file.
   - **Machine Name** - Enter the resolvable FQDN of the Identity Collector client computer. Then the ISE Server pxGrid client list shows this FQDN (**Administration > pxGrid Services > Client Name**), and it must be approved.

f. Enter the Client Settings:

- **Certificate File** - Select the Identity Collector certificate file (in `jks` format), generated by the ISE Server. See the *Cisco pxGrid* documentation.
- **Certificate Key** - Enter the key for the Identity Collector certificate file.

Enter the Client Settings:

g. Click **OK**.

2. In the Identity Collector, add a new Query Pool, or edit a current Query Pool.

   See *"Identity Collector - Query Pools" on page 96*.

3. In the Identity Collector, add a new Filter for the login events, or edit a current Filter.

   See *"Identity Collector - Filters for Login Events" on page 98*.

4. Connect the Identity Collector to the Check Point Identity Server.

   See *"Identity Collector - Connecting to an Identity Awareness Gateway" on page 78*

Parsing Events with "Postured" Status as Login Events

By default, Identity Collector does not parse Cisco ISE events with "Postured" status as login events in Cisco PxGrid 2.0. To configure Identity Collector to parse such events, set values of Windows Registry parameters on the server where Identity Collector is installed. This feature is available starting from Identity Collector version 82.120.0000.

Prerequisites

- The "`state`" of the Cisco ISE event must be "`Postured`".
- The Cisco ISE event must include a "`postureStatus`" with one of these values:
  - `Compliant`
  - `Pending`
  - `NonCompliant`
  - `Unknown`

Example Event

This is an example of a "Postured" Cisco ISE event that Identity Collector can parse.

```
{
"sessions": [
```

```
{
...
"state": "POSTURED",
"userName": "USER",
"ipAddresses": [
"1.2.3.4"
],
...
"postureStatus": "Compliant",
...
}
],
...
}
```

To configure Identity Collector to parse events with "Postured" status:

1. On the Windows server where Identity Collector is installed, stop the Identity Collector service.
2. In the Windows registry, go to "`HKLM\SOFTWARE\WOW6432Node\CheckPoint\IdentityCollector\`".
3. Set the value of the "`EnableIsePosturedEvents`" registry key to `1`.
4. Set the value of the "`AcceptablePostureEvents`" registry key to one or more posture statuses for Identity Collector to parse as login events. Put a semicolon between names of posture statuses.

   For example: `Compliant;Pending;NonCompliant;Unknown`
5. Start the Identity Collector service.

Identity Collector - Working with Syslog Messages

Identity Collector can receive and process Syslog messages that contain identity information.

Identity Collector can use these syslog messages as an additional identity source for the Identity Servers.

Important - Make sure your network and the Windows Server Firewall allow the incoming Syslog traffic on the Identity Collector computer. By default, Syslog traffic uses UDP port 514.

To configure the Identity Collector to work with Syslog messages:

1. Create a new Syslog Parser.
    a. Open the Identity Collector application.
    b. From the top toolbar, click **Syslog Parsers**.
    c. Click **New Parser**.

d. Enter the Syslog Parser information.

Syslog Parser Information

- **Object Name** - Enter the Syslog Parser name to show in the Identity Collector.
- (Optional) Enter your comment.
- **Message Subject** - The beginning of a log of the event.

  Select **Regex** option, if the Message Subject is a regular expression.
- **Event Type** - Select **Login**, or **Logout**.
- **Delimiter** - A character that separates all the fields.
- **Username Prefix** - The prefix of a username attribute. It is a sequence of characters, which precedes the username value.
- **Username** - The username attribute. Must be written inside parentheses.
- **Machine Prefix** - The prefix of a machine name attribute. It is a sequence of characters, which precedes the machine name value.
- **Machine** - The machine name attribute. Must be written inside parentheses.
- **Address Prefix** - The prefix of an address attribute. It is a sequence of characters, which precedes the address value.
- **Address** - The address attribute. Must be written inside parentheses.
- **Domain Prefix** - The prefix of a domain name attribute. It is a sequence of characters, which precedes the domain name value.
- Domain - The domain name attribute. Must be written inside parentheses.
- **Is Domain Mandatory** - Select this option to discard messages without the domain attribute.
- **Test Message** - Enter a test syslog message and click the **?** icon to confirm that your parser works correctly.

Important - Enter only the value of the attribute inside parentheses.

e. Click **OK**.

Additional information about how Syslog Parser works

Syslog parser uses regular expressions with *ECMAScript* syntax.

To get an attribute, syslog parser uses this regular expression:

```
/<Message Subject>.*<Attribute Prefix><Attribute>
[\\n|<Delimiter>].*$/.
```

Any unnecessary attributes should be empty. You must use at least one of these pairs:

- Address and Username
- Address and Machine

Example syslog message:

```
LOCAL7.INFO: May 30 2017 11:15:45: %ASA-6-113004: AAA user
accounting Successful : server = 192.168.1.1 : user =
johndoe\n
```

The Syslog Parser for this message can look like this:

- Message subject: `(AAA user accounting Successful)`
- Regex: `True`
- Event Type: `Login`
- Delimiter: `\s:`
- Username Prefix: `user\s=`
- Username: `\s(\w+)`
- Address Prefix: `server\s=`
- Address: `\s+(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})`

2. Add a Syslog Server as an Identity Source.
   a. Open the Identity Collector application.
   b. From the left navigation toolbar, click **Identity Sources**.
   c. From the top toolbar, click **New Source > Syslog**.

d. Enter the Syslog Server information.

- **Syslog Server Name** - Enter the Syslog Server name to show in the Identity Collector.
- Optional: Enter your comment.
- **IP Address** - Enter the IPv4 address of the Syslog Server.
- **Port** - Enter the applicable port on the Syslog Server.
- **Site** - Enter the Site name of the Syslog Server.
- **Parser** - Select a current Syslog parser, or create a new one.

3. In the Identity Collector, add a new Query Pool, or edit a current Query Pool.

   See *"Identity Collector - Query Pools" on page 96*.

4. In the Identity Collector, add a new Filter for the login events, or edit a current Filter.

   See *"Identity Collector - Filters for Login Events" on page 98*.

   Connect the Identity Collector to the Check Point Identity Server.

   See *"Identity Collector - Connecting to an Identity Awareness Gateway" on page 78*

Note - If you imported a previously exported configuration, the Identity Collector's GUI may not show the Syslog Parsers immediately. In this case, close and reopen the Identity Collector.

Identity Collector - Query Pools

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 is assigned to an Identity Server (which is an Identity Awareness Gateway). The Identity Collector collects information from the Identity Sources in the Query Pools and sends the information to the Identity Servers.

Note - Identity Collector queries only the Identity Sources that are selected in the Query Pool.

Example

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

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

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

The administrator, therefore, creates two Query Pools:

- A query pool which contains all the Active Directory Domain Controllers in the `Asia.com` domain.
- A query pool which contains all the Active Directory Domain Controllers in the `Euro.com` domain.

The administrator configures:

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

Adding a New Query Pool

1. Open the Identity Collector application.
2. At the top, click **Query Pools**.
3. From the top toolbar, click **New Query Pool** ().
4. Enter the name for the Query Pool to show in the Identity Collector.
5. (Optional) Enter the comment.
6. Select the Identity Sources from which to collect identities.
7. Click **OK**.

Editing a Current Query Pool

1. Open the Identity Collector application.
2. At the top, click **Query Pools**.
3. Select the applicable Filter.
4. From the top toolbar, click **Edit Query Pool** ().
5. Select the Identity Sources from which to collect identities.
6. Click **OK**.

Deleting a Current Query Pool

1. Open the Identity Collector application.
2. At the top, click **Query Pools**.
3. Select the applicable Filter.
4. From the top toolbar, click **Delete Query Pool** ().
5. Click **Yes** to confirm.
6. Click **OK**.

Identity Collector - Filters for Login Events

You can configure Identity Collector to filter the login events. Identity Collector sends events that match the filter criteria to the Identity Server.

Starting with version R80.67.0000, Identity Collector has these types of filter sets:

- **Global Filter** - Is applied for all Identity Servers configured in the Identity Collector instance. This filter is good to use for Service Accounts.
- **Regular Filters** - Are applied to one or more Identity Servers. These filters are located in the Identity Collector GUI **Identity Server** view.

To add a new Filter for login events in the Identity Collector:

1. Open the Identity Collector application.
2. From the top toolbar, click **Filters**.
3. From the top toolbar, click **New Filter** ().
4. Enter the name for the Filter to show in the Identity Collector.
5. (Optional) Enter the comment.
6. Configure the filter:
   - **Network Filter** - Defines IP addresses and networks to **Include** or **Exclude**
   - **Identity Filter** - Defines user names and computer names to **Include** or **Exclude**
   - **Domain Filter** - Defines domain names to or **Include** or **Exclude**
   - **Group Filter** - (starting from version R81.018.0000) - Defines groups to **Include** or **Exclude**
7. Click **OK**.

To edit a current Filter for login events in the Identity Collector:

1. Open the Identity Collector application.
2. From the top toolbar, click **Filters**.
3. Select the applicable Filter.
4. From the top toolbar, click **Edit Filter** ().
5. Configure the Filter:
   - **Network Filter** - Defines IP addresses and networks to **Include** or **Exclude**.
   - **Identity Filter** - Defines user names and computer names to **Include** or **Exclude**.
   - **Domain Filter** - Defines domain names to **Include** or **Exclude**.
6. Click **OK**.

To delete a current Filter for login events in the Identity Collector:

1. Open the Identity Collector application.
2. From the top toolbar, click **Filters**.
3. Select the applicable Filter.
4. From the top toolbar, click **Delete Filter** ().
5. Click **Yes** to confirm.
6. Click **OK**.

Cache:

The cache saves associations (user-to-IP address) that the Identity Collector creates for a time interval (the default is 5 minutes).

If the event happens again during that interval, the Identity Collector does not send it to the Identity Server.

Identity Collector - Send Monitoring Information

You can configure Identity Collector to send monitoring information to the Identity Awareness Gateway R80.20 and higher.

Each Identity Collector instance that is connected to the Identity Awareness Gateway sends information about the identity sources configured in the Query Pool that is linked to it. This information includes: type, name, host, and event counters.

Monitoring is **not** enabled by default. To enable monitoring, on the Windows Server add a registry key named "`MonitoringEnabled`" and set its value to "`1`" (Type: "`DWORD`").

Full file path:

- On 32-bit Windows Servers:

```
HKEY_LOCAL_MACHINE\SOFTWARE\CheckPoint\IdentityCollector\
```

- On 64-bit Windows Servers:

```
HKEY_LOCAL_
MACHINE\SOFTWARE\Wow6432Node\CheckPoint\IdentityCollector\
```

The default interval for sending monitoring information is `10` seconds. You can configure this interval in the "`MonitoringInterval`" registry key (Type: "`DWORD`".

You can use these methods to query the data:

- SNMP- Relevant SNMP Object Identifiers (OIDs) are located in the `$FWDIR/conf/identity_server.cps` file on the Identity Awareness Gateway.
- CLI of an Identity Awareness Gateway:
  - On Identity Awareness Gateways of all versions:

```
cpstat identityServer -f idc
```

  - On the PDP Identity Awareness Gateways R80.30 and higher:

```
pdp idc status
```

Identity Collector - Alias Feature

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

To enable the Alias feature on the Identity Collector client computer:

1. Go to this folder:

   `C:\ProgramData\CheckPoint\IdentityCollector\`

2. Create a new configuration file:

   `DomainDictionaryAliases.cfg`

3. The structure of the configuration file must follow this pattern:

   < name from which to convert >=< name to which to convert >

   Notes
   - There is no space between the equal sign and the name of the domain or the alias name.
   - Each line shows one conversion.

   Example:

   If the nickname of "`something.com`" is "`someone`", add this line in the file:
   `someone=something.com`

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

4. Save the changes in the file.

5. Restart the Identity Collector service:

   - Service Name - `IDCService`
   - Service Display Name - `Check Point Identity Collector`

Identity Collector - Automatic LDAP Group Update

Important - This solution is applicable only to a Security Gateway when used as an Identity Server.

Identity Collector automatically recognizes changes to LDAP group memberships and updates the identity information, including Access Roles.

This capability is now available using Identity Collector.

This capability was already available in AD Query and in R80.40. Starting in R81 it is available in Identity Collector, as well.

The LDAP Group Update feature is on by default for a user's membership updates. For group membership updates, it is off by default. You can turn it on manually from the CLI.

When enabling update of group membership movement, the system recalculates LDAP group membership for ALL users in ALL Groups. This may have a performance impact.

- Users moving from one LDAP group to another – on by default.
- Moving a group to a different group (nested groups)– off by default.
- Group deletion – off by default.

To activate automatic LDAP group update for a group's membership MOVEMENT:

On the Identity Awareness Gateway (each Cluster Member) command line, run:

```
pdp idc groups_update {on|off|status}
```

Parameters

Parameter	Description
`on`	The pdp performs "update all" to get the current LDAP group status.
`off`	Disables the feature (default setting)
`status`	Shows the current status of the feature

For improved performance, the information about LDAP users and groups is cached by the Identity Awareness Gateway. If the information about a current group is already cached, the group update is not reflected until the cache is updated.

By default the cache is updated every 15 minutes.

The Group Update flow:

1. The Identity Collector receives a notification about a group change. It does this by listening to the IDs of group change events.
2. The Identity Collector forwards the notification to the PDP Identity Awareness Gateway.
3. The PDP Identity Awareness Gateway behavior depends on the status of the group update settings.

Group Update Setting	Behavior
A user or a machine	PDP performs the action "update specific" for this user or machine to get the current status
A group with the feature disabled	PDP does nothing. This is the default setting.
A group with the feature enabled	PDP performs the action "update all" to get the current status. You can enable the feature with this command: `pdp idc groups_update on`

Identity Collector - Service Account Exclusion

Important - This solution is applicable only to a Security Gateway when used as an Identity Server.

About Service Accounts

A Service Account is a user account that provides a security context for services that run on Windows Server operating systems. The security context determines which local and network resources a service can use.

Identity Collector gets information for usernames and for device Service Accounts.

The Identity Collector Service Account Exclusion feature automatically detects Service Accounts to conserve resources and lessen user management overhead on an Identity Awareness Gateway.

Example

When the Identity Collector identifies a login event, it creates a new entry in a *<key>:<value>* pair format.

For example: `user_1:192.168.1.10`

The process counts each time it identifies a login event for the same *<key>:<value* pair. When the number of simultaneous logins exceeds a pre-configured threshold value, the account is defined as a Service Account. The same account (username) can have more than one associated IP address.

If Service Account Exclusion is configured, the session is revoked and the account is removed from the database on the Identity Awareness Gateway. All the information for this account is deleted.

Availability

The feature is available starting from these Security Gateway versions:

Version	Availability
R81.20 and higher	Starting from Check Point R81.20.
R81.10	R81.10 Jumbo Hotfix Accumulator - from Take 14
R81	R81 Jumbo Hotfix Accumulator - from Take 51
R80.40	R80.40 Jumbo Hotfix Accumulator -from Take 131

Important - In Security Gateway versions for which the feature is available, it is enabled by default.

Terms

Term	Description
Detect Mode	The process detects Service Accounts and does not revoke sessions. The process shows the list of detected Service Accounts.
Prevent Mode (Auto-Exclude Mode)	The Identity Awareness Gateway detects Service Accounts that it receives from Identity Collector. The PDP then revokes the account's current sessions, and blocks any future sessions.
Detection Interval	The time interval, during which Identity Collector counts the number of logins to identify the account as a Service Account.
Exception	Identity Collector treats accounts on the exception list as regular accounts, and does not revoke future sessions from these accounts. When Prevent Mode (Auto Exclude) is enabled, the administrator can add Service Accounts to the exception list.
Threshold	The minimum number of simultaneous logins for the same account during the Detection Interval that identifies it as a Service Account. Example: The Detection Interval is 5 minutes and the threshold is 100 simultaneous logins. If there are 100 or more simultaneous logins during this interval, Identity Collector treats the account as a Service Account.

Service Account Database

Identity Awareness Gateway saves the session identifier and username c associated with an identified Service Account in the `$FWDIR/conf/idc_servacc.db` file. The Service Account information loads from the file after a policy installation or reboot.

Configuration on Identity Awareness Gateway

The administrator can exclude the applicable Service Account information from the Identity Awareness process (Policy Decision Point / PDP) and its memory to conserve the gateway resources.

See the table below for a description of relevant parameters. For more information, see the *CLI Reference Guide* for your version of the Security Gateway > Chapter "Identity Awareness Commands" > Section "pdp" > Section "pdp idc" > parameter "`service_accounts <options>`".

Parameter	Description
Mode	By default, the Prevent Mode (Auto-Exclude) is enabled. When Prevent Mode is enabled, Detect Mode is disabled. When you disable Prevent Mode, Detect Mode is enabled. **Note** - When you change from Detect Mode to Prevent Mode, the PDP revokes all sessions that are marked as a Service Account.
Threshold	Configure the number of simultaneous logins, after which the PDP detects all usernames as Service Accounts.
Detection Interval	Configure the length of the interval. **Note** - A change in the interval length affects the detection interval for the Identity Agent for a Terminal Server feature. For more information about this feature, see *"Identity Agent for a Terminal Server" on page 45*

To change the detection interval

1. Connect to the command line on the Identity Awareness Security Gateway / each Cluster Member.
2. Log in to the Expert mode.
3. Back up the current `$FWDIR/conf/pdp_overriding_attrs.C` file, if it exists:

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

4. Edit the current `$FWDIR/conf/pdp_overriding_attrs.C` file:

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

5. Configure the applicable value for the `idc_muh_interval` attribute:

   ```
   (
       :idc_muh_serviceaccount_interval (<NUMBER OF SECONDS>)
   )
   ```

   Default Value: `3600` seconds

   Accepted Values: from `1` to `86400` seconds
6. Save the changes in the file and exit the editor.
7. In SmartConsole, install the Access Control policy.

Limitations

- In a Cluster and in Scalable Platforms, the Cluster Members and Security Group Members do not synchronize the information about Service Accounts.
  - In ClusterXL High Availability mode, Service Account detection and exclusion restarts after a cluster fail-over.
  - In ClusterXL Load Sharing mode and Scalable Platforms, each Cluster Member and Security Group Member detects its own Service Accounts.

    As a workaround, we recommend that you add a filter in the Identity Collector with the known Service Accounts. See *"Identity Collector - Filters for Login Events" on page 98*
- If a Service Account entry already exists in the exception list, this is the only command that removes it from the exception list:

  ```
  pdp idc service_accounts delete_exception <username_1>
  <username_2> ... <username_N>
  ```

  After the account's session times out, the PDP removes the account from the exception list.
- An Identity Collector that identifies login events with User Principal Name (UPN) (example: `user_1@domain.com`) records the account with the `SAMAccountName` property (example: `user_1`).

Troubleshooting

To view the list of accounts and the number of IP addresses these accounts use

Step	Instructions
1	Connect to the command line on the Identity Awareness Gateway.
2	Log in to the Expert mode.
3	Run: `pdp __ed show_srv_account_tracker`

Example Output:

```
auto_test_106->5
```

Output Explanation:

The account (user) `auto_test_106` uses `5` different IP addresses (5 sessions).

If you configure the threshold value to `6`, the next login event matches the threshold value and marks the account as a Service Account.

Collecting the debug

Step	Instructions
1	Connect to the command line on the Identity Awareness Gateway.
2	Log in to the Expert mode.
3	Configure the PDP debug options: `pdp debug set IDC all CCC_SERVICE all IDC_ SRV_ACC_PERSISTENCE_DB all IDP all`
4	Start the PDP debug: `pdp debug on`
5	Replicate the issue.

6	Set the PDP debug options:
	`pdp debug reset`
	`pdp debug set TRACKER all`

Step	Instructions
7	Stop the PDP debug: `pdp debug off`
8	Collect and examine the debug output files: `$FWDIR/log/pdpd.elg*`

Example 1

This excerpt from a debug shows a new login event record for the user account "`johndoe`":

```
[9619 4058363776]@MyGW[26 Apr 13:50:26]  [CCC_SERVICE
(TD::Events)] pdp::IDCEvent::shouldPreventAccount: service
account mechanism is in detection mode, no prevention.
[9619 4058363776]@MyGW[26 Apr 13:50:26]  [IDC (TD::Events)]
pdp::AssociationsDB::addAccountByIPToIPMap: first login of
that username
[9619 4058363776]@MyGW[26 Apr 13:50:26]  [IDC (TD::Events)]
pdp::AssociationsDB::aboveServiceAccountThreshold: account
johndoe has 1 connected IPs and does not exceed the service
account threshold (6)
[9619 4058363776]@MyGW[26 Apr 13:50:26]  [CCC_SERVICE
(TD::Events)] pdp::IDCEvent::addUserToServiceAccountMechanism:
account johndoe was considered in service account detection
mechanism
```

Example 2

An administrator configured the Prevent Mode (Auto-Exclude Mode).

This excerpt from a debug shows that:

1. The user account "`johndoe`" exceeds the configured Service Account threshold.
2. The PDP increments the counter.
3. The user account "`johndoe`" is a Service Account.
4. The PDP revokes the current sessions for this user account.

```
[15408 4057798528]@MyGW[28 Apr 13:12:02]  [IDC (TD::Events)]
pdp::AssociationsDB::aboveServiceAccountThreshold: account
johndoe is above service account threshold
[15408 4057798528]@MyGW[28 Apr 13:12:02]  [CCC_SERVICE
(TD::Events)] pdp::IDCEvent::shouldPreventAccount: the user
johndoe is a new service account and prevention is on,
reporting it as service account and revoking existing
sessions.
```

Example 3

An administrator configured the Detect Mode.

This excerpt from a debug shows that the PDP records a user (account) login:

```
[27214 4058212224]@MyGW[28 Apr 10:32:06]  [CCC_SERVICE
(TD::Events)] pdp::IDCEvent::shouldPreventAccount: service
account mechanism is in detection mode, no prevention.
[27214 4058212224]@MyGW[28 Apr 10:32:06]  [IDC (TD::Events)]
pdp::AssociationsDB::aboveServiceAccountThreshold: account
johndoe has 2 connected IPs and does not exceed the service
account threshold (3)
[27214 4058212224]@MyGW[28 Apr 10:32:06]  [CCC_SERVICE
(TD::Events)] pdp::IDCEvent::addUserToServiceAccountMechanism:
account johndoe was considered in service account detection
mechanism
```

Identity Collector - Forwarding Identities to an Event Log Collector

How to configure Log Collector in Identity Collector

1. Configure Event Log forwarding on Windows Server 2008 and higher, which requires a Source and Target (Collector) server.

   For information on log forwarding and how to enable it, see Configure Event Log Forwarding in Windows Server 2012 R2.

2. Before you do the next step, make sure that the events are successfully populating within the Event Viewer of the Collector server, specifically in **Windows Logs** > **Forwarded Events**.

3. Go to the Identity Collector > **Identity Sources**, select **New Source** > **Active Directory** > **Add Manually**.

4. Enter the domain and IP address and select the option **Is Forwarded Event Log Collector**.

5. When the Identity Source is successfully connected, add it to the related Query Pool. You should now see the number of events incrementing.

Identity Collector - Advanced Configuration

1. In the Identity Collector client, from the left navigation toolbar, click **Settings**.
2. Configure the advanced setting.

Category	Setting	Description
Activity Log		Logs the date and time of activities done in the Identity Collector. This log is cleared every time the Identity Collector GUI restarts.
Settings > Identity Reporting	**Association time-to-live**	How long this association stays on the PDP Identity Awareness Gateway. The default is `720` minutes (`12` hours).
	Cache time-to-live	The cache saves associations (username-to-IP address) that the Identity Collector creates for a specified time. If the event occurs again during that time, the Identity Collector does not send the event to the Identity Awareness Gateway again. The default is `300` seconds (`5` minutes).
	Ignore machine identities	If you select this option, the Identity Collector sends user identities and does not send machine identiteis. By default, this option is cleared. Starting from Identity Collector version 82.120.0000, you can specify from which identity sources to ignore machine identities. By default, after you select **Ignore machine identities**, these checkboxes are also selected: ▪ **Active Directory** ▪ **Cisco ISE** ▪ **Syslog** If you want Identity Collector to send machine identities from an identity source, clear the checkbox for the identity source.

Category	Setting	Description
	Ignore RDP events	During Remote Desktop login, two login events occur in the Domain Controller. The two login events have the same username but two different IP addresses: the computer where the user logs in and the computer that the user accesses remotely. In this option, the Identity Collector ignores the IP address of the computer where the user logs in because it is redundant. This is the default option. The Event ID of the ignored event is `4624`. The Type of the ignored event is `10`.
	Clear Cache	Clears all the entries saved in the cache. The Identity Collector creates new cache entries when it receives new associations.
Settings > Debugging		Lets you configure the debug topics and severity of collected internal messages in the Identity Collector. Location of the output files is configured in this file: `C:\ProgramData\CheckPoint\IdentityCollector\ServiceDebugPath.cfg` The output files are: ■ `{LOCATION}\ia_ag.log` ■ `{LOCATION}\ia_idcgui_0.log` ■ `{LOCATION}\ia_ag_tracker.log` ■ `{LOCATION}\IDCLogs\ia_IDC_xxx.log`
Settings > ISE Servers	**Session Keep-alive**	The Identity Collector goes over its internal Cisco ISE sessions database once during the interval time period. If Identity Collector finds expired sessions, it queries the Cisco ISE Server to see if the session is still alive. Then, Identity Collector updates the Identity Awareness Gateway accordingly. This value sets the interval. The default is 1 minute.
Settings > eDirectory	**LDAP Query Interval**	This value sets the frequency for Identity Collector to query eDirectory LDAP servers. The default is `20` seconds.
	Initial Fetch Time Frame	This value sets how long Identity Collector waits for eDirectory LDAP servers during initial fetch. The default is `720` minutes (`12` hours).

Category	Setting	Description
Settings > Logins Monitor	**Event expiration time**	The maximum time that the **Logins Monitor** Table stores each login record.
	Cache time-to-live	The maximum time interval between two different login events by the same user or the same computer that are treated as one **Logins Monitor** record.
	Auto refresh time	The interval of time for the user interface of the Logins Monitor to refresh its display, when it requests an update of login records.
	Ignore revoked events	When selected, the **Logins Monitor** tab stores and shows only the latest login event (both user and computer event) for each IP address.
Cloud Settings	**Full directory synchronization**	Syncs all identities to the cloud.

Identity Collector - Protocols and Ports

Identity Collector uses these protocols and ports:

Direction	Port	Protocol
Identity Collector to Identity Server	443	Proprietary Check Point protocol, over HTTPS. Used for ongoing connection between the agent and the Identity Server.
Identity Collector to Microsoft Active Directory Domain Controller	53	DNS
Identity Collector to Microsoft Active Directory Domain Controller	389	LDAP
Identity Collector to Microsoft Active Directory Domain Controller	636	LDAPS **Note** - Starting from R81.08.0000, you can use LDAPS through port 636 when you use "NetIQ eDirectory" and "Active Directory". See: ■ *"Identity Collector - Working with NetIQ eDirectory LDAP Servers" on page 84* ■ *"Identity Collector - Working with Active Directory" on page 80*
Identity Collector to Microsoft Active Directory Domain Controller	135, and dynamically allocated ports	DCOM protocol, which uses DCE/RPC. **Note** - DCOM uses DCE/RPC. If the Active Directory Domain Controller uses Windows Firewall, configure it to allow Identity Collector traffic: enable **Remote Event Log Management > Remote Event Log Management (RPC)**.
Identity Collector to Cisco ISE Server	5222	Session subscribe. Gets notifications of new login or logout events from the Cisco ISE Server.
Identity Collector to Cisco ISE Server	8910	Bulk session download. Fetches all the active sessions from the Cisco ISE Server.

Identity Collector - Optimization

Exclude multi-user machines

After the Identity Collector works for some time, you can check the number of multi-user computers, and add them to the **Network Exclusion List**.

To do so, run this command on the Identity Awareness Gateway (each Cluster Member):

```
pdp idc muh show
```

Exclude service accounts

After the Identity Collector works for some time, you can see how many service accounts there are, and add them to the **Identity Exclusion List**.

To do so, run this command on the Identity Awareness Gateway (each Cluster Member):

```
pdp idc service_accounts
```

Consolidate Groups

If the Identity Awareness Gateway receives the user groups from the Cisco Identity Collector (SGT), it does not fetch them from the user directory.

If you enable group consolidation, the Identity Awareness Gateway fetches the group even if it receives groups from the Identity Collector:

```
pdp idc groups_consolidation status
```

How to increase number and size of logs in Identity Collector

The logs of the Identity Collector on a Windows server are located in `C:\windows\temp\ia_ag.log*`. The default configuration includes ten files. In scenarios where the environment accommodates a substantial user base and all severity topics are activated for logging, all the files could be rotated quickly. This could require you increase the number and maximum size of log files.

The size of the debug files and the number of files are configurable through the registry.

Change the following registry values:

- `\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\CheckPoint\IdentityCollector\DebugMaxFiles -- Number of files`
- `\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\CheckPoint\IdentityCollector\DebugMaxSize -- Debug file size (in bytes)`

If these registry values do not exist, create them with the necessary value.

After changing the registry values, it is necessary to restart the Identity Collector service to keep the changes.

1. On Windows Server machine open **Task Manager** > **Services**.
2. Find a service named `IDCService`, right-click on it and select **Restart**.

Identity Collector - Debug

How to debug Identity Collector

The Identity Collector has two main components:

1. **User Interface**

   The frontend of the application is responsible for the graphical user interface (GUI) and passes the communication of data to the backend (Service).

2. **Service**

   Executes the IDC logic, such as establishes communication with identity sources and gateways, filtering, parsing, and more.

In most cases, the debugging should be enabled on the *service* side.

Note - In Windows 2016, the debugs are located in `C:\Temp\` (not in `C:\Windows\Temp\`)

User Interface debug:

- File location (where "X" is an index):

  `C:\Windows\Temp\ia_idcgui_X.log`

- To increase the default debug level, change the registry key value to 0:

  `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\CheckPoint\IdentityCollector\GUILoggerLevel`

Service debug:

- File location (should be up to 10 files):

  `C:\Windows\Temp\ia_ag.log*`

- The default debug level is "`Events`".

  To change it, go to the Identity Collector Application > **Settings** > **Debugging**.

- To increase the number/size of log files, see *"How to increase number and size of logs in Identity Collector" on page 118*.

ISE integration debug:

- File location (should be up to 10 files):

  `C:\Windows\Temp\ia_ise_extension.log*`

- To increase the number/size of log files, see *"How to increase number and size of logs in Identity Collector" on page 118*.
- The `pxGrid` entry point function for new events from the ISE Server is the `onChange` function.

DMP files:

- File location - If the Identity Collector crashes, collect the required dump files from `C:\Windows\Temp\IDCLogs\`
- Each crash creates log files, which include the required information.

Database files:

- File location:

  `%PROGRAMDATA%\CheckPoint\IdentityCollector`

- For a replication, upload this folder or run **Export Configuration** in the Identity Collector application.

Advanced Configuration of Identity Clients

This section describes how to configure and work with additional options for Identity Clients.

Configuring Global Parameters in SmartConsole

You can change advanced global parameters to control the behavior of Identity Agent for a User Endpoint Computer or Identity Agent for a Terminal Server.

This global parameters apply to all Identity Awareness Gateways this Management Server manages.

You can change some of the settings in SmartConsole and others with the Identity Agent Configuration Utility (see *"Creating Custom Identity Clients" on page 147*).

Procedure:

1. In SmartConsole, in the top left corner, click **Menu** and click **Global properties**.
2. In the left navigation tree, click **Advanced** > **Configure**.
3. Expand **Identity Awareness** and click **Agent**.
4. Configure the applicable parameters.
5. Click **OK**.
6. Install the Access Control policy on all managed Identity Awareness Gateways.

You can also create custom Identity Clients. See *"Creating Custom Identity Clients" on page 147*.

Identity Agent for a User Endpoint Computer - Parameters in Windows Registry

You can add attributes to Identity Agent on a Windows endpoint computers to control its behavior.

To add a new attribute to Identity Agent:

1. On the Windows endpoint computer:
   a. Click **Start**.
   b. Enter "`Run`" and press the Enter key.
   c. Enter "`regedit`" and press the Enter key.

      Windows Registry Editor opens.
2. In the top address bar, go to the required file path for the Identity Agent type and the Windows OS type:

Identity Agent Type	Windows OS Type	File Path
Full Identity Agent or MUH Identity Agent	32-bit Windows	`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\CheckPoint\IA`
Full Identity Agent or MUH Identity Agent	64-bit Windows	`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\CheckPoint\IA`
Light Identity Agent	32-bit Windows or 64 bit Windows	`Computer\HKEY_CURRENT_USER\SOFTWARE\CheckPoint\IA`

Identity Agent Attributes

You can control the behavior of an Identity Agent with different attributes in Windows Registry.

Identity Agent Attributes

Attribute Name	Description	Branch in Registry	Attribute Type	Default Value	Comments
`DelayBetweenConnAttempts`	Configures the delay time between failures - how much time to wait (in milliseconds) between failures.	"IA"	`REG_DWORD`	`10000` milliseconds	See sk88520 .

Identity Agent Attributes (continued)

Attribute Name	Description	Branch in Registry	Attribute Type	Default Value	Comments
`DelayFactorBetweenConnAttempts`	Configures the delay factor - multiplication factor for the delay time between failures. To activate this parameter, assign it a value greater than or equal to `2`.	"IA"	`REG_DWORD`	`1`	See sk88520.
`MaxDelayBetweenConnAttempts`	Configures the maximum delay time between failures (in milliseconds).	"IA"	`REG_DWORD`	`900000` milliseconds (15 minutes)	See sk88520.

Identity Agent Attributes (continued)

Attribute Name	Description	Branch in Registry	Attribute Type	Default Value	Comments
ConnectionNumRetries	Configures the maximum number of connection attempts before the client resets the connection.	"IA"	REG_DWORD	2	See sk88520.
NumberOfAttemptsDiscoverPdp	Configures the maximum number of failed attempts to discover PDP (Discovery Mode) before the client resets the connection.	"IA"	REG_DWORD	6	Added in R81.004.0000 (see sk170756).

Identity Agent Attributes (continued)

Attribute Name	Description	Branch in Registry	Attribute Type	Default Value	Comments
`DelayTimeToDiscoverPdp`	After the Identity Agent reaches the configured number of failed attempts, how much time it waits before the next attempt (in milliseconds).	"IA"	`REG_DWORD`	`300000` millisecons	Added in R81.004.0000 (see sk170756).
`PdpDNSDiscoveryEnabled`	Enables (`1`) or disables (`0`) the search in the DNS Server in discovery mode.	"IA"	`REG_DWORD`	`1`	Added in R81.004.0000 (see sk170756).

Identity Agent Attributes (continued)

Attribute Name	Description	Branch in Registry	Attribute Type	Default Value	Comments
`CabDir`	Configures the path where to create the `Cab` file after "`collect logs`" operation (by priority lookup, from global to the user context).	"IA"	`REG_SZ`	`%temp%`	Added in R80.234.000
`LogsEnabled`	Enables (`1`) or disables (`0`) logs.	"IA"	`REG_DWORD`	`1`	Added in R80.234.000

Identity Agent Attributes (continued)

Attribute Name	Description	Branch in Registry	Attribute Type	Default Value	Comments
`InterfaceNameToExclude`	Configures an interface that the Identity Agent excludes in discovery mode when it matches the configured rule lists form the Active Directory database se	"IA"	`REG_SZ`	[NAME OF INTERFACE]	Only one interface can be selected. This parameter was added in R81.018.0000.

Identity Agent Attributes (continued)

Attribute Name	Description	Branch in Registry	Attribute Type	Default Value	Comments
`InterfaceNameToUse`	Configures an interface that the Identity Agent uses in discovery mode when it matches the configured rule lists form the Active Directory database.	"IA"	`REG_SZ`	--	Only one interface can be selected. This parameter was added in R81.018.0000.
`EventLogsEnabled`	Enables (`1`) or disables (`0`) the Identity Agent from writing logs in the Windows Event Viewer.	"IA"	`REG_DWORD`	`0`	This parameter was added in R81.018.0000.

Identity Agent Attributes (continued)

Attribute Name	Description	Branch in Registry	Attribute Type	Default Value	Comments
`FilteredEventLogs`	Configures the list of states that do not have an event log created.	"IA"	`REG_SZ`	For MUH, default ="`16`" For Identity Agent for Window, default= [`EMPTY`]"	See sk103682.
`UserKerberosAuthDisabled`	Enables (`0`) or disables (`1`) user authentication with Kerberos.	"IA"	`REG_DWORD`	`0`	Added in R80.234.000
`MachineReportEnabled`	Enables (`1`) or disables (`0`) collection of a machine report during the "collect logs" operation.	"IA"	`REG_DWORD`	`0`	Added in R81.005.0000

Identity Agent Attributes (continued)

Attribute Name	Description	Branch in Registry	Attribute Type	Default Value	Comments
AgentGlobalPropsBuffer	Global properties downloaded from Management and the Gateway.	"IA"	REG_BINARY	None	
DisableBalloonNotifications	Enables (0) or disables (1) balloon notifications.	"IA"	REG_DWORD	0	See sk163577.
DisableDisconnect	Enables (0) or disables (1) a user to disconnect from the server.	"IA"	REG_DWORD	0	Added in R80.234.000
HideGui	Shows (0) or hides (1) the client GUI from the end user.	"IA"	REG_DWORD	0	See sk121335.

Identity Agent Attributes (continued)

Attribute Name	Description	Branch in Registry	Attribute Type	Default Value	Comments
`DisableSettings`	Enables (`0`) or disables (`1`) a user to change the Identity Agent settings from the User Interface.	"IA"	`REG_DWORD`	`0`	Added in R80.234.000
`DisableQuit`	Enables (`0`) or disables (`1`) a user to close the Identity Agent.	"IA"	`REG_DWORD`	`0`	Added in R80.234.000

Identity Agent Attributes (continued)

Attribute Name	Description	Branch in Registry	Attribute Type	Default Value	Comments
`IsFirstTimeActivation`	Enables (`1`) or disables (`0`) a baloon message that asks users if this is the first time they are using Identity Agent.	"IA"	`REG_DWORD`	`1`	Added in R80.234.000
`DefaultGateway`	Enables (`1`) or disables (`0`) manual configuration of the IP address and DNS name of the Default Gateway.	"IA"	`REG_SZ`	""	Added in R80.234.000

Identity Agent Attributes (continued)

Attribute Name	Description	Branch in Registry	Attribute Type	Default Value	Comments
`Fingerprint`	Configures the server's certificate fingerprint string.	"IA" `\TrustedGateways\SERVER_CN`	`REG_SZ`	None	Added in R80.234.000
`PdpDiscoveryEnabled`	Enables (`1`) or disables (`0`) the PDP Discovery Mode.	"IA"	`REG_DWORD`	`1`	Added in R80.234.000

Identity Agent Attributes (continued)

Attribute Name	Description	Branch in Registry	Attribute Type	Default Value	Comments
DefaultGatewayEnabled	Enables (1) or disables (0) manual configuration of a PDP Gateway. Manual configuration includes the predefined advanced rule base.	"IA"	REG_BINARY	0	Added in R80.234.000
PredefinedPDPConnRUBUsed	Enables (1) or disables (0) the predefined advanced rulebase.	"IA"	REG_DWORD	0	Added in R80.234.000

Identity Agent Attributes (continued)

Attribute Name	Description	Branch in Registry	Attribute Type	Default Value	Comments
`PredefinedPDPConnectRuleBase`	The name of the manually predefined advanced rulebase.	"IA"	`REG_BINARY`	None	Added in R80.234.000
`ResolveFQDN`	Enables (`1`) or disables (`0`) the user to connect with the FQDN format.	"IA"	`REG_DWORD`	`0`	See sk87200.
`ResolveUPN`	Enables (`1`) or disables (`0`) the user to connect with UPN format.	"IA"	`REG_DWORD`	`0`	See sk110858.

Identity Agent Attributes (continued)

Attribute Name	Description	Branch in Registry	Attribute Type	Default Value	Comments
`DisableTagging`	Enables (`0`) or disables (`1`) packet tagging.	"IA"	`REG_DWORD`	`0`	Added in R80.234.000
`IsHandleSessionEventEnabledMuh2`	Enables (`1`) or disables (`0`) the user identification through the running process or sessions event with MUH2.	"IA"	`REG_DWORD`	`1`	Added in R81.004.0000. See sk170635.
`SharedSecret`	Configures the MUH agent's shared secret.	"IA"	`REG_SZ`	""	Added in R80.234.000

Identity Agent Attributes (continued)

Attribute Name	Description	Branch in Registry	Attribute Type	Default Value	Comments
MUHMonitoringEnabled	Enables (1) or disables (0) the MUH monitoring.	"IA"	REG_DWORD	0	See *"Identity Agent for a Terminal Server - Monitoring" on page 62*.
MUHMonitoringInterval	If the MUH monitoring is enabled, this attribute configures the interval (in seconds) at which the MUH Agent sends monitoring information to the Security Gateway.	"IA"	REG_DWORD	15 seconds	See *"Identity Agent for a Terminal Server - Monitoring" on page 62*.

Identity Agent Attributes (continued)

Attribute Name	Description	Branch in Registry	Attribute Type	Default Value	Comments
`MUHCollectLogsForAllUsersEnabled`	Determines who can collect logs in the MUH agents - administrators (`0`) or all users (`1`).	"IA"	`REG_DWORD`	`0`	Added in R80.234.000
`EnablePortProbing`	Enables (`1`) or disables (`0`) the verification if ports (source or destination) used for a connection are available.	"UIP"	`REG_DWORD`	`0`	See sk117089.

Identity Agent Attributes (continued)

Attribute Name	Description	Branch in Registry	Attribute Type	Default Value	Comments
ExcludedTCPPorts	Configures MUH1 to exclude the specified TCP ports.	"UIP"	REG_SZ	1-9999	Added in R80.234.000
ExcludedUDPPorts	Configures MUH1 to exclude the specified UDP ports.	"UIP"	REG_SZ	1-9999	Added in R80.234.000
MaxNumOfPortsPerUser	Configures the maximum number of ports that MUH1 can allocate per user.	"UIP"	REG_DWORD	900	Added in R80.234.000

Identity Agent Attributes (continued)

Attribute Name	Description	Branch in Registry	Attribute Type	Default Value	Comments
PortsMinPerUser	Configures the minimum number of ports that MUH1 can allocate per user.	"UIP"	REG_DWORD	20	Added in R80.234.000
IAConfigToolPath	Configures the path for the Identity Agent configuration tool.	"IA"	REG_SZ	""	Added in R81.004.0000

Identity Agent Attributes (continued)

Attribute Name	Description	Branch in Registry	Attribute Type	Default Value	Comments
`AdvancedDistributedConfigurationEnabled`	Enables (`1`) or disables (`0`) the use of the Advanced Distributed Configuration tool (it supports multiple domain controllers).	"IA"	`REG_DWORD`	`1`	Added in R81.018.0000

Identity Agent Attributes (continued)

Attribute Name	Description	Branch in Registry	Attribute Type	Default Value	Comments
`UserAuthMethods`	Determines which authentication methods to use for user authentication. The value `1` enables all user authentication. The value `0` disables all user authentication.	"IA"	`REG_DWORD`	`1`	Added in R80.234.000

Identity Agent Attributes (continued)

Attribute Name	Description	Branch in Registry	Attribute Type	Default Value	Comments
	Use the value `0` for an Identity Agent that only requires authentication by machine identity.				

Identity Agent Attributes (continued)

Attribute Name	Description	Branch in Registry	Attribute Type	Default Value	Comments
`MachineAuthMethods`	Determines which authentication methods to use for user authentication. The value `1` enables all machine authentication The value `1` disables all machine authentication.	"IA"	`REG_DWORD`	`1`	Added in R80.234.000

Identity Agent Attributes (continued)

Attribute Name	Description	Branch in Registry	Attribute Type	Default Value	Comments
	Use the value `0` for an Identity Clients that only requires authentication by user identity.				
`KerberosGetUserNameRetries`	Configures the number of times that the Identity Agent tries to fetch the logged-on username for user authentication with Kerberos.	"IA"	`REG_DWORD`	`15`	Added in R81.022.0000

Creating Custom Identity Clients

You can use the Identity Agent Configuration Utility to create custom installation packages for:

- Identity Agent for a User Endpoint Computer
- Identity Agent for a Terminal Server

The Identity Agent Configuration Utility "`IAConfigTool.exe`" is installed as part of Identity Agent for a User Endpoint Computer and Identity Agent for a Terminal Server..

Identity Agent for a User Endpoint Computer and Identity Agent for a Terminal Server. have many advanced configuration parameters.

Some of these parameters are related to the installation process, while others are related to Identity Client functionality.

All of the configuration parameters have default values that are configured with the product and can remain unchanged.

Identity Client Type	Description
Full Identity Agent for a User Endpoint Computer	Predefined Identity Client that includes packet tagging and computer authentication. It applies to all users of the computer on which it is installed. To use the Full Identity Client type, Administrator permissions are necessary.
Light Identity Agent for a User Endpoint Computer	Predefined Identity Client that does not include packet tagging and computer authentication. You can install this Identity Client individually for each user on the target computer. Administrator permissions are not necessary.
Identity Agent for a Terminal Server Version 1 (MUH v1)	Predefined Identity Client that installs Managed Asset Detection (MAD) services and the Multi-user host driver on Citrix and Terminal Servers. This Identity Client type cannot be used for endpoint computers.
Identity Agent for a Terminal Server Version 2 (MUH v2)	Predefined Endpoint Identity Client that installs Managed Asset Detection (MAD) services and the Multi-User Host (MUH) 2 driver on Citrix and Terminal Servers. This Endpoint Identity Client type cannot be used for endpoint computers.

Installing Microsoft .NET Framework

You must install Microsoft .NET Runtime framework 4.0 or higher before you install and run the Identity Agent Configuration Utility.

Working with the Identity Agent Configuration Utility

Getting the source MSI File

To create a custom Identity Client installation package, you must first download the customizable MSI file from sk134312 to your management computer. This is the computer, on which you use the Identity Agent Configuration Utility.

Running the Identity Agent Configuration Utility

You must install the Identity Client on your management client computer. The Identity Agent Configuration Utility is installed in the Identity Agent installation directory.

To run the Identity Agent Configuration Utility:

1. Go to the Identity Agent installation directory.
   a. Click **Start > All Programs > Check Point > Identity Agent**.
   b. Right-click the Identity Client shortcut and select **Properties** from the menu.
   c. Click **Open File Location** (**Find Target** in some Windows versions).
      - Example path on Windows 64-bit:

        ```
        C:\Program Files (x86)\CheckPoint\Identity Agent\IAConfigTool.exe
        ```

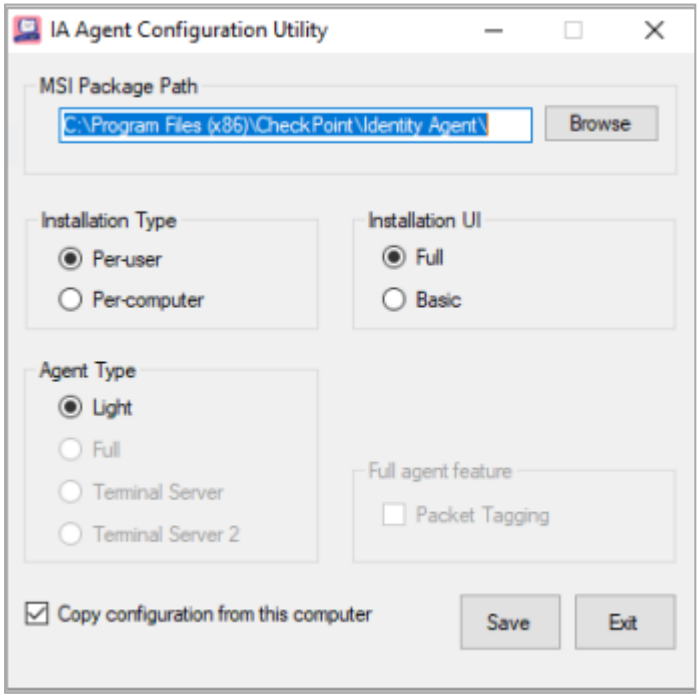
      - Example path on Windows 32-bit:

        ```
        C:\Program Files\CheckPoint\Identity Agent\IAConfigTool.exe
        ```

2. Double-click **IAConfigTool.exe**.

   The Identity Agent Configuration Utility opens.

   Example:



Configuring the Identity Client

You must configure all the features and options in the Identity Agent Configuration Utility window:

1. MSI Package Path

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

   Installation Type

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

   - **Per-User**

     Install the Light Identity Agent only for the user who does the installation. Administrator permissions are **not** necessary for this installation.

   - **Per Computer**

     Install any Identity Agent type for all users on the computer. Administrator permissions are necessary for this installation type.

2. 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.

   Identity Client Type

   Select the type of Identity Client to install:

   - **Full Identity Agent for a User Endpoint Computer**

     Predefined Identity Client includes packet tagging and computer authentication. It applies to all users of the computer that it is installed on. To use the Full Identity Client type, Administrator permissions are necessary.

- **Light Identity Agent for a User Endpoint Computer**

  Predefined Identity Client that does not include packet tagging and computer authentication. You can install this Identity Client individually for each user on the target computer. Administrator permissions are not necessary. You must select the **Per-Computer installation** type for this agent type.

- **Terminal Server Identity Agent Version 1 (MUH v1)**

  Predefined Identity Client that installs MAD services and the Multi-user host driver on Citrix and Terminal Servers. This Identity Client type cannot be used for endpoint computers.

- **Terminal Server Identity Agent Version 2 (MUH v2)**

  Predefined Endpoint Identity Client that installs MAD services and the Multi-User Host (MUH) 2 driver on Citrix and Terminal Servers. This Endpoint Identity Client type cannot be used for endpoint computers.

3. Full agent feature

   Select this feature for the Full Identity Agent:

   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 necessary if you have Firewall rules that use **Access Roles** and IP Spoofing is enabled.

4. Copy configuration

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

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

Configuring a Custom Identity Client with the Captive Portal

To configure a custom Identity Client with the Captive Portal:

1. Upload the custom `customAgent.msi` package to this directory on the Identity Awareness Gateway:

   ```
   /opt/CPNacPortal/htdocs/nacclients/
   ```

2. Configure the Captive Portal to distribute the custom Identity Client:
   a. Connect with SmartConsole to the Management Server that manages this Identity Awareness Gateway.
   b. From the left navigation panel, click **Gateways & Servers**.
   c. Open the Identity Awareness Gateway object.
   d. From the left tree, click the **Identity Awareness** page.
   e. Near the **Browser-Based Authentication** option, click the **Settings** button.
   f. In the section **Identity Agent Deployment from the Portal**, select **Require users to download** and select to **Identity Client - Custom**.
   g. Click **OK** to close the **Portal Settings** window.
3. Click **OK** to close the **Check Point Gateway** window.
4. Install the Access Control Policy on this Identity Awareness Gateway.

Automatic Reconnection to Prioritized Policy Decision Point (PDP) Gateways

Identity Agent for a User Endpoint Computer and Identity Agent for a Terminal Server can reconnect to the original Policy Decision Point (PDP) Security Gateway after it recovers from a failure.

To configure the automatic reconnection to a higher-priority PDP Security Gateway:

1. Configure the PDP Security Gateway:
   a. Connect to the command line on the PDP Identity Awareness Gateway.
   b. Log in to the Expert mode.
   c. Get the current recovery interval value:

      ```
      pdp auth recovery_interval show
      ```

   d. Configure the applicable recovery interval value (in seconds):

      ```
      pdp auth recovery_interval set <1-864000>
      ```

2. Install the Access Control Policy on this PDP Identity Awareness Gateway.

CLI Reference

Syntax	Description
`pdp auth recovery_interval show`	Shows the recovery interval
`pdp auth recovery_interval set < value>`	Sets the recovery interval value between `1` and `864000` seconds
`pdp auth recovery_interval enable`	Enables the automatic reconnection to a higher-priority PDP Security Gateway
`pdp auth recovery_interval disable`	Disables the automatic reconnection to a higher-priority PDP Security Gateway

Notes

- The value of the `recovery_interval` parameter controls the recovery interval. During the recovery interval, the Identity Client searches for a higher priority PDP Security Gateway.
- You can set the recovery interval between `1` and `864000` seconds. The default recovery interval value is `14400` seconds.
- On a VSX Gateway, configure the `recovery_interval` parameter in the context of each Virtual System with Identity Awareness enabled.
- The Identity Client fetches the value of the `recovery_interval` parameter when it connects to the PDP Security Gateway. Therefore, you must set the same value on all applicable PDP Security Gateways in your environment.
- Site priority depends on the priority configured in the Identity Agent Distributed Configuration Tool. Site priority does not rely on other methods, such as DNS resolving.
- When two or more sites are unreachable, the Identity Client tries to reconnect to the primary site only one time. If the attempt fails, the Identity Client reconnects to the primary site gradually.

Kerberos SSO Compliance

The Identity Awareness Single Sign-On (SSO) solution for Identity Clients lets you transparently authenticate users that are logged in to the domain. After a user authenticates to the domain once, the user has access to all authorized network resources without additional authentication. This solution is available for:

- Identity Agent for a User Endpoint Computer
- Identity Agent for a Terminal Server

These are some major benefits of Identity Clients SSO:

- **User and computer identity**
- **Minimal user intervention**

  The administrators do all the necessary configuration steps, and no input from a user is necessary.

- **Seamless connectivity**

  There is transparent authentication when users are logged in to the domain. If you do not configure SSO, users enter their credentials manually. You can let users save their 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 packet tagging to prevent IP Spoofing. In addition, Identity Clients give 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 for Windows 2000 and above.

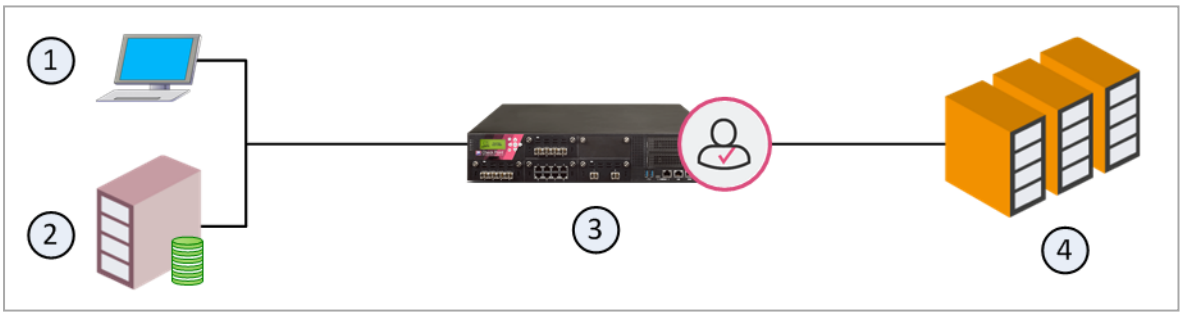
The Kerberos protocol uses tickets. Tickets are encrypted data packets issued by a trusted authority, in this case the Active Directory (AD). When a user logs in, the user authenticates to a domain controller that provides an initial *ticket granting ticket* (TGT). This ticket proves the user's identity. When the user authenticates against the Identity Awareness Gateway, the Identity Client presents this ticket to the domain controller and requests a service ticket (SR) for a specific Security Gateway. The Identity Client then presents this service ticket to the Security Gateway that grants access.

How SSO Works

This is the workflow for SSO:

1. The user logs in to the computer and authenticates to the AD server.
2. The AD sends an initial ticket (TGT) to the computer.
3. The Identity Client connects to the Identity Awareness Gateway, which then requests the identity.
4. The Identity Client requests an SR (service ticket) for the Identity Awareness 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 Identity Awareness Gateway and the AD server.
6. The Identity Client sends the SR to the Identity Awareness Gateway.
7. The Identity Awareness Gateway uses the shared secret to decrypt the ticket and confirms the user identity.
8. The user gets access to resources behind the Identity Awareness Gateway.



Item	Description
1	Computer for the user
2	Active Directory Domain Controller server
3	Identity Awareness Gateway
4	Resources behind the Identity Awareness Gateway

SSO Configuration

SSO configuration includes these steps:

1. **Configuration in Active Directory**

   In this step, you create a user account and map it to a Kerberos principal name.

   To use Kerberos with Active Directory, 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 (see the *Identity Awareness Administration Guide* for your version > Section "Mapping the User Account to a Kerberos Principal Name").

   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 fails.

   To configure Active Directory for Kerberos:

   a. Make a new user account (see the *Identity Awareness Administration Guide* for your version > Section "Creating a New User Account").

   b. Open Windows Command Prompt (**Start** > **Run** > **cmd**).

   c. Run:

   ```
   setspn -A ckp_pdp/<domain_full_dns_name> <username>
   ```

   To see users associated with the principle name, run:

   ```
   setspn -Q ckp_pdp*/*
   ```

2. **Configuration in SmartConsole**

   In this step, you configure an LDAP Account Unit object to work with SSO.

   To use this account, configure an Account Unit in SmartConsole (see the *Identity Awareness Administration Guide* for your version > Section "Configuring an Account Unit").

Transparent Kerberos SSO Authentication

Identity Awareness can recognize Microsoft group membership data in the Kerberos tickets that are granted by any domain controller configured in SmartConsole. This solution is available for:

- Identity Agent for a User Endpoint Computer
- Identity Agent for a Terminal Server

The Transparent Kerberos SSO Authentication feature is disabled by default.

Note - On VSX Gateway, run the commands in the context of the Virtual System with enabled Identity Awareness Software Blade.

1. Connect to the command line on the Identity Awareness Gateway.
2. On a VSX Gateway, go to the context of the Virtual System with the enabled Identity Awareness Software Blade.

   See the *VSX Administration Guide* for your version.
3. Configure the Transparent Kerberos SSO Authentication.

   Configure the Transparent Kerberos SSO Authentication

   - To see if the feature is enabled or disabled, run:

     ```
     pdp auth fetch_by_sid status
     ```

   - To enable the feature, run:

     ```
     pdp auth fetch_by_sid enable
     ```

   - To disable the feature, run:

     ```
     pdp auth fetch_by_sid disable
     ```

Configure the Identity Client to support domains that are not configured in SmartConsole

- To see if the feature is enabled or disabled, run:

```
pdp auth kerberos_any_domain status
```

- To enable the feature, run:

```
pdp auth kerberos_any_domain enable
```

- To disable the feature, run:

```
pdp auth kerberos_any_domain disable
```

Configure the Identity Client to send updated Kerberos tickets upon policy installation

By default, the Identity Client fetches and sends a Kerberos ticket to the Identity Awareness Gateway only during a re-authentication (based on the Identity Client settings).

You can force the Identity Client to send an updated Kerberos ticket when you install Access Control Policy on the Identity Awareness Gateway.

- To see if the feature is enabled or disabled on the Identity Awareness Gateway, run:

```
pdp auth reauth_agents_after_policy status
```

- To enable the feature, run:

```
pdp auth reauth_agents_after_policy enable
```

- To disable the feature, run:

```
pdp auth reauth_agents_after_policy disable
```

4. Install the Access Control Policy on this Identity Awareness Gateway (Virtual System).

Glossary

A

Access Role
Access Role objects let you configure network access according to: Networks, Users and user groups, Computers and computer groups, Remote Access Clients. After you activate the Identity Awareness Software Blade, you can create Access Role objects and use them in the Source and Destination columns of Access Control Policy rules.

AD Query
Check Point clientless identity acquisition tool. It is based on Active Directory integration and it is completely transparent to the user. The technology is based on querying the Active Directory Security Event Logs and extracting the user and computer mapping to the network address from them. It is based on Windows Management Instrumentation (WMI), a standard Microsoft protocol. The Check Point Security Gateway communicates directly with the Active Directory domain controllers and does not require a separate server. No installation is necessary on the clients, or on the Active Directory server.

Anti-Bot
Check Point Software Blade on a Security Gateway that blocks botnet behavior and communication to Command and Control (C&C) centers. Acronyms: AB, ABOT.

Anti-Spam
Check Point Software Blade on a Security Gateway that provides comprehensive protection for email inspection. Synonym: Anti-Spam & Email Security. Acronyms: AS, ASPAM.

Anti-Virus
Check Point Software Blade on a Security Gateway that uses real-time virus signatures and anomaly-based protections from ThreatCloud to detect and block malware at the Security Gateway before users are affected. Acronym: AV.

Application Control
Check Point Software Blade on a Security Gateway that allows granular control over specific web-enabled applications by using deep packet inspection. Acronym: APPI.

Audit Log
Log that contains administrator actions on a Management Server (login and logout, creation or modification of an object, installation of a policy, and so on).

B

Bridge Mode
Security Gateway or Virtual System that works as a Layer 2 bridge device for easy deployment in an existing topology.

Browser-Based Authentication
Authentication of users in Check Point Identity Awareness web portal - Captive Portal, to which users connect with their web browser to log in and authenticate.

C

Captive Portal
A Check Point Identity Awareness web portal, to which users connect with their web browser to log in and authenticate, when using Browser-Based Authentication.

Cloud Credentials
Specific credentials from identity providers used by the Identity Collector to connect seamlessly to the Infinity Portal. These credentials are essential for establishing a secure and efficient connection between the Identity Client and the Infinity Portal.

Cloud Services
Refers to a centralized identities solution provided by Infinity Identity and Directory Sync. These services offer identity management and directory synchronization capabilities, hosted and managed in the cloud.

Cluster
Two or more Security Gateways that work together in a redundant configuration - High Availability, or Load Sharing.

Cluster Member
Security Gateway that is part of a cluster.

Compliance
Check Point Software Blade on a Management Server to view and apply the Security Best Practices to the managed Security Gateways. This Software Blade includes a library of Check Point-defined Security Best Practices to use as a baseline for good Security Gateway and Policy configuration.

Content Awareness
Check Point Software Blade on a Security Gateway that provides data visibility and enforcement. Acronym: CTNT.

CoreXL
Performance-enhancing technology for Security Gateways on multi-core processing platforms. Multiple Check Point Firewall instances are running in parallel on multiple CPU cores.

CoreXL Firewall Instance
On a Security Gateway with CoreXL enabled, the Firewall kernel is copied multiple times. Each replicated copy, or firewall instance, runs on one processing CPU core. These firewall instances handle traffic at the same time, and each firewall instance is a complete and independent firewall inspection kernel. Synonym: CoreXL FW Instance.

CoreXL SND
Secure Network Distributer. Part of CoreXL that is responsible for: Processing incoming traffic from the network interfaces; Securely accelerating authorized packets (if SecureXL is enabled); Distributing non-accelerated packets between Firewall kernel instances (SND maintains global dispatching table, which maps connections that were assigned to CoreXL Firewall instances). Traffic distribution between CoreXL Firewall instances is statically based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type. The CoreXL SND does not really "touch" packets. The decision to stick to a particular FWK daemon is done at the first packet of connection on a very high level, before anything else. Depending on the SecureXL settings, and in most of the cases, the SecureXL can be offloading decryption calculations. However, in some other cases, such as with Route-Based VPN, it is done by FWK daemon.

CPUSE
Check Point Upgrade Service Engine for Gaia Operating System. With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself.

D

DAIP Gateway
Dynamically Assigned IP (DAIP) Security Gateway is a Security Gateway, on which the IP address of the external interface is assigned dynamically by the ISP.

Data Loss Prevention
Check Point Software Blade on a Security Gateway that detects and prevents the unauthorized transmission of confidential information outside the organization. Acronym: DLP.

Data Type
Classification of data in a Check Point Security Policy for the Content Awareness Software Blade.

Directory Sync
A solution that holds static Directory information regarding users, groups, devices, and memberships. .

Distributed Deployment
Configuration in which the Check Point Security Gateway and the Security Management Server products are installed on different computers.

Dynamic Object
Special object type, whose IP address is not known in advance. The Security Gateway resolves the IP address of this object in real time.

E

Endpoint Policy Management
Check Point Software Blade on a Management Server to manage an on-premises Harmony Endpoint Security environment.

Expert Mode
The name of the elevated command line shell that gives full system root permissions in the Check Point Gaia operating system.

G

Gaia
Check Point security operating system that combines the strengths of both SecurePlatform and IPSO operating systems.

Gaia Clish
The name of the default command line shell in Check Point Gaia operating system. This is a restricted shell (role-based administration controls the number of commands available in the shell).

Gaia Portal
Web interface for the Check Point Gaia operating system.

H

Hotfix
Software package installed on top of the current software version to fix a wrong or undesired behavior, and to add a new behavior.

HTTPS Inspection
Feature on a Security Gateway that inspects traffic encrypted by the Secure Sockets Layer (SSL) protocol for malware or suspicious patterns. Synonym: SSL Inspection. Acronyms: HTTPSI, HTTPSi.

I

ICA
Internal Certificate Authority. A component on Check Point Management Server that issues certificates for authentication.

Identity Agent
Check Point dedicated client agent installed on Windows-based user endpoint computers. This Identity Agent acquires and reports identities to the Check Point Identity Awareness Security Gateway. The administrator configures the Identity Agents (not the end users). There are two types of Identity Agents - Full and Light. You can download the Full and Light Identity Agent package from the Captive Portal - 'https://<Gateway_IP_Address>/connect' or from Support Center.

Identity Agent Configuration Utility
Check Point utility that creates custom Identity Agent installation packages. This utility is installed as a part of the Identity Agent: go to the Windows Start menu > All Programs > Check Point > Identity Agent > right-click the 'Identity Agent' shortcut > select 'Properties' > click 'Open File Location' ('Find Target' in some Windows versions > double-click 'IAConfigTool.exe').

Identity Agent Distributed Configuration Tool
Check Point Identity Agent control tool for Windows-based client computers that are members of an Active Directory domain. The Distributed Configuration tool lets you configure connectivity and trust rules for Identity Agents - to which Identity Awareness Security Gateways the Identity Agent should connect, depending on its IPv4 / IPv6 address, or Active Directory Site. This tool is installed a part of the Identity Agent: go to the Windows Start menu > All Programs > Check Point > Identity Agent > open the Distributed Configuration. Note - You must have administrative access to this Active Directory domain to allow automatic creation of new LDAP keys and writing.

Identity Awareness
Check Point Software Blade on a Security Gateway that enforces network access and audits data based on network location, the identity of the user, and the identity of the computer. Acronym: IDA.

Identity Broker
Identity Sharing mechanism between Identity Servers (PDP): (1) Communication channel between PDPs based on Web-API (2) Identity Sharing capabilities between PDPs - ability to add, remove, and update the identity session.

Identity Collector
Check Point dedicated client agent installed on Windows Servers in your network. Identity Collector collects information about identities and their associated IP addresses and sends it to the Check Point Security Gateways for identity enforcement, you can download the Identity Collector package from the Support Center.

Identity Collector Identity Sources
Identity Sources for Check Point Identity Collector - Microsoft Active Directory Domain Controllers, Cisco Identity Services Engine (ISE) Servers, or NetIQ eDirectory Servers.

Identity Collector Query Pool
A list of Identity Sources for Check Point Identity Collector.

Identity Logging
Check Point Software Blade on a Management Server to view Identity Logs from the managed Security Gateways with enabled Identity Awareness Software Blade.

Identity Server
Check Point Security Gateway with enabled Identity Awareness Software Blade.

Internal Network
Computers and resources protected by the Firewall and accessed by authenticated users.

IPS
Check Point Software Blade on a Security Gateway that inspects and analyzes packets and data for numerous types of risks (Intrusion Prevention System).

IPsec VPN
Check Point Software Blade on a Security Gateway that provides a Site to Site VPN and Remote Access VPN access.

J

Jumbo Hotfix Accumulator
Collection of hotfixes combined into a single package. Acronyms: JHA, JHF, JHFA.

K

Kerberos
An authentication server for Microsoft Windows Active Directory Federation Services (ADFS).

L

Log Server
Dedicated Check Point server that runs Check Point software to store and process logs.

Logging & Status
Check Point Software Blade on a Management Server to view Security Logs from the managed Security Gateways.

M

Management Interface
(1) Interface on a Gaia Security Gateway or Cluster member, through which Management Server connects to the Security Gateway or Cluster member. (2) Interface on Gaia computer, through which users connect to Gaia Portal or CLI.

Management Server
Check Point Single-Domain Security Management Server or a Multi-Domain Security Management Server.

Manual NAT Rules
Manual configuration of NAT rules by the administrator of the Check Point Management Server.

Mobile Access
Check Point Software Blade on a Security Gateway that provides a Remote Access VPN access for managed and unmanaged clients. Acronym: MAB.

Multi-Domain Log Server
Dedicated Check Point server that runs Check Point software to store and process logs in a Multi-Domain Security Management environment. The Multi-Domain Log Server consists of Domain Log Servers that store and process logs from Security Gateways that are managed by the corresponding Domain Management Servers. Acronym: MDLS.

Multi-Domain Server
Dedicated Check Point server that runs Check Point software to host virtual Security Management Servers called Domain Management Servers. Synonym: Multi-Domain Security Management Server. Acronym: MDS.

N

NAC
Network Access Control. This is an approach to computer security that attempts to unify endpoint security technology (such as Anti-Virus, Intrusion Prevention, and Vulnerability Assessment), user or system authentication and network security enforcement. Check Point's Network Access Control solution is called Identity Awareness Software Blade.

Network Object
Logical object that represents different parts of corporate topology - computers, IP addresses, traffic protocols, and so on. Administrators use these objects in Security Policies.

Network Policy Management
Check Point Software Blade on a Management Server to manage an on-premises environment with an Access Control and Threat Prevention policies.

O

Open Server
Physical computer manufactured and distributed by a company, other than Check Point.

P

PDP
Check Point Identity Awareness Security Gateway that acts as Policy Decision Point: acquires identities from identity sources; shares identities with other gateways.

PEP
Check Point Identity Awareness Security Gateway that acts as Policy Enforcement Point: receives identities via identity sharing; redirects users to Captive Portal.

Provisioning
Check Point Software Blade on a Management Server that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: SmartProvisioning, SmartLSM, Large-Scale Management, LSM.

Publisher PDP
Check Point Identity Awareness Security Gateway that gets identities from an identity source/remote PDP and shares identities to a remote PDP. The Publisher PDP: (1) Initiates an HTTPS connection to the Subscriber PDP for each Identity to be shared (2) Verifies the CN and OU present in the subject field of the certificate presented (3) Verifies that the CA's certificate matches the certificate that was approved in advance by the administrator (4) Checks if the certificate presented is revoked (5) Shares identities including the information about user(s), machine(s) and Access Roles in the form of HTTP POST requests.

Q

QoS
Check Point Software Blade on a Security Gateway that provides policy-based traffic bandwidth management to prioritize business-critical traffic and guarantee bandwidth and control latency.

R

Rule
Set of traffic parameters and other conditions in a Rule Base (Security Policy) that cause specified actions to be taken for a communication session.

Rule Base
All rules configured in a given Security Policy. Synonym: Rulebase.

S

SecureXL
Check Point product on a Security Gateway that accelerates IPv4 and IPv6 traffic that passes through a Security Gateway.

Security Gateway
Dedicated Check Point server that runs Check Point software to inspect traffic and enforce Security Policies for connected network resources.

Security Management Server
Dedicated Check Point server that runs Check Point software to manage the objects and policies in a Check Point environment within a single management Domain. Synonym: Single-Domain Security Management Server.

Security Policy
Collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.

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

SIC
Secure Internal Communication. The Check Point proprietary mechanism with which Check Point computers that run Check Point software authenticate each other over SSL, for secure communication. This authentication is based on the certificates issued by the ICA on a Check Point Management Server.

SmartConsole
Check Point GUI application used to manage a Check Point environment - configure Security Policies, configure devices, monitor products and events, install updates, and so on.

SmartDashboard
Legacy Check Point GUI client used to create and manage the security settings in versions R77.30 and lower. In versions R80.X and higher is still used to configure specific legacy settings.

SmartProvisioning
Check Point Software Blade on a Management Server (the actual name is "Provisioning") that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: Large-Scale Management, SmartLSM, LSM.

SmartUpdate
Legacy Check Point GUI client used to manage licenses and contracts in a Check Point environment.

Software Blade
Specific security solution (module): (1) On a Security Gateway, each Software Blade inspects specific characteristics of the traffic (2) On a Management Server, each Software Blade enables different management capabilities.

Standalone
Configuration in which the Security Gateway and the Security Management Server products are installed and configured on the same server.

Subscriber PDP
Check Point Identity Awareness Security Gateway that gets identities from a remote PDP. The Subscriber PDP: (1) Presents the configured SSL certificate to the Publisher PDP (2) Receives the information from the Publisher PDP after verifying the pre-shared secret in the POST requests.

T

Terminal Servers Identity Agent
Dedicated client agent installed on Microsoft® Windows-based application server that hosts Terminal Servers, Citrix XenApp, and Citrix XenDesktop services. This client agent acquires and reports identities to the Check Point Identity Awareness Security Gateway. In the past, this client agent was called Multi-User Host (MUH) Agent. You can download the Terminal Servers Identity Agent from Support Center.

Threat Emulation
Check Point Software Blade on a Security Gateway that monitors the behavior of files in a sandbox to determine whether or not they are malicious. Acronym: TE.

Threat Extraction
Check Point Software Blade on a Security Gateway that removes malicious content from files. Acronym: TEX.

Transactions
In the context of the Identity Collector, involves the aggregation of events from identity sources, the creation of a request, and the sending of this request to a target. The target then replies with a response. A transaction refers to this request-response.

U

Updatable Object
Network object that represents an external service, such as Microsoft 365, AWS, Geo locations, and more.

URL Filtering
Check Point Software Blade on a Security Gateway that allows granular control over which web sites can be accessed by a given group of users, computers or networks. Acronym: URLF.

User Directory
Check Point Software Blade on a Management Server that integrates LDAP and other external user management servers with Check Point products and security solutions.

V

VSX
Virtual System Extension. Check Point virtual networking solution, hosted on a computer or cluster with virtual abstractions of Check Point Security Gateways and other network devices. These Virtual Devices provide the same functionality as their physical counterparts.

VSX Gateway
Physical server that hosts VSX virtual networks, including all Virtual Devices that provide the functionality of physical network devices. It holds at least one Virtual System, which is called VS0.

Z

Zero Phishing
Check Point Software Blade on a Security Gateway (R81.20 and higher) that provides real-time phishing prevention based on URLs. Acronym: ZPH.