How to Troubleshoot Identity Awareness Issues

18 September 2011
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.

Latest Documentation
The latest version of this document is at: http://supportcontent.checkpoint.com/documentation_download?ID=12625
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>18 September 2011</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments
(mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on How to Troubleshoot Identity Awareness Issues ).
Important Information .................................................................................. 3
How to Troubleshoot Identity Awareness Issues ............................................. 5
Objective .................................................................................................. 5
  Impact on the Environment and Warnings ................................................. 5
  Supported OS ......................................................................................... 5
  Supported Appliances ............................................................................ 5
Before You Start ....................................................................................... 5
  Related Documentation ......................................................................... 5
  Assumed Knowledge ............................................................................ 5
Troubleshooting General AD Integration .................................................... 6
  User Groups and Access Roles are Not Enforced or Logged .................... 6
  Users Fail to Authenticate .................................................................... 6
Troubleshooting AD Query ......................................................................... 6
  Users are Not Detected .......................................................................... 6
  AD Query Fails to Connect to Domain Controllers .................................. 7
  Not All Users are Detected .................................................................... 7
  Small Number of Users are Detected ..................................................... 7
  A Service User is Connected to an IP Address ......................................... 7
  Multiple Users are Connected to Same IP Address ................................. 8
  SmartView Tracker User Name and Group Membership Error Messages ... 8
Troubleshooting Identity Awareness Configuration Wizard ........................ 8
  SmartDashboard Fails to Connect .......................................................... 8
  WMI (DCE-RPC) Test Failed ................................................................... 8
  LDAP Connectivity Failed ..................................................................... 9
  Using the Wizard Again to Create Other Domains .................................... 9
Troubleshooting Access Roles .................................................................... 10
  Domain Users or Groups Do Not Appear in the List ................................ 10
  Slow AD Tree ....................................................................................... 10
Troubleshooting Captive Portal .................................................................. 10
  Server Not Found or a Clear Screen ........................................................ 10
  Endless Redirect Loop .......................................................................... 11
  Portal Enters a Loop when Agent is Connected ...................................... 12
  Client IP Address Identified Incorrectly .................................................. 12
  Cannot Authenticate With Correct Credentials ...................................... 12
  Changes in Portal Settings are Not Seen ................................................ 12
  Identity Agent is Installed But Get the Captive Portal .............................. 13
  Captive Portal Bad Appearance .............................................................. 13
Troubleshooting Identity Agent .................................................................. 13
  Agent Fails to Connect to Server ............................................................ 13
  Kerberos Does Not Work ....................................................................... 14
  Kerberos Does Not Work for All Users .................................................. 14
  Kerberos Does Not Work for One User ................................................. 14
Troubleshooting Distributed Environments ................................................. 15
  User Access Based on Identity Agent Works But Not AD Query ............. 15
  Identities are Not Propagated to the Identity Server ............................... 15
Index ....................................................................................................... 17
How to Troubleshoot Identity Awareness Issues

Objective

This document explains how to troubleshoot Identity Awareness issues. Identity Awareness lets you easily configure in SmartDashboard network access and auditing based on network location and:

- The identity of a user
- The identity of a machine

When Identity Awareness identifies a source or destination, it shows the IP address of the user or machine with a name.

Impact on the Environment and Warnings

- Check Point R75 and higher

Supported OS

- SecurePlatform
- IPSO

Supported Appliances

- UTM-270 and higher

Before You Start

Related Documentation

- R75 Identity Awareness Administration Guide
  (http://supportcontent.checkpoint.com/documentation_download?ID=11662)
- R75.20 Identity Awareness Administration Guide
  (http://supportcontent.checkpoint.com/documentation_download?ID=12268)

Assumed Knowledge

- Use of Identity Awareness
- Use of Active Directory
Troubleshooting General AD Integration

User Groups and Access Roles are Not Enforced or Logged

**Issue**
Users are identified successfully, but their user groups and Access Roles are not enforced or logged correctly.

**Solution**
1. Make sure that there is one LDAP Account Unit for each AD domain. If you must configure domain controllers for each gateway (for AD Query for example), see the Advanced AD Query section in the R75.20 Identity Awareness Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=12268).
2. If the configured user group is the primary group for the user account, there is no solution. Workaround: Change the AD account to be a member of the group.

Users Fail to Authenticate

**Issue**
Users fail to authenticate in Captive Portal or Identity Agent and the user name and password are correct.

**Solution**
1. Make sure that the user's account is not locked or expired.
2. If there are multiple accounts with the same user name, the AD user must authenticate with domain\user. For example, CORP.ACME.COM\jdoe. This can occur in organizations with multiple AD domains or in an AD domain and internal user database.

Troubleshooting AD Query

Users are Not Detected

**Issue**
AD Query is connected successfully to all domain controllers, but users are not detected. Furthermore, there are some events in SmartView Monitor.

**Solution**
Make sure that the necessary auditing logs are generated on the Security Event log of the domain controllers.
- On 2003 domain controllers the events are 672, 673, and 674.
- On 2008 domain controllers the events are 4624, 4768, 4769, and 4770.
AD Query Fails to Connect to Domain Controllers

Issue
AD Query fails to connect to the domain controllers. You can see this in SmartView Tracker, SmartView Monitor or you can run `adlog a dc` in expert mode.

Solution

Not All Users are Detected

Issue
Not all users are detected.

Solution
AD Query must be configured to communicate with the actual domain controller that the user is connected to. This is necessary because security event logs are not replicated.

Make sure that the domain controller that the user is connected to belongs to the AD Query account unit.

You can use `echo %LOGONSERVER%`

If AD Query was configured through the wizard and the SmartDashboard computer is not a member of the domain, then only one domain controller is entered into the LDAP Account unit.

Small Number of Users are Detected

Issue
AD Query is successfully connected to the domain controllers and receives events, but the number of users detected is relatively low. Numbers detected can be seen in SmartView Monitor or with `adlog a query all`.

Solution
1. Make sure that users / IP addresses are not ignored. You can configure this in SmartDashboard.
2. Make sure that users do not go through a NAT (with Check Point NAT) to the firewall. If the events in the security event log are generated with a NAT IP address, they will be ignored automatically.

NAT is not supported by AD Query.

A Service User is Connected to an IP Address

Issue
AD Query shows that a different user is connected to a user's IP address. This can be a service user (for example, an anti virus company name) that is connected besides the actual user.

Solution
AD Query does not know the difference between an actual user that logged in and a service account that logged in from the same computer. You can filter service accounts in SmartDashboard.

To learn more about filtering service accounts, see the R75.20 Identity Awareness Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=12268).
Multiple Users are Connected to Same IP Address

**Issue**
After a user logs off and a different user logs on, AD Query still thinks that both users are connected.

**Solution**
AD Query aggregates users and permissions. Only after the first user’s session is timed out, the user’s session is revoked. To change this behavior, you can configure the Assume only one user per machine option in SmartDashboard. This option requires that you also ignore the service account.

To learn more about assuming only one user for a machine, see the R75.20 Identity Awareness Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=12268).

SmartView Tracker User Name and Group Membership Error Messages

**Issue**
SmartView Tracker error messages show that the gateway could not fetch group membership for users and the user names contain non-English characters.

**Solution**
In GuiDBedit, enable the EnableUnicode attribute on the LDAP account unit.


Troubleshooting Identity Awareness Configuration Wizard

SmartDashboard Fails to Connect

**Issue**
The Identity Awareness Configuration Wizard fails to open. A message states that “SmartDashboard failed to connect to...”. The error message starts with SmartDashboard and not gateway.

**Solution**

WMI (DCE-RPC) Test Failed

**Issue**
The Identity Awareness Configuration Wizard fails. An error message states WMI(DCE-RPC) test failed or shows an equivalent message.

AD Query is configured, but users are not identified in logs and cannot get access based on their identity.

In SmartView Monitor or with the adlog a dc command line in Expert mode, you see domain controllers that the Security Gateway fails to connect to.
Solution

LDAP Connectivity Failed

Issue
There are two parts to this issue:
1. The Identity Awareness Configuration Wizard fails stating that LDAP connectivity failed. This also occurs when the administrator has selected a working account unit in it.
2. LDAP connectivity test fails without an obvious cause and only LDAP over SSL is supported on the domain controllers.

Solution
The Identity Awareness Configuration Wizard works only with LDAP (not LDAPS). It disregards the use ssl option on the account unit. If LDAP (as opposed to LDAPS) is disabled, the wizard fails and the administrator needs to configure the account unit manually.

Using the Wizard Again to Create Other Domains

Issue
An administrator wants to use the wizard again to create other domains.

Solution
Clear the Enable Identity Awareness checkbox in SmartDashboard and then select it again. This selection will rerun the wizard.

Login DN and AD Forest Errors

Issue
Identity Awareness Configuration Wizard fails, possibly stating that it:
- Could not fill in the Login DN parameter in the LDAP Account Unit
- The customer Active Directory forest contains more than one Active Directory Domain

Solution
Learn more about configuring Identity Awareness for forests with more than one domain (usually subdomains), see the R75.20 Identity Awareness Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=12268).
Troubleshooting Access Roles

Domain Users or Groups Do Not Appear in the List

Issue
There is a red X on the domain name and no domain users or groups are available in the list.

Solution
Make sure that SmartDashboard has a working connection to the domain controller.

Slow AD Tree

Issue
The AD tree is slow to show results.

Solution
This occurs when there are many sibling folders in the AD tree. There is no solution for this issue.

Troubleshooting Captive Portal

Server Not Found or a Clear Screen

Issue
Browsing to http://www.myIAServer.com/connect shows “Server Not Found” or a clear screen.

Solution
Make sure you configured Identity Awareness correctly:

- Did you enable Identity Awareness?
- Did you connect to the correct URL?
- Did you configure DNS?
- Did you define a rule and install policy?
Endless Redirect Loop

Issue
There is an endless redirect loop when this environment is deployed.

Solution
1. Prevent this type of environment when possible.
2. Add the Captive Portal as an exception in the browser proxy settings.
Portal Enters a Loop when Agent is Connected

**Issue**
If a user is revoked from the system, the client machine can enter an endless loop when trying to browse to a web site. The loop occurs since the gateway is redirecting to the Captive Portal and the Captive Portal assumes that the agent is connected and directs the web browser to the original URL.

**Solution**
You should know about this problem. Don’t revoke an IP in this situation.

Client IP Address Identified Incorrectly

**Issue**
The client IP address is identified incorrectly.

**Solution**
All clients that go through the proxy are reported with the proxy IP address and not their own IP address.
Work with x-forwarded-for to:
- Make sure that the proxy is configured to send x-forwarded-for in its header.
- Make sure that APPI (Application Control) is running. APPI is the component that reads this header.

Cannot Authenticate With Correct Credentials

**Issue**
You cannot authenticate with correct credentials.

**Solution**
1. Are your credentials in English only?
   - If not – make sure you enabled the SupportUnicode field in the LDAP account unit server object with GuiDBedit.
     - Use the GuiDBedit command:
     ```
     modify servers <ldap au name> SupportUnicode 'true'
     ```
     To learn more, see sk32030 (http://supportcontent.checkpoint.com/solutions?id=sk32030).

2. Make sure that pdpd is running.

3. Use domain\user when you have more than one account with the same name.

Changes in Portal Settings are Not Seen

**Issue**
After you customize portal images or other customization changes, you do not see the changes in the portal or the web browser.
Identity Agent is Installed But Get the Captive Portal

**Issue**
The Identity Agent has been installed on my computer, but I keep getting the Captive Portal.

**Solution**
Make sure the Identity Agent is:
- Working
- Connected
- Authenticated

If you use an Internet Explorer browser, when you are connected and authenticated you are redirected to your initial destination. Other browsers do not work like this.

Captive Portal Bad Appearance

**Issue**
The Captive Portal looks bad.

**Solution**
1. Make sure you are using a supported browser:
   - Internet Explorer 6,7,8
   - Safari 5
   - Firefox 3
   - Chrome 8
2. Reload the portal page in your browser

Troubleshooting Identity Agent

Agent Fails to Connect to Server

**Issue**
The umbrella icon on a user's computer is closed and the agent fails to connect to the server.

**Solution**
Do these steps until one works.
1. Try to configure the gateway manually.
2. Make sure the gateway's discovery configuration is correct.
3. If the problem is only for one computer, make sure the DNS settings and network configuration are correct.

4. Reset Agent settings:
   a) Double-click the umbrella icon.
   b) Go to Advanced > Reset to defaults and try to connect.

5. Restart the service:
   a) Open a command line with computer administrator credentials.
   b) Enter `sc stop madservice` and then `sc start madservice`

6. If no users can connect with the Identity Agent, make sure the gateway uses an internal interface to communicate with the client. It not, change this setting from Identity Awareness gateway properties > Identity Agent Settings.

Kerberos Does Not Work

Issue
Kerberos does not work on this network.

Solution
1. Read the Kerberos section in the R75.20 Identity Awareness Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=12268) and do the steps carefully.
2. Make sure that you enter the KTPass command manually and not with copy and paste.
3. Make sure you have the same output.
4. If you did all of the steps and it never worked, delete the user and follow the steps in the R75.20 Identity Awareness Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=12268).

Kerberos Does Not Work for All Users

Issue
Kerberos does not work for all users.

Solution
1. Make sure the date and time on the server is correct including daylight savings time.
2. Make sure the gateway Kerberos user is not locked out.
3. Reset the user password on the domain controller.
4. Make sure the account is not disabled.

Kerberos Does Not Work for One User

Issue
Kerberos Does Not Work for One User

Solution
1. Make sure the user's time and date are synchronized with the Kerberos server and the Identity Server (including Day Lights Saving).
2. Make sure the user is not locked out.
3. Make sure the user has a Kerberos ticket.
4. If you recently changed the gateway Kerberos user password, log out and then log in again.
Troubleshooting Distributed Environments

User Access Based on Identity Agent Works But Not AD Query

**Issue**
A user is authenticated based on Identity Agent but not with AD Query.

**Solution**
1. Make sure that AD Query is configured correctly (adlog utility).
2. Make sure the user is in the AD Query database using the adlog utility.
3. Make sure communication has been established between the Identity Server and Identity Gateway (use `pdp` and `pep` commands).
4. If the user is in the AD Query database but is not in the Identity Gateway database (use `pep show user all`)
   a) Issue a "sync" between the Identity Server and Identity Gateway (use `pdp control sync`).
   b) Make sure the user is in the Identity Gateway (use `pep show user all`).

Identities are Not Propagated to the Identity Server

**Issue**
The Identity Server that is set to share identities is not getting identities.

**Solution**
1. Make sure that the daemons `pepd` and `pdpd` are up and running.
2. Make sure that the Identity Server is configured to connect to the Identity Gateway (run `pdp c p` on the Identity Server).
3. Make sure that communication is possible to the main IP address of the remote gateway in both directions. Do this with a ping from one gateway to the other gateway's main IP. If you are testing connectivity from the Identity Server, then the remote gateway is the Identity Gateway and vice-versa.
4. If communication is not possible through the main IP address, use sk60701 ([http://supportcontent.checkpoint.com/solutions?id=sk60701](http://supportcontent.checkpoint.com/solutions?id=sk60701)). This instructs you how to change the IP address used for the communication channel.
A
A Service User is Connected to an IP Address • 7
AD Query Fails to Connect to Domain Controllers • 7
Agent Fails to Connect to Server • 13
Assumed Knowledge • 5
B
Before You Start • 5
C
Cannot Authenticate With Correct Credentials • 12
Captive Portal Bad Appearance • 13
Changes in Portal Settings are Not Seen • 12
Client IP Address Identified Incorrectly • 12
D
Domain Users or Groups Do Not Appear in the List • 10
E
Endless Redirect Loop • 11
H
How to Troubleshoot Identity Awareness Issues • 5
I
Identities are Not Propagated to the Identity Server • 15
Identity Agent is Installed But Get the Captive Portal • 13
Impact on the Environment and Warnings • 5
Important Information • 3
K
Kerberos Does Not Work • 14
Kerberos Does Not Work for All Users • 14
Kerberos Does Not Work for One User • 14
L
LDAP Connectivity Failed • 9
Login DN and AD Forest Errors • 9
M
Multiple Users are Connected to Same IP Address • 8
N
Not All Users are Detected • 7
O
Objective • 5
P
Portal Enters a Loop when Agent is Connected • 12
R
Related Documentation • 5
S
Server Not Found or a Clear Screen • 10
Slow AD Tree • 10
Small Number of Users are Detected • 7
SmartDashboard Fails to Connect • 8
SmartView Tracker User Name and Group Membership Error Messages • 8
Supported Appliances • 5
Supported OS • 5
T
Troubleshooting Access Roles • 10
Troubleshooting AD Query • 6
Troubleshooting Captive Portal • 10
Troubleshooting Distributed Environments • 14
Troubleshooting General AD Integration • 6
Troubleshooting Identity Agent • 13
Troubleshooting Identity Awareness Configuration Wizard • 8
U
User Access Based on Identity Agent Works But Not AD Query • 15
User Groups and Access Roles are Not Enforced or Logged • 6
Users are Not Detected • 6
Users Fail to Authenticate • 6
Using the Wizard Again to Create Other Domains • 9
W
WMI (DCE-RPC) Test Failed • 8