Agent Download Issues on Client Machine

Problem

The client machine browser displays a “no policy matched” error message after user authentication and authorization. This issue applies to user sessions during the client provisioning phase of authentication.

Possible Causes

The client provisioning policy is missing required settings.

Posture Agent Download Issues

Remember that downloading the posture agent installer requires the following:

- The user must allow the ActiveX installer in the browser session the first time an agent is installed on the client machine. The client provisioning download page prompts for this.
- The client machine must have Internet access.

Resolution

- Ensure that a client provisioning policy exists in Cisco ISE. If yes, verify the policy identity group, conditions, and type of agent defined in the policy. Also ensure whether or not there is any agent profile configured under **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources** > **Add** > **NAC or AnyConnect Posture Profile**, even a profile with all default values.
- Try re-authenticating the client machine by bouncing the port on the access switch.

- Endpoints, on page 1
- Session Trace for an Endpoint, on page 8
- Global Search for Endpoints, on page 10

Endpoints

These windows enable you to configure and manage endpoints that connect to your network.

Endpoint Settings

Table 1: Endpoint Settings

Field Name	Usage Guidelines
MAC Address	Enter the MAC address in hexadecimal format to create an endpoint statically. The MAC address is the device identifier for the interface that is connected to the Cisco ISE enabled network.
Static Assignment	Check this check box when you want to create an endpoint statically in the Endpoints window and the status of static assignment is set to static. You can toggle the status of static assignment of an endpoint from static to dynamic or from dynamic to static.
Policy Assignment	(Disabled by default unless the **Static Assignment** is checked) Choose a matching endpoint policy from the **Policy Assignment** drop-down list. You can do one of the following: • If you do not choose a matching endpoint policy, but use the default endpoint policy Unknown, then the static assignment status is set to dynamic for the endpoint that allows dynamic profiling of an endpoint. • If you choose a matching endpoint policy other than Unknown, then the static assignment status is set to static for that endpoint and the **Static Assignment** check box is automatically checked.
Static Group Assignment	Check this check box when you want to assign an endpoint to an identity group statically. In you check this check box, the profiling service does not change the endpoint identity group the next time during evaluation of the endpoint policy for these endpoints, which were previously assigned dynamically to other endpoint identity groups. If you uncheck this check box, then the endpoint identity group is dynamic as assigned by the ISE profiler based on policy configuration. If you do not choose the Static Group Assignment option, then the endpoint is automatically assigned to the matching identity group the next time during evaluation of the endpoint policy.

Field Name	Usage Guidelines

Identity Group Assignment	Choose an endpoint identity group to which you want to assign the endpoint.
	You can assign an endpoint to an identity group when you create an endpoint statically, or when you do not want to use the **Create Matching Identity Group** option during evaluation of the endpoint policy for an endpoint.
	Cisco ISE includes the following system created endpoint identity groups:
	• Blacklist
	• GuestEndpoints
	• Profiled
	  • Cisco IP-Phone
	  • Workstation
	• RegisteredDevices
	• Unknown

Related Topics

Identified Endpoints
Create Endpoints with Static Assignments of Policies and Identity Groups

Endpoint Import from LDAP Settings

Table 2: Endpoint Import from LDAP Settings

Field Name	Usage Guidelines
Connection Settings	
Host	Enter the hostname, or the IP address of the LDAP server.
Port	Enter the port number of the LDAP server. You can use the default port 389 to import from an LDAP server, and the default port 636 to import from an LDAP server over SSL. **Note** Cisco ISE supports any configured port number. The configured value should match the LDAP server connection details.
Enable Secure Connection	Check the **Enable Secure Connection** check box to import from an LDAP server over SSL.
Root CA Certificate Name	Click the drop-down arrow to view the trusted CA certificates. The Root CA Certificate Name refers to the trusted CA certificate that is required to connect to an LDAP server. You can add (import), edit, delete, and export trusted CA certificates in Cisco ISE.

Field Name	Usage Guidelines
Anonymous Bind	You must enable either the **Anonymous Bind** check box, or enter the LDAP administrator credentials from the slapd.conf configuration file.
Admin DN	Enter the distinguished name (DN) configured for the LDAP administrator in the slapd.conf configuration file. Admin DN format example: cn=Admin, dc=cisco.com, dc=com
Password	Enter the password configured for the LDAP administrator in the slapd.conf configuration file.
Base DN	Enter the distinguished name of the parent entry. Base DN format example: dc=cisco.com, dc=com.
Query Settings	
MAC Address objectClass	Enter the query filter, which is used for importing the MAC address, for example, ieee802Device.
MAC Address Attribute Name	Enter the returned attribute name for import, for example, macAddress.
Profile Attribute Name	Enter the name of the LDAP attribute. This attribute holds the policy name for each endpoint entry that is defined in the LDAP server. When you configure the **Profile Attribute Name** field, consider the following: • If you do not specify this LDAP attribute in the **Profile Attribute Name** field or configure this attribute incorrectly, then endpoints are marked "Unknown" during an import operation, and these endpoints are profiled separately to the matching endpoint profiling policies. • If you configure this LDAP attribute in the **Profile Attribute Name** field, the attribute values are validated to ensure that the endpoint policy matches with an existing policy in Cisco ISE, and endpoints are imported. If the endpoint policy does not match with an existing policy, then those endpoints will not be imported.
Time Out	Enter the time in seconds. The valid range is from 1 to 60 seconds.

Related Topics

Identified Endpoints
Import Endpoints from LDAP Server

Endpoint Profiling Policies Settings

Table 3: Endpoint Profiling Policies Settings

Field Name	Usage Guidelines
Name	Enter the name of the endpoint profiling policy that you want to create.

Field Name	Usage Guidelines
Description	Enter the description of the endpoint profiling policy that you want to create.
Policy Enabled	By default, the **Policy Enabled** check box is checked to associate a matching profiling policy when you profile an endpoint. When unchecked, the endpoint profiling policy is excluded when you profile an endpoint.
Minimum Certainty Factor	Enter the minimum value that you want to associate with the profiling policy. The default value is 10.
Exception Action	Choose an exception action, which you want to associate with the conditions when defining a rule in the profiling policy. The default is NONE. The exception actions are defined in the following location: **Policy > Policy Elements > Results > Profiling > Exception Actions**.
Network Scan (NMAP) Action	Choose a network scan action from the list, which you want to associate with the conditions when defining a rule in the profiling policy, if required. The default is NONE. The exception actions are defined in the following location: **Policy > Policy Elements > Results > Profiling > Network Scan (NMAP) Actions**.
Create an Identity Group for the policy	Check one of the following options to create an endpoint identity group: • **Yes, create matching Identity Group** • **No, use existing Identity Group hierarchy**
Yes, create matching Identity Group	Choose this option to use an existing profiling policy. This option creates a matching identity group for those endpoints and the identity group will be the child of the Profiled endpoint identity group when an endpoint profile matches an existing profiling policy. For example, the Xerox-Device endpoint identity group is created in the Endpoints Identity Groups page when endpoints discovered on your network match the Xerox-Device profile.

Field Name	Usage Guidelines
No, use existing Identity Group hierarchy	Check this check box to assign endpoints to the matching parent endpoint identity group using hierarchical construction of profiling policies and identity groups. This option allows you to make use of the endpoint profiling policies hierarchy to assign endpoints to one of the matching parent endpoint identity groups, as well as to the associated endpoint identity groups to the parent identity group. For example, endpoints that match an existing profile are grouped under the appropriate parent endpoint identity group. Here, endpoints that match the Unknown profile are grouped under Unknown, and endpoints that match an existing profile are grouped under the Profiled endpoint identity group. For example, • If endpoints match the Cisco-IP-Phone profile, then they are grouped under the Cisco-IP-Phone endpoint identity group. • If endpoints match the Workstation profile, then they are grouped under the Workstation endpoint identity group. The Cisco-IP-Phone and Workstation endpoint identity groups are associated to the Profiled endpoint identity group in the system.
Parent Policy	Choose a parent profiling policy that are defined in the system to which you want to associate the new endpoint profiling policy. You can choose a parent profiling policy from which you can inherit rules and conditions to its child.
Associated CoA Type	Choose one of the following CoA types that you want to associate with the endpoint profiling policy: • No CoA • Port Bounce • Reauth • Global Settings that is applied from the profiler configuration set in Administration > System > Settings > Profiling
Rules	One or more rules that are defined in endpoint profiling policies determine the matching profiling policy for endpoints, which allows you to group endpoints according to their profiles. One or more profiling conditions from the policy elements library are used in rules for validating endpoint attributes and their values for the overall classification.

Field Name	Usage Guidelines
Conditions	Click the plus [+] sign to expand the Conditions anchored overlay, and click the minus [-] sign, or click outside the anchored overlay to close it. Click **Select Existing Condition from Library** or **Create New Condition (Advanced Option)** . **Select Existing Condition from Library**: You can define an expression by selecting Cisco predefined conditions from the policy elements library. **Create New Condition (Advanced Option)**: You can define an expression by selecting attributes from various system or user-defined dictionaries. You can associate one of the following with the profiling conditions: • An integer value for the certainty factor for each condition • Either an exception action or a network scan action for that condition Choose one of the following predefined settings to associate with the profiling condition: • Certainty Factor Increases: Enter the certainty value for each rule, which can be added for all the matching rules with respect to the overall classification. • Take Exception Action: Triggers an exception action that is configured in the Exception Action field for this endpoint profiling policy. • Take Network Scan Action: Triggers a network scan action that is configured in the Network Scan (NMAP) Action field for this endpoint profiling policy.
Select Existing Condition from Library	You can do the following: • You can choose Cisco predefined conditions that are available in the policy elements library, and then use an AND or OR operator to add multiple conditions. • Click the Action icon to do the following in the subsequent steps: • **Add Attribute or Value**: You can add ad-hoc attribute or value pairs • **Add Condition from Library**: You can add Cisco predefined conditions • **Duplicate**: Create a copy of the selected condition • **Add Condition to Library**: You can save ad-hoc attribute/value pairs that you create to the policy elements library • **Delete**: Delete the selected condition.

Field Name	Usage Guidelines

Create New Condition (Advance Option)	You can do the following:
	• You can add ad-hoc attribute/value pairs to your expression, and then use an AND or OR operator to add multiple conditions.
	• Click the Action icon to do the following in the subsequent steps:
	  • **Add Attribute or Value**: You can add ad-hoc attribute or value pairs
	  • **Add Condition from Library**: You can add Cisco predefined conditions
	  • **Duplicate**: Create a copy of the selected condition
	  • **Add Condition to Library**: You can save ad-hoc attribute/value pairs that you create to the policy elements library
	  • **Delete**: Delete the selected condition. You can use the AND or OR operator

Related Topics

Cisco ISE Profiling Service
Create Endpoint Profiling Policies
Endpoint Context Visibility Using UDID Attribute

Endpoint Context Visibility Using UDID Attribute

The Unique Identifier (UDID) is an endpoint attribute that identifies MAC addresses of a particular endpoint. An endpoint can have multiple MAC addresses. For example, one MAC address for the wired interface and another for the wireless interface. The AnyConnect agent generates a UDID for that endpoint, and saves it as an endpoint attribute. The UDID remains constant for an endpoint; the UDID does not change with the AnyConnect installation or uninstallation. When using UDID, **Context Visibility** window (**Context Visibility > Endpoints > Compliance**) displays one entry instead of multiple entries for endpoints with multiple NICs. You can ensure posture control on a specific endpoint rather than on a Mac address.

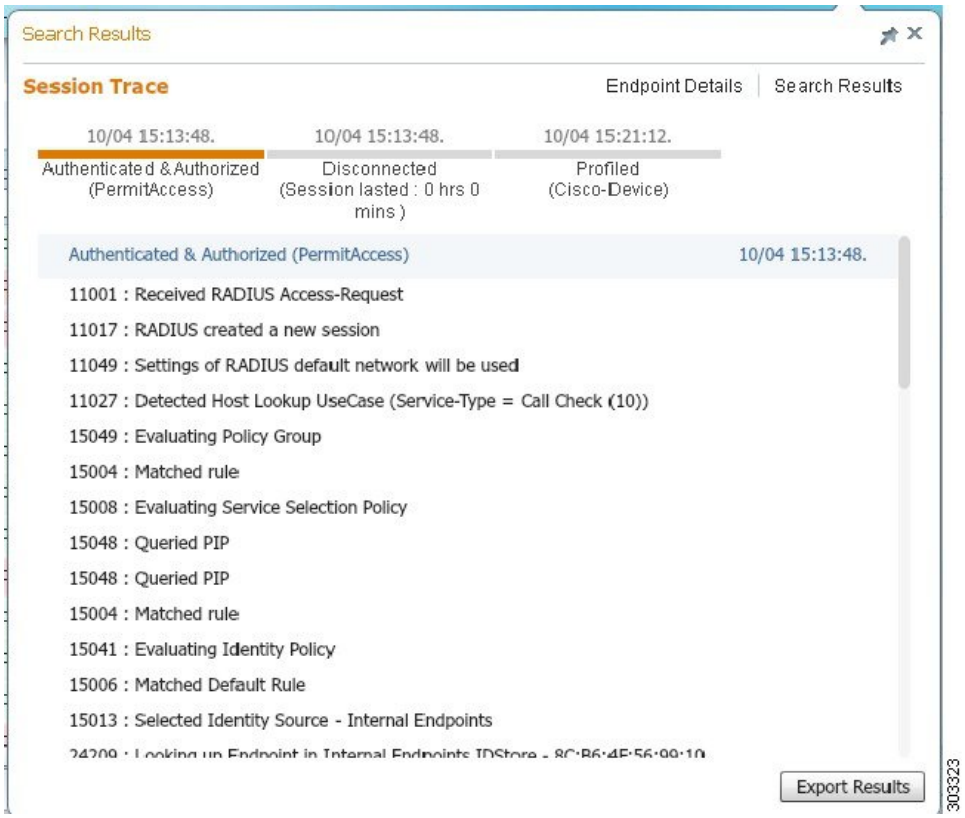
Note The endpoint must have AnyConnect 4.7 or higher to create the UDID.

Session Trace for an Endpoint

You can use the global search box available at the top of the Cisco ISE home page to get session information for a particular endpoint. When you search with a criteria, you get a list of endpoints. Click on any of these endpoints to see the session trace information for that endpoint. The following figure shows an example of the session trace information displayed for an endpoint.

Note The dataset used for search is based on Endpoint ID as indexes. Therefore, when authentication occurs, it is mandatory to have Endpoint IDs for the endpoints for those authentications to include them in the search result set.

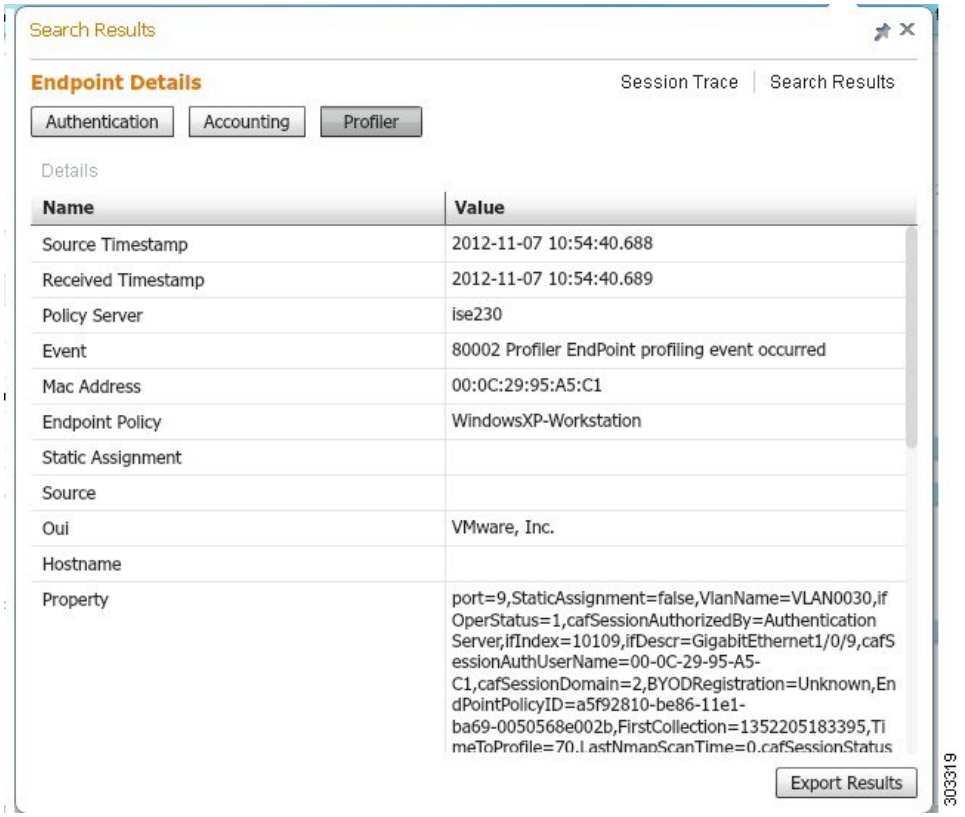
Figure 1: Session Trace of an Endpoint



You can use the clickable timeline at the top to see major authorization transitions. You can also export the results in .csv format by using the **Export Results** option. The report gets downloaded to your browser.

You can click the **Endpoint Details** link to see more authentication, accounting, and profiler information for a particular endpoint. The following figure shows an example of endpoint details information displayed for an endpoint.

Figure 2: Endpoint Details



Session Removal from the Directory

Sessions are cleaned from the session directory on the Monitoring and Troubleshooting node as follows:

- Terminated sessions are cleaned 15 minutes after termination.
- If there is authentication but no accounting, then such sessions are cleared after one hour.
- All inactive sessions are cleared after five days.

Global Search for Endpoints

You can use the global search box available at the top of the Cisco ISE home page to search for endpoints. You can use any of the following criteria to search for an endpoint:

- User name
- MAC Address
- IP Address
- Authorization Profile
- Endpoint Profile

- Failure Reason
- Identity Group
- Identity Store
- Network Device name
- Network Device Type
- Operating System
- Posture Status
- Location
- Security Group
- User Type

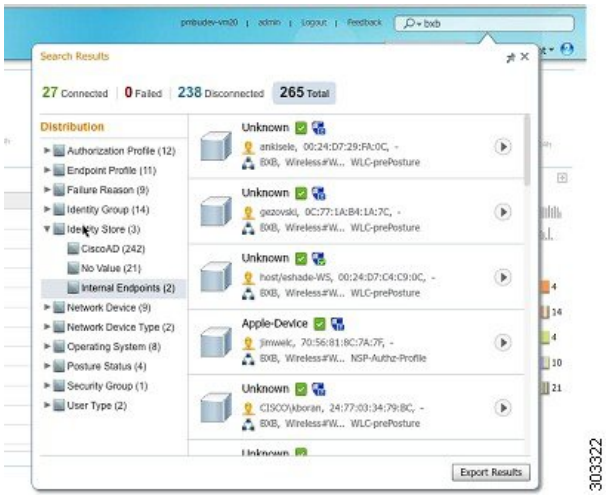
You should enter at least three characters for any of the search criteria in the Search field to display data.

Note If an endpoint has been authenticated by Cisco ISE, or its accounting update has been received, it can be found through the global search. Endpoints that have been manually added and are not authenticated by or accounted for in Cisco ISE will not show up in the search results.

The search result provides a detailed and at-a-glance information about the current status of the endpoint, which you can use for troubleshooting. Search results display only the top 25 entries. You can use filters to narrow down the results.

The following figure shows an example of the search result.

Figure 3: Search Result For Endpoints



You can use any of the properties in the left panel to filter the results. You can also click on any endpoint to see more detailed information about the endpoint, such as:

- Session trace

- Authentication details
- Accounting details
- Posture details
- Profiler details
- Client Provisioning details
- Guest accounting and activity