Table of Contents

About the User Directory Plugin ................................................................. 3
  Endpoint User Details........................................................................... 3
  Verify Endpoint Authentication.......................................................... 3
  User Directory Inventory .................................................................... 4
  HTTP Login Action ............................................................................ 5
  HTTP Sign Out Action ...................................................................... 6
  Guest Management ............................................................................ 6
    Related Documentation .................................................................... 7
  Guest Registration Inventory ............................................................ 8

Supported Servers .................................................................................. 8

Requirements ......................................................................................... 9

Install the Plugin ................................................................................... 9

Configuration ......................................................................................... 10
  Add Servers ....................................................................................... 11
    Microsoft Active Directory Server Settings ................................... 14
    Novell eDirectory, Oracle Directory, IBM Lotus Notes and OpenLDAP Server Settings ................. 15
    RADIUS Server Settings ................................................................. 17
    TACACS Server Settings ................................................................. 18
  Test .................................................................................................. 18
  Replicas ............................................................................................ 19
  Advanced Settings ............................................................................ 20
  Define Additional Servers .................................................................. 22

Working with CounterACT Policies ....................................................... 23
  Detect Endpoints with User Directory Attributes .............................. 23

Display User Directory Information at the Console ............................... 24

Additional CounterACT Documentation ............................................... 25
  Documentation Portal ...................................................................... 26
  Customer Support Portal ................................................................. 26
  CounterACT Console Online Help Tools ............................................ 26
About the User Directory Plugin

The User Directory Plugin resolves endpoint user details and performs endpoint authentication via authentication and directory servers.

The plugin also enables a variety of other features for handling network guests and the sponsors who approve guest access to the network.

Endpoint User Details

The plugin is used to resolve an extensive range of endpoint details, for example the LDAP display name, department name and email addresses. This information is displayed in the Console, Detections pane and in other Console windows.

See Detect Endpoints with User Directory Attributes for more information.

Verify Endpoint Authentication

Use the User Directory Plugin in conjunction with the CounterACT HTTP Login action to verify endpoint authentication to the network.
The action lets you prompt endpoint users to authenticate. Users are presented with a Login page at each attempt to access the network. A valid user name and password must be entered. You can also define the action so that users are prompted to enter the name of the domain server through which they authenticate. Refer to the CounterACT Console User Manual (Working with Actions > Authenticate Actions > HTTP Login) for more information about this action.

User Directory Inventory

Use the plugin to activate the User Directory view in the Inventory tab. The Inventory presents a real-time display of network information, such as user directory information, at multiple levels.
Refer to the CounterACT Console User Manual for information about working in the Inventory view.

**HTTP Login Action**

The plugin activates the *HTTP Login* action. This action is typically used in a Corporate/Guest policy to classify your network into the following CounterACT groups:

- Corporate Hosts
- Signed In Hosts
- Guest Hosts

**HTTP Login** options can be used to prompt users at guest hosts to register with the network. Guest users sign in with valid credentials or register as guests by providing identity information.

Refer to the CounterACT Console User Manual for more information about working with the HTTP Login action and related guest registration options.
HTTP Sign Out Action

The plugin activates the HTTP Sign Out action. This action signs out previously logged-in users when an event, or an operator decision, requires them to log in again. To display the Login window so that the user can sign in again, select the Open sign-in window after authentication checkbox in the HTTP Login action. This action updates the Signed In Status property to Not Signed In.

For example, you can use this action in a policy that requires users to re-authenticate following a specific event, such as a Link Down Trap (Trap Received property).

Guest Management

This plugin enables the CounterACT Guest Management Portal. The portal provides comprehensive tools for managing network guests requesting access to your corporate network.

Corporate sponsors can use the portal for various tasks, including:

- Add, approve, decline or revoke guest access to the network.
- Assign or update network access approval periods.
- Assign tags to guests in order to categorize them. The tags can be used later in CounterACT policies.
To access the Guest Management Portal:

1. Enter the following address in your browser:
   
   https://X.X.X.X/sponsor
   
   where X.X.X.X is the address of your Enterprise Manager or stand-alone Appliance.

   You must define the plugin to work with a Microsoft Active Directory server when using Guest Management Portal. See Microsoft Active Directory Server Settings for details.

   CounterACT operators can work with a range of tools to manage the guest registration and approval process.

Related Documentation

Refer to the Guest Management Portal How-to Guides for sponsors and CounterACT operators for information about working with the portal. These documents are located on the ForeScout, CounterACT User Manuals page.

Refer to the CounterACT Console User Manual for information about working with:

- The HTTP Login action. This action is used to prompt guest registration.
- The Guest Registration feature. This feature is used to define guest parameters, such as password policies or automated sponsor and guest notifications.
Guest Registration Inventory

Use the plugin to activate the Guest Registration view in the Console, Inventory. The Inventory presents a real-time display of network activity at multiple levels.

Refer to the CounterACT Console User Manual for information about working in the Inventory view.

Once the plugin is installed you can also generate reports based on the information shown in the Inventory, Guest Registration display. Refer to the CounterACT Reports Plugin Configuration Guide for information about working with the Guest Registration report.

To work with guest reports verify that the Reports Plugin, version 3.2.0 or above, is installed.

Supported Servers

The following User Directory servers are supported:

- Microsoft Active Directory
- Novell eDirectory
- Oracle Directory
- IBM Lotus Notes
- OpenLDAP Server
You can work with more than one server type simultaneously. For example, if your organization uses Microsoft Active Directory for retrieving user details and a RADIUS server for verifying authentication, you can configure the plugin to work with both these server types.

Requirements

- CounterACT version 7.0.0.
- Service Pack 2.2.0 or above. It is recommended to install the latest service pack to take advantage of the most current CounterACT updates.
- Appliances or an Enterprise Manager must be able to access the User Directory servers.
- You must define a Microsoft Active Directory server when using Guest Management tools. See Guest Management for more information about Guest Management tools.

Install the Plugin

CounterACT is delivered with several bundled plugins, including this plugin. New plugin functionality and supporting data may become available independently between major CounterACT version releases. This section describes how to install the plugin when a new plugin version becomes available between releases.

To install the plugin:

1. Acquire a copy of the plugin in either one of the following ways:
   - If you are installing a Beta release of this plugin, acquire the plugin .fpi file from your ForeScout representative or contact beta@forescout.com.
   - Otherwise, navigate to the Customer Support, Base Plugins page and download the plugin .fpi file.
2. Save the file to the machine where the CounterACT Console is installed.
3. Log into the CounterACT Console and select Options from the Tools menu.
5. Select **Install**. The Open dialog box opens.

6. Browse to and select the saved plugin `.fpi` file.

7. Select **Install**.

8. An installation or upgrade information dialog box and a license agreement dialog box will open. Accept the license agreement to proceed with the installation.

9. Once the installation is complete, select **Close**. The plugin is listed in the Plugins pane.

**Configuration**

A basic User Directory server configuration was most likely carried out via the Console Initial Setup Wizard, which opens when you first log in to the Console. The configuration defined at the Wizard automatically appears in the User Directory pane of the **Options** window.
Procedures for creating additional configurations are described in this document.
You can connect additional User Directory servers to CounterACT components, and
define user and domain credentials, replica servers and other parameters. The
configuration can also be tested.

**Access to Servers**
You may not have the required user Scope permissions to configure User Directory
servers or to work with the IP addresses assigned to them. If this happens you will
receive an error message when attempting configuration. Contact your CounterACT
Administrator if required.

**Add Servers**
This section describes how to define User Directory servers.

**To add User Directory servers:**

1. Log in to the Console and select **Options** from the **Tools** menu. The Options

2. Select **Add**. The Add Server, General pane opens.
**Add Server**

**Name**
Enter the hostname of the server.

**Type**
Select a server type. The wizard displays configuration parameters for the type of server you select.

**Use as directory**
Select to use the server as a directory to retrieve user information.

**Use for authentication**
Select to use the server for user authentication.

**Use for Console Login**
Select to use the server for user authentication when logging in to the Console.

**Include parent groups**
Select to detect the group that the user is a member of, as well as parent groups. Policies with the *User Directory* > *Member Of* property resolve this information.

For Microsoft Active Directory servers, the plugin does not support having both the *Include parent groups* setting and the *Targeted Group Resolution* setting, located in the *Advanced* page/tab, enabled. Attempting to apply such a configuration fails.

**Comment**
Enter comments if required.

3. Select **Next**. The **Settings** pane opens. Parameters in the **Settings** pane vary, depending on the server type that you selected and the plugin features that you enabled. Parameter differences, based on server type, are described.
CounterACT® User Directory Plugin Configuration Guide

Communication

Address/DNS Detection

For a Microsoft Active Directory server, either define the IP address of the server or select the DNS Detection checkbox to instruct CounterACT to learn directory servers based on the domain name that you configure in the Directory section Domain field. For DNS Detection, optionally define the frequency with which the plugin queries domain controller addresses, see Advanced Settings.

Use DNS Detection to have CounterACT automatically learn directory replica addresses. This is recommended in network environments where there are several domain controllers that function as replicas. For all other server types, define the IP address of the server in the Address field.

Port / Use TLS

Enter the server port in the Port field. Select the Use TLS checkbox to instruct CounterACT to use TLS to encrypt communication with the User Directory server. Ensure that TLS communication is supported and enabled on the User Directory server.
Define which CounterACT devices can communicate with the server being configured. The All option is recommended as it enables faster resolution; however, if you select All, make sure that all CounterACT Appliances have access to the server being configured.

Host IP assignments made to a particular Appliance may be out of your user Scope. When this happens, you cannot work with the configuration.

An Appliance marked with an empty red circle indicates that you have no access to any IP addresses managed by the Appliance.

An Appliance marked with a slashed circle indicates that you have access to only a portion of the IP addresses managed by the Appliance. Scope definitions are made by CounterACT administrators in the Console User Profile pane (Tools > Options > Console User Profiles).

Microsoft Active Directory Server Settings
This section describes server details required when working with Microsoft Active Directory Server.
Directory

**Domain**: The domain name (e.g. MyCompany.com).
When the **Communication** section’s **DNS Detection** checkbox is selected, the plugin uses the domain name, defined in the **Domain** field, to automatically learn the addresses of directory servers.
The domain name may contain up to 63 characters. You may use alphanumeric and any of the following special characters:

- `! @ # $ % ^ & ( ) - _ ' { } . ~`

**Characters that are not allowed**:
- `\ * + = | : ; " ? < > ,`
- The first character cannot be a period (.)
- Empty spaces are not allowed

**Administrator**: Credentials to authenticate to the directory for querying other user details.

**Password**: The Administrator’s password.

---

**Additional Domain Aliases** (optional)

Alternative names for the domain being configured.

**None**: A user is looked up in this directory only if its domain name matches the directory domain configured above.

**Any**: A user is looked up in this directory regardless of the user’s domain name.

**Specify**: Specify a comma separated list of domain names. A user is looked up in this directory if its domain name matches one of the listed domain names or the directory domain name configured above.

---

**Novell eDirectory, Oracle Directory, IBM Lotus Notes and OpenLDAP Server Settings**

This section describes details required when working with the following servers:

- Novell eDirectory
- Oracle Directory
- IBM Lotus Notes
- OpenLDAP
You may need to perform advanced configurations when working with these servers. See **Advanced Settings**.

| **Directory** | **Base DN**: The root of the LDAP directory tree where users should be looked up.  
**Administrator Bind DN**: Bind DN of a user allowed to look up other users in the directory.  
**Password**: The Administrator's password.  
**Authentication Bind DN Pattern**: The Authentication Bind DN pattern is used to construct a Bind DN when authenticating a user to the server. The pattern should contain the string `{user}`, which is replaced by a user's name. The constructed string is used as a Bind DN to perform the authentication of a user. Validate by ensuring that an asterisk is included in the string.  
Example: CN={user},ou=user,o=MyCompany |
| **Additional Domain Aliases (optional)** | **None**: A user is looked up in this directory only if its domain name matches the directory domain configured above.  
**Any**: A user is looked up in this directory regardless of the user's domain name.  
**Specify**: Alternative names for the domain being configured.  
Example: Mycompany.com,lab.mycompany.com |
domain name.

**Specify:** Specify a comma separated list of domain names. A user is looked up in this directory if its domain name matches one of the listed domain names or the directory domain name configured above.

### RADIUS Server Settings
This section describes details required when working with RADIUS.

Configure the following parameter:

<table>
<thead>
<tr>
<th>Directory</th>
<th><strong>Shared Secret:</strong> A shared key is used to authenticate the RADIUS transaction. Specify the shared key as defined on the RADIUS server for transactions coming from this CounterACT Appliance</th>
</tr>
</thead>
</table>

![Add Server](image)
**TACACS Server Settings**

This section describes details required when working with TACACS.

Configure the following parameters:

<table>
<thead>
<tr>
<th><strong>Directory</strong></th>
<th><strong>Shared Secret</strong>: A shared key is used to authenticate the TACACS transaction. Specify the shared key as defined on the TACACS server for transactions coming from this CounterACT Appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Authentication Method</strong>: The following authentication methods are available:</td>
</tr>
<tr>
<td></td>
<td>- <strong>CHAP</strong>: A secure challenge response method (Recommended)</td>
</tr>
<tr>
<td></td>
<td>- <strong>PAP</strong>: Plain text method</td>
</tr>
<tr>
<td></td>
<td>- <strong>ASCII</strong>: Clear text method compatible with older TACACS versions</td>
</tr>
</tbody>
</table>

**Test**

Define parameters for testing the connection between the server and the User Directory Plugin. The **Directory** test verifies that information can be resolved for the user name entered. The **Authentication** test verifies user authentication against the credentials provided.

There is no Directory test for RADIUS and TACACS servers.

For Microsoft Active Directory servers, the fields in the Authentication section are populated with the information entered in the Settings page.
**Directory**

*User:* A user name to query. This should be a valid user in the domain.

**Authentication**

*User:* Credentials to test if authentication works.

*Password:* The Administrator’s password.

---

**Replicas**

Specify organizational replica servers to be used as backups if the User Directory server, defined in the **General** page, fails. This configuration is optional.
To add a replica server:

1. Select **Add**. The Add Replica dialog box opens.

2. Enter a replica name and IP address.

3. Indicate which Appliance/Enterprise Manager can access the replica server.

4. Select **OK**. The server that you defined is added to the **Replicas** page.

5. Select **Finish**.

6. The configuration that you defined appears in the **User Directory** pane.

**Advanced Settings**

Advanced settings for a User Directory server can be configured only after the server is added to the User Directory Plugin. These settings cannot be defined using the **Add Server** wizard.
Use Advanced settings as follows:

- Enter **User Filter** and **Query Size** values to match the values of these parameters as defined in your server, if the default values at the server were updated.

- Select **Search and Bind** to perform authentication in scenarios where there are several groups and domains. If your plugin Test indicates *Authentication Failed* you may need to do this.

- Select **Targeted Group Resolution** to have CounterACT optimize the way it retrieves group information. Instead of retrieving a full listing of groups at regular intervals - the default method - the plugin stores primary group IDs and selectively queries for further group information. Use to reduce traffic in enterprise class network environments with complex group hierarchies.

Settings provided in the **Advanced** tab can only be accessed after completing server configuration using the **Add Server** wizard. Advanced settings might not be available for all server types.

**To define advanced settings:**

1. Complete the User Directory Plugin configuration.
2. Select the configuration from the User Directory pane.
3. Select **Edit**. The Edit Server dialog box opens.
4. Select the **Advanced** tab.

![Edit Server Dialog Box](image)
5. Define the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Filter</td>
<td>The attribute used to identify users. For multiple attributes, separate each string with a comma. If the field is empty, the following defaults are used:</td>
</tr>
<tr>
<td></td>
<td>- For Microsoft Active Directory – sAMAccountName</td>
</tr>
<tr>
<td></td>
<td>- For Novell eDirectory – cn or uid</td>
</tr>
<tr>
<td></td>
<td>- For Oracle Directory – uid</td>
</tr>
<tr>
<td></td>
<td>- For IBM Lotus Notes – cn or uid</td>
</tr>
<tr>
<td></td>
<td>- For OpenLDAP Server – cn or uid</td>
</tr>
<tr>
<td></td>
<td>- For Radius/TACACS – Not applicable</td>
</tr>
<tr>
<td>Query Size</td>
<td>This setting applies to Microsoft Active Directory servers only. Decrease this value if you encounter SizeLimit server errors (default is 1000).</td>
</tr>
<tr>
<td>Search and Bind</td>
<td>This setting defines how CounterACT locates users when LDAP Bind DN settings are not configured, and users may be in one of several Organizational Units.</td>
</tr>
<tr>
<td></td>
<td>When this setting is selected, CounterACT binds to the directory as an Admin user and searches the LDAP tree for the username. When the username is found, CounterACT authenticates the user and binds as that user.</td>
</tr>
<tr>
<td>Targeted Group Resolution</td>
<td>This setting applies to Microsoft Active Directory servers only. When selected, CounterACT optimizes its retrieval of group information. Use this option to reduce traffic with Microsoft Active Directory servers in large-scale network environments.</td>
</tr>
<tr>
<td></td>
<td>For newly added servers, this setting is enabled by default. To have CounterACT optimize its retrieval of group information from Microsoft Active Directory servers already configured for the plugin, explicitly enable this setting.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The plugin does not support having both the Targeted Group Resolution setting and the Include parent groups setting, located in the General page/tab, enabled. Attempting to apply such a configuration fails.</td>
</tr>
<tr>
<td>DNS Detection Refresh Interval</td>
<td>This setting applies to Microsoft Active Directory servers only. For use with the DNS Detection feature, see Add Servers, DNS Detection.</td>
</tr>
<tr>
<td></td>
<td>Optionally define the frequency, in seconds, with which the plugin queries domain controller addresses.</td>
</tr>
</tbody>
</table>

**Define Additional Servers**

Typically there are several User Directory servers in a network environment. You can select Add and repeat the procedures of this section to manually define additional servers.
In many cases it is useful to use an existing server profile as the basis for a new server definition. Follow this procedure to duplicate and modify an existing server configuration.

**To base a new server definition on an existing server configuration:**

1. Select the existing server in the User Directory pane and select **Duplicate**.
2. The Edit Server wizard appears. Most fields duplicate the settings of the existing server.
3. Modify the copy to create a new server definition.
   
   You must supply a unique IP address to differentiate this server.

4. Select **OK**. The new server definition appears in the User Directory pane.

## Working with CounterACT Policies

Use CounterACT policy tools to detect endpoints with specific User Directory attributes. For example, create a policy that detects endpoint users in a specific Active Directory department or with a specific distinguished name.

### Detect Endpoints with User Directory Attributes

This section lists User Directory attributes that can be detected on endpoints using a CounterACT policy.

- **Account is Disabled** (Active Directory only)
- **Account is Expired** (Active Directory only)
- **Company** (Active Directory only)
- **Department** (Active Directory only)
- **Display name** (Active Directory only)
- **Distinguished name**
- **Email**
- **Employee number** (Oracle Directory only)
- **Initials**
- **Last name**
- **LDAP user name**
- **Member of**
- **Mobile phone**
- **Password Last Set**
- **Phone**
- **Street address**
• Title (Active Directory only)
• User given name

Refer to the CounterACT Console User Manual for details about working with CounterACT policies.

Display User Directory Information at the Console

Information learned by the User Directory Plugin can be viewed at the Console, Detections pane.
To display/hide information:

1. Right-click a table header from the **Detections** pane.

2. Select **Add/Remove Columns**.

3. Expand the **Properties** node.

4. Select the items related to User Directory information.

5. Should your screen become cluttered, due to numerous, opened columns in the Console, right-click a column and select **Remove Column**.

**Additional CounterACT Documentation**

For more detailed information about the CounterACT features described here or additional CounterACT features and plugins, refer to the following resources:

- [Documentation Portal](#)
- Customer Support Portal
- CounterACT Console Online Help Tools

Documentation Portal
The ForeScout Documentation Portal is a Web-based library containing information about CounterACT tools, features and functionality and integrations.

To access the Documentation Portal:
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

Customer Support Portal
The Customer Support Portal provides links to CounterACT version releases, service packs, plugins and modules as well as related documentation. The portal also provides a variety of How-to Guides, Installation Guides and more.

To access the Customer Support Portal:
2. Select the CounterACT version you want to discover.

CounterACT Console Online Help Tools
Access information directly from the CounterACT Console.

Console Help Buttons
Use context sensitive Help buttons to quickly access information about the tasks and topics you are working with.

Console User Manual
1. Select CounterACT Help from the Help menu.
**Plugin Help files**

1. After the plugin is installed, select **Options** from the **Tools** menu and then select **Plugins**.
2. Select the plugin and then select **Help**.

**Documentation Portal**

1. Select **Documentation Portal** from the **Help** menu.
Legal Notice

Copyright © ForeScout Technologies, Inc. 2000-2017. All rights reserved. The copyright and proprietary rights in this document belong to ForeScout Technologies, Inc. ("ForeScout"). It is strictly forbidden to copy, duplicate, sell, lend or otherwise use this document in any way, shape or form without the prior written consent of ForeScout. All other trademarks used in this document are the property of their respective owners.

These products are based on software developed by ForeScout. The products described in this document are protected by U.S. patents #6,363,489, #8,254,286, #8,590,004, #8,639,800 and #9,027,079 and may be protected by other U.S. patents and foreign patents.

Redistribution and use in source and binary forms are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use acknowledge that the software was developed by ForeScout.

Unless there is a valid written agreement signed by you and ForeScout that governs the below ForeScout products and services:

- If you have purchased any ForeScout products, your use of such products is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you have purchased any ForeScout support service ("ActiveCare"), your use of ActiveCare is subject to your acceptance of the terms set forth at http://www.forescout.com/activecare-maintenance-and-support-policy/;
- If you have purchased any ForeScout Professional Services, the provision of such services is subject to your acceptance of the terms set forth at http://www.forescout.com/professional-services-agreement/;
- If you are evaluating ForeScout’s products, your evaluation is subject to your acceptance of the applicable terms set forth below:
  - If you have requested a General Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/evaluation-license/.
  - If you have requested an Early Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/early-availability-agreement/.
  - If you have requested a Beta Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/beta-test-agreement/.
  - If you have purchased any ForeScout Not For Resale licenses, such license is subject to your acceptance of the terms set forth at http://www.forescout.com/nfr-license/.

Send comments and questions about this document to: documentation@forescout.com

2017-06-29 14:35