ForeScout CounterACT®

Authentication Module: User Directory Plugin

Configuration Guide

Version 6.3

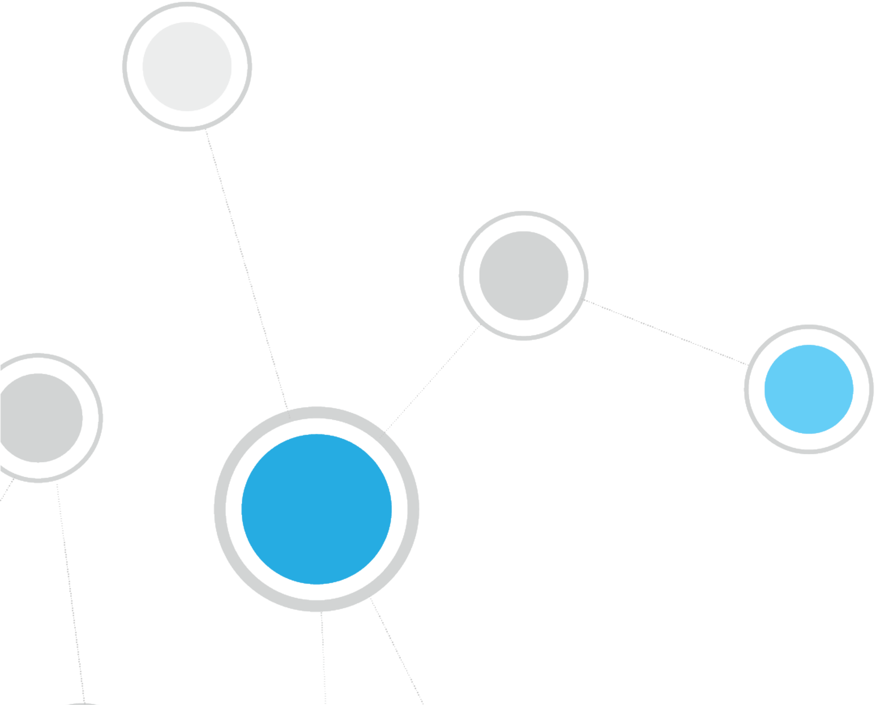


Table of Contents

About the User Directory Plugin

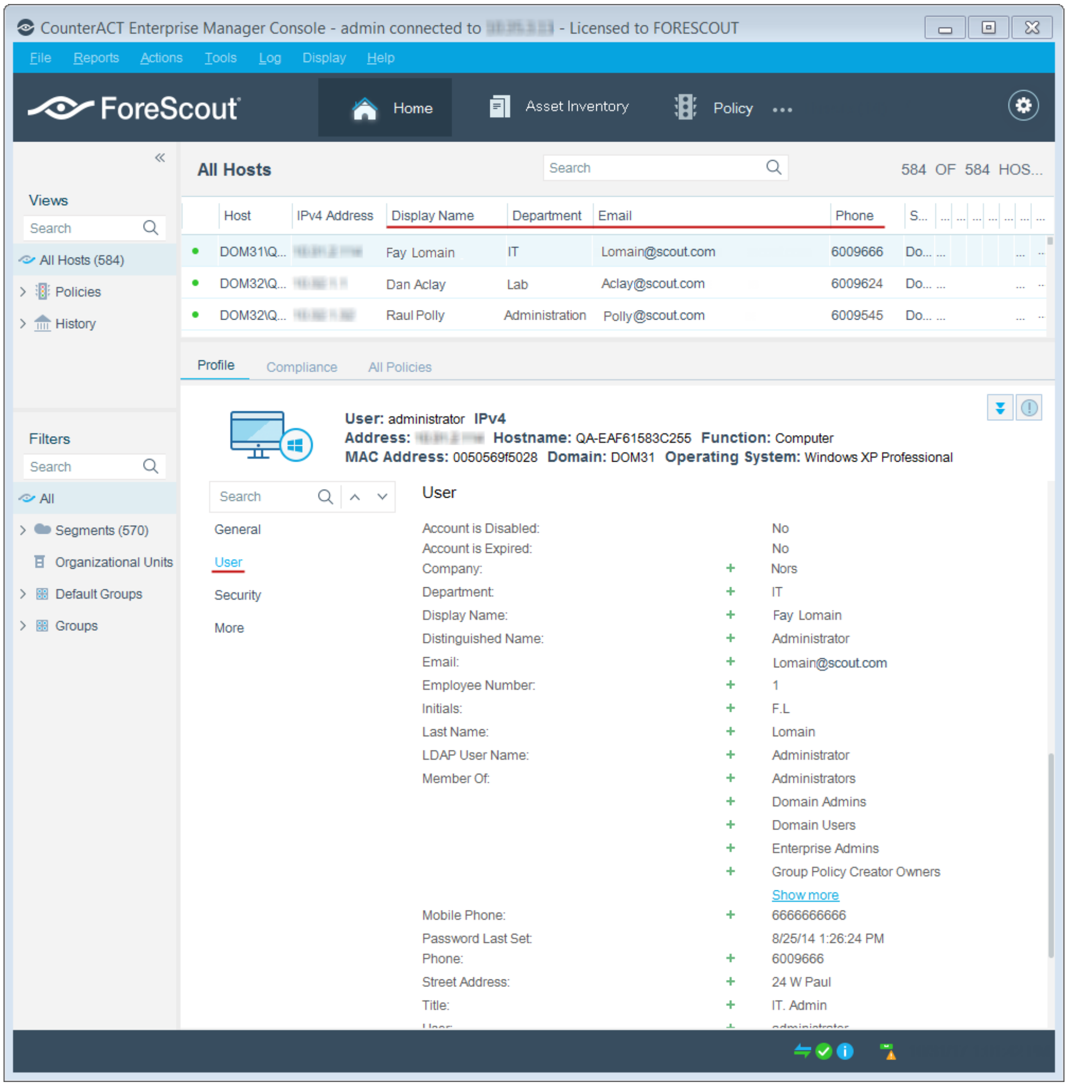
The User Directory Plugin is a component of the ForeScout CounterACT® Authentication Module. See Authentication Module Information for details about the module.

The User Directory Plugin resolves endpoint user details and defines the authentication and directory servers used for endpoint authentication. A real-time display of network information at multiple levels, including user directory information, is available from the Console.

The plugin also enables a variety of other features for handling network guests and the sponsors who approve guest access to the network. These features are described in the *Guest Management Portal How-to Guides* for Sponsors and Operators, and in the *CounterACT Administration Guide*.

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.



CounterACT Enterprise Manager Console - admin connected to [redacted] - Licensed to FORESCOUT

All Hosts — Search — 584 OF 584 HOS...

	Host	IPv4 Address	Display Name	Department	Email	Phone	S...
●	DOM31\Q...	[redacted]	Fay Lomain	IT	Lomain@scout.com	6009666	Do... ...
●	DOM32\Q...	[redacted]	Dan Aclay	Lab	Aclay@scout.com	6009624	Do... ...
●	DOM32\Q...	[redacted]	Raul Polly	Administration	Polly@scout.com	6009545	Do... ...

User: administrator **IPv4 Address:** [redacted] **Hostname:** QA-EAF61583C255 **Function:** Computer
MAC Address: 0050569f5028 **Domain:** DOM31 **Operating System:** Windows XP Professional

User

Account is Disabled:		No
Account is Expired:		No
Company:	+	Nors
Department:	+	IT
Display Name:	+	Fay Lomain
Distinguished Name:	+	Administrator
Email:	+	Lomain@scout.com
Employee Number:	+	1
Initials:	+	F.L
Last Name:	+	Lomain
LDAP User Name:	+	Administrator
Member Of:	+	Administrators
	+	Domain Admins
	+	Domain Users
	+	Enterprise Admins
	+	Group Policy Creator Owners
		Show more
Mobile Phone:	+	6666666666
Password Last Set:		8/25/14 1:26:24 PM
Phone:	+	6009666
Street Address:	+	24 W Paul
Title:	+	IT. Admin

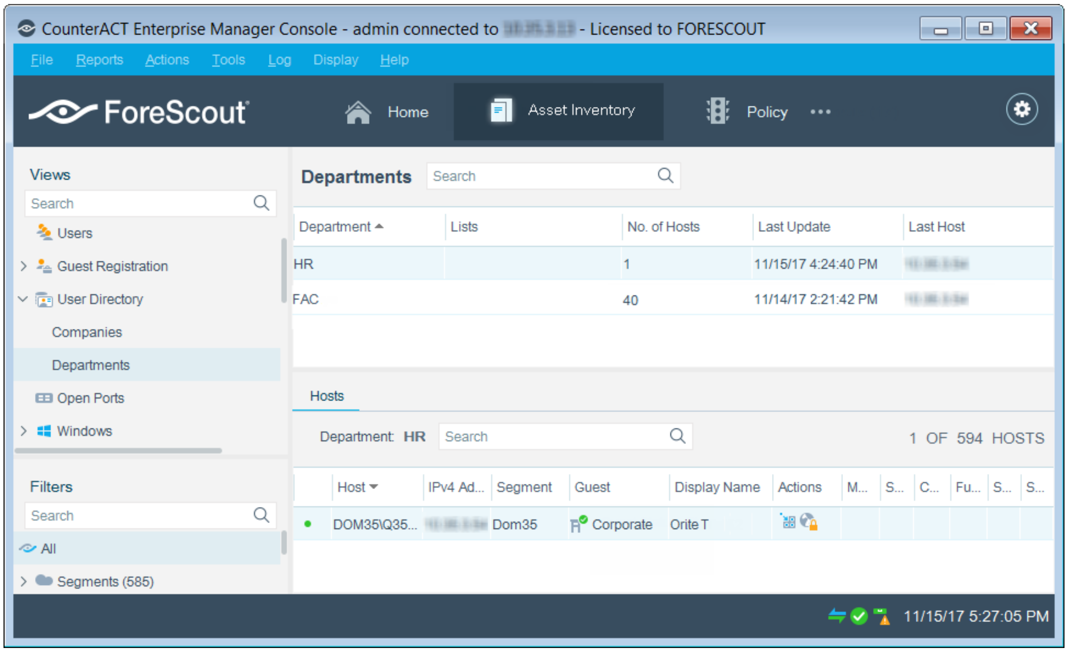
See Detect Endpoints with User Directory Attributes for more information.

Endpoint Authentication

Use the the CounterACT *HTTP Login* action to prompt endpoint users to authenticate. You can define the action so that users at guest hosts and guests are prompted to register with the network before receiving valid credentials. Users are presented with a *Login* page at each attempt to access the network. A valid user name and password must be entered. Refer to the *CounterACT Administration Guide* for more information about this action. See Additional CounterACT Documentation for information on how to access the guide.

User Directory Inventory

The Console Asset Inventory view presents a real-time display of network information, including user directory information, at multiple levels.



Department ▲	Lists	No. of Hosts	Last Update	Last Host
HR		1	11/15/17 4:24:40 PM	[redacted]
FAC		40	11/14/17 2:21:42 PM	[redacted]

Department: HR Search 1 OF 594 HOSTS

Host ▾	IPv4 Ad...	Segment	Guest	Display Name	Actions	M...	S...	C...	Fu...	S...	S...
● DOM35\Q35...	[redacted]	Dom35	Corporate	Orite T							

Refer to the *CounterACT Administration Guide* for information about working in the Asset Inventory view. See Additional CounterACT Documentation for information on how to access the guide.

Related Documentation

Refer to the *Guest Management Portal How-to Guide*s for sponsors and CounterACT operators for information about working with the portal. See Additional CounterACT Documentation for information on how to access these guides.

Refer to the *CounterACT Administration Guide* 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.

Supported Servers

The following user directory and authentication servers are supported:

- Microsoft Active Directory
- Novell eDirectory
- Oracle Directory
- IBM Lotus Notes
- OpenLDAP Server
- RADIUS

- TACACS

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.

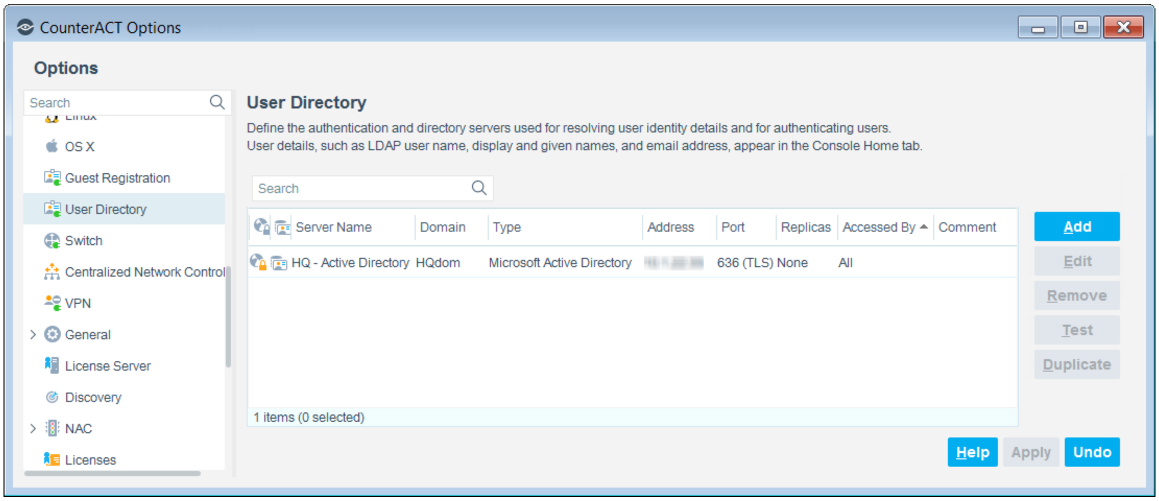
Requirements

The plugin requires the following CounterACT releases and other CounterACT components:

- CounterACT version 8.0.
- Appliances or an Enterprise Manager able to access the User Directory servers.
- An active Maintenance Contract for CounterACT devices.

Configuration

A basic User Directory server configuration was most likely carried out via the Console Initial Setup Wizard, which opens the first time you log in to the Console. The server configuration defined in the Wizard automatically appears in the **User Directory** pane of the **Options** window.



User Directory

Define the authentication and directory servers used for resolving user identity details and for authenticating users.
User details, such as LDAP user name, display and given names, and email address, appear in the Console Home tab.

Server Name	Domain	Type	Address	Port	Replicas	Accessed By	Comment
HQ - Active Directory	HQdom	Microsoft Active Directory	[redacted]	636 (TLS)	None	All	

1 items (0 selected)

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.

Procedures for defining additional server configurations are described in this document. To edit an existing configuration, select the configuration and then select **Edit**.

Access to Servers

User scopes are defined by CounterACT administrators in the **Console User Profile** pane (**Tools** > **Options** > **Console User Profiles**). If you do not have the required user scope permissions to configure User Directory servers or to work with the IP addresses assigned to them, you will receive an error message when attempting configuration. Contact your CounterACT Administrator if required.

Configuring Servers to Work with Certificates

To ensure secure communication, CounterACT can:

- verify certificates presented by external services and applications
- present system certificates to external services and applications for them to authenticate CounterACT

To configure the plugin to use certificates when communicating with a user directory server:

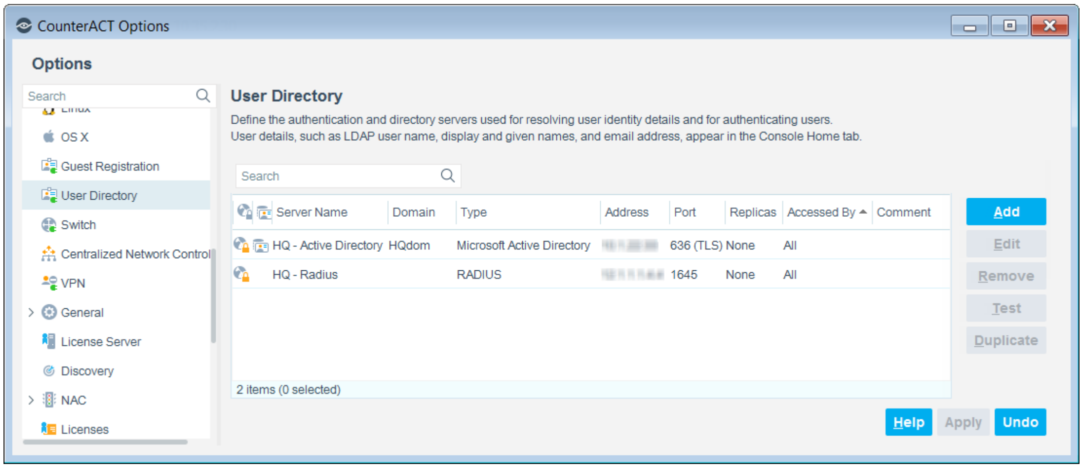
1. Go to Tools > Options > Certificates, and ensure that system and trusted certificates are configured for this scope.
2. In the User Directory Communication settings, set the server port to **636** (or any port configured for secure communication), and select **Use TLS**.
3. Complete the server definitions.
4. After the server is defined, select the server, select Edit > Advanced, and configure the Certificate Settings section.

Define Servers

This section describes how to define User Directory servers.

To add or edit User Directory servers:

1. Log in to the Console and select **Options** from the **Tools** menu. The Options pane opens. Select **User Directory**. The User Directory pane appears.



User Directory

Define the authentication and directory servers used for resolving user identity details and for authenticating users.
User details, such as LDAP user name, display and given names, and email address, appear in the Console Home tab.

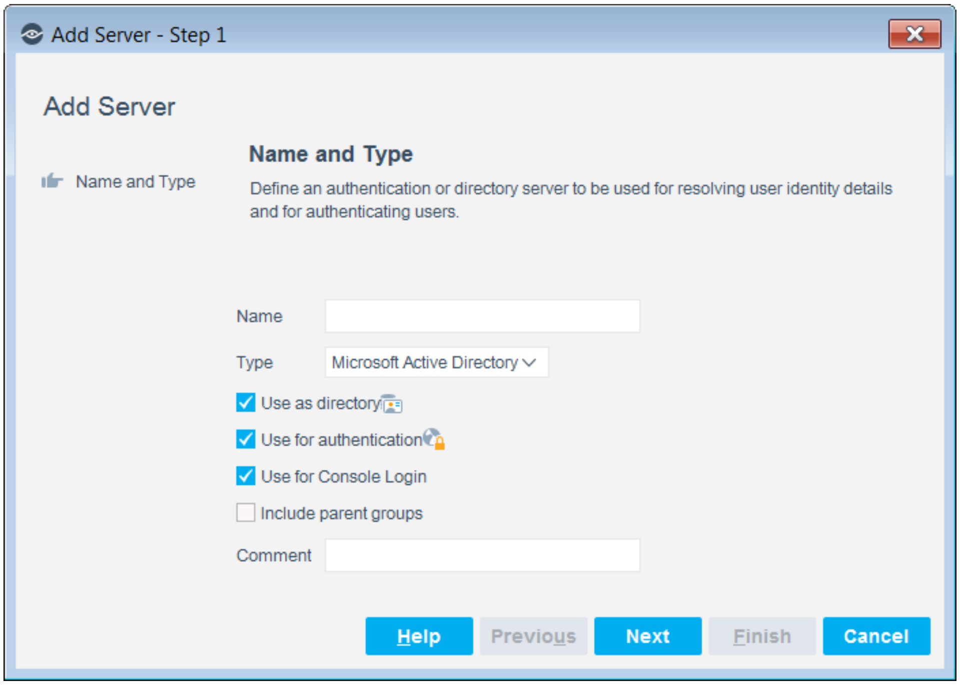
Server Name	Domain	Type	Address	Port	Replicas	Accessed By	Comment
HQ - Active Directory	HQdom	Microsoft Active Directory	[redacted]	636 (TLS)	None	All	
HQ - Radius		RADIUS	[redacted]	1645	None	All	

2 items (0 selected)

2. Select **Add**, or select an existing server configuration and select **Edit**. The Name and Type tab opens.

Name and Type Configuration Tab

This tab describes the type of server to be defined.



Add Server - Step 1

Add Server

Name and Type

Name and Type

Define an authentication or directory server to be used for resolving user identity details and for authenticating users.

Name

Type Microsoft Active Directory

☑ Use as directory

☑ Use for authentication

☑ Use for Console Login

☐ Include parent groups

Comment

Name	Enter the hostname of the server. ***Note:*** *This value cannot be edited.*
Type	Select a server type. The wizard will display configuration parameters for the type of server selected here. ***Note:*** *This value cannot be edited.*
Use as directory	Not available for RADIUS and TACACS server types. 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	Available for Microsoft Active Directory server type only. 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. The plugin does not support having the following two settings both enabled: ▪ Include parent groups setting ▪ Targeted Group Resolution advanced setting Attempting to apply such a configuration fails.
Comment	Enter comments if required.

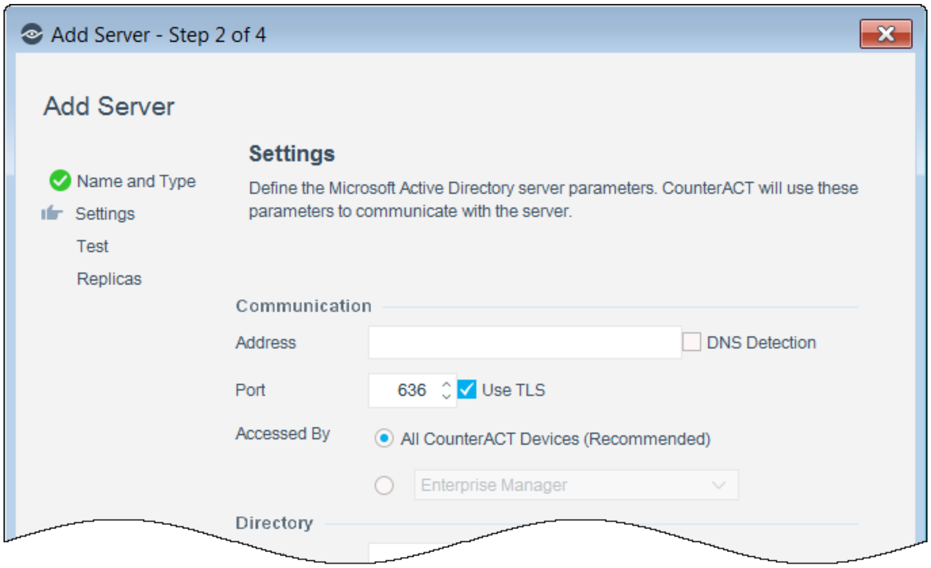
3. Select **Next**. The **Settings** tab opens.

Settings Configuration Tab

Parameters in the **Settings** tab vary, depending on the server type that you selected and the plugin features that you enabled. Parameter differences, based on server type, are described.

Communication Settings

This section describes the server communication details required regardless of the server type used.



Add Server - Step 2 of 4

Add Server

- ✓ Name and Type
- Settings
- Test
- Replicas

Settings

Define the Microsoft Active Directory server parameters. CounterACT will use these parameters to communicate with the server.

Communication

Address: □ DNS Detection

Port: 636 ☑ Use TLS

Accessed By: ● All CounterACT Devices (Recommended)

○ Enterprise Manager

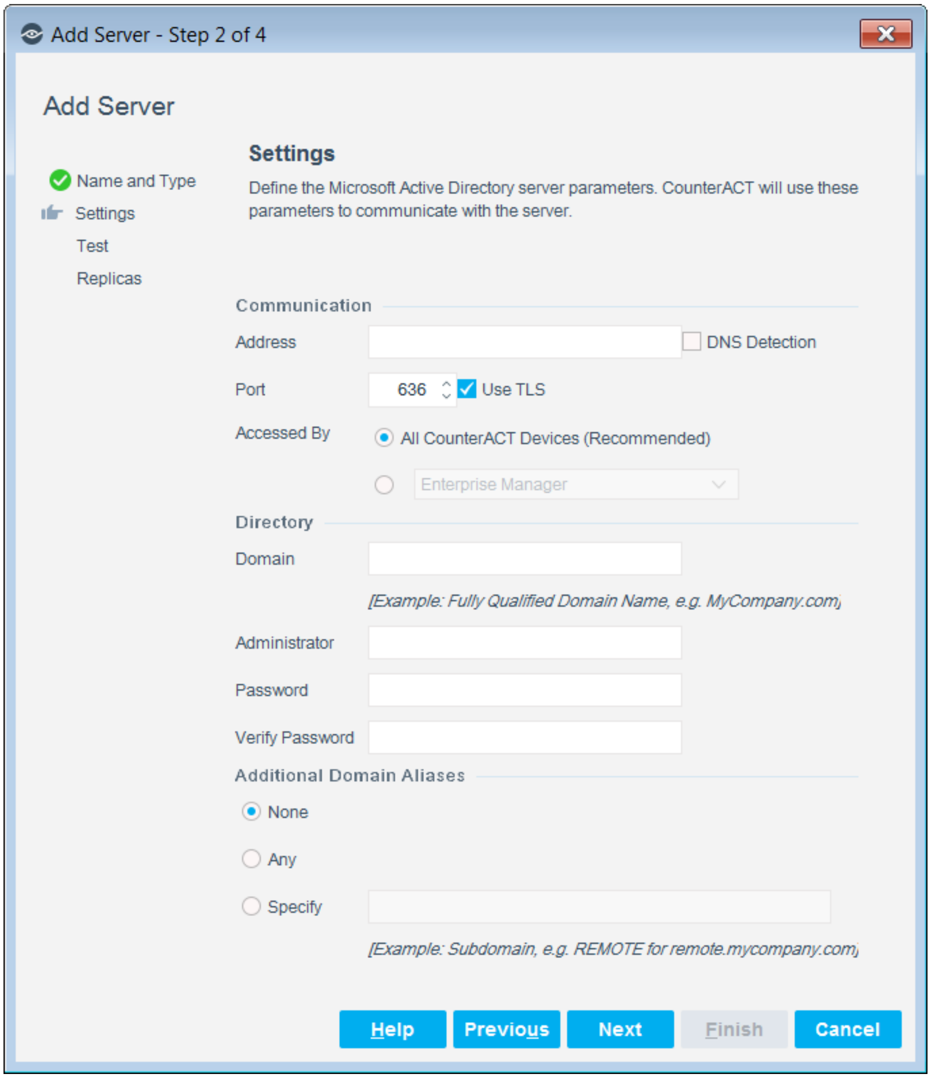
Directory

Address/DNS Detection	Do one of the following: ▪ Enter the remote address of the server, such as an IP address, an FQDN address string, or an IPv6 address string. For server types other than Microsoft Active Directory, this is the only option. ▪ 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. This option applies to Microsoft Active Directory servers only. For more information, see [DNS Detection for Microsoft Active Directory](). You can later change the frequency with which the plugin queries domain controller addresses. See [DNS Detection Refresh Interval]().
Port	Enter the server port in the **Port** field. ▪ For RADIUS servers, the default port is 1645. ▪ For TACACS servers, the default port is 49. ▪ For all other servers, the default port is 636.
Use TLS	For some server types, you can to instruct CounterACT to use TLS to encrypt communication with the User Directory server. By default, **Use TLS** is enabled. Ensure that TLS communication is supported and enabled on servers used as directories to retrieve user information. The User Directory Plugin can communicate with servers that support TLS 1.1 or TLS 1.2. It cannot communicate with servers that support TLS 1.0 only.
Accessed By	Select which CounterACT devices can communicate with the server being configured. The **All** option is recommended as it enables faster resolution. If you select **All**, make sure that all CounterACT Appliances have access to the server being configured.

Microsoft Active Directory Server Settings

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

🗎 *For a description of the* Communication *settings, see [Communication Settings]().*



Add Server - Step 2 of 4

Add Server

- ✓ Name and Type
- Settings
- Test
- Replicas

Settings

Define the Microsoft Active Directory server parameters. CounterACT will use these parameters to communicate with the server.

Communication

Address: □ DNS Detection

Port: 636 ☑ Use TLS

Accessed By: ● All CounterACT Devices (Recommended)

○ Enterprise Manager

Directory

Domain:

[Example: Fully Qualified Domain Name, e.g. MyCompany.com]

Administrator:

Password:

Verify Password:

Additional Domain Aliases

● None

○ Any

○ Specify

[Example: Subdomain, e.g. REMOTE for remote.mycompany.com]

<table>
<tr><td><b>Directory</b></td><td><b><i>Domain</i></b>: The domain name (e.g. MyCompany.com).
When the Communication Settings' <b>DNS Detection</b> checkbox is selected, the plugin uses the domain name, defined in the <b>Domain</b> field, to automatically learn the addresses of directory servers.
Domain name restrictions:
▪ The domain name may contain up to 63 characters.
▪ The domain name may contain:
- alphanumeric characters
- any of the following special characters:
! @ # $ % ^ & ( ) - _ ' { } . ~
▪ The domain name may <i>not</i> contain:
- empty spaces
- a period (.) as the first character
- any of the following special characters:
\ * + = | : ; , " ? < >
<b><i>Administrator</i></b>: Credentials to authenticate to the directory for</td></tr>
</table>

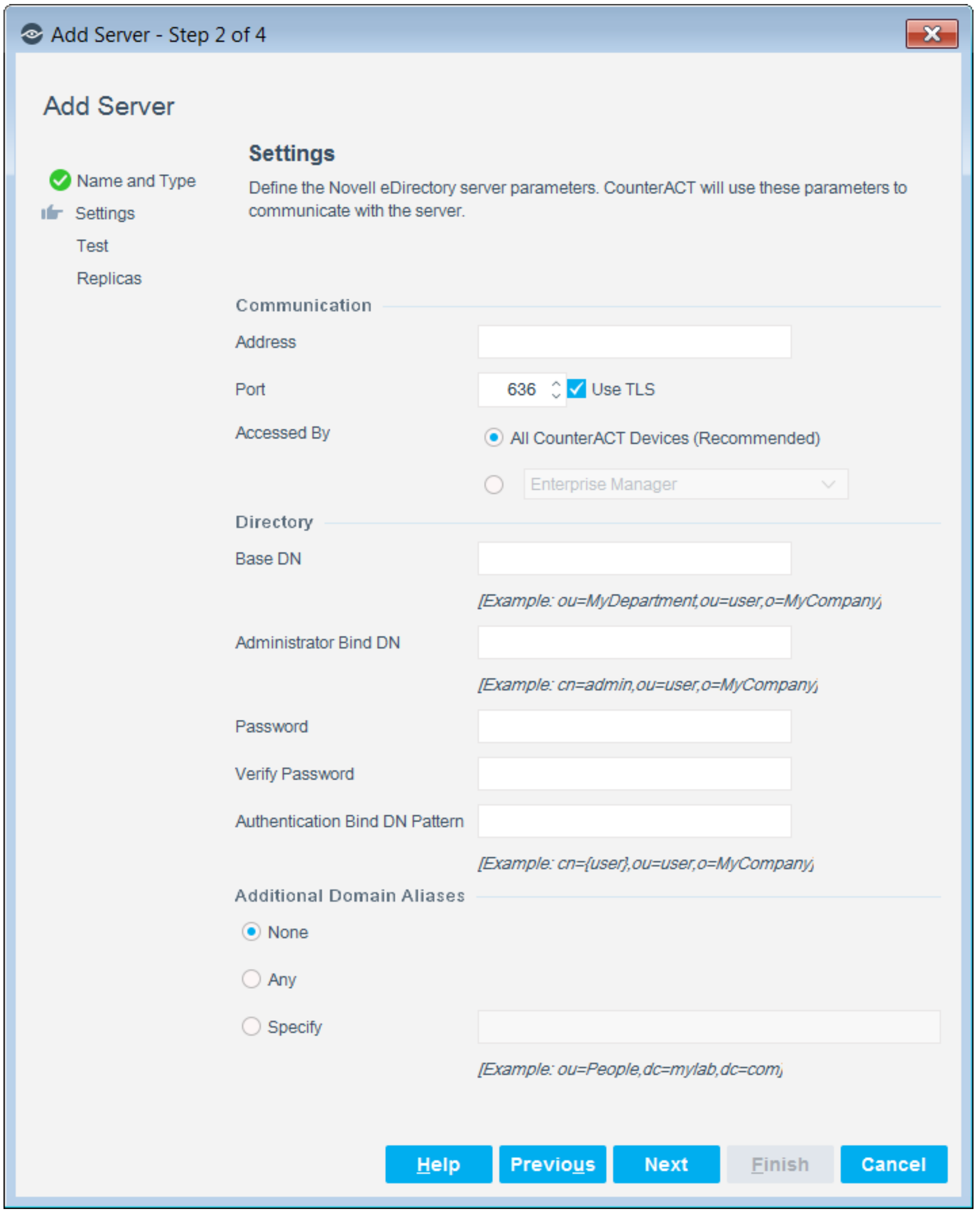
	querying other user details. ***Password***: The Administrator’s password.
Additional Domain Aliases (optional)	Alternative names for the domain being configured. ***None***: A user is looked up in this directory only if its domain name matches the directory domain defined in the **Domain** field. ***Any***: 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 Server
- IBM Lotus Notes
- OpenLDAP Server

For a description of the Communication *settings, see Communication Settings*.



Add Server - Step 2 of 4

Add Server

Settings

Define the Novell eDirectory server parameters. CounterACT will use these parameters to communicate with the server.

Communication

Address

Port 636 ☑ Use TLS

Accessed By ● All CounterACT Devices (Recommended)

○ Enterprise Manager

Directory

Base DN

[Example: ou=MyDepartment,ou=user,o=MyCompany]

Administrator Bind DN

[Example: cn=admin,ou=user,o=MyCompany]

Password

Verify Password

Authentication Bind DN Pattern

[Example: cn={user},ou=user,o=MyCompany]

Additional Domain Aliases

● None

○ Any

○ Specify

[Example: ou=People,dc=mylab,dc=com]

You may need to perform advanced configurations when working with these servers. See Advanced Settings Configuration Tab.

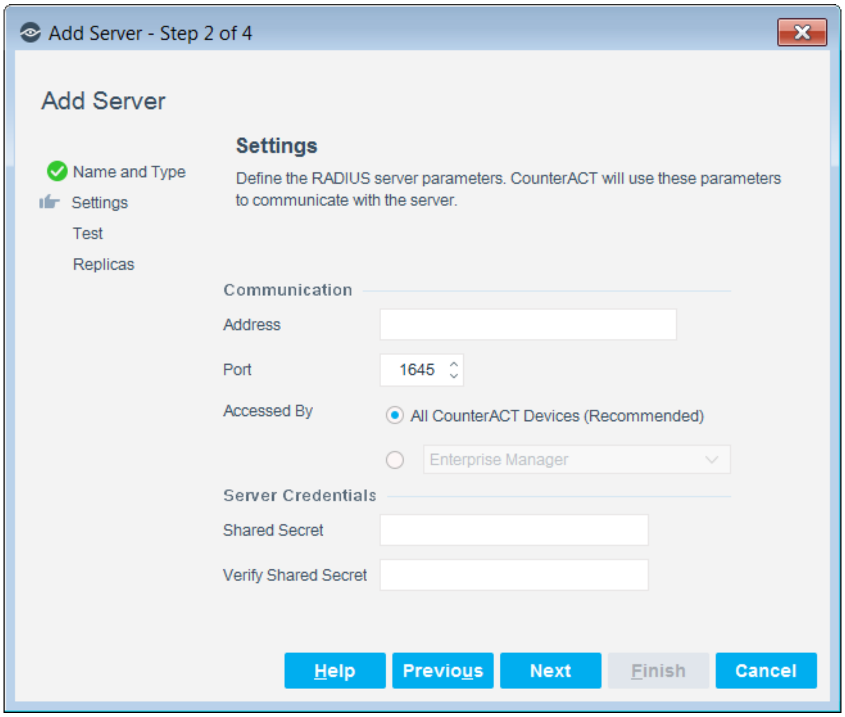
Directory	***Base DN***: The root of the LDAP directory tree where users should be looked up. ***Administrator Bind DN***: Bind DN of a user allowed to look up other users in the directory. ***Password***: The Administrator's password. ***Authentication Bind DN Pattern***: Used to construct a Bind DN string when authenticating a user to the server. The pattern must contain the string *{user}*, which will be replaced by the username during each authentication request. Example: CN={user},ou=user,o=MyCompany

Additional Domain Aliases (optional)	Alternative names for the domain in which to look up users. ***None***: The user is looked up in this directory only if the endpoint's domain name matches the domain name of this directory. ***Any***: The user is looked up in this directory regardless of the endpoint's domain name. ***Specify***: Specify a comma separated list of domain names. The user is looked up in this directory if the endpoint's domain name matches the domain name of this directory or a name in the list.

RADIUS Server Settings

This section describes details required when working with RADIUS.

🗎 *For a description of the* Communication *settings, see* *Communication Settings*.



Add Server - Step 2 of 4

Add Server

Settings

Define the RADIUS server parameters. CounterACT will use these parameters to communicate with the server.

Communication

Address:

Port: 1645

Accessed By: ● All CounterACT Devices (Recommended) ○ Enterprise Manager

Server Credentials

Shared Secret:

Verify Shared Secret:

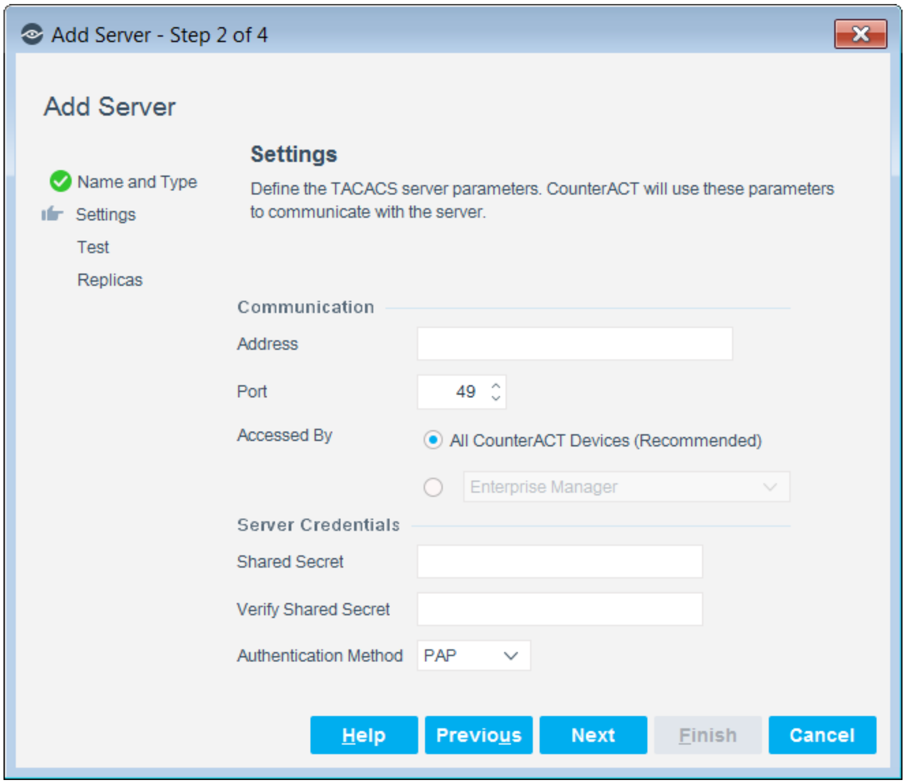
Configure the following parameter:

Server Credentials	***Shared Secret***: The shared key is used to authenticate the RADIUS transaction. Enter the shared key as defined on the RADIUS server for transactions coming from this CounterACT Appliance.

TACACS Server Settings

This section describes details required when working with TACACS.

🗎 *For a description of the* Communication *settings, see* *Communication Settings*.



Add Server - Step 2 of 4

Add Server

- ✓ Name and Type
- Settings
- Test
- Replicas

Settings

Define the TACACS server parameters. CounterACT will use these parameters to communicate with the server.

Communication

Address

Port: 49

Accessed By: ● All CounterACT Devices (Recommended) ○ Enterprise Manager

Server Credentials

Shared Secret

Verify Shared Secret

Authentication Method: PAP

Configure the following parameters:

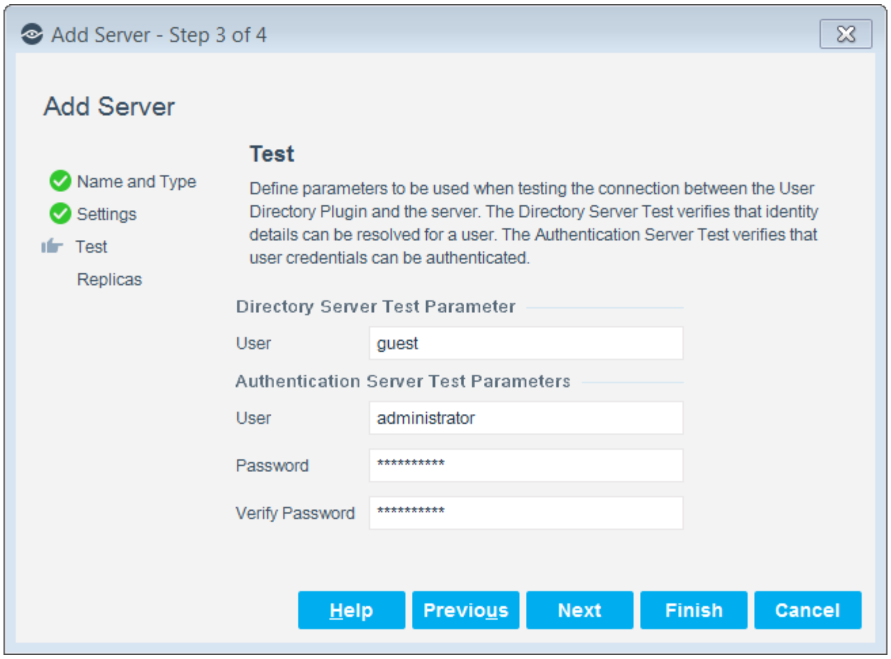
Server Credentials	***Shared Secret***: The shared key is used to authenticate the TACACS transaction. Enter the shared key as defined on the TACACS server for transactions coming from this CounterACT Appliance. ***Authentication Method***: The method CounterACT uses for user authentication against the TACACS server. The list is in ascending order of security. ▪ ***ASCII***: User passwords are transmitted in plain text; compatible with older TACACS versions ▪ ***PAP*** (Password Authentication Protocol): User passwords are encrypted symmetrically with the TACACS shared secret and transmitted ▪ ***CHAP*** (Challenge Handshake Authentication Protocol): Challenge-response method; plain-text user passwords are needed by both CounterACT and the TACACS server, but they are not transmitted ▪ ***ARAP*** (AppleTalk Remote Access Protocol): Apple implementation of CHAP ▪ ***MS-CHAP*** (Microsoft CHAP): More secure version of CHAP; plain text user passwords are not needed by CounterACT or the TACACS server

Test Configuration Tab

Define parameters for testing the connection between a server and the User Directory Plugin. The **Directory Server Test** verifies that information can be resolved for the user name entered. The **Authentication Server Test** verifies user authentication using 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 Administrator information entered in the Settings tab.



Test

Define parameters to be used when testing the connection between the User Directory Plugin and the server. The Directory Server Test verifies that identity details can be resolved for a user. The Authentication Server Test verifies that user credentials can be authenticated.

Directory Server Test Parameter

User guest

Authentication Server Test Parameters

User administrator

Password **********

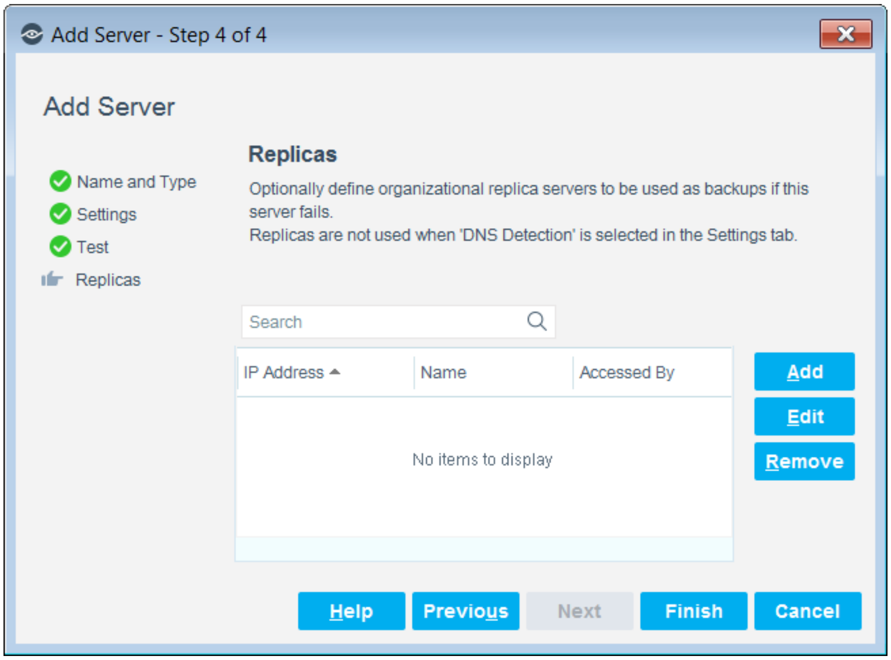
Verify Password **********

Directory	***User***: A user name to query. This should be a valid user in the domain.
Authentication	***User*** and ***Password***: Valid login credentials for testing if authentication works.

Replicas Configuration Tab

Specify organizational replica servers to be used as backup servers if the User Directory server defined in the **Name and Type** tab fails. This configuration is optional.

For details about how replica servers are used for Microsoft Active Directory, see DNS Detection for Microsoft Active Directory.



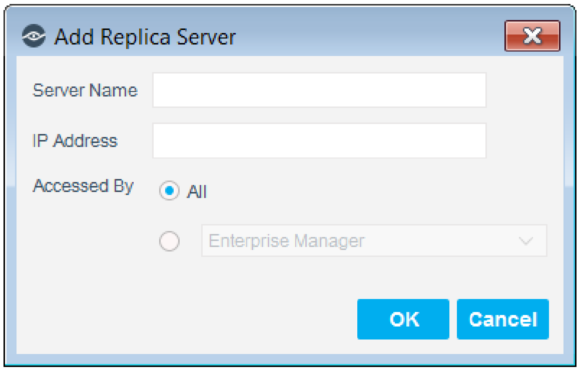
Replicas

Optionally define organizational replica servers to be used as backups if this server fails.
Replicas are not used when 'DNS Detection' is selected in the Settings tab.

IP Address ▲	Name	Accessed By
No items to display		

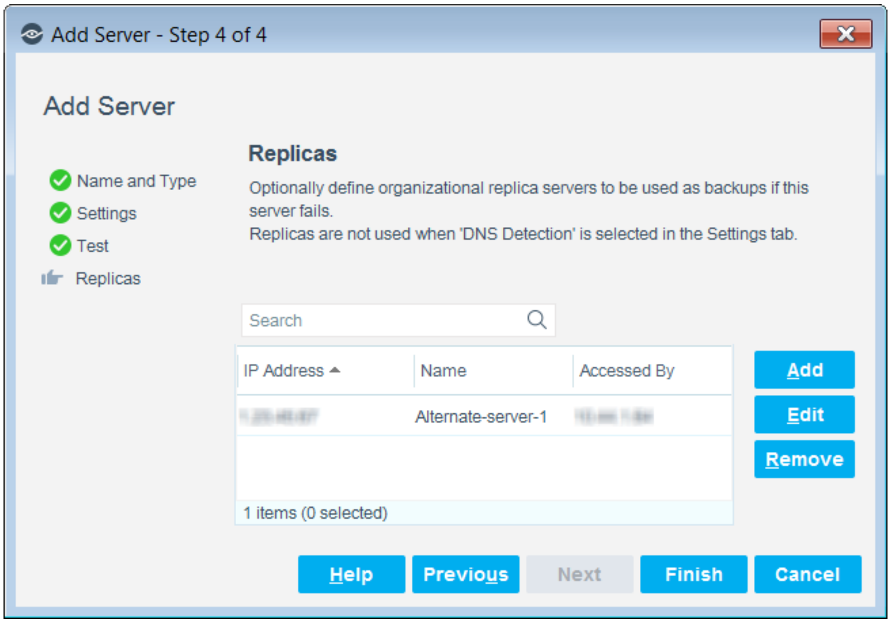
To add a replica server:

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



Server Name
IP Address
Accessed By ● All
○ Enterprise Manager

2. Enter the replica server name.
3. Enter the remote address of the replica server, such as an IP address, an FQDN address string, or an IPv6 address string.
4. Indicate which Appliance or Enterprise Manager can access the replica server.
5. Select **OK**. The server that you defined is added to the **Replicas** tab.



Add Server - Step 4 of 4

Add Server

Replicas

Optionally define organizational replica servers to be used as backups if this server fails.
Replicas are not used when 'DNS Detection' is selected in the Settings tab.

IP Address ▲	Name	Accessed By
[redacted]	Alternate-server-1	[redacted]

1 items (0 selected)

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

Advanced Settings Configuration Tab

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 in the **Add Server** wizard.

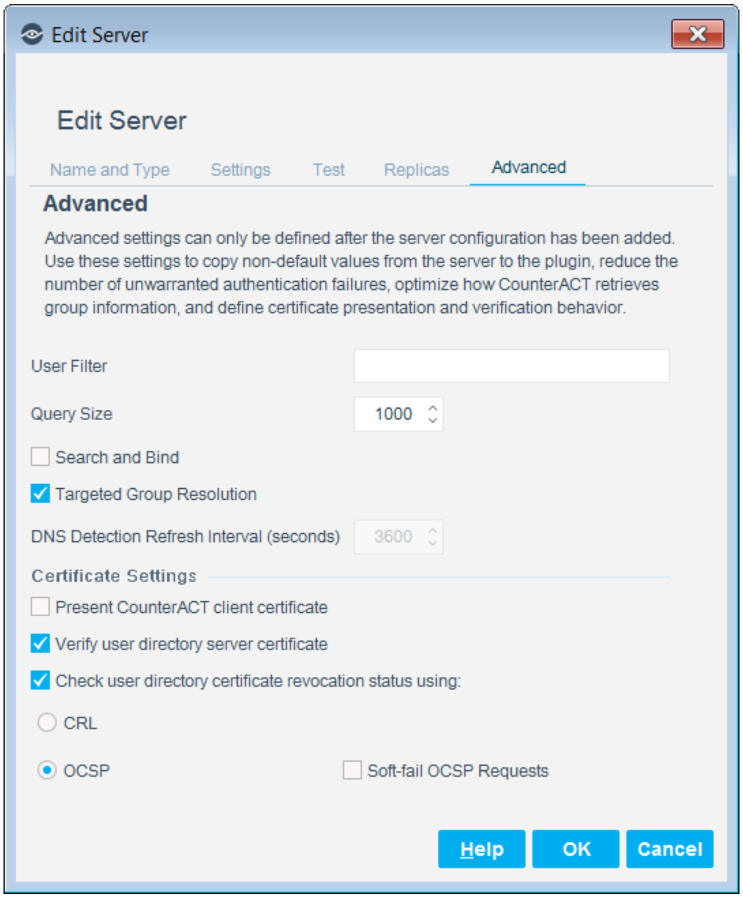
Advanced settings are not available for RADIUS and TACACS server types.

Use Advanced settings to:

- Copy non-default values from the server to the plugin.
- Reduce the number of unwarranted authentication failures in scenarios where there are several groups and domains.
- Optimize the way CounterACT retrieves group information.
- Define if CounterACT presents a client certificate and if it verifies the user directory server certificate.

To define advanced settings for a server:

1. Complete the User Directory Plugin configuration for the server.
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

Name and Type | Settings | Test | Replicas | Advanced

Advanced

Advanced settings can only be defined after the server configuration has been added. Use these settings to copy non-default values from the server to the plugin, reduce the number of unwarranted authentication failures, optimize how CounterACT retrieves group information, and define certificate presentation and verification behavior.

User Filter:

Query Size: 1000

□ Search and Bind

☑ Targeted Group Resolution

DNS Detection Refresh Interval (seconds): 3600

Certificate Settings

□ Present CounterACT client certificate

☑ Verify user directory server certificate

☑ Check user directory certificate revocation status using:

○ CRL

● OCSP □ Soft-fail OCSP Requests

5. Define the following settings:

User Filter	This attribute is used to identify users. For multiple attributes, separate each string with a comma. If the field is empty, the following defaults are used: ▪ For Microsoft Active Directory – sAMAccountName ▪ For Novell eDirectory – cn or uid ▪ For Oracle Directory – uid ▪ For IBM Lotus Notes – cn or uid ▪ For OpenLDAP Server – cn or uid
Query Size	This setting defines the maximum number of queries sent to the server simultaneously. Decrease this value if you encounter SizeLimit server errors. The default is 1000. This setting applies to Microsoft Active Directory servers only.

Search and Bind	This setting does not apply to Microsoft Active Directory servers. If your User Directory Plugin test results indicate that authentication failed, this setting may resolve the problem. In environments where there are multiple groups and domains, a Bind DN pattern might not produce a unique DN for each user, and user authentication cannot proceed. When this setting is selected, the User Directory Plugin ignores the Bind DN pattern, and: **1.** Binds to the directory with the user credentials entered in the Administrator Bind DN field in the **Settings** tab. **2.** Searches the directory for a user with the same name as the authentication request's username field. **3.** Retrieves the user's unique DN from the directory. **4.** Binds with the DN and the authentication request's Password field.
Targeted Group Resolution	When selected, CounterACT optimizes the way it retrieves group information. Use this option to reduce traffic in large-scale network environments with complex group hierarchies. Instead of the default method of retrieving a full listing of groups at regular intervals, this setting instructs the plugin to store primary group IDs and then to selectively query for further group information. This setting applies to Microsoft Active Directory servers only. For newly added servers, this setting is enabled by default. ***Note***: For Microsoft Active Directory servers, you cannot enable both the *Targeted Group Resolution* setting and the *Include parent groups* setting, located in the **Name and Type** tab.
DNS Detection Refresh Interval	This setting applies to Microsoft Active Directory servers for which *DNS Detection* was selected in the **Settings** tab. See DNS Detection for Microsoft Active Directory. This setting defines the frequency, in seconds, with which the plugin queries domain controller addresses.
Certificate Settings	These settings define how certificates are used and verified between CounterACT and the server. For detailed information about defining and provisioning certificates, refer to the *CounterACT Administration Guide* section that describes how to configure the certificate interface.
Present CounterACT client certificate	When selected, CounterACT presents a client certificate to the user directory server.
Verify user directory server certificate	When selected, CounterACT verifies the user directory server certificate.

Check user directory certificate revocation status using	When selected, CounterACT checks that the user directory server certificate has not been revoked. ▪ ***CRL***: Check if the certificate is in the Certificate Revocation List (CRL) of the issuing Certificate Authority. ▪ ***OCSP***: Send an Online Certificate Status Protocol (OCSP) request for the certificate revocation status. - ***Soft-fail OCSP Requests***: If CounterACT could not receive a response from the OCSP Responder, the certificate is considered valid. By default, hard-fail is applied.

Define Additional Similar Servers

Typically there are several User Directory servers in a network environment. You can repeat the Configuration procedures to manually define additional servers.

In many cases it is useful to use an existing server profile as the basis for a new server configuration. Follow this procedure to duplicate and modify an existing server configuration.

To create a new server configuration based 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 address to differentiate this server.*

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

Verify That the Plugin Is Running

After configuring the plugin, verify that it is running.

To verify:

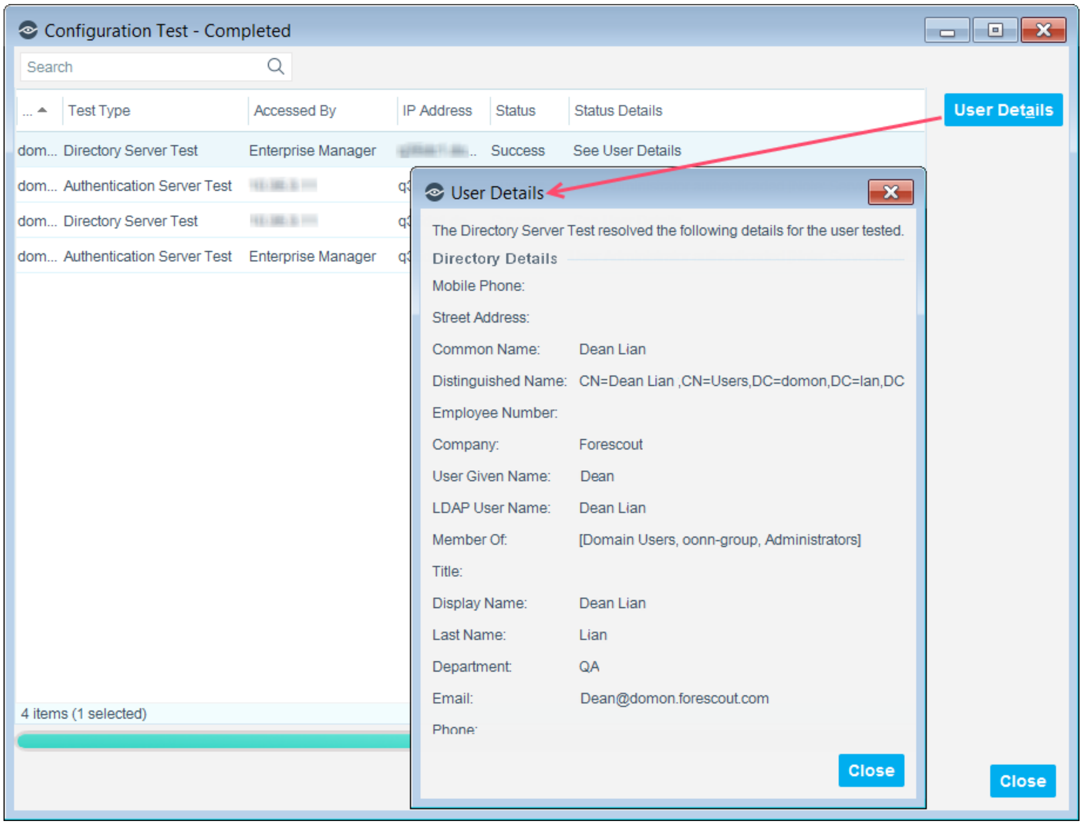
1. Select **Tools**>**Options** and then select **Modules**.
2. Navigate to the plugin and select **Start** if the plugin is not running.

Test the Configuration

To ensure that the plugin can connect to a server, it is recommended to run a test using the settings defined in Test Configuration Tab.

To test a server configuration:

1. Select the server in the User Directory pane and select **Test**. A configuration test runs for each CounterACT device selected in the Accessed By field.
2. To see the results of a Directory test, select the row and select **User Details**.



...	Test Type	Accessed By	IP Address	Status	Status Details
dom...	Directory Server Test	Enterprise Manager	[redacted]..	Success	See User Details
dom...	Authentication Server Test	[redacted]	q3		
dom...	Directory Server Test	[redacted]	q3		
dom...	Authentication Server Test	Enterprise Manager	q3		

4 items (1 selected)

User Details

The Directory Server Test resolved the following details for the user tested.

Directory Details

Mobile Phone:	
Street Address:	
Common Name:	Dean Lian
Distinguished Name:	CN=Dean Lian ,CN=Users,DC=domon,DC=lan,DC
Employee Number:	
Company:	Forescout
User Given Name:	Dean
LDAP User Name:	Dean Lian
Member Of:	[Domain Users, oonn-group, Administrators]
Title:	
Display Name:	Dean Lian
Last Name:	Lian
Department:	QA
Email:	Dean@domon.forescout.com
Phone:	

Working with CounterACT Policies

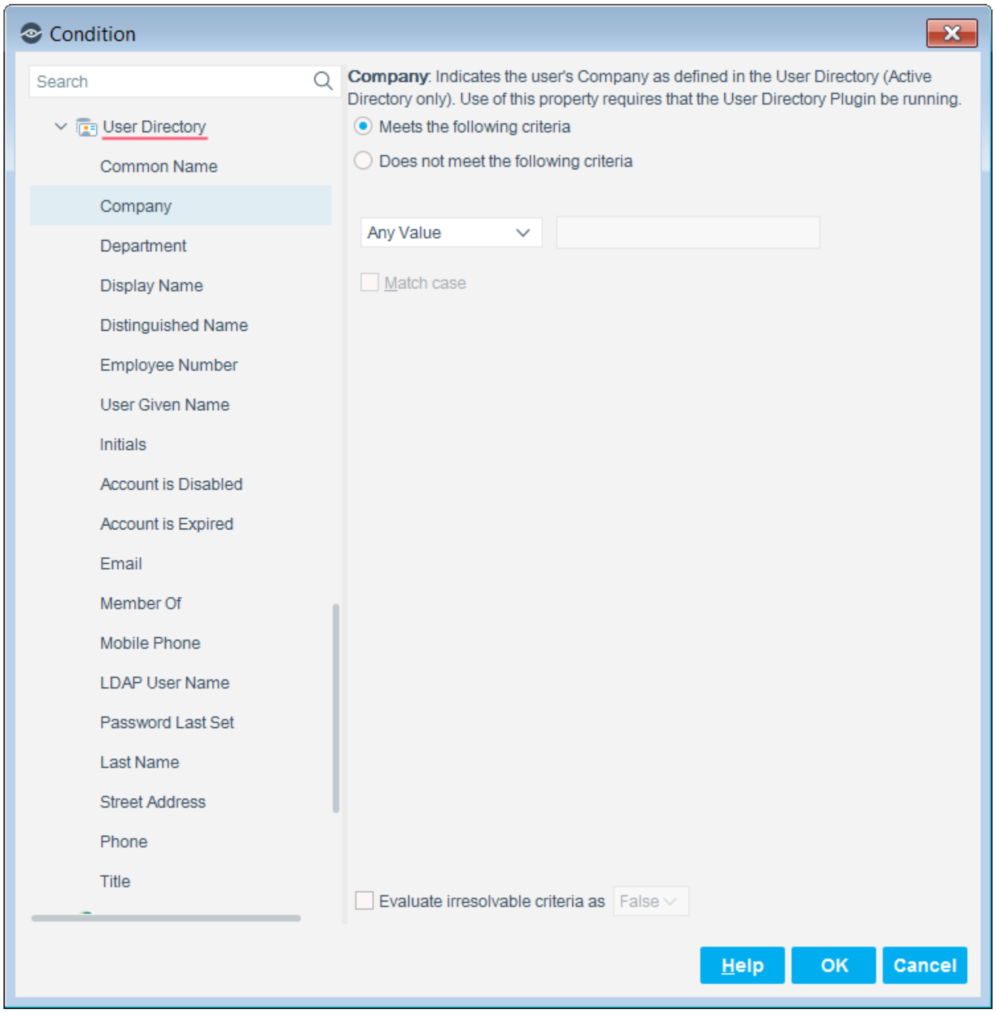
Use CounterACT policy tools to detect endpoints with specific User Directory attributes. For example, create a policy that detects endpoint users in a specific Active Directory department or with a specific distinguished name.

Detect Endpoints with User Directory Attributes

You can use a CounterACT policy to detect the following User Directory attributes on endpoints:

- *Account is Disabled* (Active Directory only)
- *Account is Expired* (Active Directory only)
- *Common Name*
- *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*



Company: Indicates the user's Company as defined in the User Directory (Active Directory only). Use of this property requires that the User Directory Plugin be running.

● Meets the following criteria

○ Does not meet the following criteria

Any Value

□ Match case

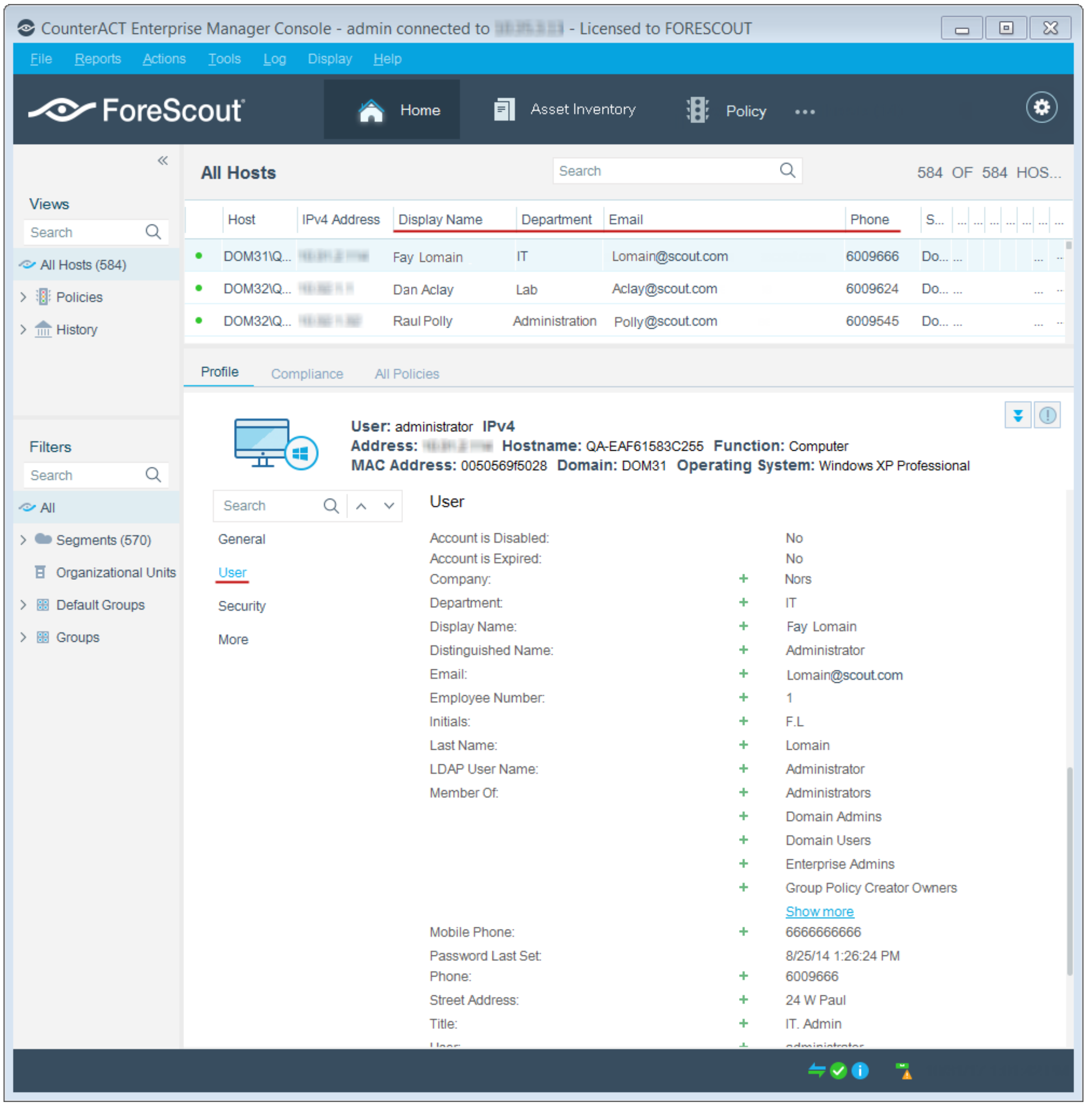
□ Evaluate irresolvable criteria as False

Refer to the *CounterACT Administration Guide* for details about working with CounterACT policies. See Additional CounterACT Documentation for information on how to access the guide.

Display User Directory Information at the Console

Information learned by the User Directory Plugin can be viewed at the Console:

- in the Detections pane
- in the User section of the Profile tab



CounterACT Enterprise Manager Console - admin connected to [redacted] - Licensed to FORESCOUT

All Hosts

584 OF 584 HOS...

	Host	IPv4 Address	Display Name	Department	Email	Phone	S...
●	DOM31\Q...	[redacted]	Fay Lomain	IT	Lomain@scout.com	6009666	Do... ...
●	DOM32\Q...	[redacted]	Dan Aclay	Lab	Aclay@scout.com	6009624	Do... ...
●	DOM32\Q...	[redacted]	Raul Polly	Administration	Polly@scout.com	6009545	Do... ...

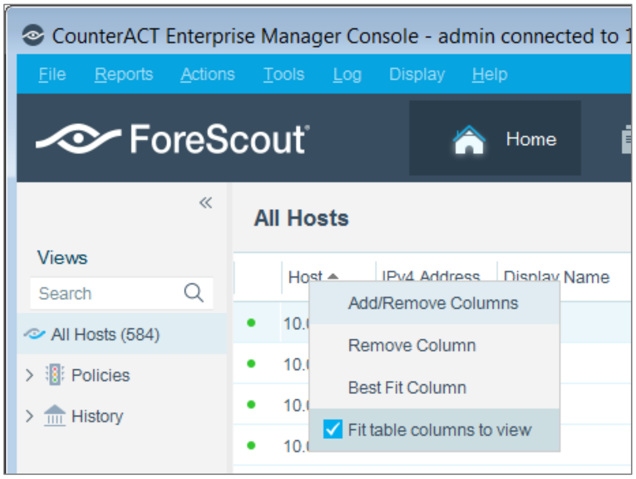
User: administrator **IPv4 Address:** [redacted] **Hostname:** QA-EAF61583C255 **Function:** Computer **MAC Address:** 0050569f5028 **Domain:** DOM31 **Operating System:** Windows XP Professional

User

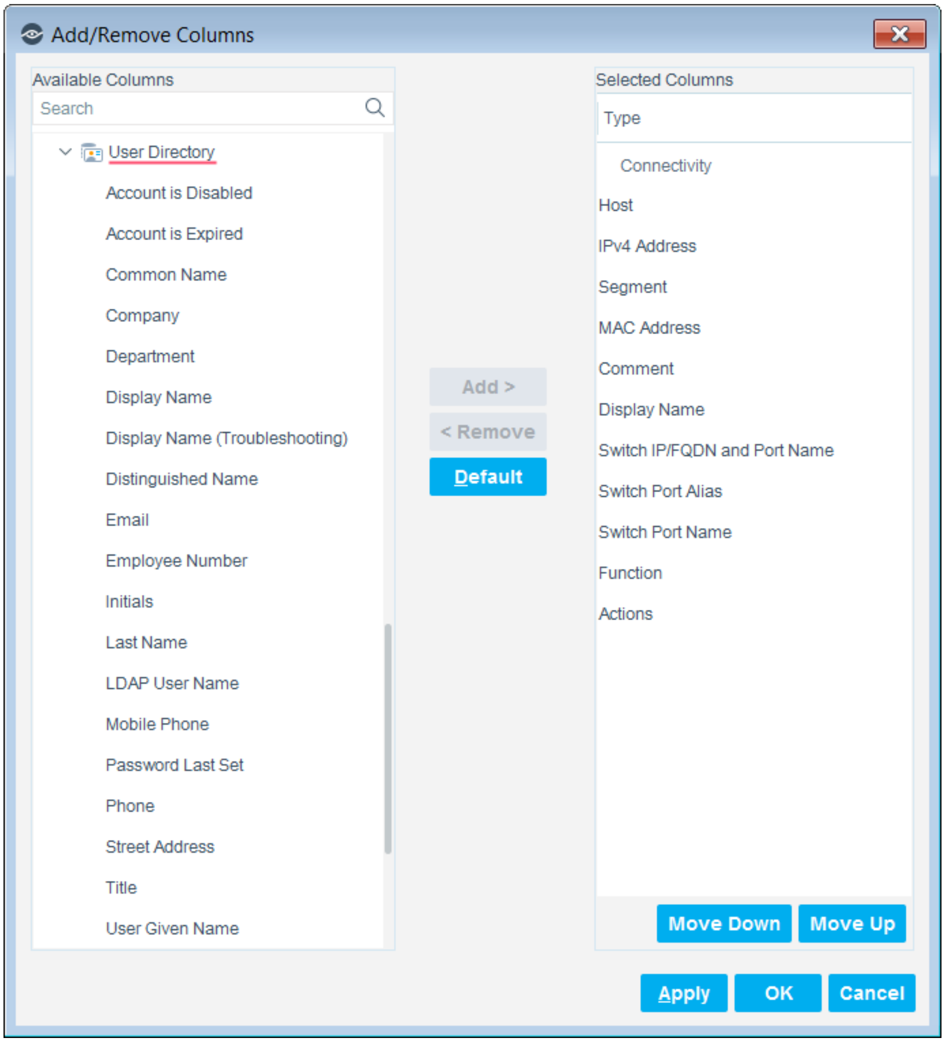
Account is Disabled:		No
Account is Expired:		No
Company:	+	Nors
Department:	+	IT
Display Name:	+	Fay Lomain
Distinguished Name:	+	Administrator
Email:	+	Lomain@scout.com
Employee Number:	+	1
Initials:	+	F.L
Last Name:	+	Lomain
LDAP User Name:	+	Administrator
Member Of:	+	Administrators
	+	Domain Admins
	+	Domain Users
	+	Enterprise Admins
	+	Group Policy Creator Owners
		Show more
Mobile Phone:	+	6666666666
Password Last Set:		8/25/14 1:26:24 PM
Phone:	+	6009666
Street Address:	+	24 W Paul
Title:	+	IT. Admin
User:	+	administrator

To display / hide columns in the Detections pane:

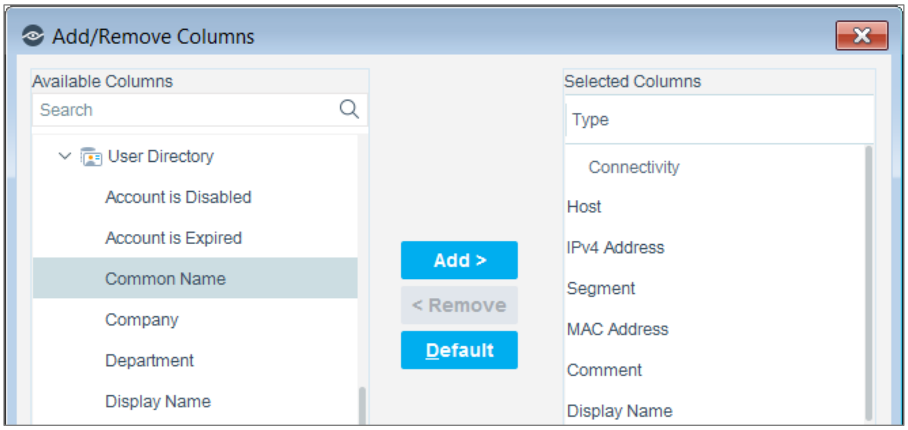
1. Right-click a table header from the **Detections** pane.



2. Select **Add / Remove Columns**.
3. Expand the **Properties** node and then expand the **User Directory** node.



4. Select each item to be displayed in a **Detections** pane column, and select the **Add** button.



5. To rearrange the order of the columns, select a column header and then select **Move Down** or **Move Up**.

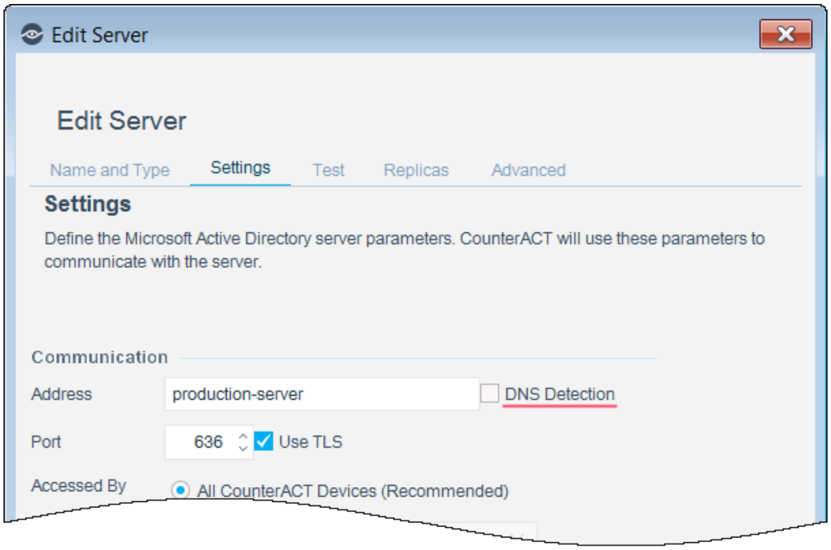
6. Should your screen become cluttered due to numerous columns displayed in the Console, right-click a column and select **Remove Column**.

Additional Information

This section provides more detailed information about the plugin.

DNS Detection for Microsoft Active Directory

The Microsoft Active Directory server configuration includes a *DNS Detection* option in the Settings tab.



Edit Server

Settings

Define the Microsoft Active Directory server parameters. CounterACT will use these parameters to communicate with the server.

Communication

Address: production-server □ DNS Detection

Port: 636 ☑ Use TLS

Accessed By: ● All CounterACT Devices (Recommended)

When DNS Detection Is Not Enabled

When the server is added, the User Directory Plugin constructs a list that includes:

- the server address configured in the Settings tab, Communication section
- all the server addresses configured in the Replicas tab

The address defined in the Settings tab is first in the list. There is no specific order among the replica servers.

For each CounterACT Appliance, the list is divided into two parts:

- IPs of servers that are accessed by the evaluating Appliance (‘accessed by me’)
- IPs of servers that are accessed by other Appliances (‘accessed by others’)

To connect to the server:

1. CounterACT attempts to connect to the first reachable server in the ‘accessed by me’ list. If the list is empty, CounterACT delegates the connection to one of the ‘accessed by others’ servers.

2. If a server is unreachable (service not available), CounterACT attempts to connect to the next server in the same list.
3. If a server is reachable but there is a timeout (congested network or firewall configuration) longer than the configured 10-second maximum timeout, CounterACT attempts to connect to the next server in the same list.

> 🗎 *The timeout parameter is configurable per Appliance using the following command:*
> ***fstool ad set_property config.timeout.value <new timeout sec>***

When DNS Detection Is Enabled

When *DNS Detection* is enabled, the user does not provide primary server or replica server IPs. CounterACT automatically learns directory server addresses. This is recommended in network environments where there are several domain controllers that function as replicas.

In DMZ environments, do not enable DNS Detection for CounterACT Appliances if the DNS server is not reachable from Appliances.

To identify the primary directory server:

1. Using DNS lookup, the User Directory Plugin constructs a list of all potential directory servers.
2. Of the potential directory servers, the quickest to respond is selected as the primary server.
3. This primary server is used for each LDAP query.

If the primary server is unreachable (service not available) when it is evaluated, the plugin will follow the procedure to identify a new primary directory server. By default, the primary server is evaluated hourly. See DNS Detection Refresh Interval.

If the primary server is reachable but there is a timeout (congested network or firewall configuration) longer than the configured 10-second maximum timeout, the plugin will follow the procedure to identify a new primary directory server.

> 🗎 *The timeout parameter is configurable per Appliance using the following command:*
> ***fstool ad set_property config.timeout.value <new timeout sec>***

Compatibility Across Servers

Endpoint properties in the user directories are shared with CounterACT. The following table shows which properties are mapped from each directory type to CounterACT.

CounterACT Property Tag	MS Active Directory	Novell eDirectory	Oracle Directory	IBM Lotus Notes	OpenLDAP
ad_cn	cn	cn	cn	cn	cn
ad_company	company	company	company	company	company
ad_department	department	department	department	department	department

CounterACT Property Tag	MS Active Directory	Novell eDirectory	Oracle Directory	IBM Lotus Notes	OpenLDAP
ad_displayname	displayname	displayname	displayname	displayname	displayname
ad_employeenumber	employeenumber	employeenumber	employeenumber	employeenumber	employeenumber
ad_givenname	givenname	givenname	givenname	givenname	givenname
ad_initials	initials				
ad_isdisabled	useraccountcontrol				
ad_isexpired	accountexpires				
ad_lm_fld1					lmPassword
ad_lm_fld2					sambaLmPassword
ad_mail	mail	mail	mail	mail	mail
ad_memberof	memberof	groupMembership	memberof	groupMembership	member
ad_mobile	mobile	mobile	mobile	mobile	mobile
ad_name	name	cn	name	cn	cn
ad_nt_fld1					ntPassword
ad_nt_fld2					sambaNtPassword
ad_pwd_fld					userPassword
ad_pwdlastset	pwdlastset				
ad_sn	sn	sn	sn	sn	sn
ad_streetaddress				officestreetaddress	street
ad_telephonenumber	telephonenumber	telephonenumber	telephonenumber	telephonenumber	telephonenumber
ad_title	title	title	title	title	title
object_sid	objectSid				
primary_group_id	primaryGroupID				

Authentication Module Information

The Authentication Module provides secure network access across wired, wireless, and guest networks through its RADIUS and User Directory Plugins.

The Authentication Module is a ForeScout Base Module. Base Modules are delivered with each CounterACT release.

The User Directory and RADIUS Plugins are released and rolled back with the Authentication Module.

Refer to the *CounterACT Authentication Module Guide* for more module information, such as module requirements, upgrade and rollback instructions. See *Additional CounterACT Documentation* for information about how to access the module guide.

Additional CounterACT Documentation

For information about other CounterACT features and modules, refer to the following resources:

- Documentation Downloads
- Documentation Portal
- CounterACT Help Tools

Documentation Downloads

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** - Product Updates Portal
- ***Centralized Licensing Mode*** - Customer Portal

🗎 *Software downloads are also available from these portals.*

To learn which licensing mode your deployment is using, see Identifying Your Licensing Mode in the Console.

Product Updates Portal

The Product Updates Portal provides links to CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

1. Go to https://updates.forescout.com/support/index.php?url=counteract.
2. Select the CounterACT version you want to discover.

Customer Portal

The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:

1. Go to https://forescout.force.com/support/.
2. Select **Downloads** or **Documentation**.

Documentation Portal

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

🗎 *If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.*

To access the Documentation Portal:

1. Go to www.forescout.com/docportal.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT 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.

CounterACT Administration Guide

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 **Modules**.
2. Select the plugin and then select **Help**.

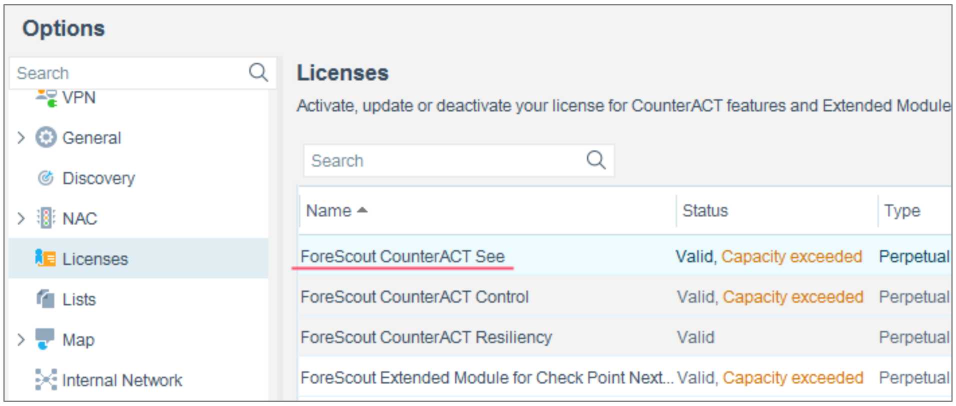
Documentation Portal

Select **Documentation Portal** from the **Help** menu.

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Licenses

Activate, update or deactivate your license for CounterACT features and Extended Module

Name	Status	Type
ForeScout CounterACT See	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Control	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Resiliency	Valid	Perpetual
ForeScout Extended Module for Check Point Next...	Valid, Capacity exceeded	Perpetual

Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Legal Notice

2018-04-10 09:21