

IDSync® AD CLOUD PORTAL

Internet Browser Access to Microsoft Active Directory for user management

Cloud Console User's Guide



IDSync[®] AD Cloud Portal

Cloud Based AD Management

©InnerApps, LLC
28350 Kensington Lane • Suite 200
Perrysburg, OH - 43551
Phone 888.908.7962 • Fax 419.931.0061

Contents

Revision History	5
General Information	6
Introduction	6
System Overview	10
System Components	11
AD Cloud Portal Concepts	12
Getting Started	13
Accessing the IDSync Cloud Console	13
Working with Active Directory Objects	16
Viewing Active Directory Objects	16
Viewing AD Computers	16
Viewing AD Contacts	19
Viewing AD Groups	20
Viewing AD Users	21
Creating Active Directory Objects	22
Creating AD Users	22
Creating AD Groups	23
Editing Active Directory Objects	24
Editing AD Users Properties	25
Enabling/Disabling AD Users	28
Changing Password for an AD User	29
Unlocking an AD User	30
Editing AD Groups Properties	32
Adding/Removing Objects to Groups	34

Revision History

04-2017

1. Initial Documentation

01-2018

2. Format changes.
3. Addition of new sections.
4. Addition of ADCP Concepts.

General Information

Introduction

Access Active Directory directly from Odin Automation and manage Users, Groups, Contacts and Computers via a web-browser (see figure 1.1-1).

Think about the benefits:

- Offer Better Customer Service with Lower Help Desk Costs. Estimated at 30% by Meta Group, password change and reset tickets represent a substantial portion of the calls handled by an IT help desk. Using the IDSync® Cloud Console, it is possible to more efficiently manage this work load and reset locked accounts or change a users' AD password more quickly from a browser-based interface by using your login to the Ingram Marketplace.

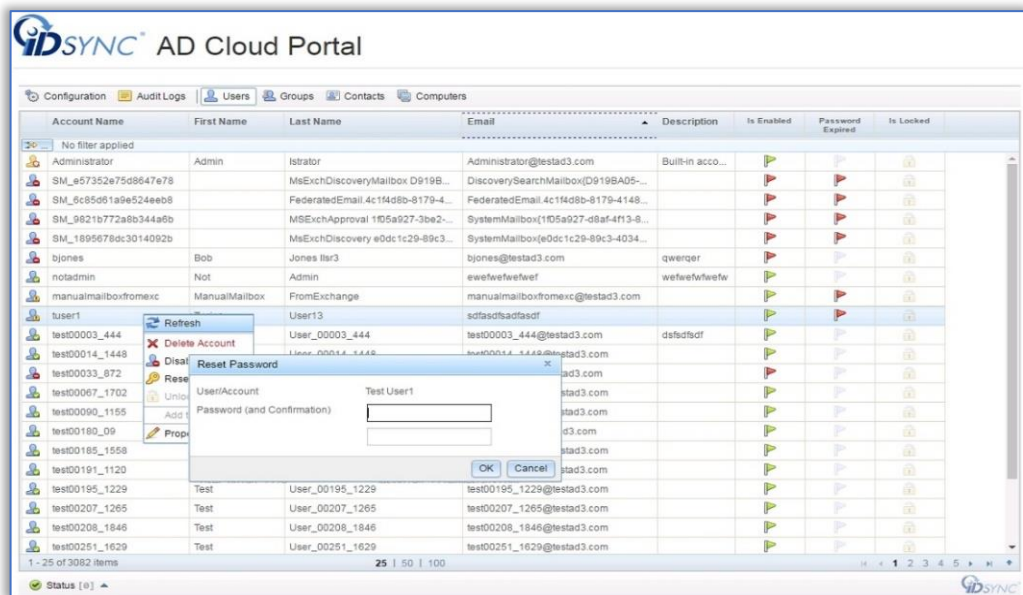


Figure 1.1-1

- Additional MSP Service and Revenue stream
 The information in the IDSync® Cloud Console is always current and updated with the most recent user information contained in Active Directory, all without any additional maintenance efforts. The IDSync® Cloud Console is intended for use by MSP's and other service providers who want to provide additional value for their customers and revenue to their bottom line.

Introduction - The Cloud Portal

- Manage Active Directory for all your Customers in one place

For an MSP that uses the IDSync® Cloud Portal, the service provider can now gain access to their customer's Active Directory through a single and convenient login to Odin Automation that shows all Active Directory users with select meta-data about each user. From within IDSync® Cloud Console you can perform multiple activities, such as creating, deleting, enabling or disabling Active Directory objects, as well as view or edit meta-data information. Similar to the operation of Active Directory, you make a change by selecting a user, and an action from the context menu. The change is automatically applied in Active Directory, Cloud Portal as well as all connected systems such as Odin Automation, Ingram Marketplace and more — all in real-time.

- Seamlessly interchange Active Directory and IDSync® Cloud Console interfaces.
 - Manage Active Directory Users, Groups, Contacts and Computers using an interface similar to the one you already know from the AD Management Console.
 - Create Users and Groups with the same level of requirements and restrictions that Active Directory has.

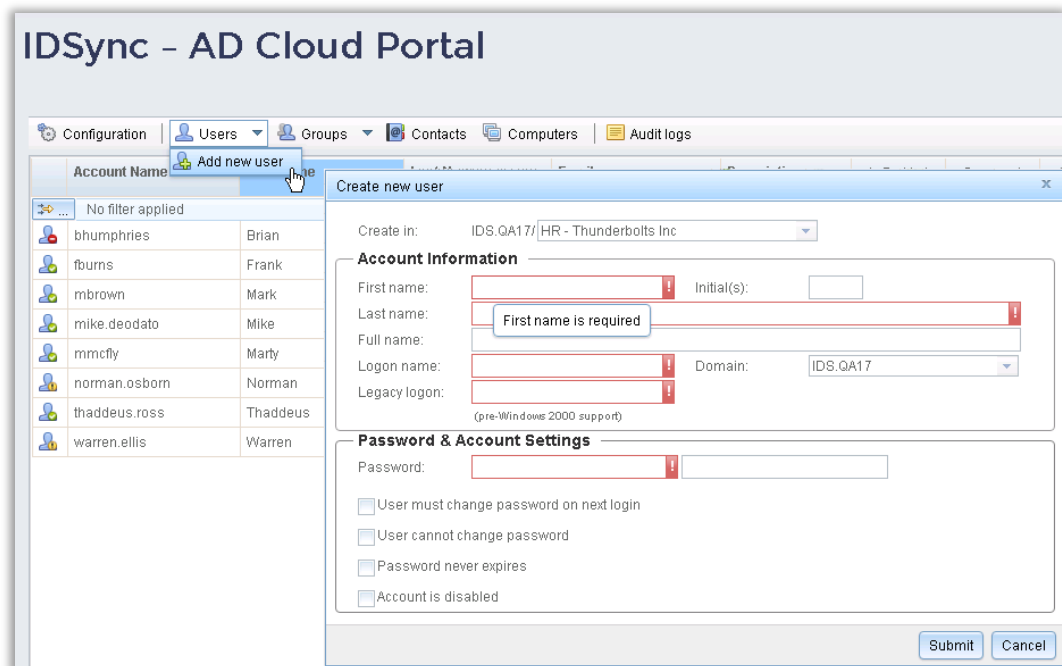


Figure 1.1-2

Introduction - The Cloud Portal

- Grant the exact set of permissions your users need, easily limiting or expanding the objects they can manage.

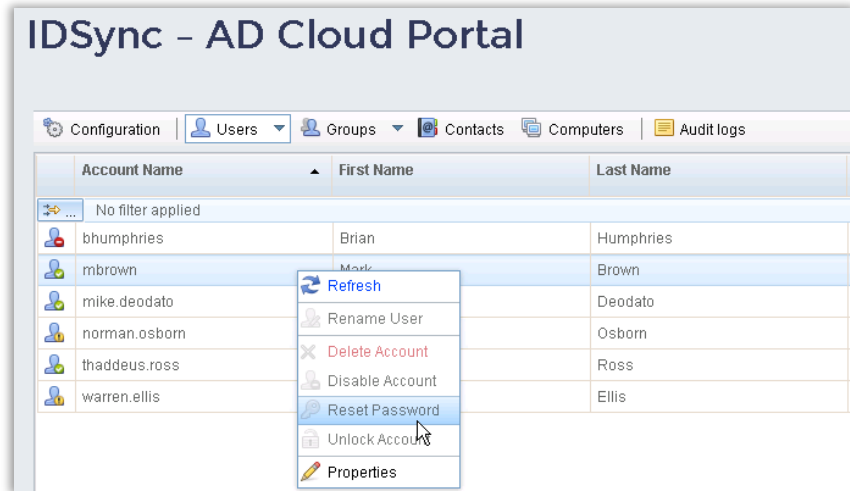


Figure 1.1-3

- Distribute Tasks, Centralize Control.

IDSync® Cloud Portal will create fully traceable records for every change that portal Users do, giving you detailed and accurate Audit logs of all the tasks that are being performed within the Active Directory objects.

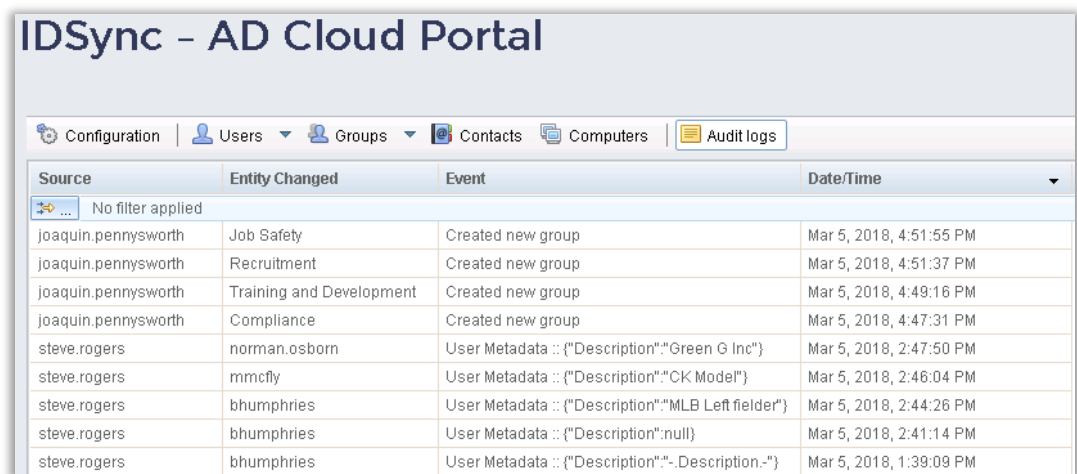


Figure 1.1-4

Introduction - The Cloud Portal

- No VPN, No RDP, No Need for AD User accounts

A primary benefit of the IDSync® Cloud Portal is to bypass the effort, cost and customer coordination required to setup and administer VPN logins for a help desk staff, for each of engineer or other service provider's customer's Active Directory environments which they support.

- Eliminate the Risk and Need to Share Passwords

And then, to go through the delay and effort to find the right tools for customer login, managing the login credentials and then finally logging in to the customer's Active Directory via a VPN, all while the user is on the phone, to make the changes requested by the user. While a VPN approach is used by many it can be slow and clumsy and comes with a fair amount of overhead, including the need to do this over and over for each service engineer or as many times happens, be open to the risks of password and rights sharing by privileged users.

- One password, One change, All applications

In the case of the IDSync® Cloud Portal by simply making the password change from the Portal, the user's AD password is reset, and that change is then automatically synchronized to AD and through other IDSync® connectors so that both the Marketplace and other application logins are enabled, satisfying the user quickly and with little effort or lost time, across all their applications with a single change in the Portal.

General Information

System Overview

IDSync® AD Cloud Portal (ADCP) provides a secure means for a managed service provider, service desk or any other service department to manage their own Active Directory (AD) Users and Groups accounts or those of their customers via a web-browser, from on-premises or remote locations.

As depicted in figure 1.2-1 below, ADCP provides secure data tunnels between the customers' network and the ODIN Marketplace, allowing any user with the proper level of rights to log in to ADCP and perform functions such as enabling/disabling AD Users, changing passwords for such users, unlocking locked accounts, etc. (the actual level of delegation depends on the customer needs or preferences). This document focuses on how to access and use the Cloud Console functionalities.

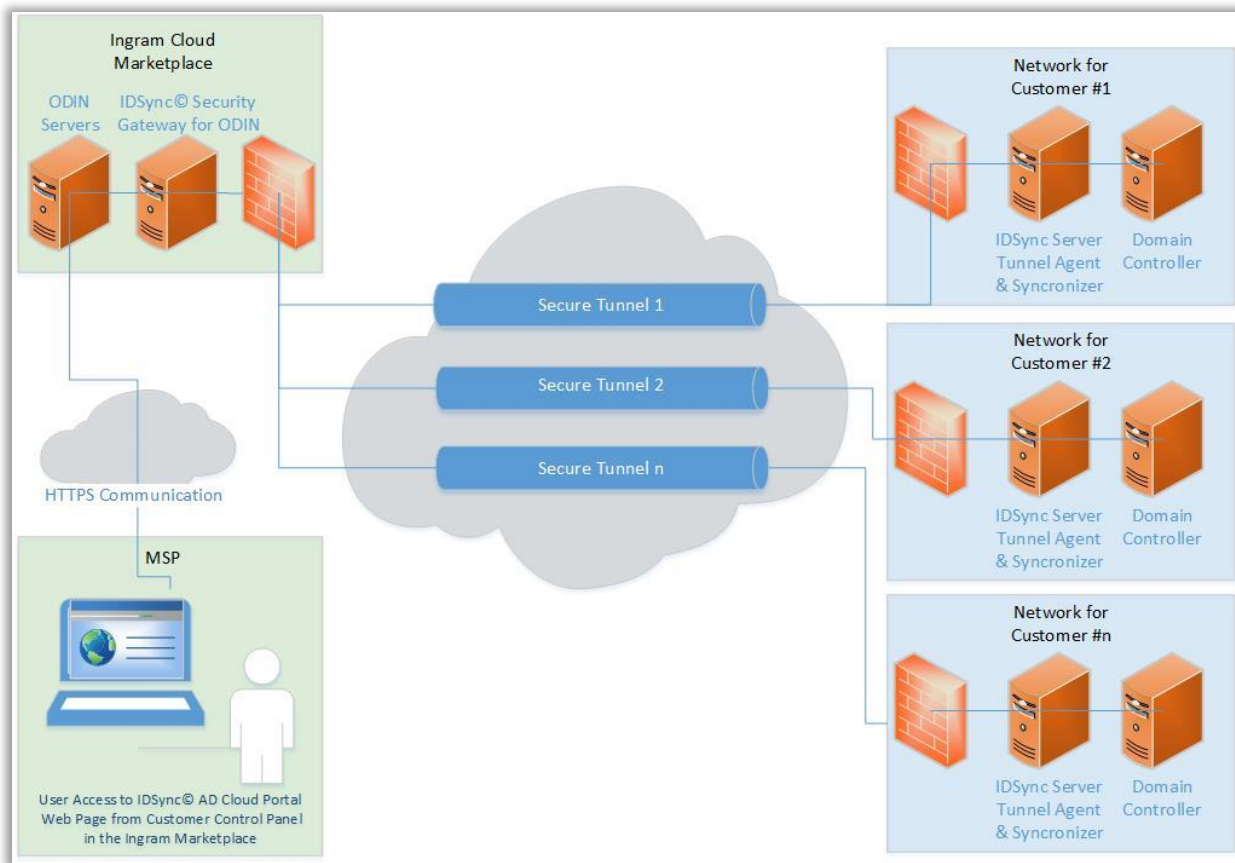


Figure 1.2-1

General Information

System Components

The IDSync® Cloud Portal System consists of four components (see figure 1.3-1):

☞ **IDSync® Management Studio** – The IDSync® Management Studio is the interface that provides the means to configure the IDSync® System and to install and monitor the IDSync® Services, which are necessary for communications between Active Directory and the AD Cloud Portal interface.

☞ **IDSync® Security Studio** – It's the configuration center for Security Users, Profiles and Scopes, which form the foundation to provide and limit the Security Rights and Access Levels that each user requires and is permitted.

☞ **IDSync® Services** – These applications operate as windows background processes and provide the required communication between Active Directory and the Cloud Portal interface.

☞ **IDSync® Cloud Console** – This is the cloud-based interface where the remote actual administration of the AD Users, Groups and Computers is enabled.

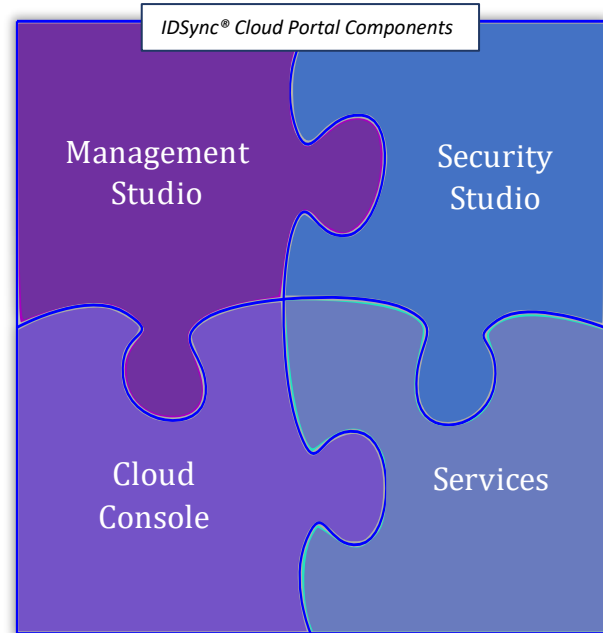
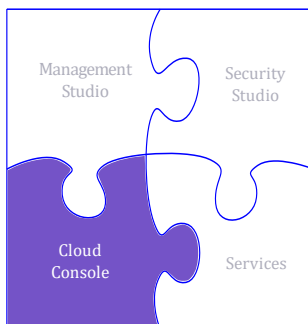


Figure 1.3-1

These components build their configurations and operations on top of a SQL Server database, where they store all the data they need to work.



This guide will focus on the IDSync® Cloud Console, and will explain the Security elements available to manage Active Directory Objects. More information about the IDSync® Management Studio and the Security Studio is available in their respective User Guides.

AD Cloud Portal Concepts

☞ **Cloud Portal User:** Any individual who is authorized to access the ADCP (using the Cloud Console or the Security Studio).

☞ **Cloud Portal Group:** A collection of Cloud Portal Users who share a common set of characteristics (for example, a common Security clearance level).

☞ **AD Secured Objects:** Any User, Group, Contact or Computer within an Active Directory environment that may be managed via ADCP.

☞ **Security Feature:** Any function that can be performed by a Cloud Portal User on an AD or Security Object, for example, editing User's Properties or running a Report.

☞ **Features Profile:** A list of Security Features that have been assigned to a Cloud Portal User or Group of Users and they can perform.

☞ **Scope:** A list of AD Users, Groups or Organizational Units that can be managed by a Cloud Console User. Along with Cloud Portal Users and Features, Scopes define a Security Profile (see figure 1.4-1).

☞ **Self-Service Profile:** An interface to perform functions (actions) limited to a single AD User (independent of other service Users), making faster and more convenient transactions (e.g., a User changing his own password).

☞ **Pre-defined and Customized Reports:** Specific and organized information showing the current state of a given set of Objects (e.g., a list of all Cloud Portal Users with assigned Profiles and Scopes). ADCP offers a Report Designer to build detailed and fully customized reports.

☞ **Managed Users Report:** A list of AD Users that are manageable via AD Cloud Console.

☞ **Transactions:** A list of changes that have occurred via ADCP. Such changes include: actions made on the Security Module (e.g., modifying a profile or a scope) as well as changes made to AD Objects (e.g., changing a User's Home Address).

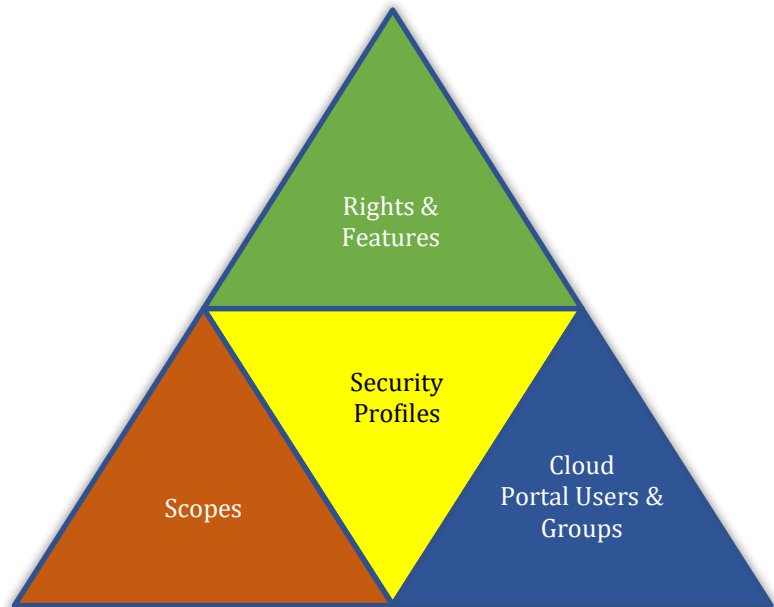
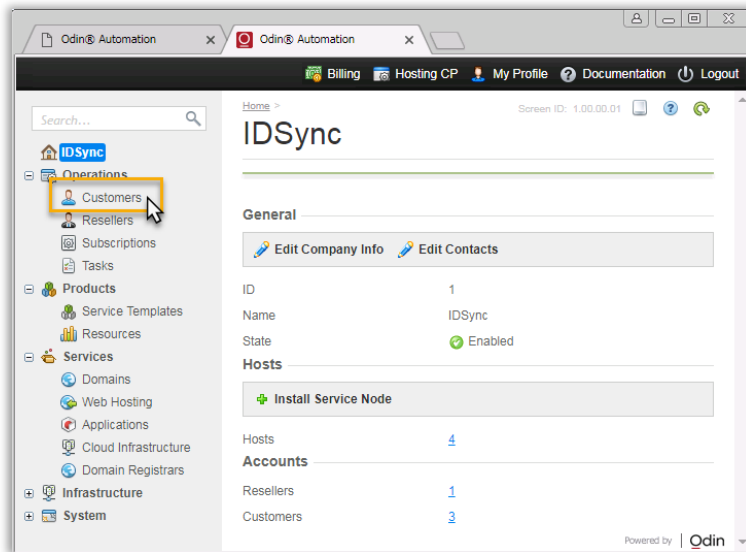


Figure 1.4-1

Getting Started

Accessing the IDSync Cloud Console

To access the IDSync Cloud Portal, an MSP begins by logging into their ODIN subscription and accessing the Reseller Control Panel as shown in figure 2.2-1.



- Then select "Customers" to bring up a list of Customers that are configured through the ODIN system.

- Once the list of customers is displayed, locate the customer for which you wish to manage the Active Directory objects.

- Select the shortcut to login as the Customer into the customer's ODIN Control Panel (see figure 2.2-2).

Figure 2.2-1

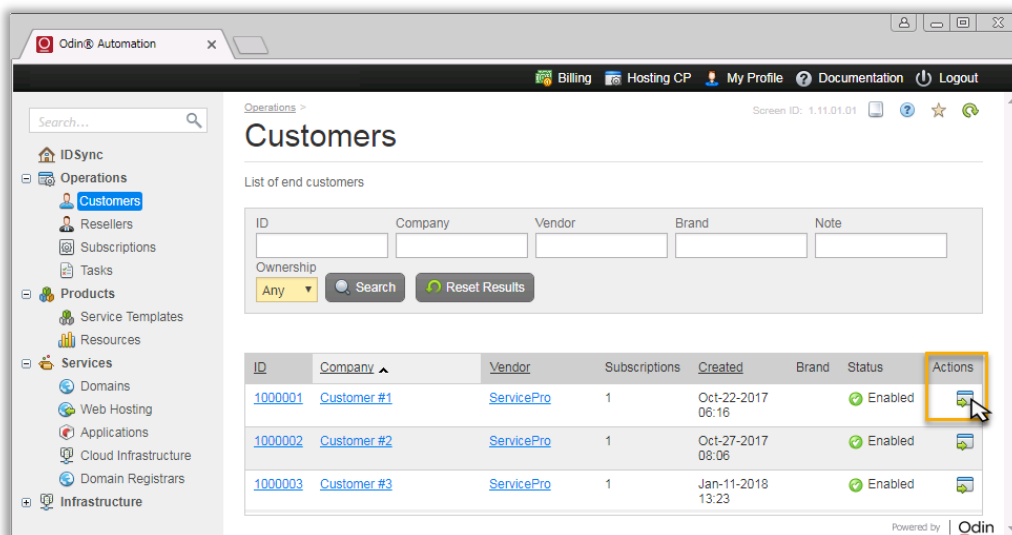


Figure 2.2-2

Accessing the IDSync Cloud Console

The shortcut to the Customer's Control Panel will bring up a window similar to the one shown in figure 2.2-3.

Locate the IDSync tab and select it to show the IDSync Control Panel.

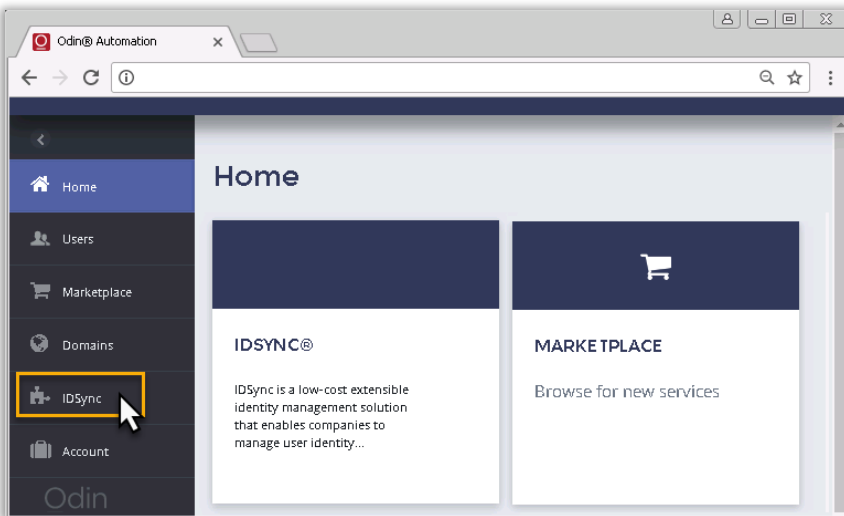


Figure 2.2-3

To begin displaying Users, Groups, Contacts, or Computers click on the desired tab, as shown in figure 2.2-4.

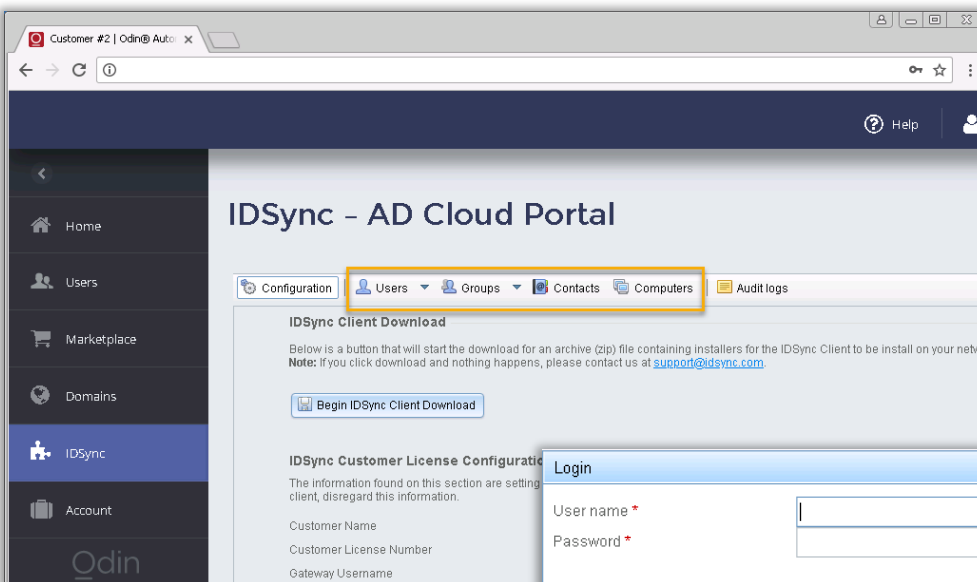


Figure 2.2-4

A Login window will then prompt for the user's credentials (the actual rights of the user will enable the correct set of actions that the user can perform).

Accessing the IDSync Cloud Console

Note that the initial load of data from on-premise Active Directory may take a few minutes depending on the size of the directory that you are working with (lab-tests show less than a minute to retrieve a 500 users directory).

While the objects are loading, a message will display, as shown in figure 2.2-5.

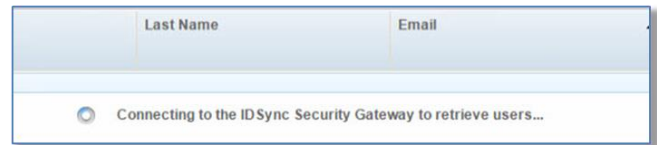
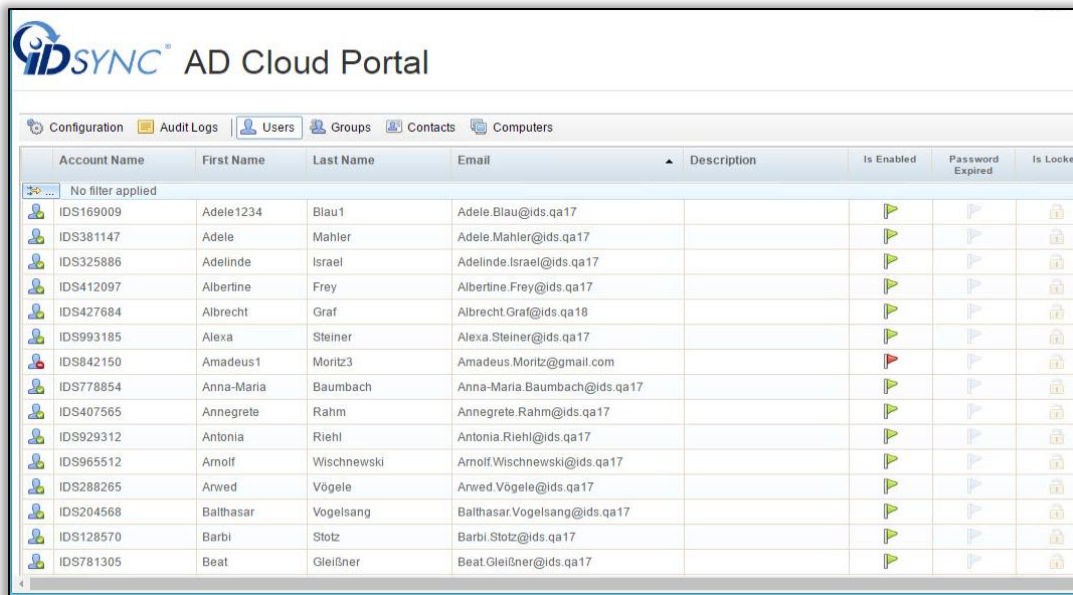


Figure 2.2-5

After selecting the Users tab in AD Cloud Portal, a list of on-premise AD Users will display.



Account Name	First Name	Last Name	Email	Description	Is Enabled	Password Expired	Is Locked
No filter applied							
IDS169009	Adele1234	Blau1	Adele.Blau@ids.qa17				
IDS381147	Adele	Mahler	Adele.Mahler@ids.qa17				
IDS325886	Adelinde	Israel	Adelinde.Israel@ids.qa17				
IDS412097	Albertine	Frey	Albertine.Frey@ids.qa17				
IDS427684	Albrecht	Graf	Albrecht.Graf@ids.qa18				
IDS993185	Alexa	Steiner	Alexa.Steiner@ids.qa17				
IDS842150	Amadeus1	Moritz3	Amadeus.Moritz@gmail.com				
IDS778854	Anna-Maria	Baumbach	Anna-Maria.Baumbach@ids.qa17				
IDS407565	Annegrete	Rahm	Annegrete.Rahm@ids.qa17				
IDS929312	Antonia	Riehl	Antonia.Riehl@ids.qa17				
IDS965512	Arnolf	Wischnewski	Arnolf.Wischnewski@ids.qa17				
IDS288265	Arwed	Vögele	Arwed.Vögele@ids.qa17				
IDS204568	Balthasar	Vogelsang	Balthasar.Vogelsang@ids.qa17				
IDS128570	Barbi	Stotz	Barbi.Stotz@ids.qa17				
IDS781305	Beat	Gleifner	Beat.Gleifner@ids.qa17				

Figure 2.2-6

Working with Active Directory Objects

Viewing Active Directory Objects

Through the IDSync AD Cloud Portal, an MSP can gain access to view Users, Groups, Contacts, and Computers within the customer's on-premise active directory. To view any of these respective categories of information, simply select the corresponding menu option as shown in figure 3.1-1.



Figure 3.1-1

Viewing AD Computers

By clicking on the Computers tab, a list of computer objects from the on-premise Active Directory will display.

To see further information about any given computer, right mouse-button on the name of the computer and select the properties menu item as shown in figure 3.1.1-1.

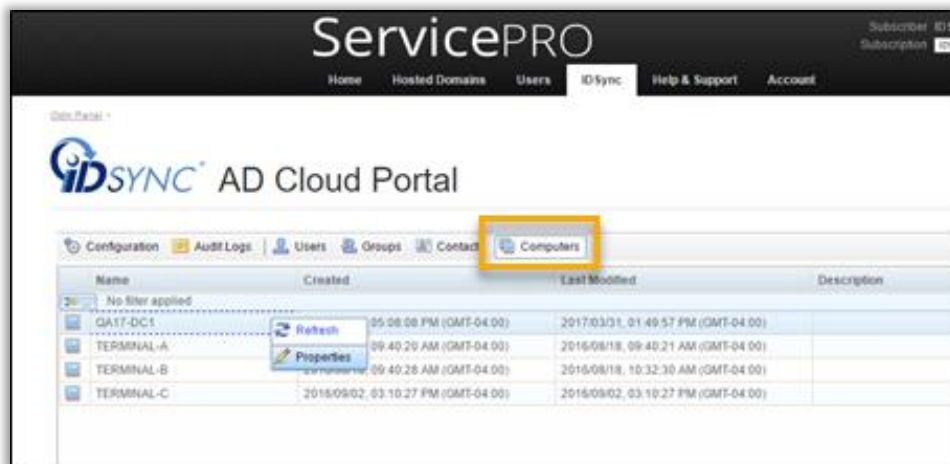


Figure 3.1.1-1

Viewing Active Directory Objects - Computers

General information about the computer includes its operating system version location and description.

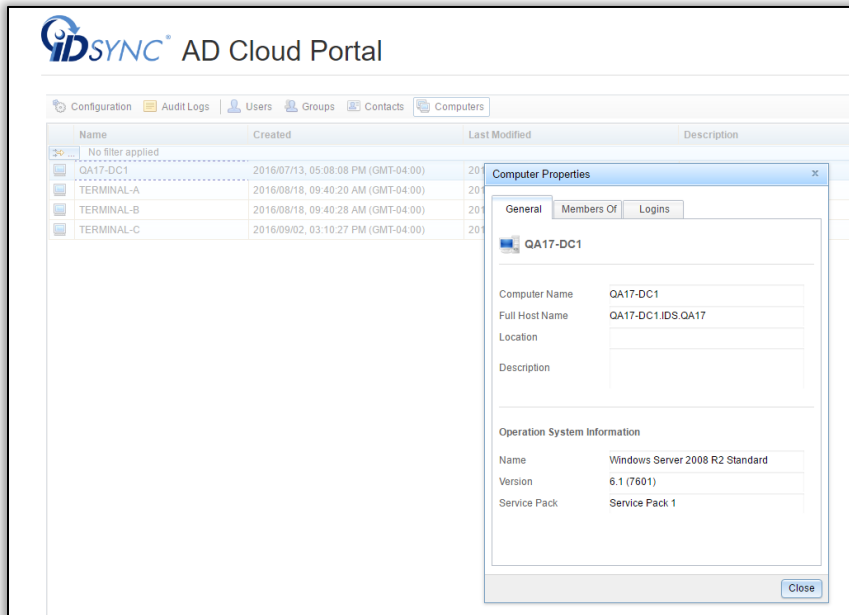


Figure 3.1.1-2

Membership information show which groups this computer is member of.

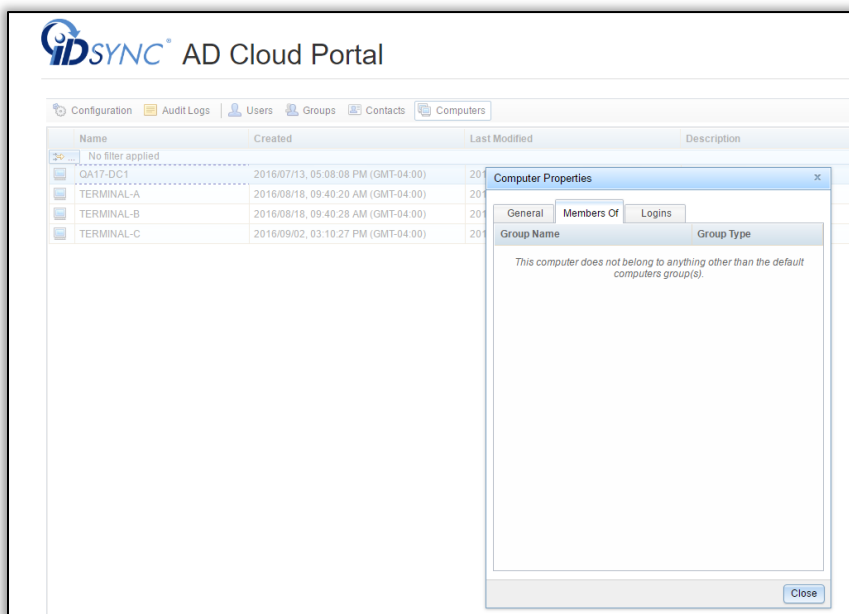
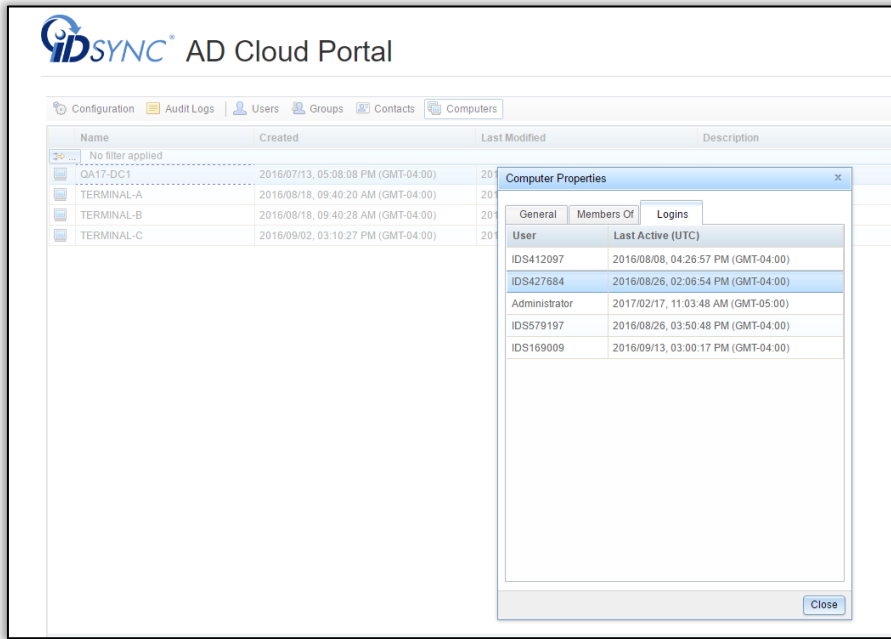


Figure 3.1.1-3

Viewing Active Directory Objects - Computers

Logins shows a record of the user accounts that have logged into the machine.



The screenshot shows the IDSync AD Cloud Portal interface. The main window displays a list of Active Directory objects under the 'Computers' tab. A 'Computer Properties' dialog box is open, showing the 'Logins' tab with a table of user login records.

Name	Created	Last Modified	Description
QAIT-DC1	2016/07/13, 05:08:08 PM (GMT-04:00)	2016/08/18, 09:40:20 AM (GMT-04:00)	2016/08/18, 09:40:28 AM (GMT-04:00)
TERMINAL-A	2016/08/18, 09:40:20 AM (GMT-04:00)	2016/08/18, 09:40:28 AM (GMT-04:00)	2016/09/02, 03:10:27 PM (GMT-04:00)
TERMINAL-B	2016/08/18, 09:40:28 AM (GMT-04:00)	2016/08/18, 09:40:28 AM (GMT-04:00)	
TERMINAL-C	2016/09/02, 03:10:27 PM (GMT-04:00)		

User	Last Active (UTC)
IDS412097	2016/08/08, 04:26:57 PM (GMT-04:00)
IDS427684	2016/08/26, 02:06:54 PM (GMT-04:00)
Administrator	2017/02/17, 11:03:48 AM (GMT-05:00)
IDS579197	2016/08/26, 03:50:48 PM (GMT-04:00)
IDS169009	2016/09/13, 03:00:17 PM (GMT-04:00)

Figure 3.1.1-4

Viewing Active Directory Objects

Viewing AD Contacts

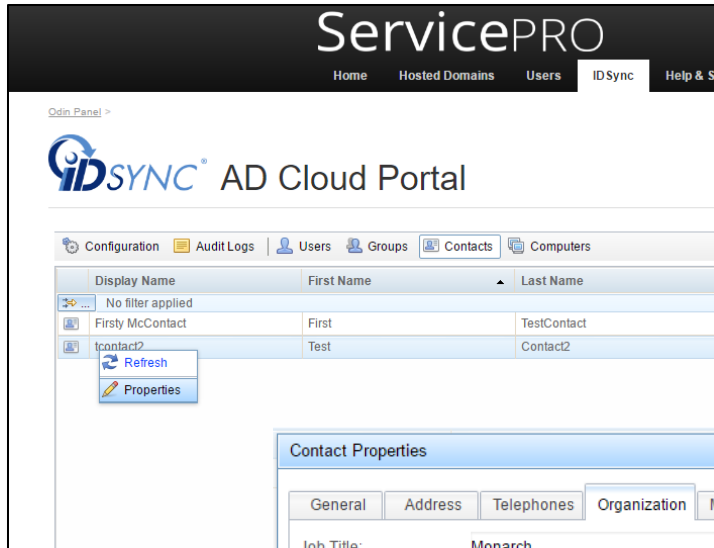
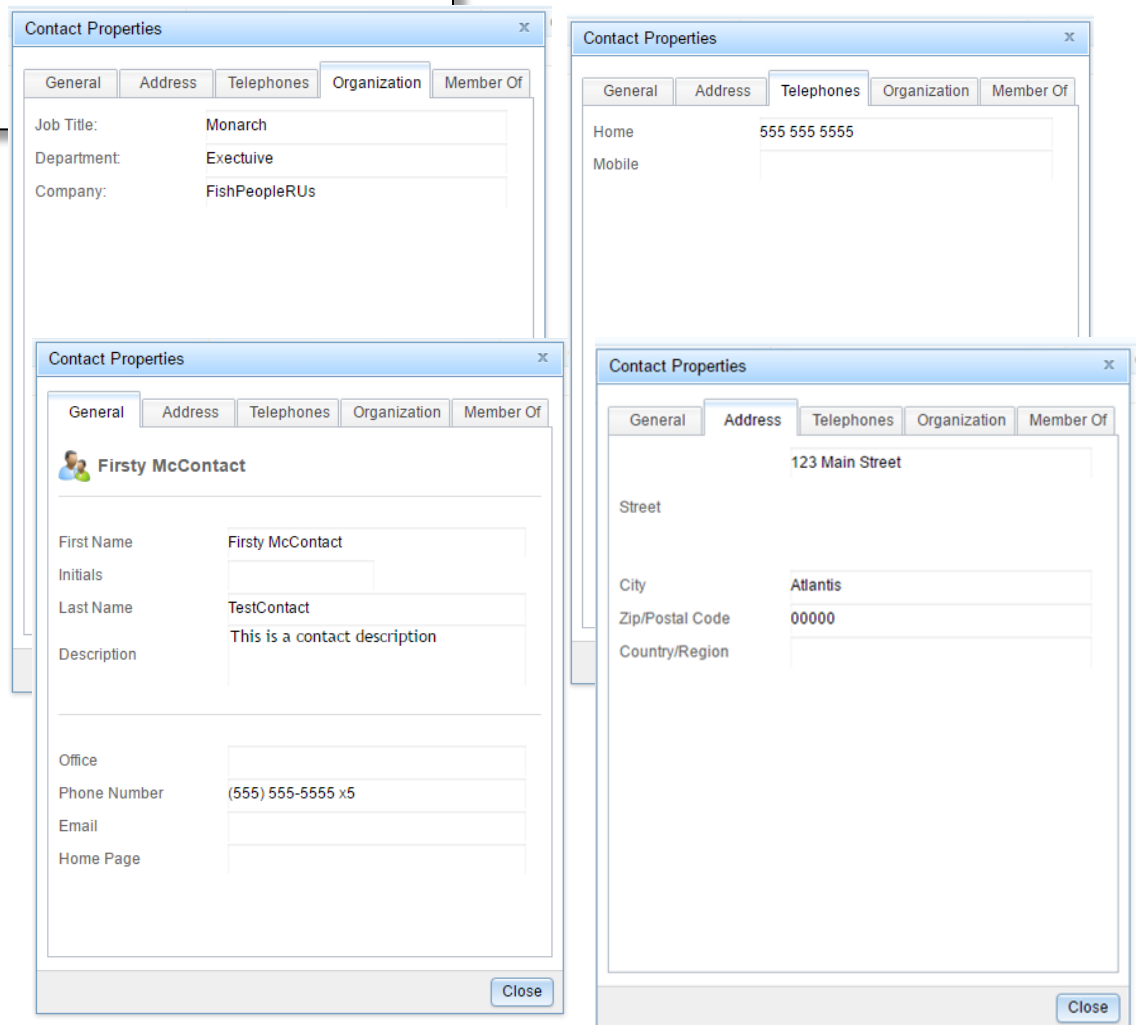


Figure 3.1.2-1

To view Active Directory Contacts, select the Contacts tab from the AD Cloud Portal.

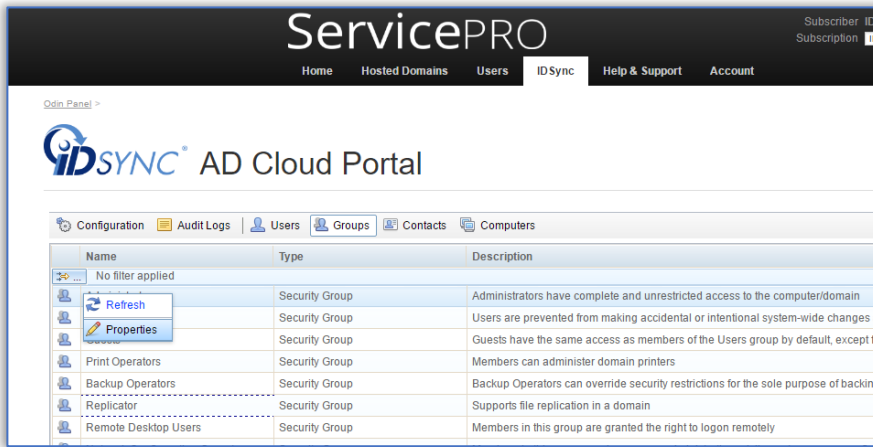
- To see further details about a specific contact, right-mouse button on the contact's name and select the properties menu option as shown in figure 3.1.2-1.



All of the familiar contact property tab sheets that would show in Active Directory Users and Computers are replicated in the IDSync AD Cloud Portal interface.

Viewing Active Directory Objects

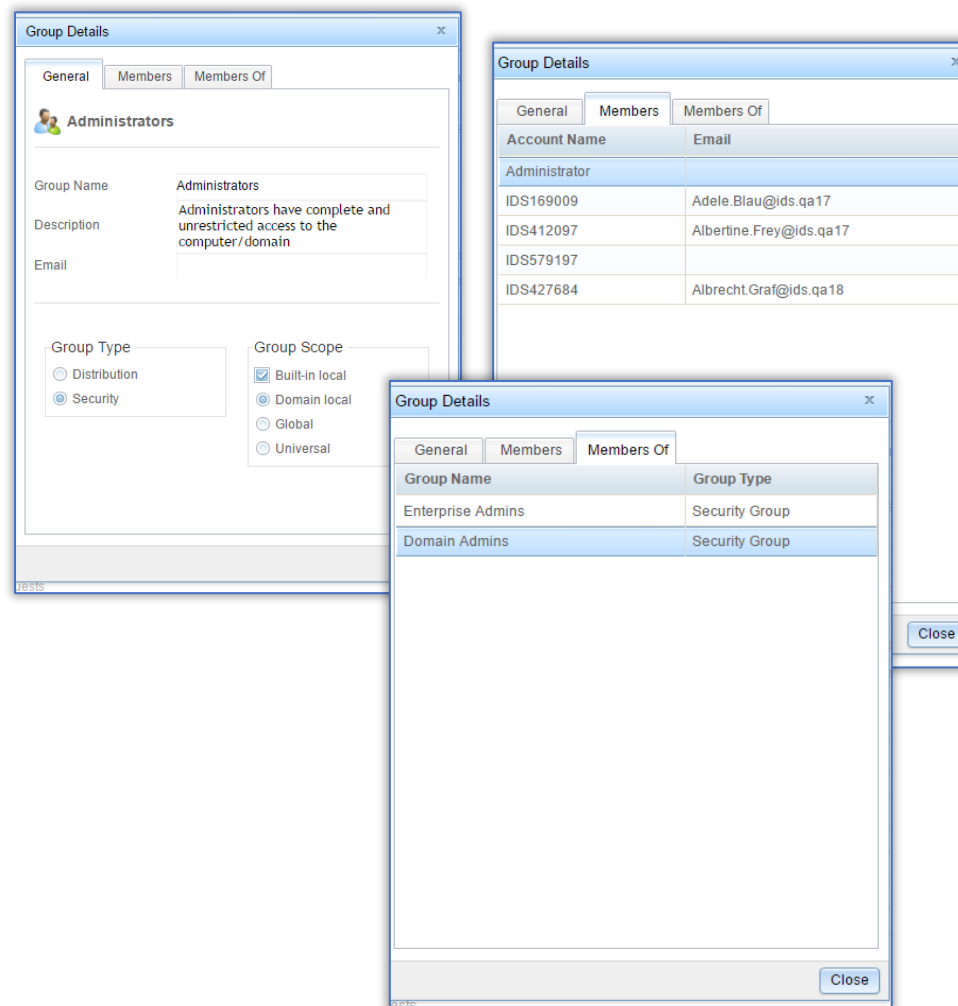
Viewing AD Groups



To view on-premise Active Directory Groups, select the Groups tab from the AD Cloud Portal. To see further details about a specific group, right-mouse button on the group's name and select the properties menu option as shown in Figure 3.1.3-1.

Figure 3.1.3-1

All of the familiar group property tab sheets that would show in Active Directory Users and Computers are replicated in the IDSync® Cloud Console interface.



Viewing Active Directory Objects

Viewing AD Users

To view on-premise Active Directory users, select the Users tab from the AD Cloud Portal. To see further details about a specific user, right-mouse button on the user's name and select the properties menu option as shown in figure 3.1.4-1.

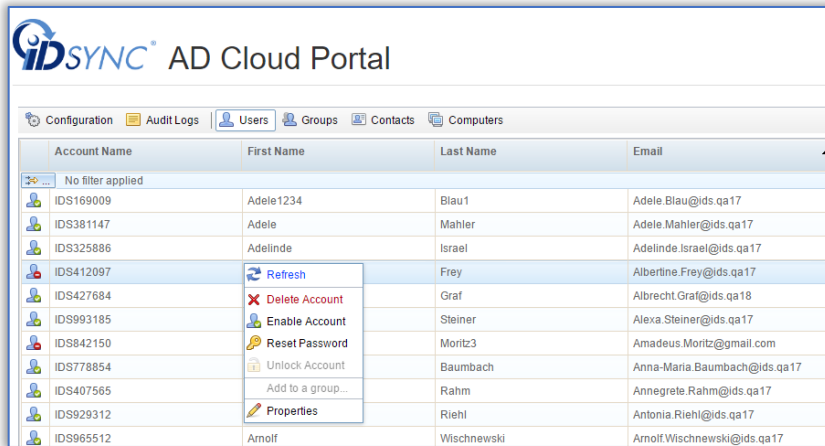


Figure 3.1.4-1

All of the familiar user property tab sheets that would show in Active Directory Users and Computers are replicated in the IDSync® Cloud Console interface.

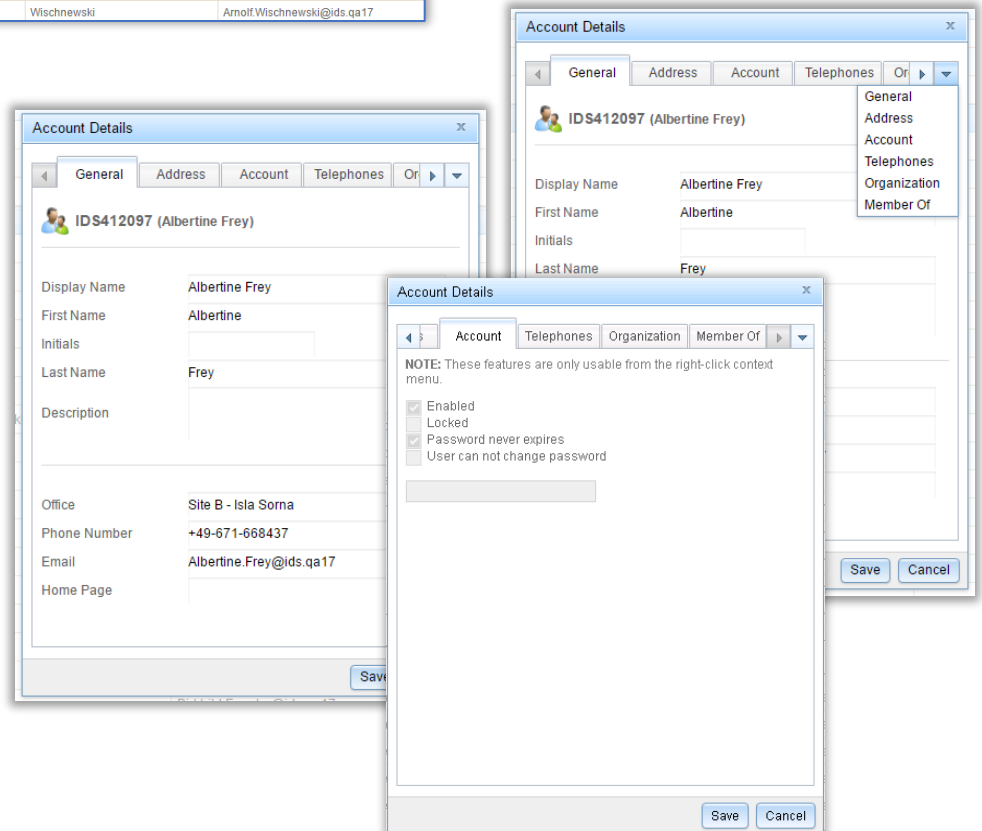


Figure 3.1.4-2

Creating Active Directory Objects

Creating AD Users

Creating Active Directory Users within the IDSync® Cloud Console is a simple process:

- Click on the arrow at the right of the Users tab and select the Add New User Option.

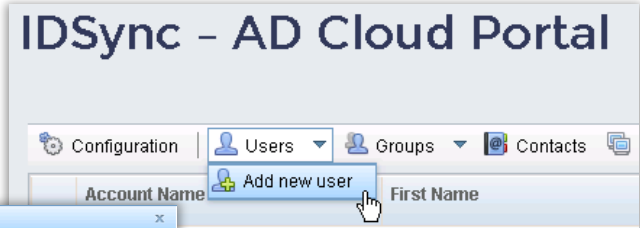


Figure 3.2.1-1

- Fill in the fields on the 'Create new user' form

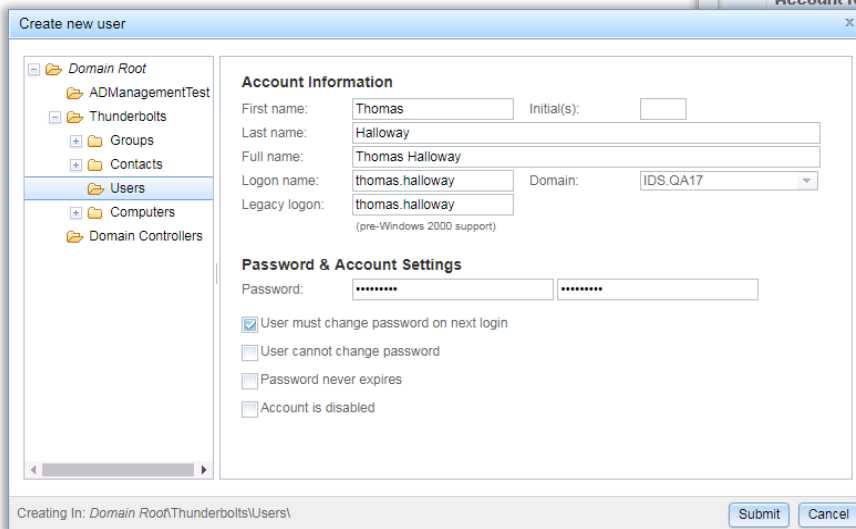


Figure 3.2.1-2

- Hit submit when ready

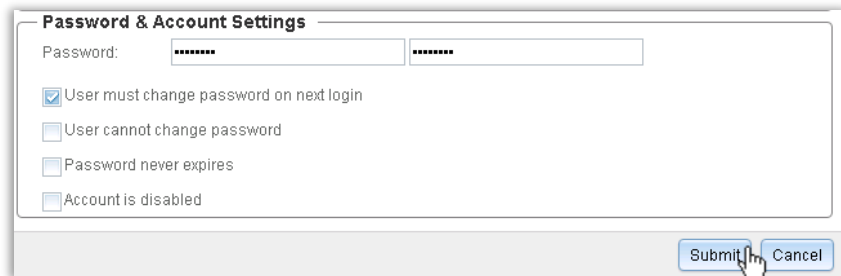


Figure 3.2.1-3

The new user will be available in Active Directory almost immediately.

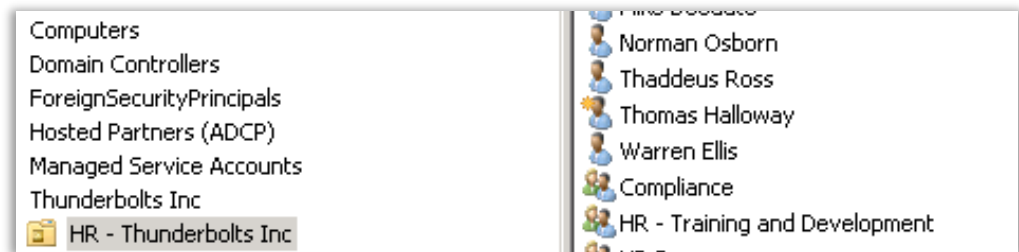


Figure 3.2.1-4

Creating AD Groups

Creating Active Directory Groups within the IDSync® Cloud Console is a simple 3-step process:

Click on the arrow at the right of the Users tab and select the Add New Group Option.

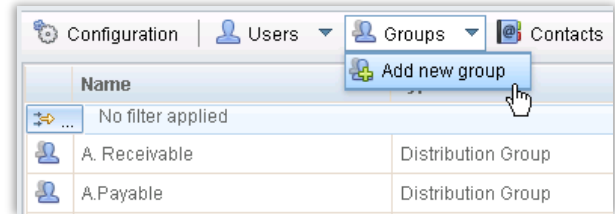


Figure 3.2.2-1

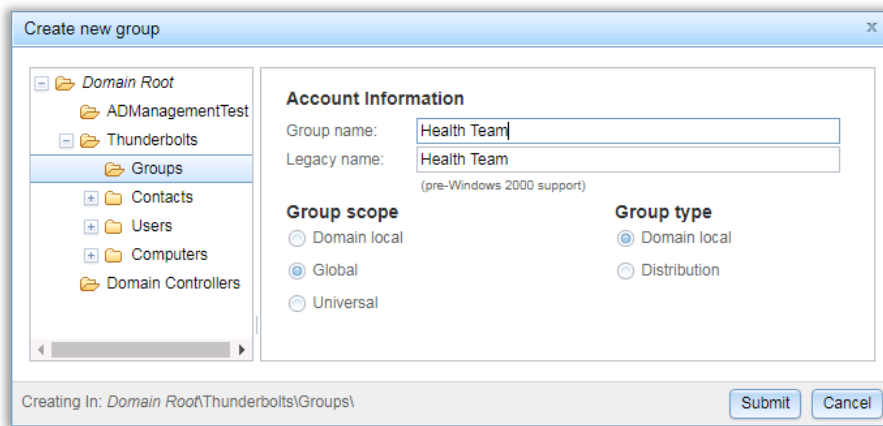


Figure 3.2.2-2

Hit submit when ready

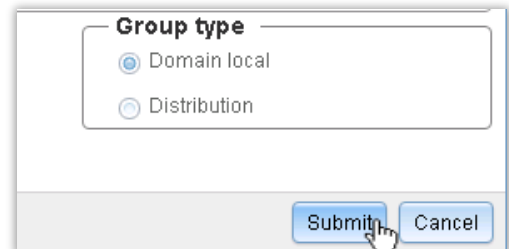


Figure 3.2.2-3

The new group will be available in Active Directory almost immediately.

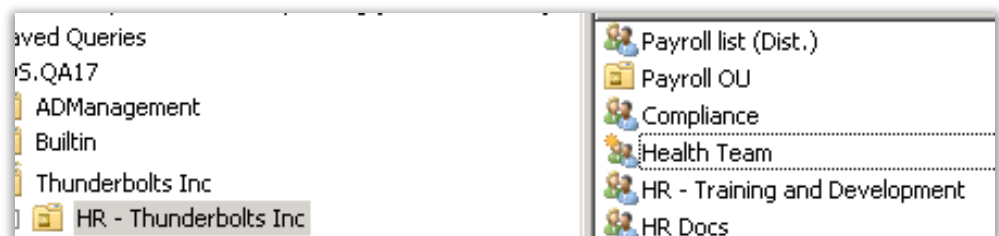


Figure 3.2.2-4

Editing Active Directory Objects

AD Cloud Portal enables the MSP to edit Active Directory properties on Users and Groups directly from the ODIN Customer’s Control Panel.

To do so, simply right mouse button on the user or group that you wish to edit and select Properties from the command menu, as shown in figure 3.3-1.

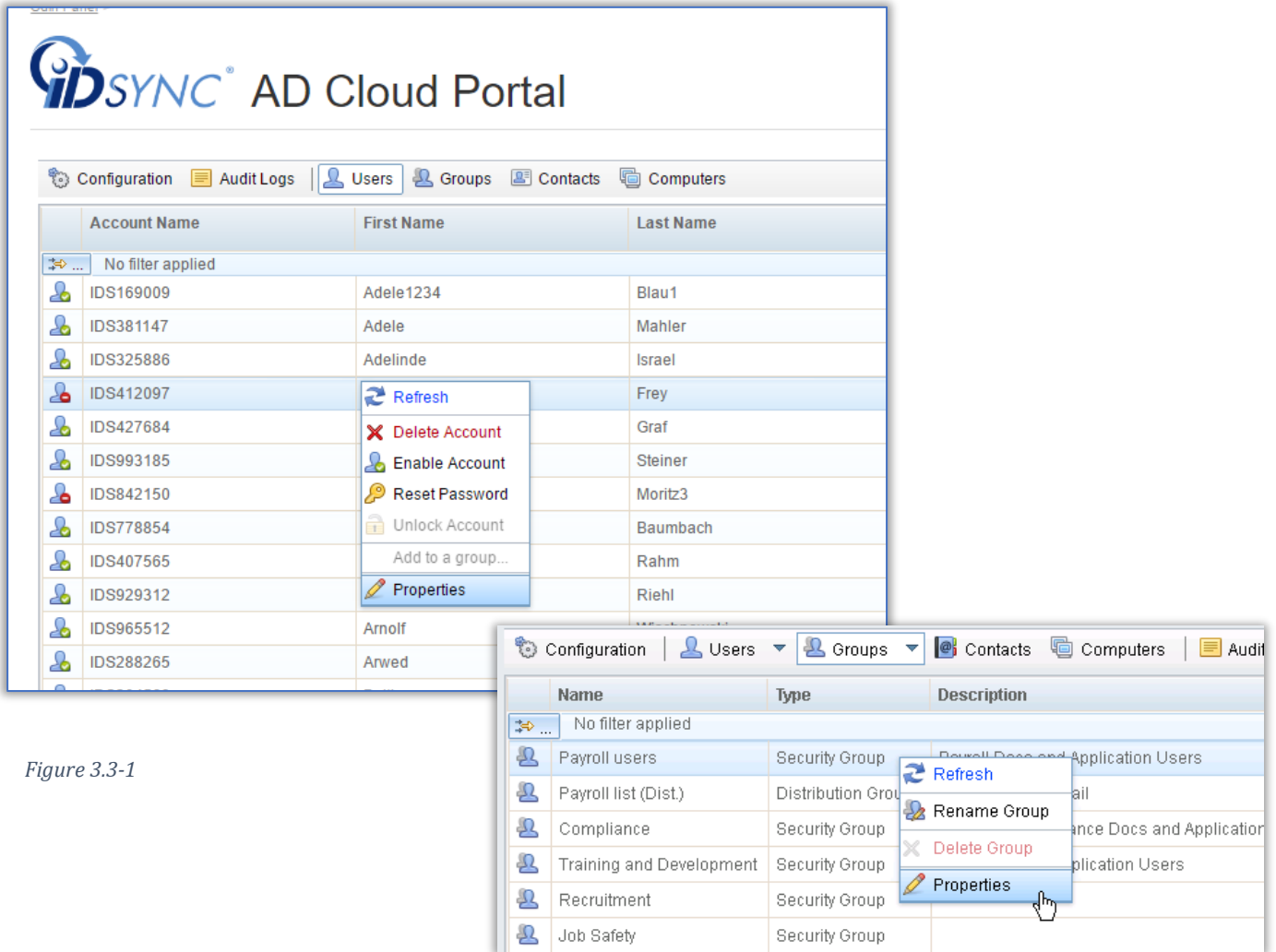
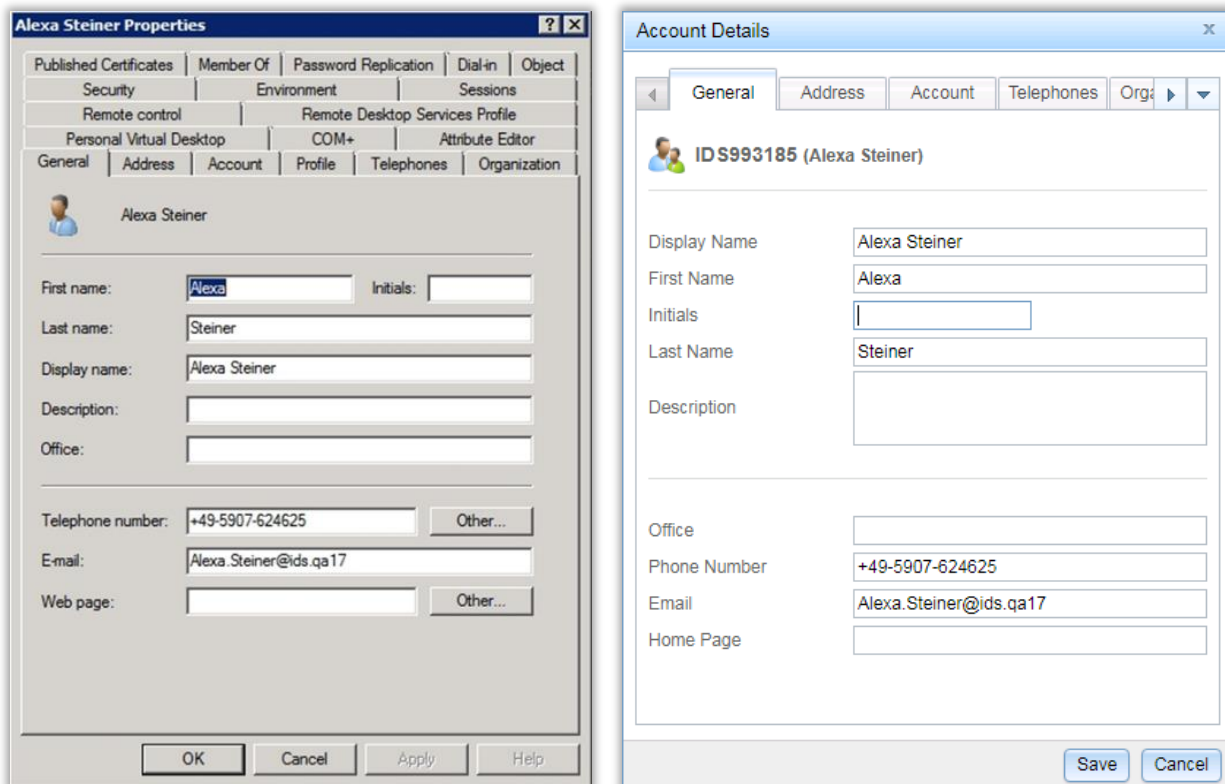


Figure 3.3-1

Editing AD Users Properties

Each of the Active Directory User properties that appear on the General, Address, Telephones and Organization tabs are replicated in the AD Cloud Console interface and may be edited through the AD Cloud Portal.

** The 'Account' tab is also replicated in the AD Cloud Console but is treated as a 'Read Only' section.



The image shows two side-by-side screenshots of user property editing interfaces. The left window, titled 'Alexa Steiner Properties', is a classic Windows-style dialog box with a tabbed interface. The 'General' tab is selected, showing fields for First name (Alexa), Last name (Steiner), Display name (Alexa Steiner), Telephone number (+49-5907-624625), and E-mail (Alexa.Steiner@ids.qa17). The right window, titled 'Account Details', is a modern web-style interface with a tabbed interface. The 'General' tab is selected, showing fields for Display Name (Alexa Steiner), First Name (Alexa), Last Name (Steiner), Telephone Number (+49-5907-624625), and Email (Alexa.Steiner@ids.qa17). Both windows have 'OK' and 'Cancel' buttons at the bottom.

Figure 3.3.1-1

Editing AD Users Properties

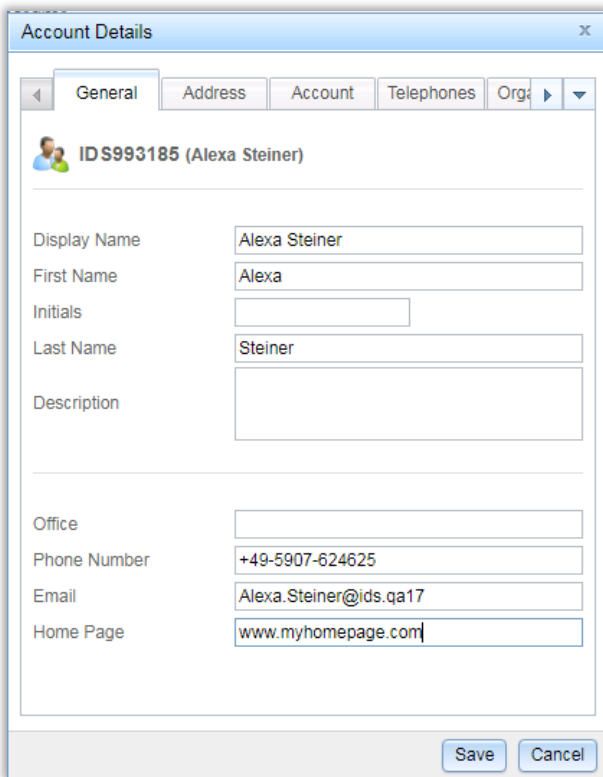
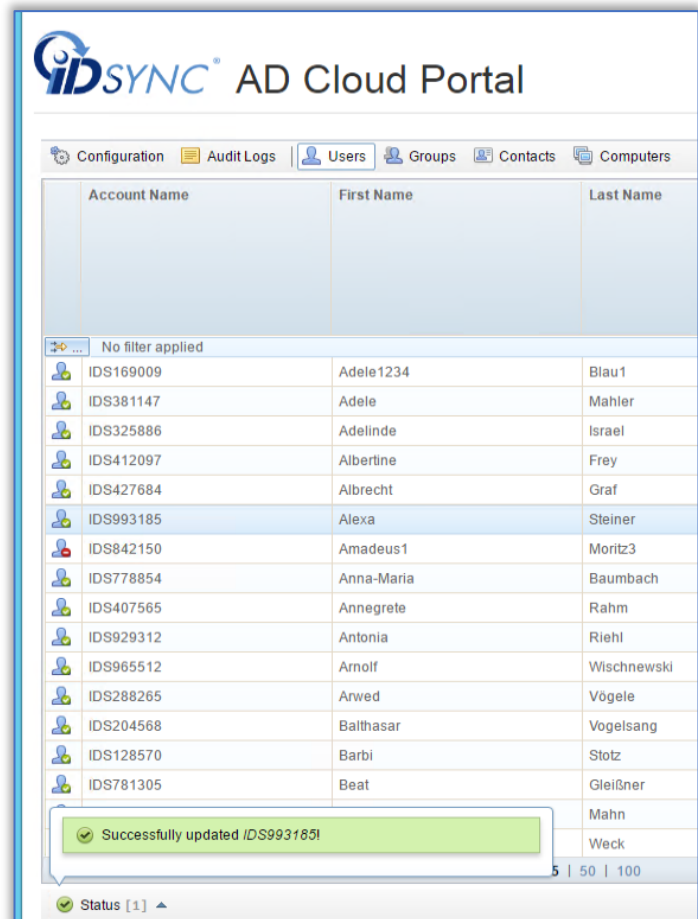


Figure 3.3.1-2

- After the changes have been completed, a success message should appear in the bottom left hand corner as shown in figure 3.3.1-3.

- To change a field in Active Directory, type in a value in the appropriate field in AD Cloud Portal's user properties as shown in figure 3.3.1-2 and click on the Save button to commit the change(s).



Account Name	First Name	Last Name
IDS169009	Adele1234	Blau1
IDS381147	Adele	Mahler
IDS325886	Adelinde	Israel
IDS412097	Albertine	Frey
IDS427684	Albrecht	Graf
IDS993185	Alexa	Steiner
IDS842150	Amadeus 1	Moritz3
IDS778854	Anna-Maria	Baumbach
IDS407565	Annegrete	Rahm
IDS929312	Antonia	Riehl
IDS965512	Arnolf	Wischnewski
IDS288265	Arwed	Vögele
IDS204568	Balthasar	Vogelsang
IDS128570	Barbi	Stotz
IDS781305	Beat	Gleißner
		Mahn
		Weck

Figure 3.3.1-3

Note: you may have to click on the word Status in the bottom left hand corner to trigger the system to display status messages.

Editing AD Users Properties

After the changes have been synchronized back to on-premise active directory, those changes should be reflected in active directory users and computers as shown in figure 3.3.1-4.

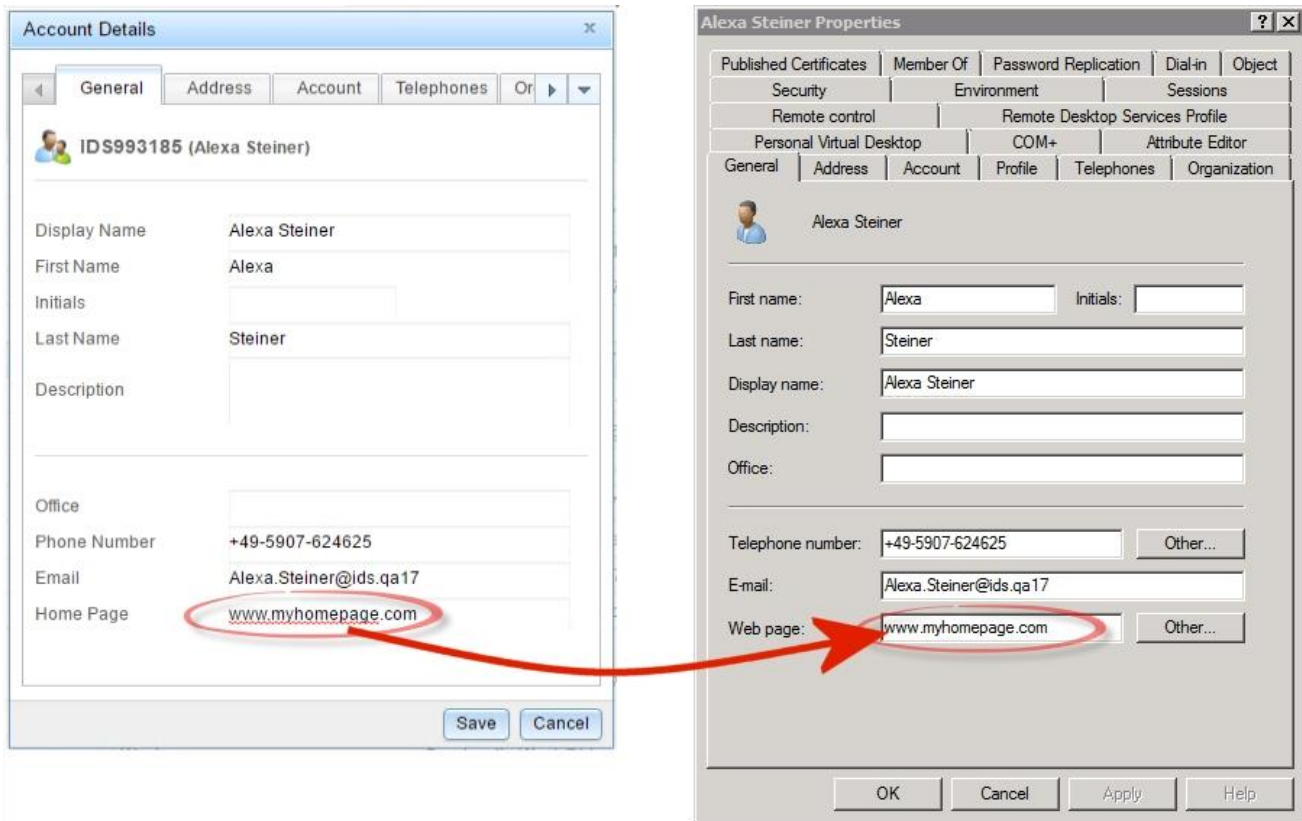


Figure 3.3.1-4

Editing Active Directory Users

Enabling/Disabling AD Users

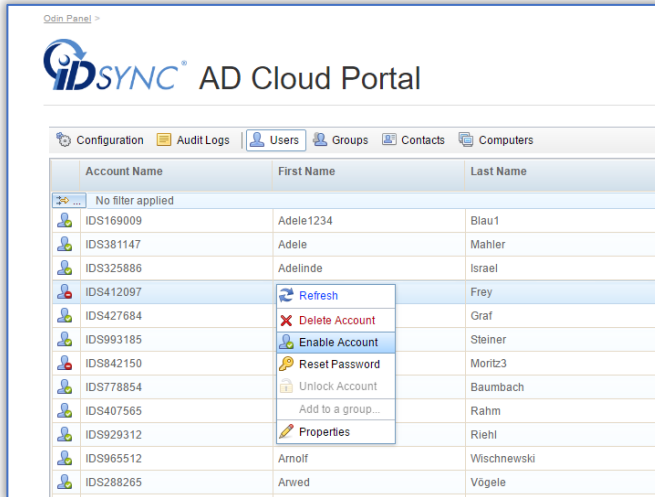


Figure 3.3.2-2

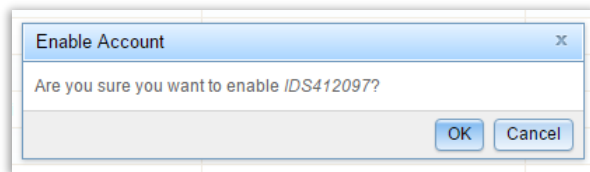


Figure 3.3.2-3

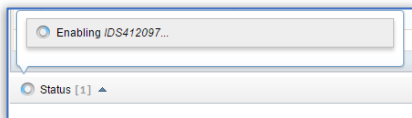


Figure 3.3.2-4

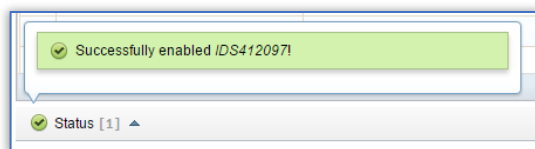


Figure 3.3.2-5

- To enable an on-premise active directory user, simply locate the disabled user from the IDSync AD Cloud Portal User's list.

A disabled user will display with an icon with a red "-" symbol as shown in figure 3.3.2-1.

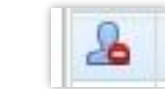


Figure 3.3.2-1

- Once the user is located, highlight the user, click the right mouse button to display the command menu as shown in Figure 3.3.2-2.
- Select "Enable Account".

A verification message will display.

- Confirm the enable command by clicking the OK button (figure 3.3.2-3).

A status message will be displayed in the bottom left-hand corner of the screen (figure 3.3.2-4).

When the Enable command completes, the status message should indicate success as shown in Figure 3.3.2-5. At this point, the user should be enabled in on-premise Active Directory.

Note: The process for disabling a user is identical to the steps for enabling a user except that you will select the "Disable user" menu option rather than the "Enable user" menu option.

Editing Active Directory Users

Changing Password for an AD User

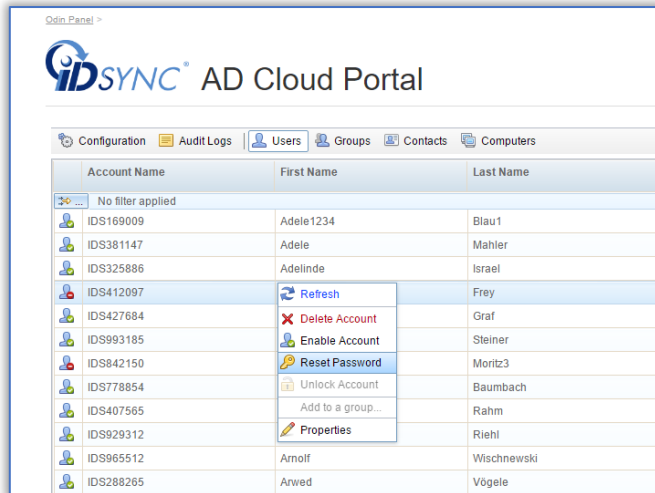


Figure 3.3.3-1

A reset password window like Figure 3.3.3-2 will open. The reset password window will perform some rudimentary password verification.

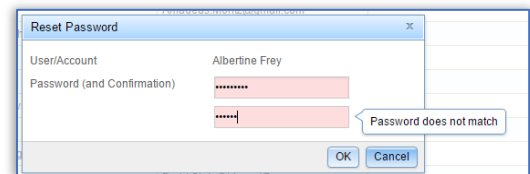


Figure 3.3.3-2

- Once you have successfully entered the new password, click OK to commit the change.

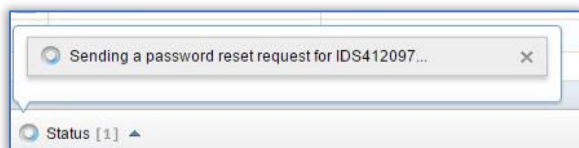


Figure 3.3.3-3

A status message will be displayed in the bottom left-hand corner of the screen.

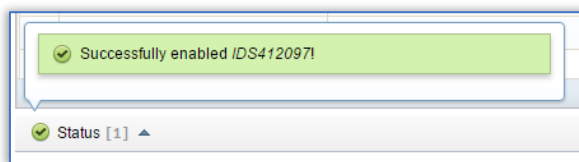


Figure 3.3.3-4

When the password change command completes, the status message should indicate success, as shown in Figure 3.3.3-4. At this point, the new password will be set for the user in on-premise Active Directory.

Editing Active Directory Users

Unlocking an AD User

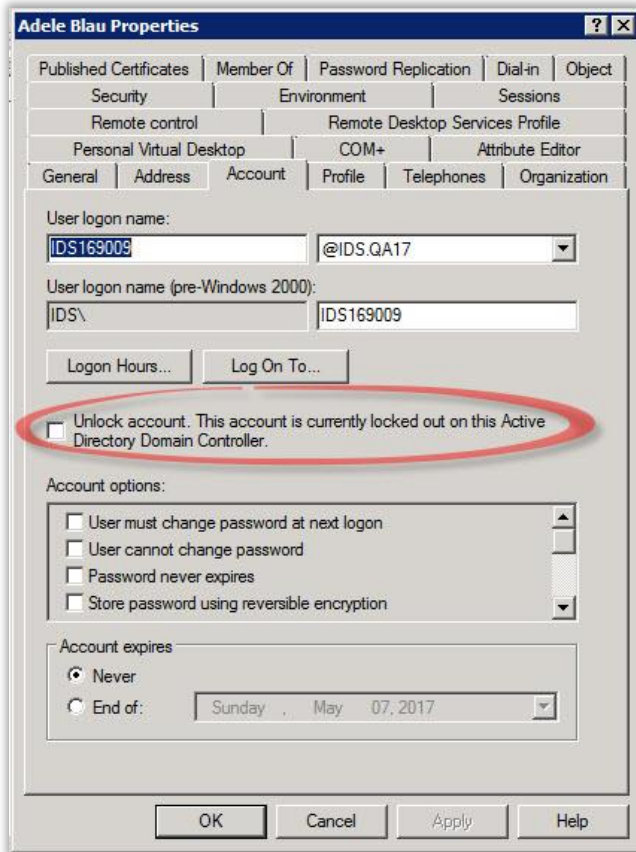


Figure 3.3.4-1

IDSync enables the MSP to remotely unlock locked user accounts. This feature is available in both the full AD Cloud Portal product and the light "Password Reset" version of the product.

A locked user account in Active Directory will display with a message like figure 3.3.4-1.

A locked user will appear in Cloud Portal as shown in figure 3.3.4-2.



Figure 3.3.4-2

Editing Active Directory Users

Unlocking an AD User

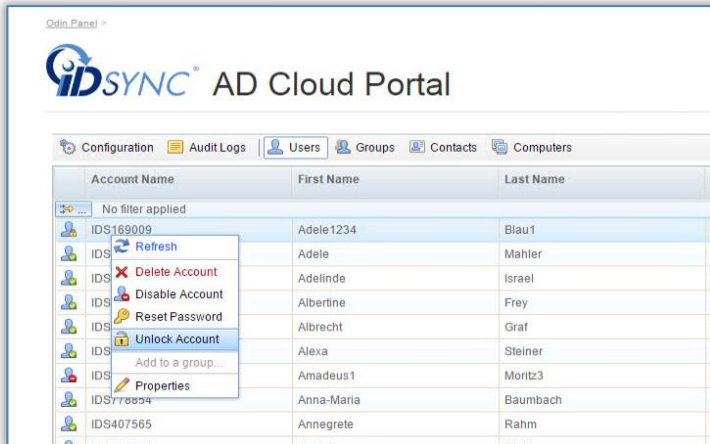


Figure 3.3.4-3

- To unlock a locked account, right mouse button on the account name of the user for which you wish to unlock. A command menu will display. Select "unlock account" from the menu.
- A confirmation message will be displayed similar to figure 3.3.4-4. Click on OK to confirm the unlock command



Figure 3.3.4-4

A status message will display in the lower left-hand corner, as shown in figure 3.3.4-5. Once it displays successful, the account will be unlocked in on-premise AD.

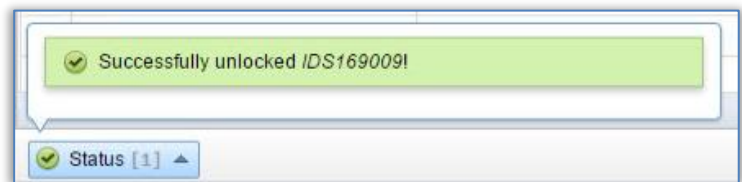


Figure 3.3.4-5

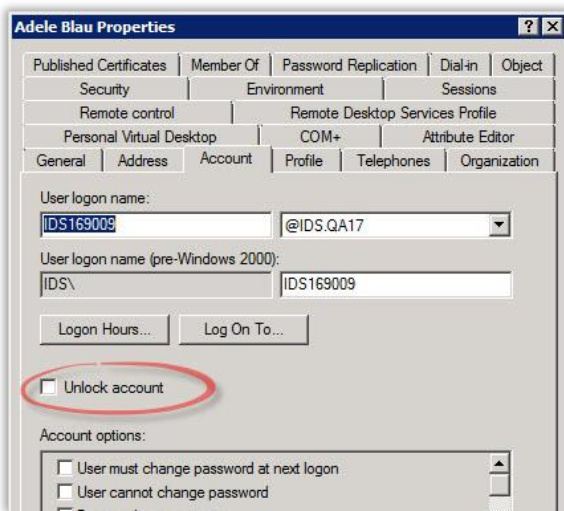
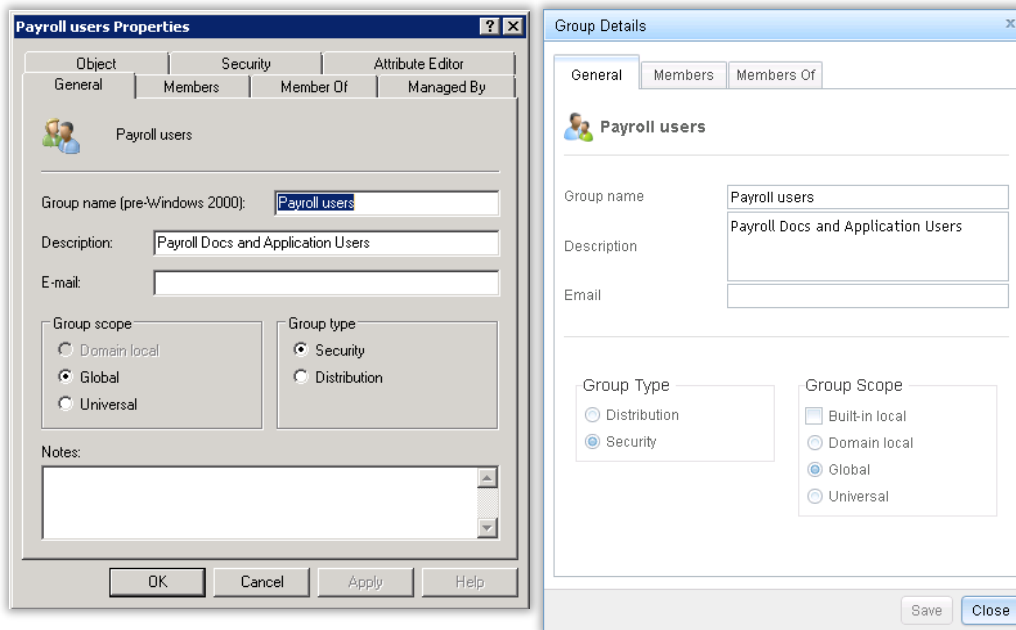


Figure 3.3.4-6

After the AD user has been unlocked, the on-premise AD user will appear with an "Unlocked account" message within Active Directory Users and Computers, as shown in figure 3.3.4-6.

Editing Active Directory Objects

Editing AD Groups Properties



Each of the Active Directory Group properties that appear on the General, Member and Member Of tabs are replicated in the AD Cloud Console interface, and may be edited through the AD Cloud Portal.

Figure 3.3.5-1

- To change a field in Active Directory, type in a value in the appropriate field in AD Cloud Portal's Group properties, as shown in figure 3.3.5-2 and click on the Save button to commit the change(s).

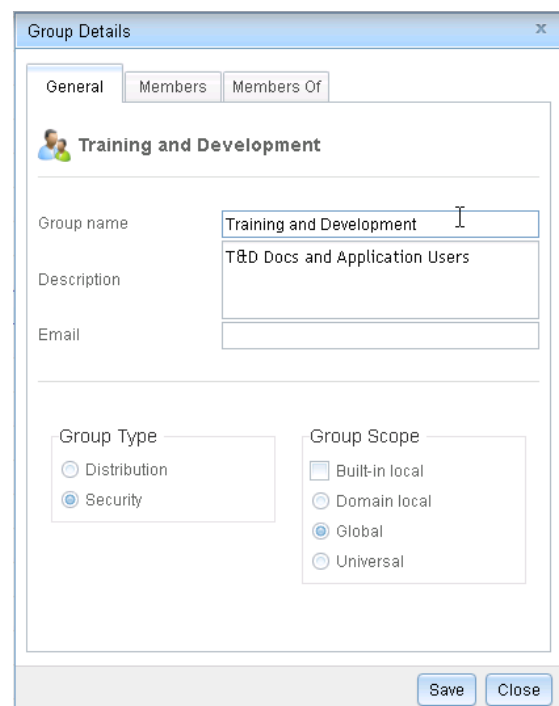


Figure 3.3.5-2

Editing AD Groups Properties

After the changes have been completed, a success message should appear in the bottom left hand corner as shown in figure 3.3.5-3.

- Note: you may have to click on the word Status in the bottom left hand corner to trigger the system to display status messages.

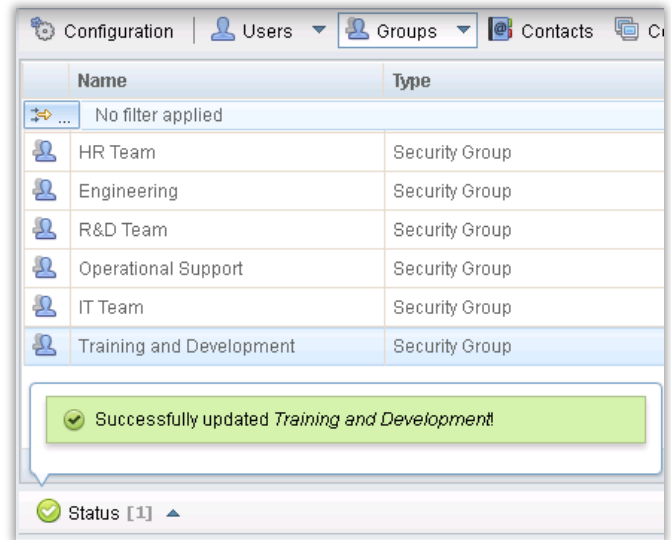


Figure 3.3.5-3

After the changes have been synchronized back to Active Directory, those changes should be reflected in the AD Group properties, as shown in Figure 3.3.5-4.

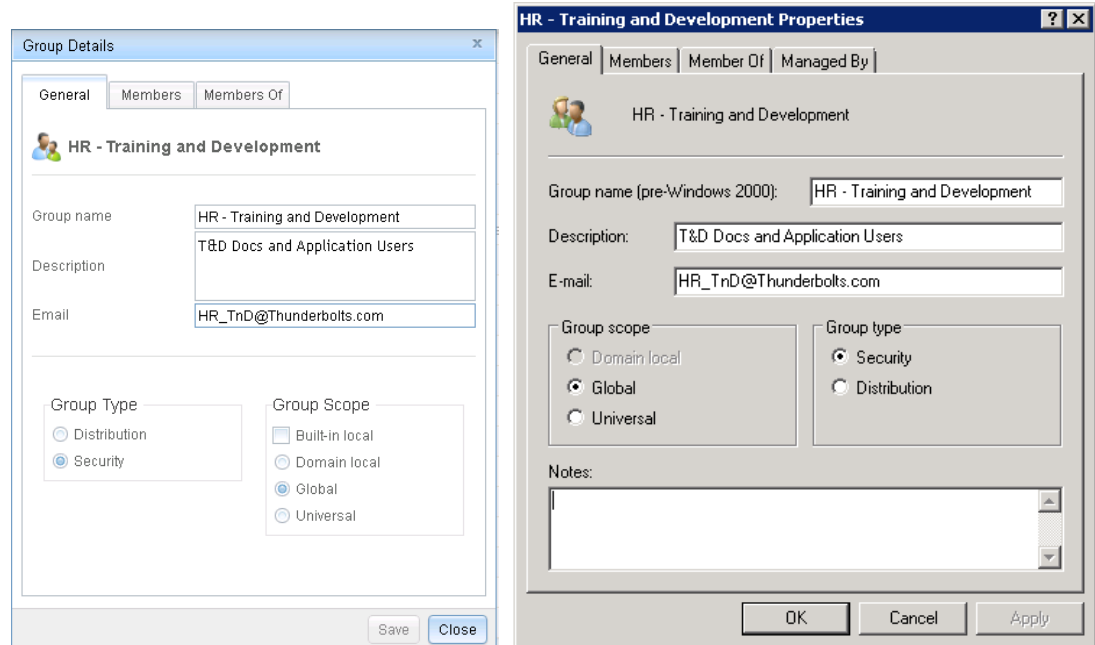


Figure 3.3.5-4

Adding/Removing Objects to Groups

Add/Remove Users to Groups

Users can be added to Groups following two different paths:

- From the User's **Member Of** tab within the user's properties page. This 'method' allows one user to be added to more than one group at a time.
- Go to the **Users** section, then look for the user that you want to add to a group.
- Right-click on the user and click on the **Properties** option.

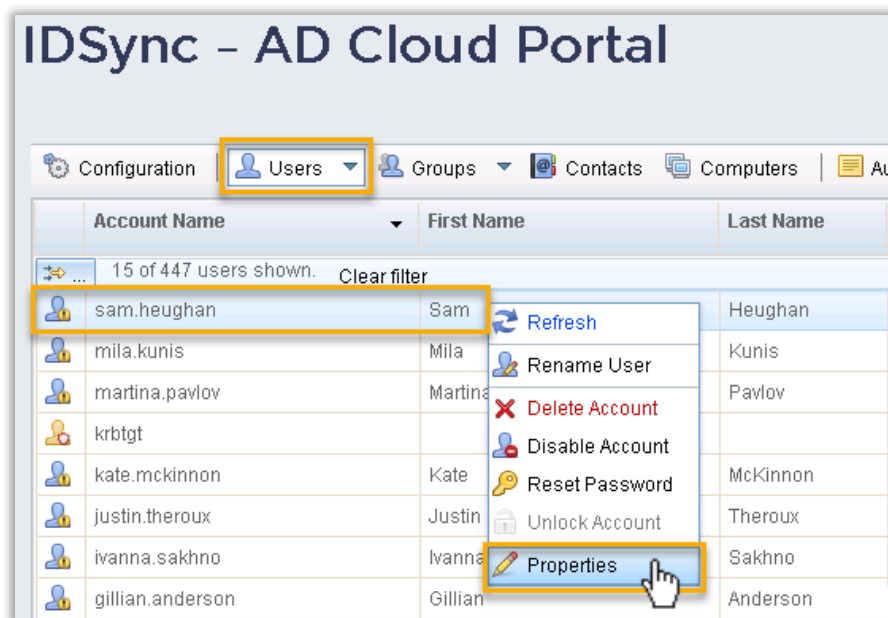


Figure 3.3.6-1

- Go to the '**Member Of**' tab (using any of the navigation buttons).

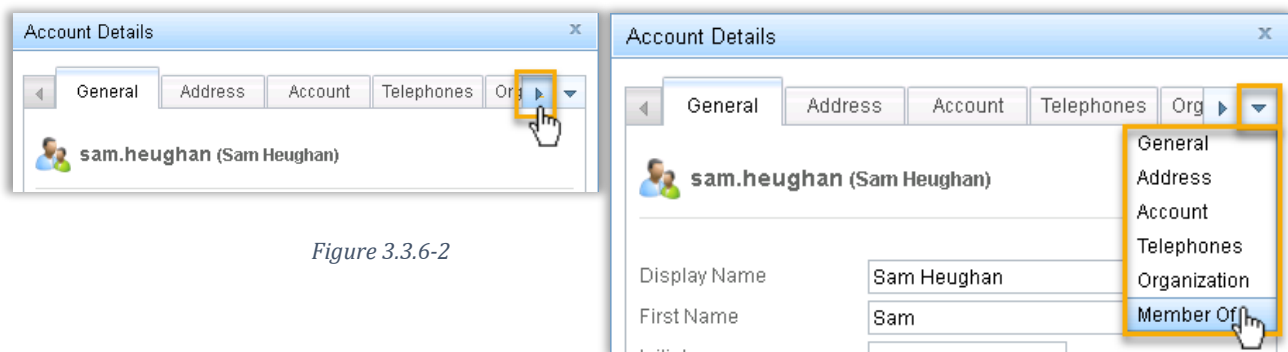


Figure 3.3.6-2

Adding/Removing Users to Groups

- Click on the Add button.

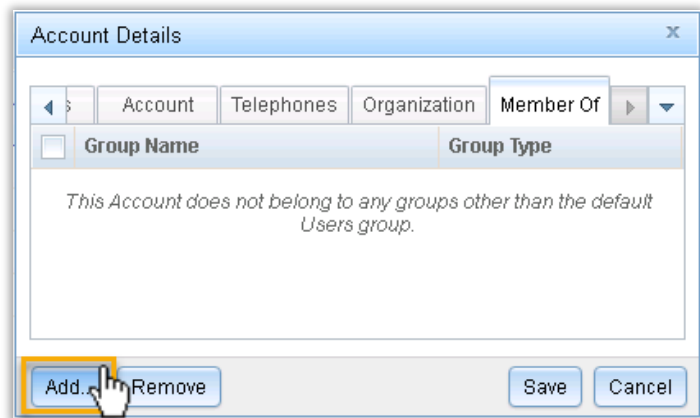


Figure 3.3.6-3



Figure 3.3.6-4

- Look for the group or groups you want the user to be added to and select each one of them (by clicking on the checkbox at the left of the group's name).

- Finally click on 'Add Selected Group(s)' to confirm this operation.



Figure 3.3.6-5

- In the Status bar look for any message regarding this addition.

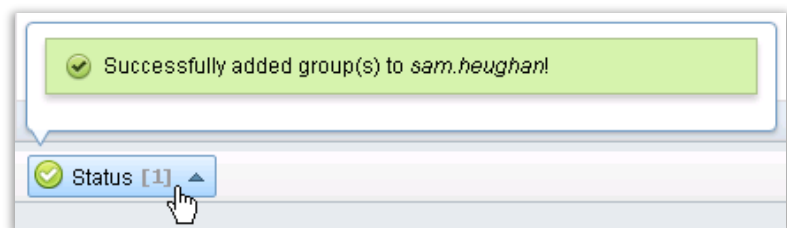


Figure 3.3.6-6

Adding/Removing Users to Groups

In a similar way, Removing a user from a Group is as simple as:

- Locate the user, open its properties page and go to the 'Member Of' tab.
- Select the group or groups you want to remove the user from (by clicking on the checkbox at the left of the group's name).

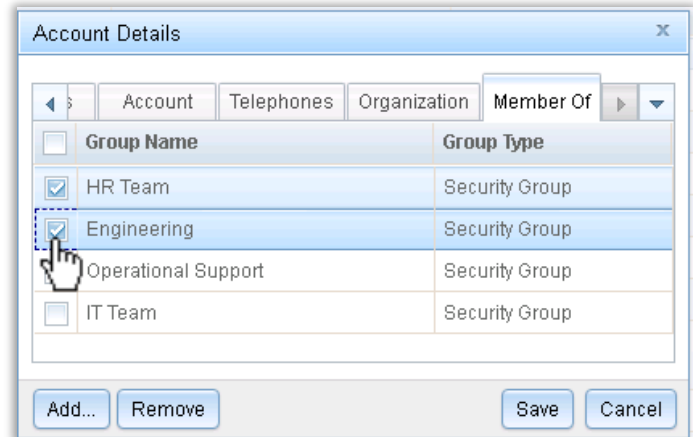


Figure 3.3.6-7

- Click on the Remove button.

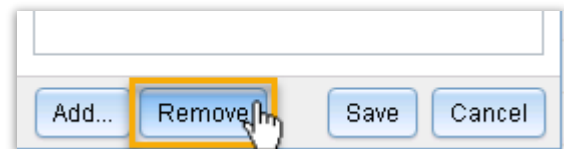


Figure 3.3.6-8

- Confirm the removal request

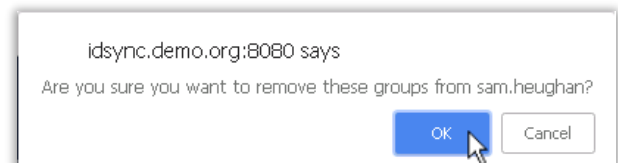


Figure 3.3.6-9

- Monitor the Status bar and look for messages regarding this request.

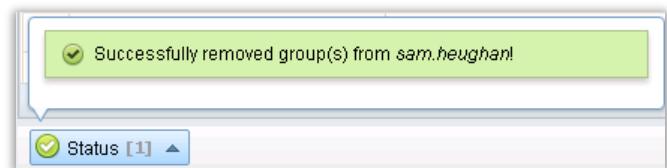


Figure 3.3.6-10

Adding/Removing Users to Groups

- Users can also be added to groups from the Group's Members tab of its properties page. This way, it's possible to add more than one user to a given group in a single transaction.

- Go to the Groups tab and locate the Group you want the user(s) to be added to.
- Right-click on the group and select the Properties option.

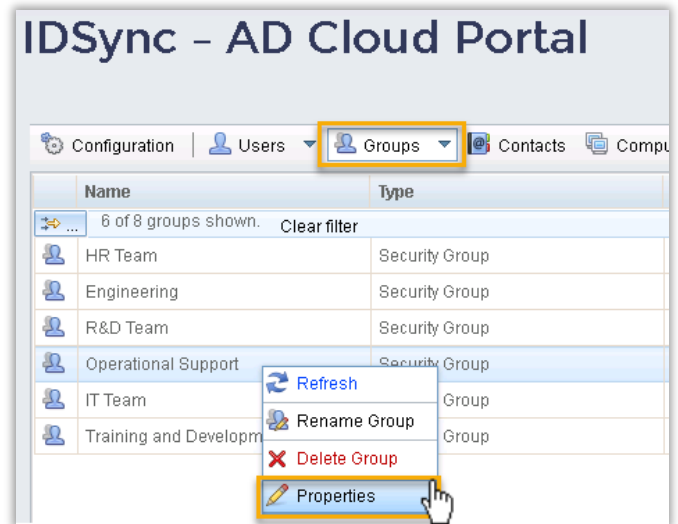


Figure 3.3.6-11

- Once the Group's properties page is open, go to the Members tab, Users section and click on the Add button.

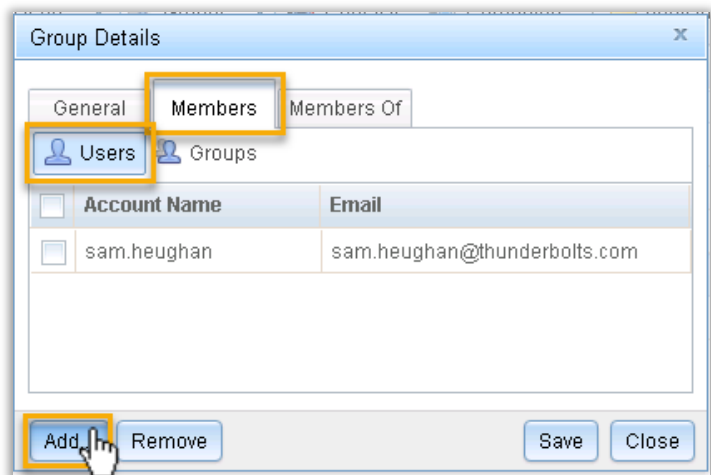


Figure 3.3.6-12

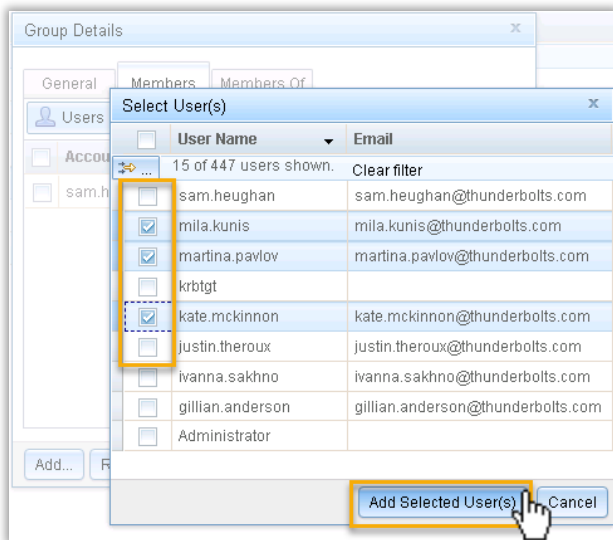


Figure 3.3.6-13

- Select the user (or users) to add to this group and click on the 'Add Selected User(s)' button

Adding/Removing Users to Groups

- Monitor the Status bar and look for messages regarding this request.

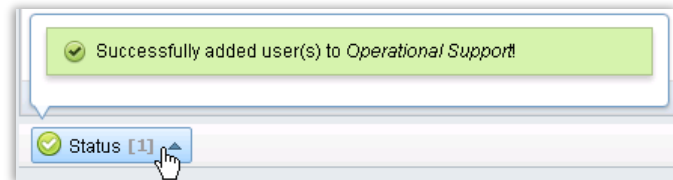


Figure 3.3.6-14

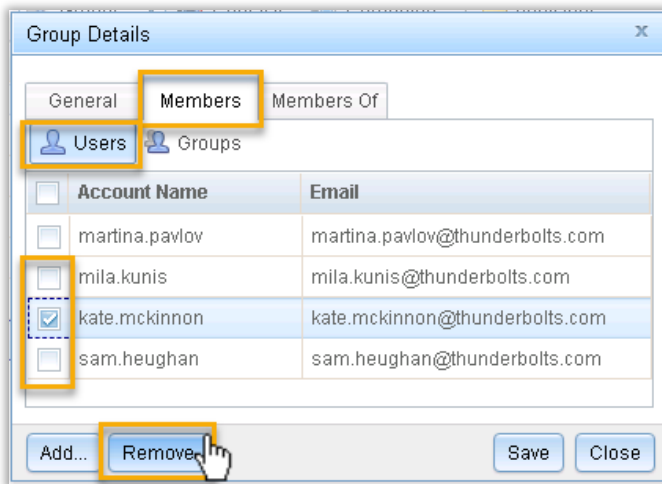


Figure 3.3.6-15

- If you're intending to Remove a user from a Group, simply select (check) the user(s) and click on the Remove button. Then confirm the removal by clicking ok on the pop-up window that will be presented.

Add/Remove Groups to Groups

In an analogous way, to add groups to other Security Groups you can follow two paths:

- Using the Group's Member Of tab within its properties page. This method allows one group to be added to more than one group at a time.
- Go to the Groups tab and locate the group you need to work with.
- Right-click on the group and select the Properties option.

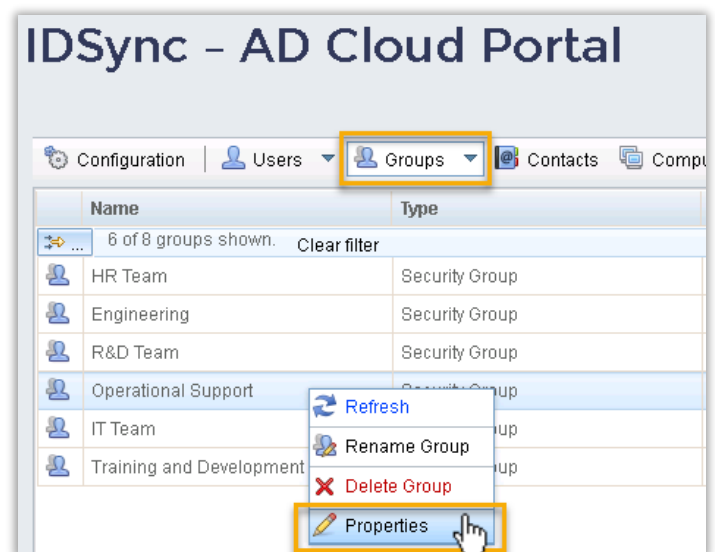


Figure 3.3.6-16

Adding/Removing Groups to Groups

- Go to the 'Member Of' tab.
- Click on the Add button.

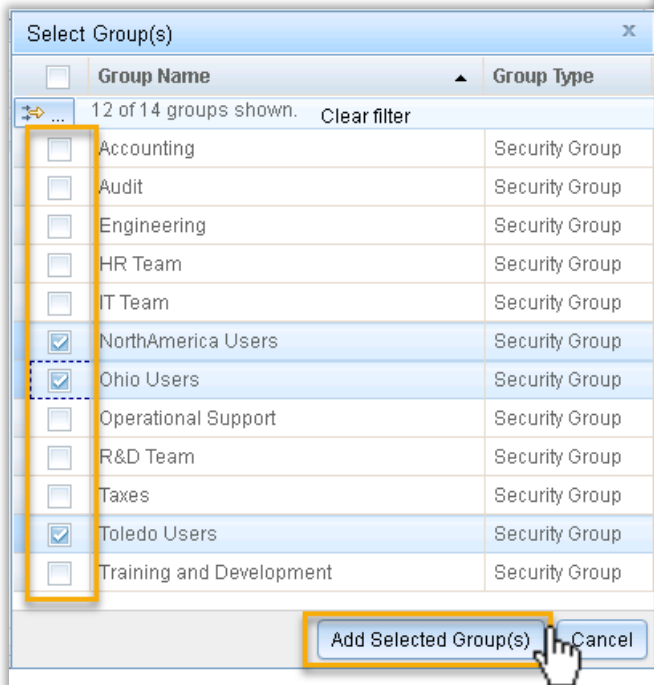


Figure 3.3.6-18

- Monitor the Status bar and look for messages regarding this request.

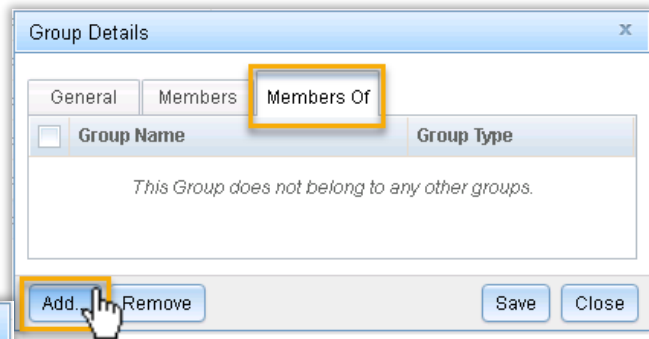


Figure 3.3.6-17

- Look for the group or groups you want this group to be added to and select each one of them (by clicking on the checkbox at the left of the group's name).
- Click on the 'Add Selected Group(s)' button to confirm this operation.

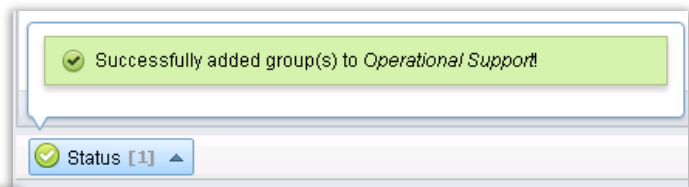


Figure 3.3.6-19

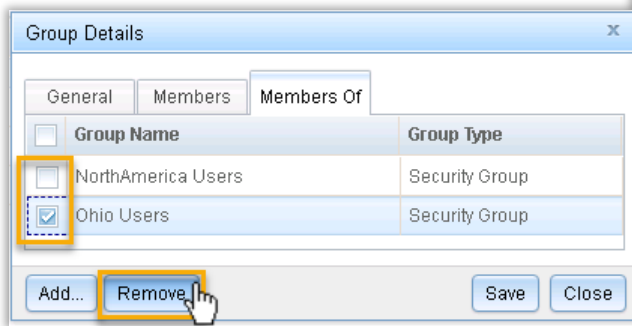


Figure 3.3.6-20

- A similar process is followed when removing a group from another group. Simply select the group that this group will be removed from and click on the Remove button.

Adding/Removing Groups to Groups

- Groups can also be added to other Security Group within the Members tab of its properties page. This way, it's possible to add more than one group to a given group in a single transaction.

- Go to the Groups tab and locate the Group you need to work with.
- Right-click on the group and select the Properties option.

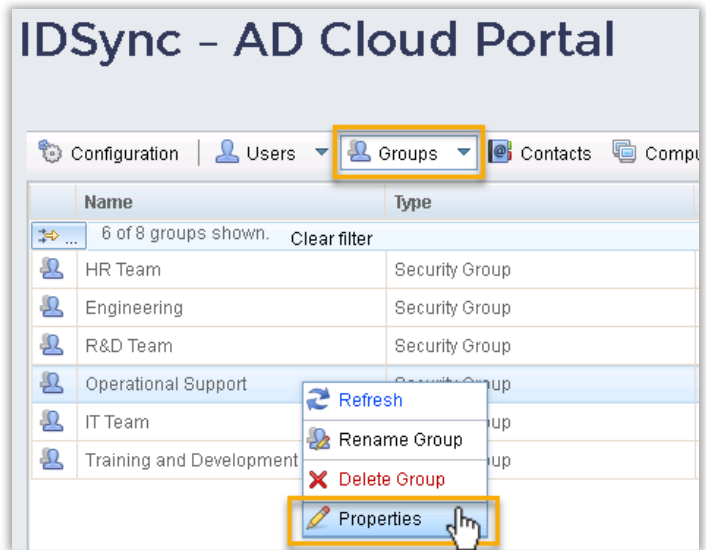


Figure 3.3.6-21

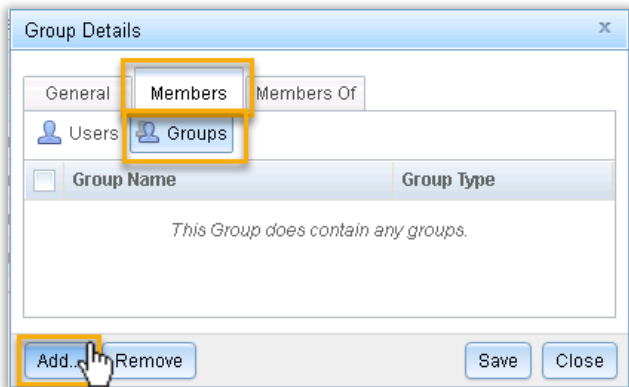


Figure 3.3.6-22

- Select the group (or groups) to add to this group and click on the 'Add Selected Group(s)' button
- Monitor the Status bar and look for messages regarding this request.

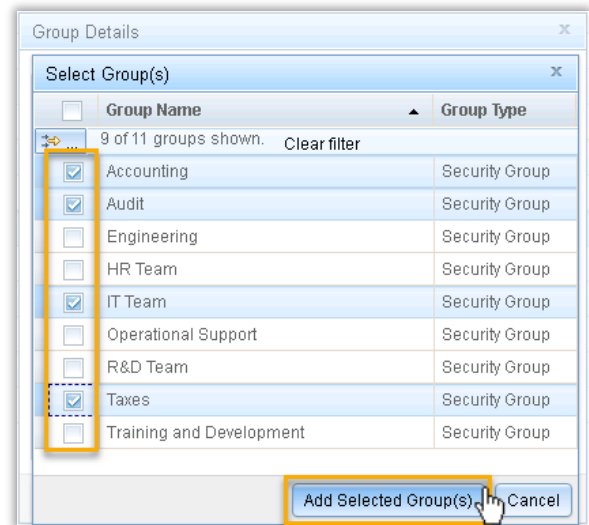


Figure 3.3.6-23

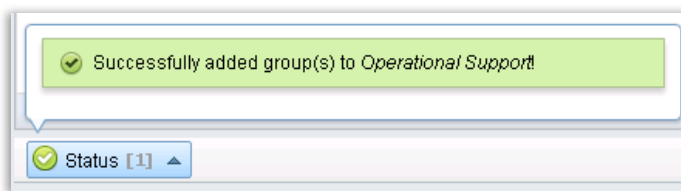


Figure 3.3.6-24