

IDSync® AD CLOUD PORTAL

Internet Browser Access to Microsoft Active Directory for user management

Management Console and Security Studio



IDSync[®] AD Cloud Portal

Cloud Based AD Management

©InnerApps, LLC
28350 Kensington Lane • Suite 200
Perrysburg, OH43551
Phone 888.908.7962 • Fax 419.931.0061

Contents

Revision History	5
General Information	6
Introduction.....	6
System Overview	6
System Components.....	7
AD Cloud Portal Concepts	8
Getting Started.....	9
The Management Console.....	9
The Security Studio Module.....	12
Login	12
Access Control	13
Self-Service Control.....	13
Reporting	13
Setup.....	14
Using the Security Studio	15
Logging in	15
First-time login	15
Security Studio Components.....	16
Features.....	17
Profiles	19
Scopes	22
Security Users	23
ADCP Security Groups	28
The Security Users, Profiles and Scopes Planner	29
Standard Reports	32
Managed Users.....	32
Transactions.....	32
Appendix A – Security Studio Planning Form	33

Revision History

04-2017

1. Initial Documentation

12-2017

2. Format changes.
3. Addition of new management options.
4. Addition of ADCP Concepts.
5. Addition of Appendix A – Security Studio Planner.

General Information

Introduction

The purpose of this document is to provide the System Administrator and other technical stakeholders with a complete and easy guide to setup and manage the IDSync® Management Console and Security Studio, both components of IDSync® AD Cloud Portal.

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 on-premise AD Users and Groups accounts or those of their customers via a web-browser, from on-premises or remote locations.

As depicted in figure 1-1 below, the IDSync® infrastructure 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 configure and manage such levels of delegation.

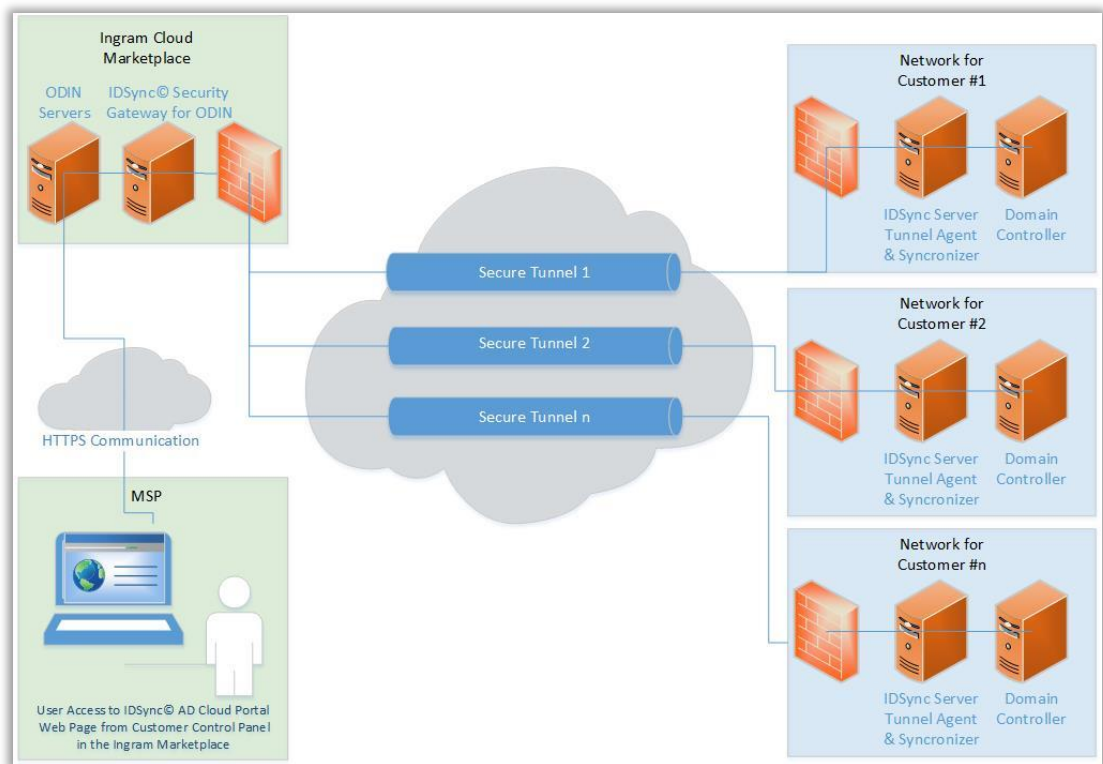


Figure 1-1

General Information

System Components

The IDSync® Cloud Portal System consists of four components (see figure 1-2):

☞ 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.

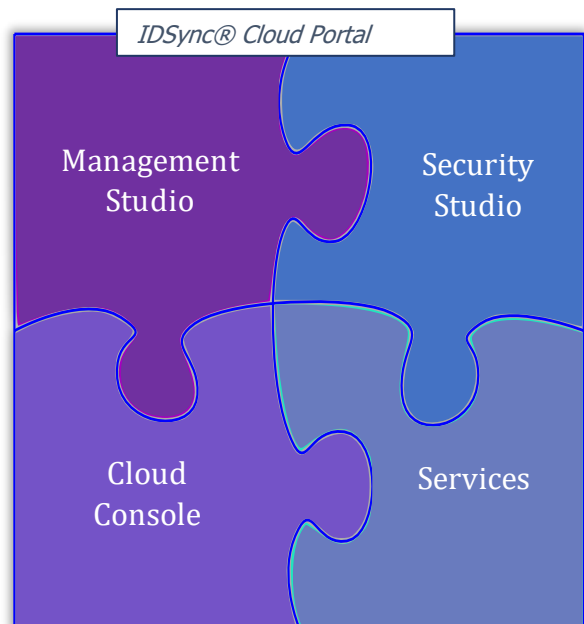


Figure 1-2

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® Security Studio, and will explain the Security elements available to control User's Rights and Access and how to use ADCP to view, create and maintain Active Directory and Security Objects. More information about the IDSync® Management Studio and the Cloud Console 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.

☞ 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).

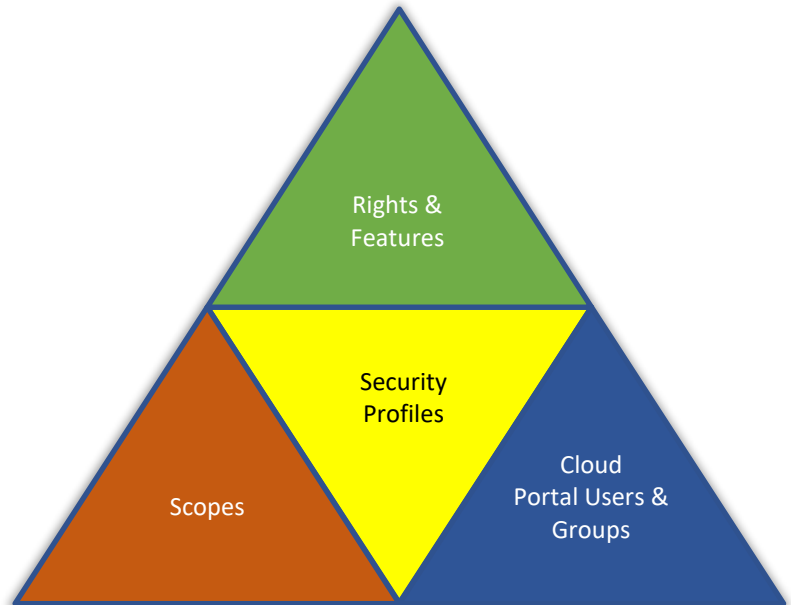


Figure 1-3

Getting Started

The Management Console

Manage Configuration settings, Services, Log-files and, of course, the Security features and functionalities for the controlled and secured web-access to your Active Directory Objects (see figure 2.1-1).

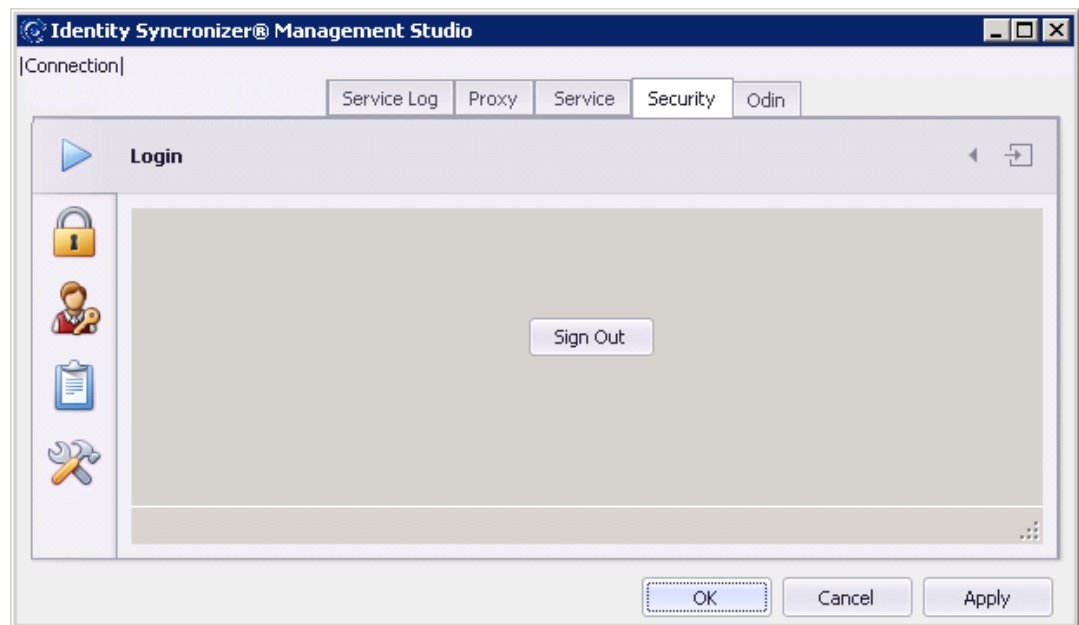


Figure 2.1-1

Here's a brief explanation of the tabs found in the IDSync® Management Studio:

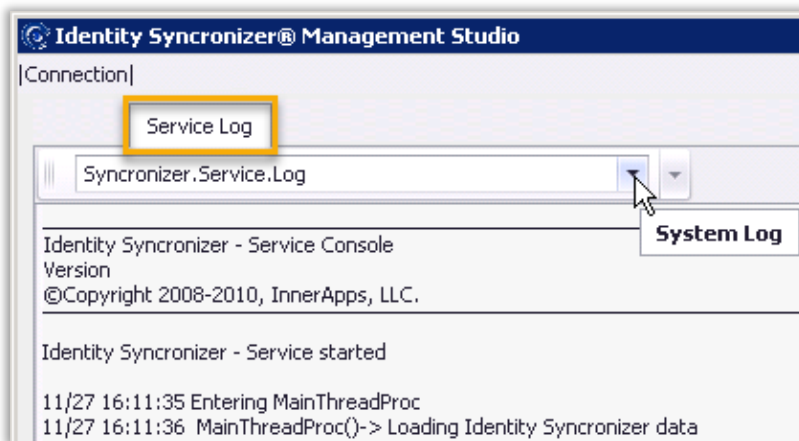


Figure 2.1-2

The **Service Log** tab brings first-hand information of what is happening in the background, by opening the log file of the application and showing relevant information of every thread that the IDSync® Service opens and every transaction it performs. See figure 2.1-2.

The Management Console

The **Proxy** tab is useful to configure the IDSync® Software to use a proxy server between the application and the Internet, in those cases where a direct connection between the server and the Internet is not possible (e.g. many companies use proxy servers to reduce the chance of a security breach). See figure 2.1-3.

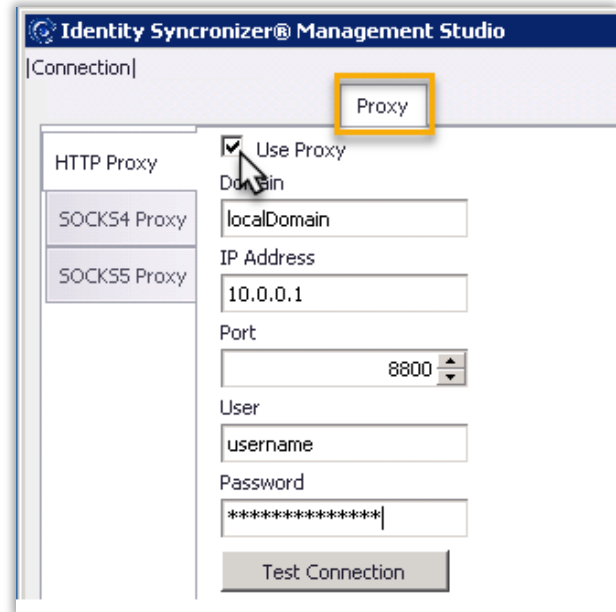


Figure 2.1-3

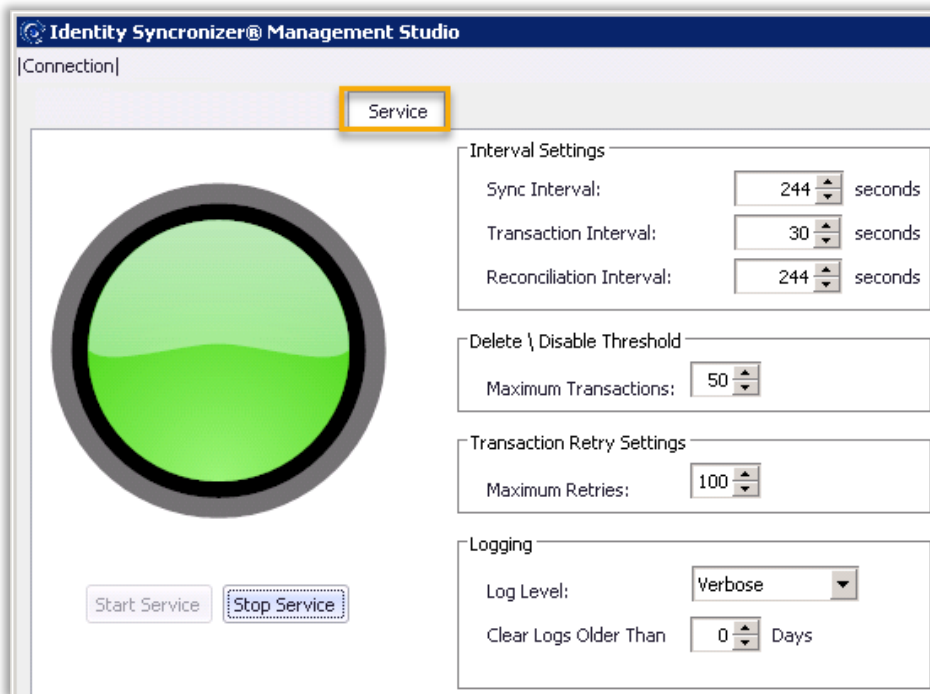
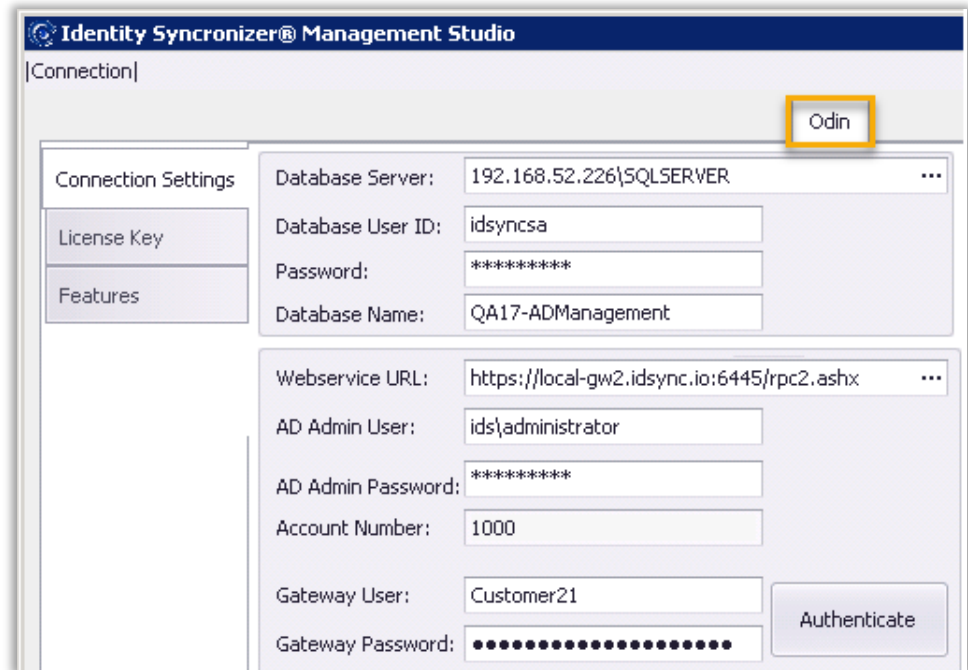


Figure 2.1-4

Stop and Start the Synchronizer's main Service, configure the intervals between information synchronizations and reconciliations, and manage the level of detail available in the log files, through the **Service** tab. See figure 2.1-4.

The Management Console

The **Odin** tab holds the information related to the IDSync® Subscription, such as License Key, Settings for connecting to Odin's URL and the Features you're granted to use. These settings are used to enable a Secure Connection to the Odin Data Center services. See figure 2.1-5.



The screenshot shows the 'Identity Synchronizer® Management Studio' interface. The 'Odin' tab is selected and highlighted with a yellow box. The interface is divided into two main sections: 'Connection Settings' and 'Features'. The 'Connection Settings' section includes fields for 'Database Server' (192.168.52.226\SQLSERVER), 'Database User ID' (idsyncsa), 'Password' (masked with asterisks), and 'Database Name' (QA17-ADManagement). The 'Features' section includes fields for 'Webservice URL' (https://local-gw2.idsync.io:6445/rpc2.ashx), 'AD Admin User' (ids\administrator), 'AD Admin Password' (masked), 'Account Number' (1000), 'Gateway User' (Customer21), and 'Gateway Password' (masked). An 'Authenticate' button is located at the bottom right of the 'Features' section.

Figure 2.1-5

Use the **Security** tab to access the Security Studio module, to configure, review and control the secured management of the Active Directory Users and Groups. See figure 2.1-6.



The screenshot shows the 'Identity Synchronizer® Management Studio' interface. The 'Security' tab is selected and highlighted with a yellow box. The interface displays a 'Login' section with a blue play button icon. Below the icon are two input fields: 'Login:' and 'Password:'. A 'Sign In' button is located at the bottom right of the login section.

Figure 2.1-6

The Security Studio Module

The **Security Studio Module** is the configuration center to define users (for both, the Portal and the Security Module), manage Profiles (to define the tasks a user can perform) and set the Scopes (or the group of Active Directory objects that will be managed).

- ☞ Access to the different sections in this module is defined based on the Security Level that each user has been granted by the System Administrator.
- ☞ By default, the System Administrator has full Access to all sections in this module.

Here's an explanation of every section of the Security Module.

Login

Since this is a secured module, its access is restricted to explicitly authenticated users,

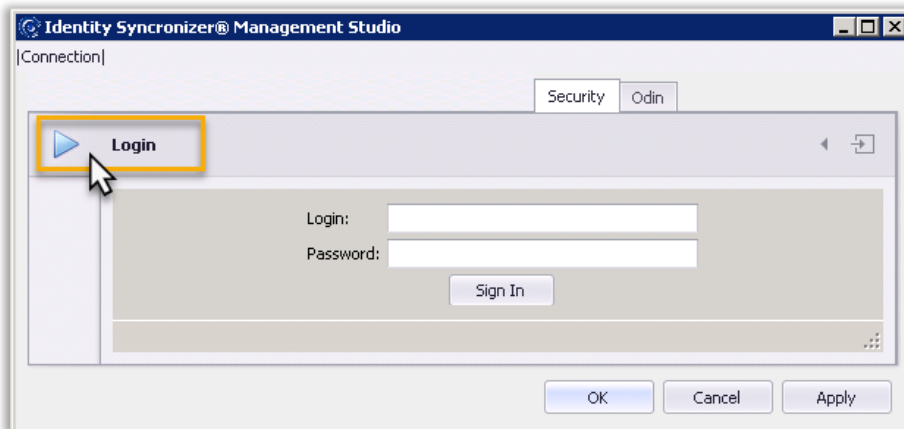


Figure 2.2-1

ensuring that not every user with access to the Management Console will be able to make changes to the Security settings (see figure 2.2-1).

Once a user has logged in to this module,

- ☞ The **Logout** button will become visible, and,
- ☞ Information related to the logged user will be shown (see figure 2.2-2).

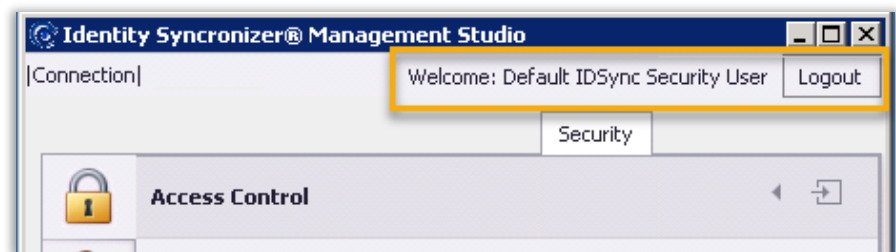


Figure 2.2-2

The Security Studio Module

Access Control

Use this section to manage Profiles, Scopes, Users and Groups. Associate those concepts to create customized Security Levels to match any number of possibilities, being as specific -user to user level- or as general -groups to groups level- as the organization requires. See Figure 2.2-3

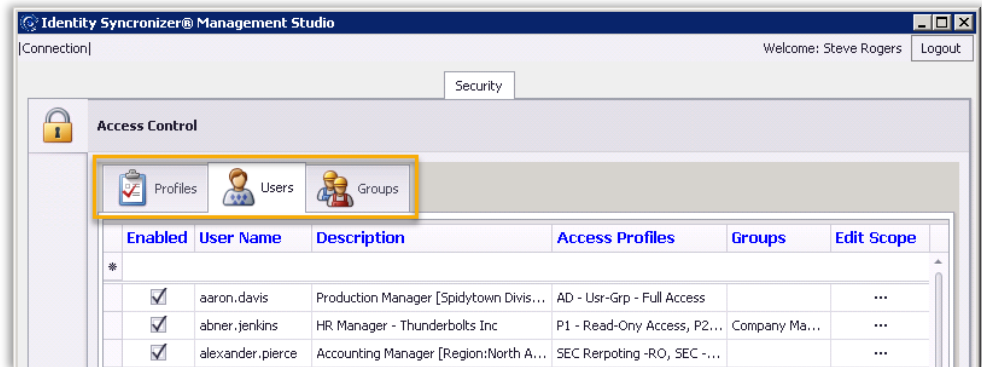


Figure 2.2-3

Self-Service Control

This is a filtered view dedicated to Self-Service services. Manage Profiles, Users and Groups to create services that are triggered and performed by any user independently of involvement of the technical staff. Avoid IT support costs by delegating actions (such as a Password Reset) to the staff that needs to perform those. See Figure 2.2-4.



Figure 2.2-4

Reporting

Get a complete view of what's going on in your environment. See detailed tracking information about changes performed in users' data or in security settings and even create customized reports to fit any company's needs.

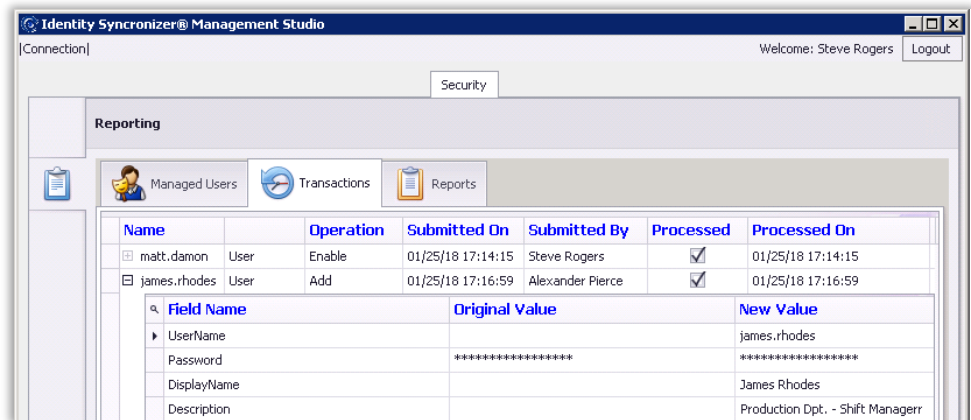
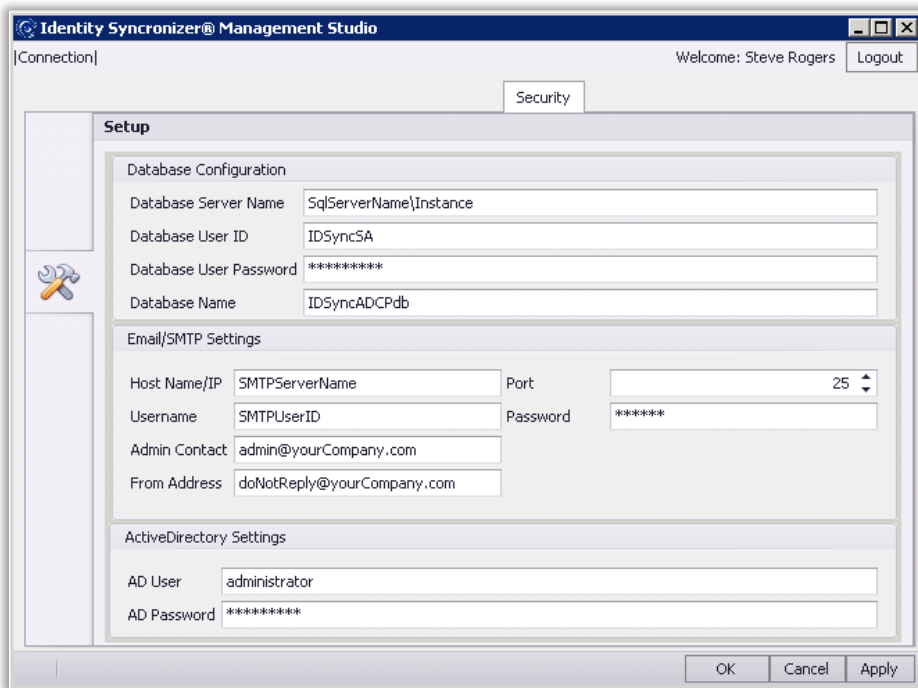


Figure 2.2-5

The Security Studio Module

Setup

Use this section to view or change the Database Configuration, SMTP settings or Active Directory credentials.



The screenshot shows the 'Security' tab in the 'Identity Synchronizer® Management Studio' application. The window title bar includes 'Welcome: Steve Rogers' and a 'Logout' button. The 'Setup' section is divided into three main areas:

- Database Configuration:**
 - Database Server Name:
 - Database User ID:
 - Database User Password:
 - Database Name:
- Email/SMTP Settings:**
 - Host Name/IP: Port:
 - Username: Password:
 - Admin Contact:
 - From Address:
- ActiveDirectory Settings:**
 - AD User:
 - AD Password:

At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

Figure 2.2-6

Using the Security Studio

The **Security Studio Module** is the configuration center to define and manage users and groups (for both, the Cloud Console and the Security Module), manage Features and Profiles (to define the tasks a user can perform) and set the Scopes (or the group of Active Directory objects that will be managed).

Logging in

To Log in to this module:

Click on the 'Login' button, located at the upper-right corner of the IDSync® Management Studio (see figure 3.1-1).

- Type in the proper credentials (if this is your first-time login, see next section in this page).
- Click OK.

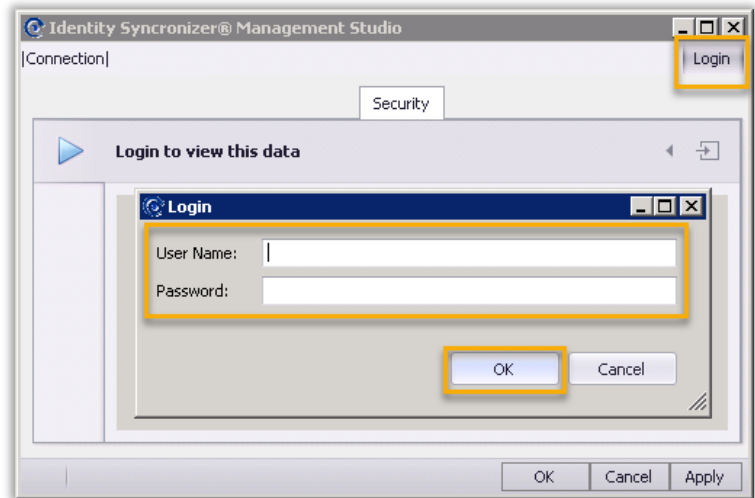


Figure 3.1-1

First-time login

If this your first-time login,

- Use 'IDSyncAdmin' as username.
- The password will be the Gateway Password (the same you used in the Odin configuration Tab). See Figure 3.1-2.

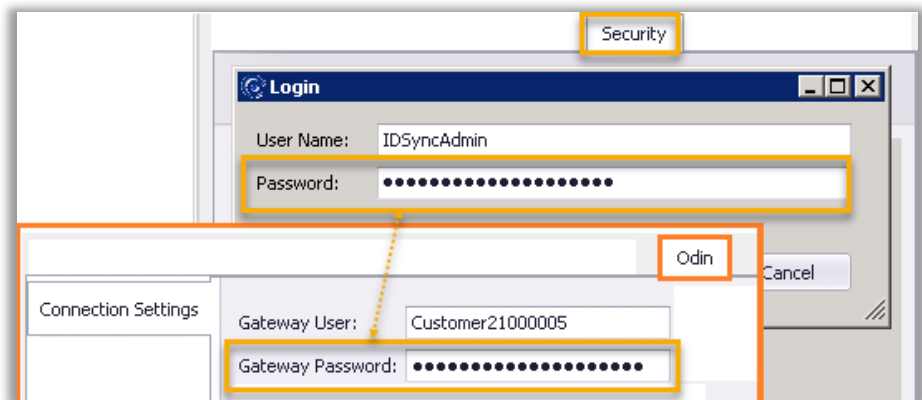


Figure 3.1-2

👉 Please, refer to the IDSync® AD Cloud Portal – Installation Guide (and look for the 'Downloading the IDSync® Management Software' section) in case you need help finding the Gateway Password.

Security Studio Components

The IDSync® Security Studio uses Features, Profiles, Scopes, Users and Groups to create customized Security Levels and permit that authorized users interact with Active Directory objects using a web-browser via a secured connection.

This section comprehensively explains these concepts and puts them together, so you can easily start managing the access to your network Directory.

Use Figure 3.2-1 as a quick-guide to the Security Studio Components.

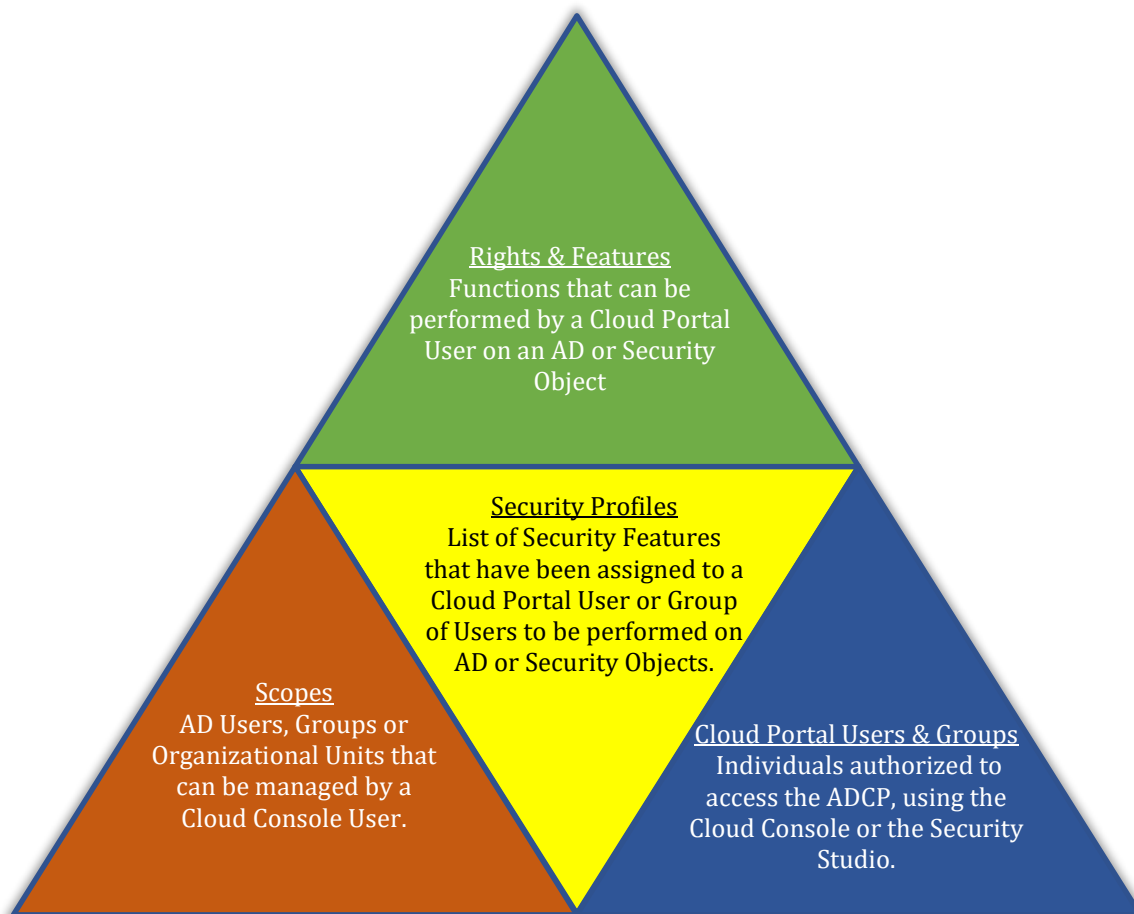


Figure 3.2-1

Security Studio Components

Features

A Security Feature is any action that a user may perform. Read or Modify Properties and Create or Delete objects are examples of features.

See the Security Studio Planning Form, in Appendix A, for a complete list of Security Features.

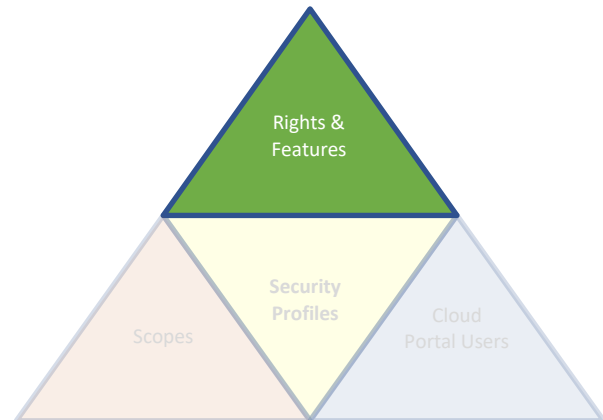


Figure 3.2-2

☞ Features are performed on objects, such as users, groups, computers or reports, etc. Examples of this kind of feature are: changing another user's telephone number, or creating or editing a report. See figure 3.2-2.

☞ Features can also be performed by a given user on itself (for example, a user changing its own password). See figure 3.2-3.

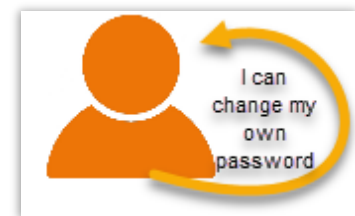


Figure 3.2-3

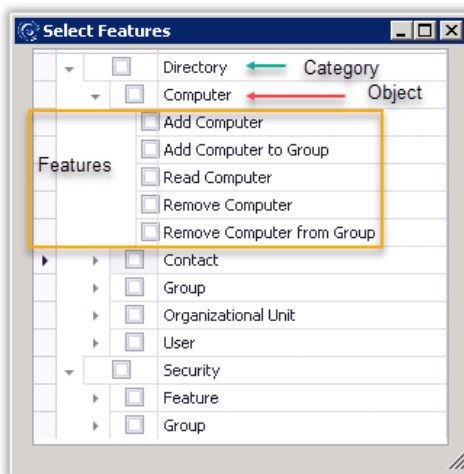


Figure 3.2-4

☞ Features are used against the object that they are going to act on. For example, if the target Object is a Group, examples of Features can be Add, Delete or Rename Group, but, if the target Object is a User, Features can be slightly different, such as Unlock User or Change User's Password.

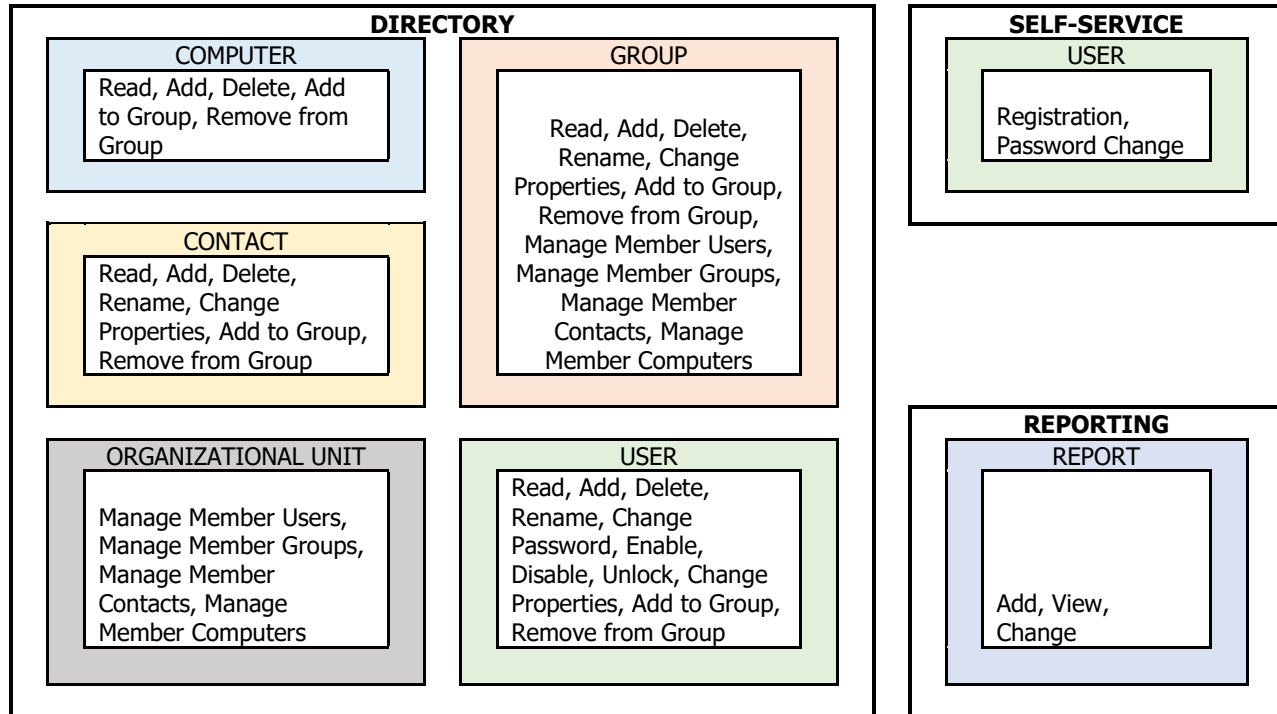
☞ The Security Studio organizes Features into Categories (such as Directory, Security, Reporting, etc.) and target Objects that those Features can act on (Computers, Groups, Profiles, etc.).

For example, 'Add Computer', 'Add Computer to Group' and 'Read Computer' are among the list of Features associated with the 'Computer' Object, in the 'Directory' Category (see figure 3.2-4).

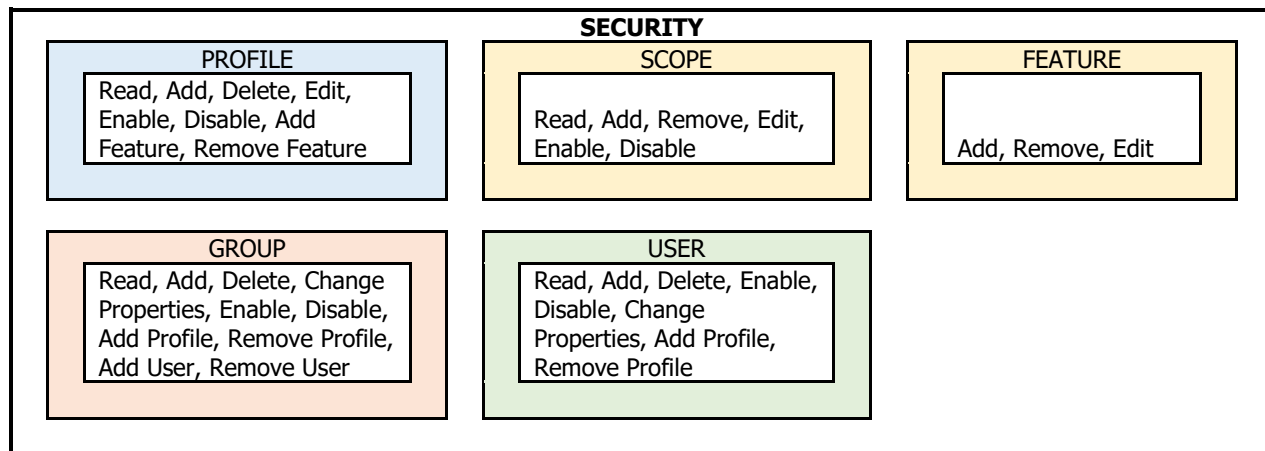
Security Studio Components - Features

The following tables show the complete collection of Features, as they pertain to each Object.

Security Features related to AD Objects and to Security Reports



Security Features related to the Security Studio Objects



Profiles

Profiles are Sets of Features, intended for a specific role, for example a Help Desk tech or an HR person. They can include any number or combination of features and can be re-used as many times as needed.

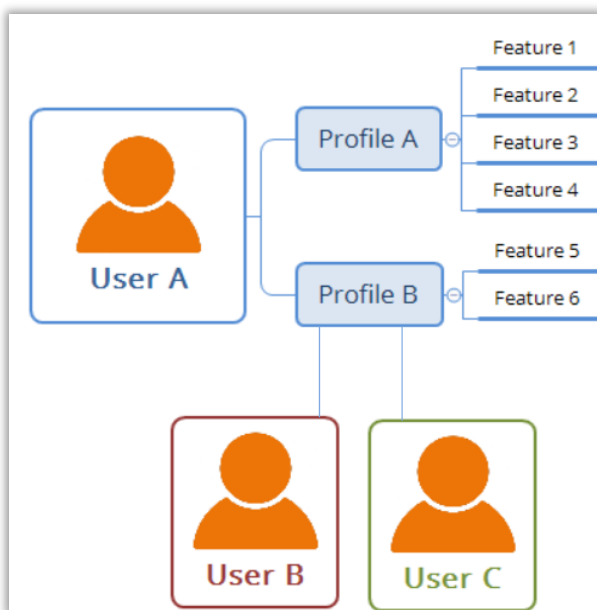
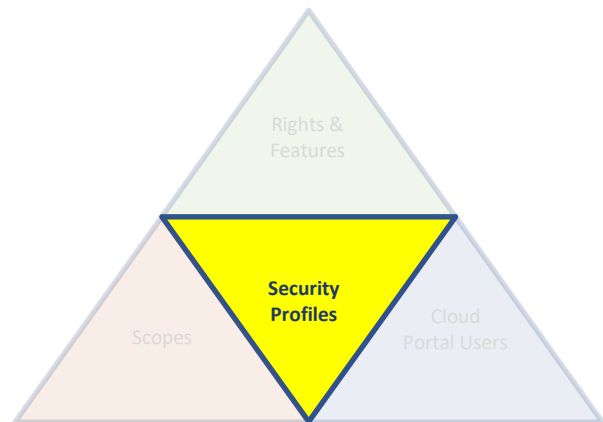


Figure 3.2-5

As shown in Figure 3.2-5, Profiles are composed of Features, and can be associated with as many Users (or Groups) as required, to properly enable any role to perform Active Directory's administration tasks

Since Profiles can include any combination of features, companies may decide to use practically any path they want to fulfill their needs in terms of Security settings.

Security Module Components - Profiles

Here's a couple of Examples to illustrate that point:

- ☞ Company 'A' decides to create department-specific profiles. This design tries to mimic the organizational chart of the company, matching operational functions with network-related management. See Figure 3.2-6

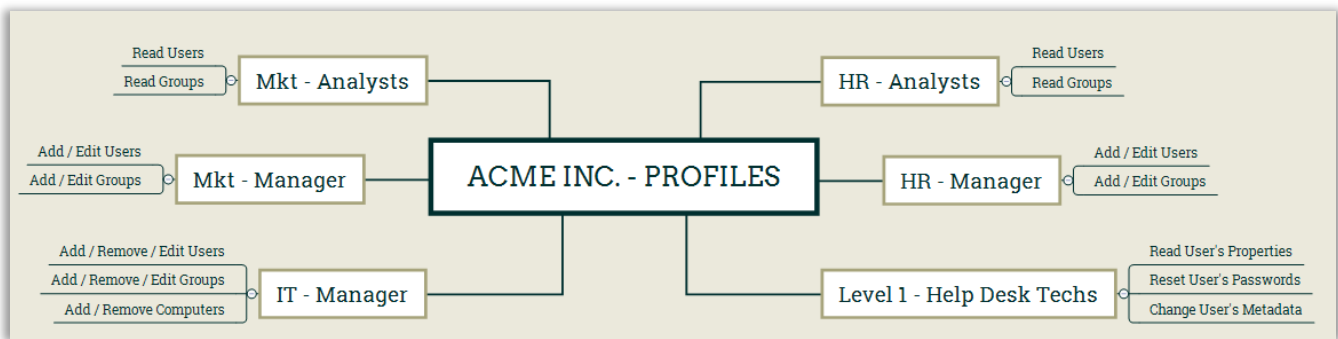


Figure 3.2-6

- ☞ Company 'B' creates general-purposes profiles, relying on the fact that actual rights will be influenced by the scope of objects they are allowed or limited.

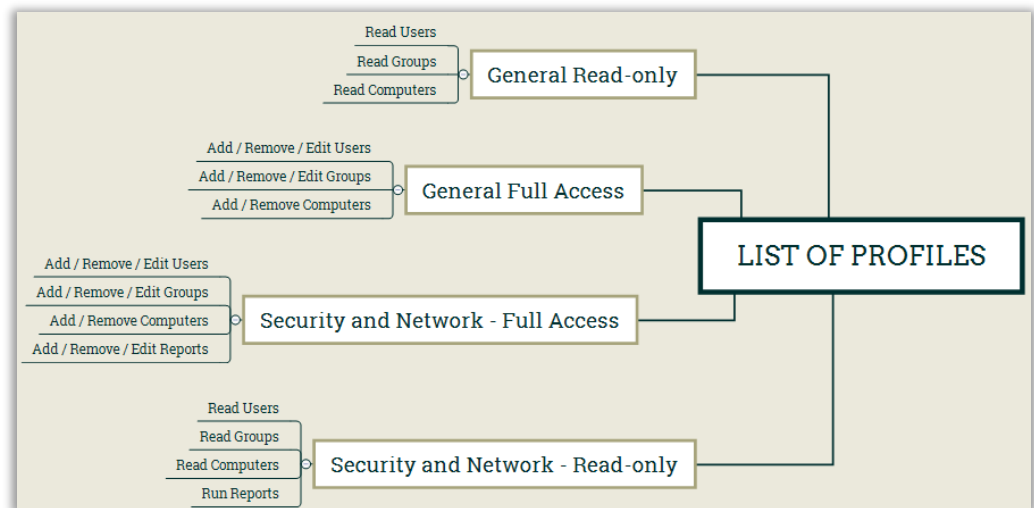


Figure 3.2-7

Security Module Components - Profiles

As shown in figure 3.2-8, creating a Security Profile is as simple as:

1. Choose a name for the Profile
2. Write a Description to document what the Profile does
3. Select the Features associated with that Profile

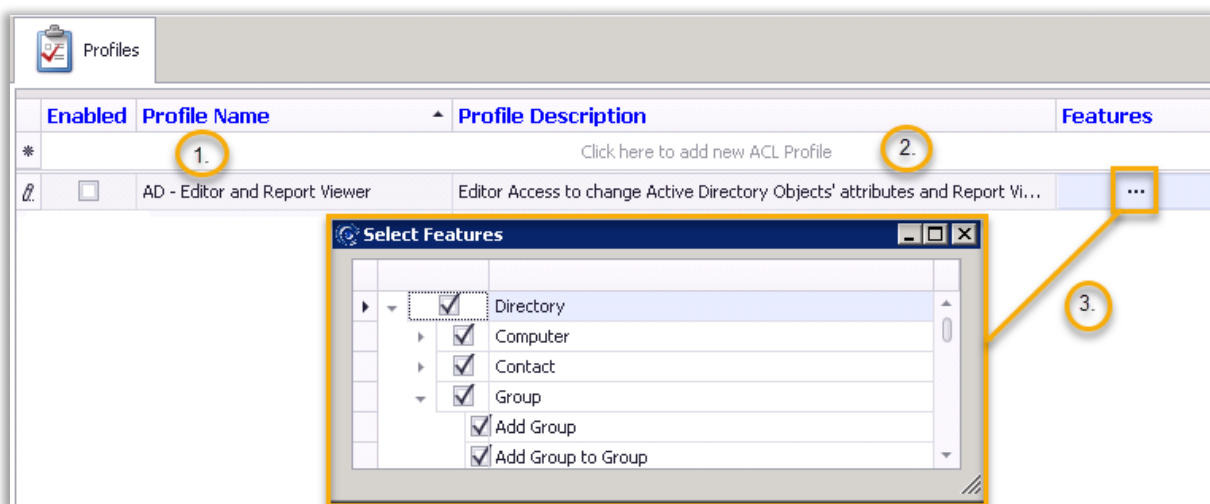
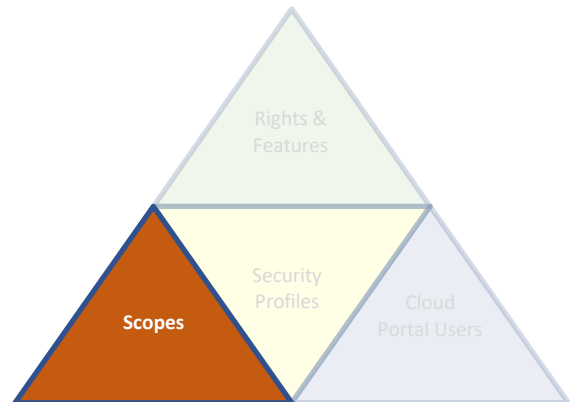


Figure 3.2-8

Scopes

A Scope identifies the Objects that can be managed by a User. These are the target Objects that will be available for their administration. The actual extent of such administration relies on the Features Profile that a given user or group is associated with.



As depicted in figure 3.2-9, the Scope is the group of Objects that a given User can manage, based on the Profile that it is associated with (having that profile a list of one or more features, or actions that the User can perform on those managed Objects).

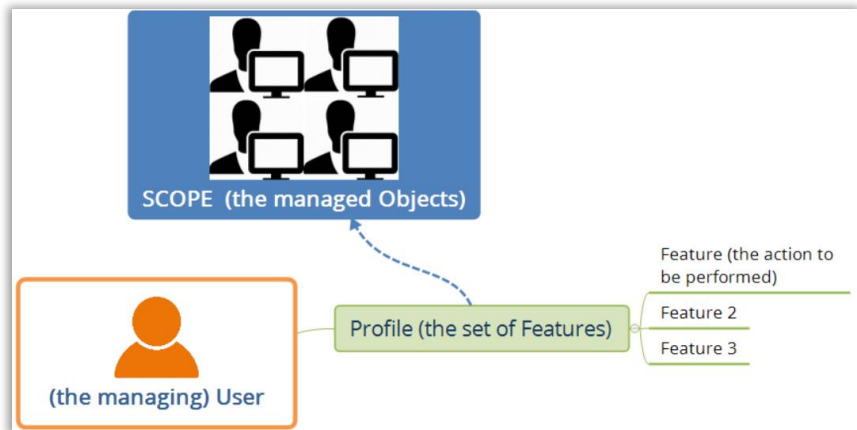


Figure 3.2-9

To define a Scope

1. Choose a Name (see figure 3.2-10).
2. Write a Description
3. Select the Active Directory Organizational Units, Groups or Users associated with that Scope.

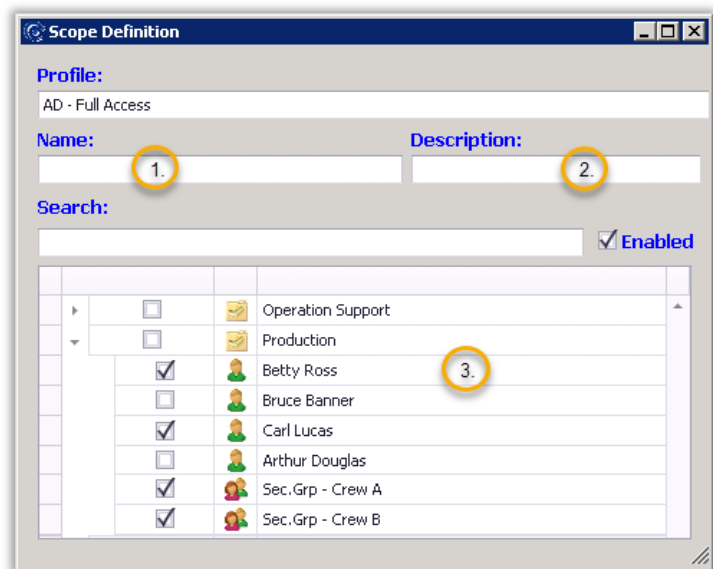
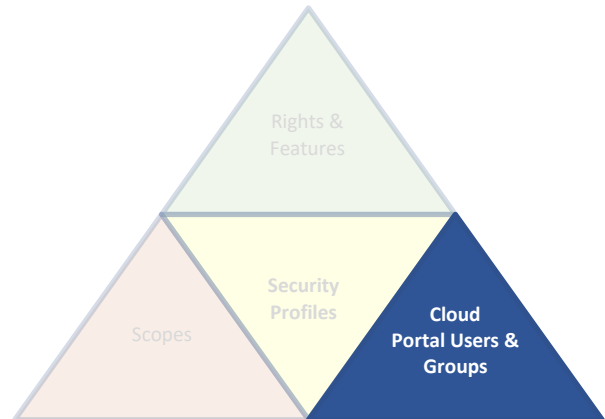


Figure 3.2-10

Security Users

These are the people authorized by the Domain owner to perform actions on Active Directory or Security Objects and are defined according to the Company's needs. These users are limited to the rights and features and scopes that have been allowed.



As shown in figure 3.2-11, to define an ADCP User, you need to:

- Set a User Name
- Set Display Name, Description and Password
- Set a Security Profile

Enabled	User Name	Display Name	Description	Password	Access Profiles	Linked To AD	Groups	Edit Scope
*	1.		2.	Click here to add a new ACL User		3.		
<input checked="" type="checkbox"/>	aaron.davis	Aaron Davis	Production Manager [Spidytown Division]	*****	AD - Usr-Grp - Full
<input checked="" type="checkbox"/>	alexander.pierce	Alexander Pierce	Accounting Manager [North America]	*****				...

Figure 3.2-11

While not mandatory, also note that ADCP Users can be linked to (or imported from) Active Directory. And, as mentioned before, ADCP Users can be associated with multiple Profiles (and multiple Scopes).

Security Users

Now, putting all the pieces together, you can have a full picture of how IDSync® AD Cloud Portal works:

- ☞ Create Profiles using sets of Features.
- ☞ Associate one or more Profiles to an ADCP User.
- ☞ Associate a Scope to an ADCP User-Profile combination.

So, every combination of ADCP User-Profile-Scope will grant that User the ability to manage (and perform different sets of actions) different sets of Active Directory Objects. See figure 3.2-12

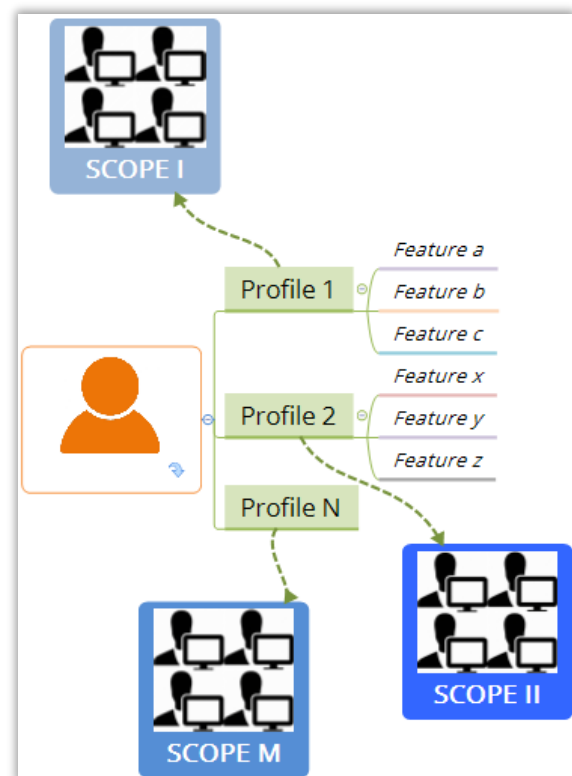


Figure 3.2-12

Security Module Components – Security Users

Let's illustrate these concepts with a detailed example.

Valerie Cooper, head of Human Resources in Thunderbolts Inc., is constantly looking for updated information regarding people in the company. Such information may include personal data, like a telephone number or the home address, or the applications that people have access to, etc. Often, she also asks for changes within her own crew, such as a network folder that a person needs access to, or access to a different printer in the office.

Just as many other organizations do, this company uses Active Directory Security Groups to manage access to file systems, network applications or devices (meaning that managing those groups directly implies to manage accesses).

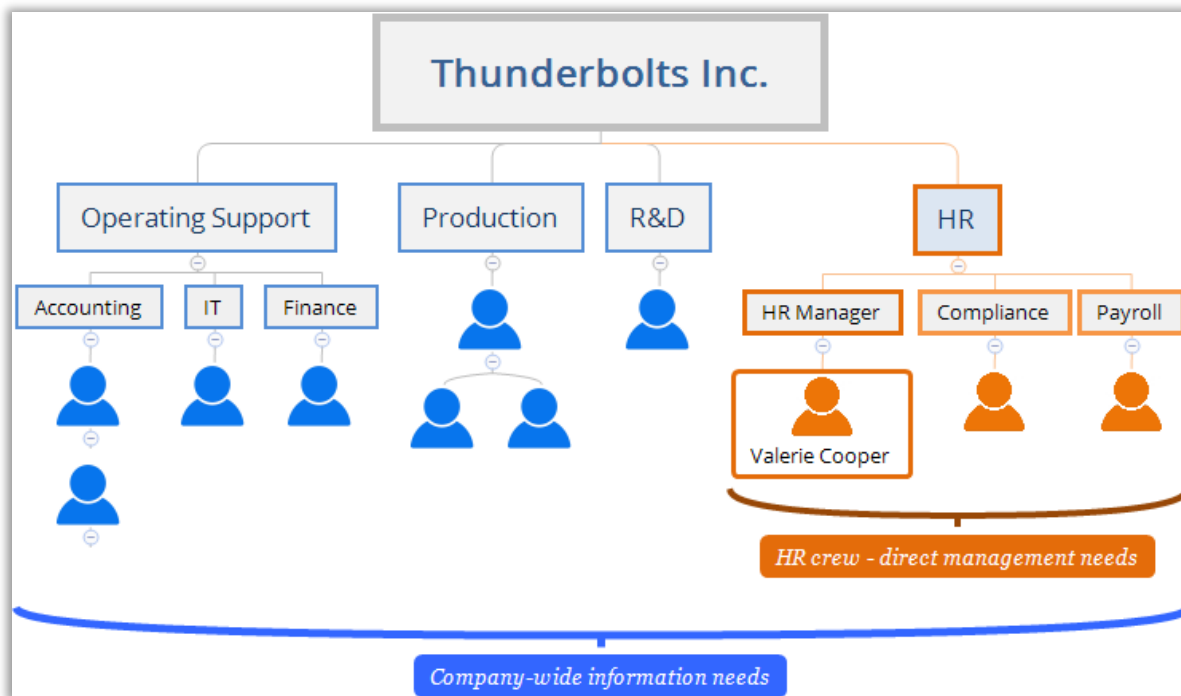


Figure 3.2-13

Figure 3.2-13 shows the company's organizational structure of the example stated above (as well as the extent of Valerie's needs).

From figure 3.2-13, we can extract some key facts:

- ☞ There are two different management 'targets' (a company-wide target group and an HR-level target group).
- ☞ One of those targets is part of the other target.

Security Module Components – Security Users

For each target there are different actions that Valerie needs to perform: while at the company-wide level she needs to gather employee’s information, at her own crew level she might need to change some properties (such as a printer she or one of the crew is needing).
Security Module Components – Security Users

- ☞ Targets (scopes) and actions (features) are constrained or limited to specific sets. So, outside those limits, Valerie does not have any type of access to Active Directory objects.

Figure 3.2-14 shows a summary of those facts, correlating those concepts with the IDSync® concepts you already know.

ADCP Security User Valerie Cooper – HR Manager		
Profile Name	Features	Scope
Read-Only Profile	- View Users Properties - View Groups Properties	'Company-wide': Operating support, Production, R&D and HR departments.
Editor Profile	- View/Change Users Properties - View/Change Groups Properties	'HR department'

Figure 3.2-14

The next three figures will show those same concepts in the IDSync® Security Portal context.

Figure 3.2-15 depicts both Profiles, with Features shown for the Read-Only Access Profile as checked.

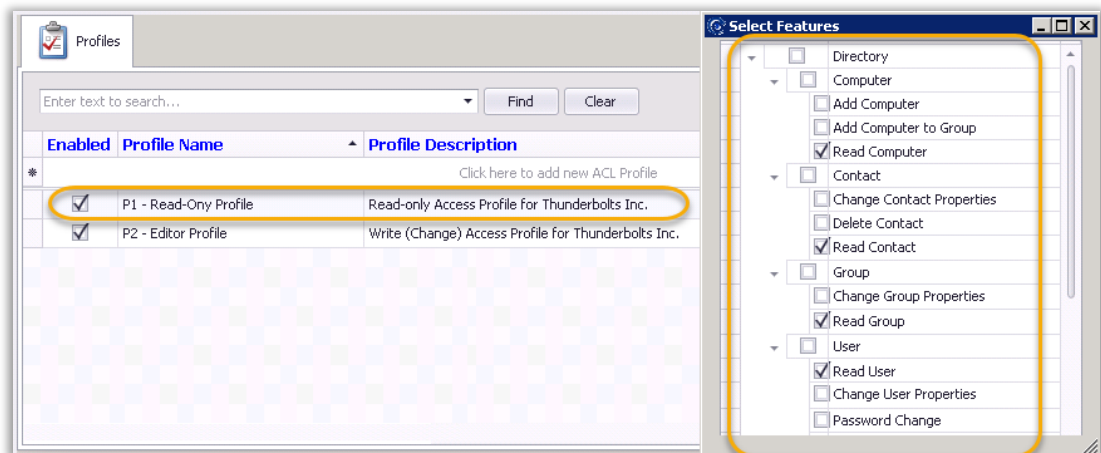
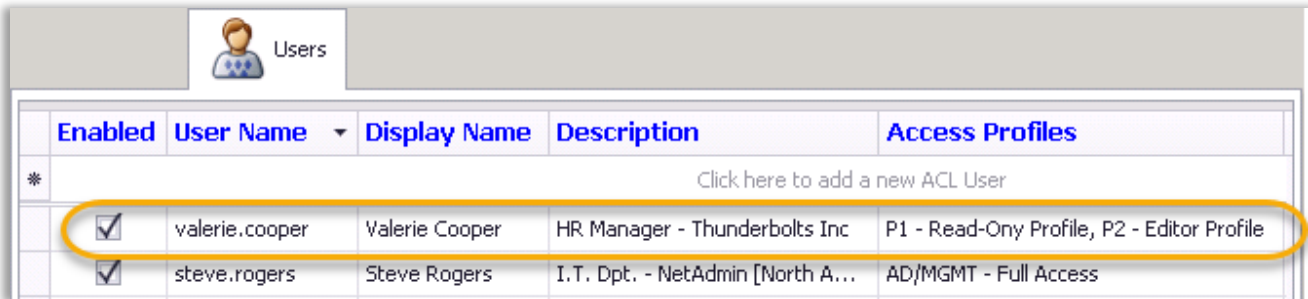


Figure 3.2-15

Security Module Components – Security Users

Figure 3.2-16 shows the Cloud Portal User created for Valerie and the Profiles it is associated with.



Enabled	User Name	Display Name	Description	Access Profiles
<input checked="" type="checkbox"/>	valerie.cooper	Valerie Cooper	HR Manager - Thunderbolts Inc	P1 - Read-Only Profile, P2 - Editor Profile
<input checked="" type="checkbox"/>	steve.rogers	Steve Rogers	I.T. Dpt. - NetAdmin [North A...	AD/MGMT - Full Access

Figure 3.2-16

Finally, figure 3.2-17 shows the Company-wide Scope, associated with the P1 – Read-only Access Profile. Also, note from this figure that, even when the Scope is designed to reach all Active Directory Objects, for security reasons there are still some (built-in) Objects which are outside the scope (such as the Domain Controller servers, or the Administrators Security Group).

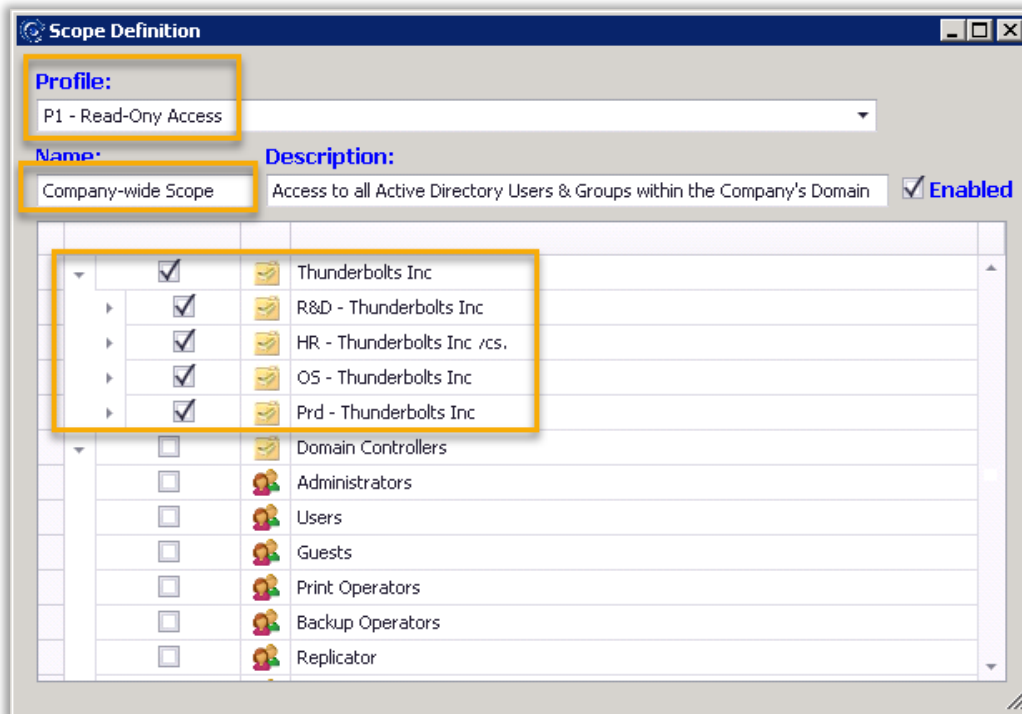


Figure 3.2-17

ADCP Security Groups

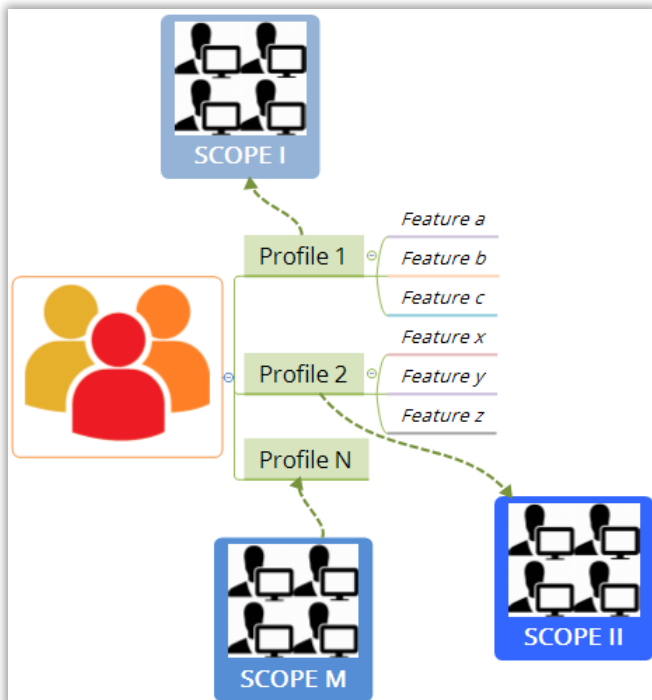


Figure 3.2-18

ADCP Security Groups are an extension of Cloud Portal and Security Users manageability. They are designed for Security Users' Bulk processing.

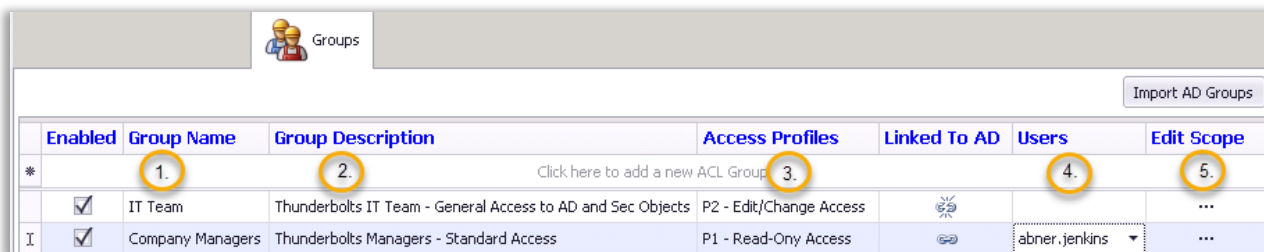
Using Security Groups optimizes user's administration time and ensures operational standardization (for example, when there's a need for equalized Security Levels).

Just as individuals, ADCP Security Groups can be associated with multiple Profiles, each one of which being also associated with a given Scope. See figure 3.2-18).

As shown in figure 3.2-19, to define an ADCP Security Group, you need to:

1. Set a Group Name
2. Set its Description
3. Associate it with one or more Security Profiles
4. Add members to the Group
5. Associate the Group's Profiles to Scopes

Also, note that ADCP Security Groups can be imported from Active Directory, to ensure re-utilization of existing AD resources.



Enabled	Group Name	Group Description	Access Profiles	Linked To AD	Users	Edit Scope
*	1.	2.	3.		4.	5.
<input checked="" type="checkbox"/>	IT Team	Thunderbolts IT Team - General Access to AD and Sec Objects	P2 - Edit/Change Access			...
<input checked="" type="checkbox"/>	Company Managers	Thunderbolts Managers - Standard Access	P1 - Read-Only Access		abner.jenkins	...

Figure 3.2-19

The Security Users, Profiles and Scopes Planner

Creating Users, Profiles and Scopes is easy and simple. But, putting together all the pieces require planning to assure that the right users are receiving both the sufficient and limited correct sets of features they need for their role.

Included in the Appendix A, later in this guide, you'll find a complete and detailed Planner to support the process of creating customized sets of Security Profiles (including Features, Users and Scopes).

Appendix A – Security Studio Planning Form

Security Studio - Users, Profiles and Scopes Planner

PROFILE (1)		HOW TO USE THIS PLANNER. (1) Define the Profile's Name and Description (2) Select the Features that will be enabled for this Profile (note that Features may be related to Active Directory or to the Security Studio). (3) Define the Scope's Name and Description (4) Select the Users, Groups or Organizational Units that are part of this Scope. (5) Define the Users or Groups that will be granted with this Profile.
NAME: A.D. - Read-only		
DESCRIPTION: Read-only Access to Active Directory Users, Contacts, Computers & Groups		
FEATURES (2)		
ACTIVE DIRECTORY	USER	
	READ	
	ADD	
	REMOVE	
	RENAME	
	EDIT	
	ENABLE	
	DISABLE	
	CHANGE PASSWORD	
	UNLOCK	
	ADD TO GROUP	
	REMOVE FROM GROUP	
CONTACT	CONTACT	
	READ	
	ADD	
	REMOVE	
	RENAME	
	EDIT	
	ADD TO GROUP	
	REMOVE FROM GROUP	
PROFILE	PROFILE	
	READ	
	ADD	
	REMOVE	
	EDIT	
	ENABLE	
	DISABLE	
	ADD FEATURE TO PROFILE	
	REMOVE FEATURE FROM PROFILE	
SECURITY	USER	
	READ	
	ADD	
	REMOVE	
	EDIT	
	ENABLE	
	DISABLE	
	ADD USER TO GROUP	
	REMOVE USER FROM GROUP	
	ADD PROFILE TO USER	
	REMOVE PROFILE FROM USER	
SCOPE (3)		
NAME: Remote Desktop Users Scope		
DESCRIPTION: All objects in the 'Remote Desktop Users' (default) Active Directory Group		
FEATURES APPLY TO THESE ACTIVE DIRECTORY NAMES (4)		
USERS		
GROUPS		
ORGANIZATIONAL UNITS		
USERS OR GROUPS FOR CLOUD CONSOLE AND/OR SECURITY STUDIO (5)		

Figure 3.3-1

The Security Users, Profiles and Scopes Planner

The Planner itself has a comprehensive step-by-step guide, to walk you through the process of developing a Features-Users-Scope Profile that can be then easily configured using the Security Module of ADCP. See figure 3.3-2.

HOW TO USE THIS PLANNER.

- (1) Define the Profile's Name and Description
- (2) Select the Features that will be enabled for this Profile (note that Features may be related to Active Directory or to the Security Studio).
- (3) Define the Scope's Name and Description
- (4) Select the Users, Groups or Organizational Units that are part of this Scope.
- (5) Define the Users or Groups that will be granted with this Profile.

Figure 3.3-2

- (1) Profile. Define the Profile's Name and Description (see figure 3.3-3). Make sure the Naming convention follows the Company's standards and that the Description perfectly reflects the meaning of the Profile. The example shown is a Read-Only Profile, for Active Directory Objects management.

PROFILE (1)	
NAME:	A.D. - Read-only
DESCRIPTION:	Read-only Access to Active Directory Users, Contacts, Computers & Groups

Figure 3.3-3

FEATURES (2)			
ACTIVE DIRECTORY	USER	READ	X
		ADD	
		REMOVE	
		RENAME	
		EDIT	
		ENABLE	
		DISABLE	
		CHANGE PASSWORD	
		UNLOCK	
		ADD TO GROUP	
REMOVE FROM GROUP			
ACTIVE DIRECTORY	CONTACT	READ	X
		ADD	
		REMOVE	
		RENAME	
		EDIT	
		ADD TO GROUP	
ACTIVE DIRECTORY	COMPUTER	READ	X
		ADD	
		REMOVE	
		ADD TO GROUP	
		REMOVE FROM GROUP	

Figure 3.3-4

- (2) Features. Choose the features you want to associate with this Profile. Be sure you enable ONLY what this user (or group of users) will need. Also, be aware that features are grouped in 4 big categories (Active Directory, Security, Reporting and Self-Service) according to the type of action needed. Figure 3.3-4 shows Read-only features (within the Active Directory section) being associated with this Profile.

The Security Users, Profiles and Scopes Planner

(3) Scope. Define the Scope's Name and Description. Try to be as detailed and illustrative as possible. See figure 3.3-5.

SCOPE	(3)
NAME: Remote Desktop Users Scope	
DESCRIPTION: All objects in the 'Remote Desktop Users' (default) Active Directory Group	

Figure 3.3-5

FEATURES APPLY TO THESE ACTIVE DIRECTORY NAMES
USERS
Builtin\Remote Desktop Users
GROUPS
All US Users
ORGANIZATIONAL UNITS
Regions>U.S.>OH ; Regions>U.S.>FL

(4) List the Active Directory Users, Groups or Organizational Units part of this scope. In this case, the example shows the Active Directory Users, Groups and O.U.'s part of the Remote Desktop Users Scope.

Figure 3.3-6

(5) ADCP Users. List the Users or Groups that will be associated with this Profile.

USERS OR GROUPS FOR CLOUD CONSOLE AND/OR SECURITY STUDIO
Builtin\Administrators
Domain Admins
HR manager

Figure 3.3-7

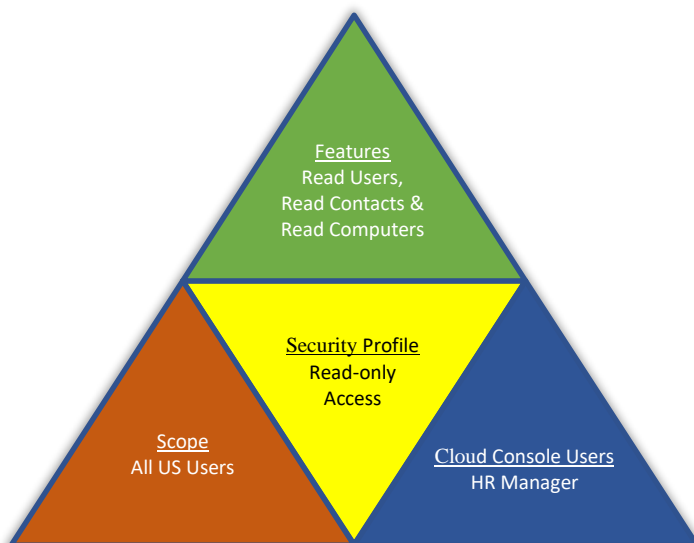


Figure 3.3-8

Figure 3.3-8 summarizes the ADCP Components (Features, Scope and Users) of the example detailed above. Together, they form the Read-Only Profile.

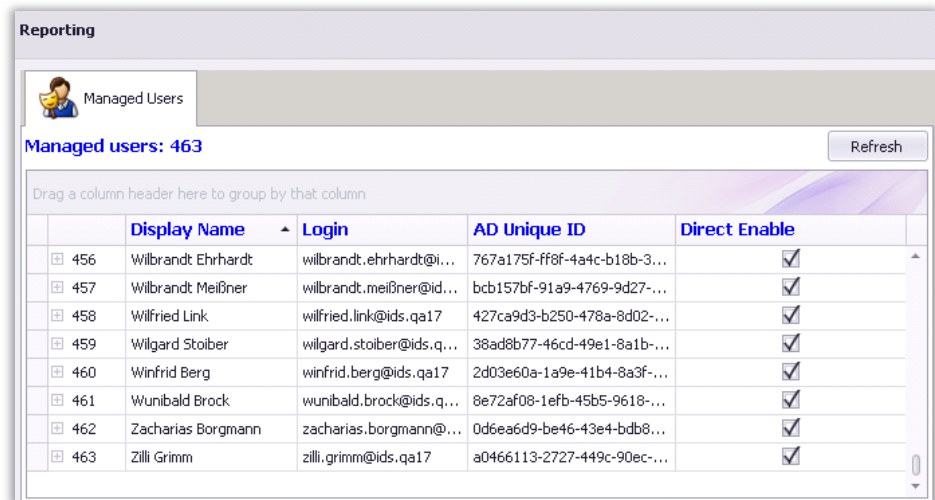
Standard Reports

ADCP offers a complete section dedicated to providing detailed information related to the software’s operation, gathered and condensed for easy understanding. This section includes:

- ☞ A list of Managed Users
- ☞ A list of all changes via ADCP, including Original and New values.
- ☞ A Reports Designer tool.

Managed Users

Quickly and easily learn all the users who are under your organization’s scopes of administration. Find in this grid detailed information of all the users in Active Directory who are being managed by the ADCP Users.



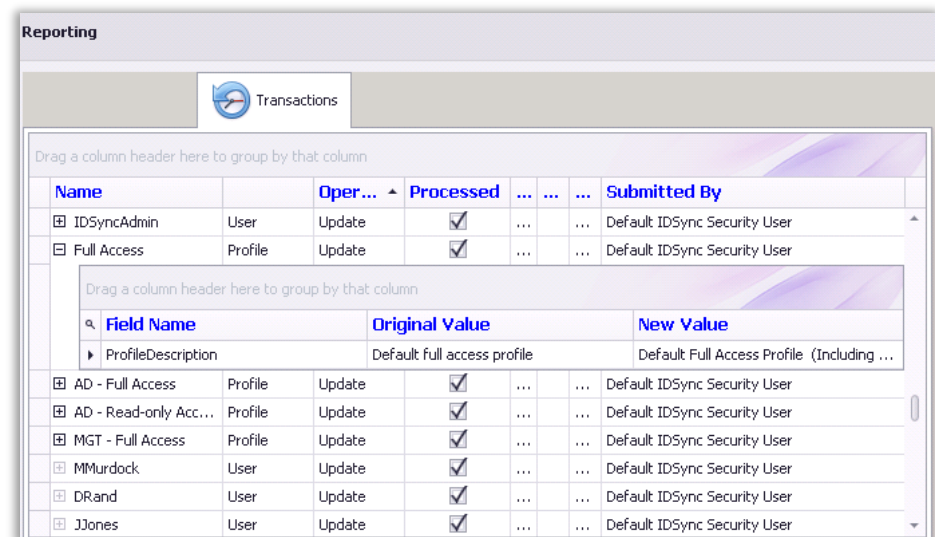
	Display Name	Login	AD Unique ID	Direct Enable
456	Wilbrandt Ehrhardt	wilbrandt.ehrhardt@i...	767a175f-ff8f-4a4c-b18b-3...	<input checked="" type="checkbox"/>
457	Wilbrandt Meißner	wilbrandt.meißner@id...	bc157bf-91a9-4769-9d27-...	<input checked="" type="checkbox"/>
458	Wilfried Link	wilfried.link@ids.qa17	427ca9d3-b250-478a-8d02-...	<input checked="" type="checkbox"/>
459	Wilgard Stoiber	wilgard.stoiber@ids.q...	38ad8b77-46cd-49e1-8a1b-...	<input checked="" type="checkbox"/>
460	Winfried Berg	winfried.berg@ids.qa17	2d03e60a-1a9e-41b4-8a3f-...	<input checked="" type="checkbox"/>
461	Wunibald Brock	wunibald.brock@ids.q...	8e72af08-1efb-45b5-9618-...	<input checked="" type="checkbox"/>
462	Zacharias Borgmann	zacharias.borgmann@...	0d6ea6d9-be46-43e4-bdb8...	<input checked="" type="checkbox"/>
463	Zilli Grimm	zilli.grimm@ids.qa17	a0466113-2727-449c-90ec-...	<input checked="" type="checkbox"/>

Figure 3.4-1

Transactions

Get detailed information about any change that has occurred in your Active Directory’s Managed Objects.

As shown in Figure 3.4-2, ADCP will show any change that has been submitted, using the Cloud Console or the Security Module, detailing who and when performed the change, as well as the previous and new values of any modified field.



Name	Oper...	Processed	Submitted By
IDSyncAdmin	User	Update	Default: IDSync Security User
Full Access	Profile	Update	Default: IDSync Security User

Field Name	Original Value	New Value
ProfileDescription	Default full access profile	Default Full Access Profile (Including ...

	Field Name	Oper...	Processed	Submitted By
AD - Full Access	Profile	Update	<input checked="" type="checkbox"/>	Default: IDSync Security User
AD - Read-only Acc...	Profile	Update	<input checked="" type="checkbox"/>	Default: IDSync Security User
MGT - Full Access	Profile	Update	<input checked="" type="checkbox"/>	Default: IDSync Security User
MMurdock	User	Update	<input checked="" type="checkbox"/>	Default: IDSync Security User
DRand	User	Update	<input checked="" type="checkbox"/>	Default: IDSync Security User
JJones	User	Update	<input checked="" type="checkbox"/>	Default: IDSync Security User

Figure 3.4-2

