



inContact®

Satisfaction as a Service

**UPTIVITY DISCOVER  
ADMINISTRATION MANUAL,  
V5.5.1**

February 2015

[www.incontact.com](http://www.incontact.com)

# UPTIVITY DISCOVER ADMINISTRATION MANUAL, V5.5.1

---

Version: 5.5.1

Revision: February 2015

About inContact: inContact (NASDAQ: [SAAS](#)) is the cloud contact center software leader, helping organizations around the globe create high quality customer experiences with a complete workforce optimization portfolio (WFO). Key portfolio offerings are **inContact Discover WFO** (tightly integrated with the core platform and completely available in the cloud) and **Uptivity Discover WFO** (comprehensive, premise-based WFO that integrates with a wide variety of telephony and contact center solutions). The portfolio also includes the WFO Suite powered by Verint<sup>®</sup>, ECHO<sup>™</sup> Customer Feedback Survey, inView<sup>™</sup> Performance Dashboard.

inContact is the only provider to combine cloud software with an enterprise-class telecommunications network for a complete customer interaction solution. Winner of Frost & Sullivan 2012 North American Cloud Company of the Year in Cloud Contact Center Solutions, inContact has deployed over 1,300 cloud contact center instances. To learn more, visit [www.inContact.com](http://www.inContact.com).

Copyright: ©2015 inContact, Inc.

Disclaimer: inContact reserves the right to update or append this document, as needed.

Contact: Send suggestions or corrections regarding this guide to [documentation@incontact.com](mailto:documentation@incontact.com).

## Table of Contents

<b>Introduction.....</b>	<b>12</b>
Audience .....	12
Goals .....	12
Assumptions .....	12
Need-to-Knows .....	12
<b>Discover Basics .....</b>	<b>14</b>
Uptivity Discover Licensing .....	15
Request a New License .....	15
View License Information .....	16
<b>Roles &amp; Permissions.....</b>	<b>17</b>
About Roles & Permissions .....	17
About the Roles List.....	19
Create a Role.....	19
Edit a Role.....	20
Copy a Role.....	20
Delete a Role .....	20
About Permissions.....	21
General Administration Permissions .....	21
System Permissions.....	21
Coaching Permissions (for use with Uptivity Discover Quality Management) ...	22
Reporting Permissions.....	23
Player Permissions.....	23

## Introduction

Survey Permissions (for organizations using Uptivity Discover Survey) .....	24
Analytics Permissions (for organizations using Uptivity Speech Analytics) .....	24
On-Demand Permissions (for organizations using Discover On-Demand) .....	25
Dashboard Permissions .....	26
Discover Toolbar Permissions .....	26
Uptivity Clarity WFM Permissions (requires Uptivity Clarity WFM) .....	26
User Edit Field Permissions .....	28
Configure Permissions for Discover Groups .....	28
Configure Permissions for ACD Groups and/or ACD Gates .....	29
Edit Role Assignments for Multiple Users .....	30
<b>Users .....</b>	<b>31</b>
About User Accounts .....	31
About the Users List .....	34
Add a User .....	35
Edit a User .....	35
Lock a User Account .....	36
Deactivate a User .....	36
Delete a User .....	37
Import Users .....	37
Export Users .....	38
Set Up an Agent to Be Recorded .....	38
<b>Discover Groups .....</b>	<b>40</b>
About the Discover Groups List .....	41

Create a Discover Group .....	41
Delete a Discover Group.....	41
Add/Remove Agents in a Discover Group.....	42
<b>Scheduling .....</b>	<b>43</b>
About the Scheduling Process Flow.....	43
About Time-Based Agent Schedules.....	44
Create a Time-Based Agent Schedule .....	44
About Number-of-Calls Based Agent Schedules .....	45
Create a Number-of-Calls Based Agent Schedule.....	45
About Custom Agent Schedules.....	46
Custom Schedule Criteria Fields .....	46
Schedule Requirements: Simple Business Rules .....	50
Schedule Expression: Advanced Business Rules .....	51
Create a Custom Agent Schedule .....	53
Find a Schedule .....	53
About the Schedule List .....	54
About Timed Schedules.....	55
Licensing for Timed Schedules .....	55
About the Timed Schedule List.....	55
Create a Timed Schedule.....	56
<b>Tools .....</b>	<b>58</b>
About the Service Manager.....	58
Start/Stop Discover Services .....	59

Introduction	
About the Archiver Console .....	60
<b>Recorder Settings .....</b>	<b>61</b>
About CTI Cores.....	61
About Buddy Cores.....	61
About Primary/Secondary Buddy Cores .....	62
About Active/Inactive Buddy Cores.....	62
Custom Lookups .....	63
Configure Custom Lookups .....	63
Import Multiple Custom Lookup Values .....	64
IP Phones.....	65
Configure IP Phone Settings .....	65
Import Multiple IP Phones .....	66
On-Demand.....	66
Transcoder .....	66
Transcoder Settings.....	67
Voice Boards .....	70
Configure Voice Board Channels .....	71
Channel Configuration Settings .....	71
<b>System Settings .....</b>	<b>72</b>
About the Uptivity API Service .....	72
About Archive Actions .....	72
About the Archive Actions List.....	73
Archive Action Settings .....	74

Customize the Location File Mask .....	77
Configure Archive Actions.....	78
About the Archiver .....	79
General Archiver Settings .....	79
System Purge Action.....	80
Removable Media Settings.....	81
MSSQL Database Backup Settings .....	81
About Custom Extensions.....	82
About Disk Space Notifications.....	82
About Info Broker.....	83
Info Broker Settings .....	83
About Locations .....	83
About Logging .....	84
About Discover Mail.....	84
Discover Mail Settings.....	84
About Notifications .....	85
About Alert Subscriptions .....	85
About E-Mail Notifications Settings .....	86
About SNMP Notifications Settings .....	87
Configure Notifications.....	87
Test Alerts.....	88
About Server Nodes.....	88
Web Media Server .....	88

Introduction	
Web Media Server Settings .....	89
About Web Server .....	90
About Workstations Settings .....	90
<b>Web Portal Settings .....</b>	<b>91</b>
About CometDaemon .....	91
About CometDaemon Settings .....	91
About Security .....	92
Site Settings .....	92
Forgot Password Settings .....	92
Active Directory Settings .....	93
Login Settings .....	94
PCI Settings .....	95
HTTP/HTTPS Settings .....	96
About Terminology .....	96
Terminology Settings .....	97
Configure Terminology .....	97
About Web Portal .....	98
Web Portal Settings .....	98
About Home Tab Widgets .....	99
About the Home Tab Widgets List .....	99
Manage Dashboards .....	100
<b>Appendix: System Security in Discover .....</b>	<b>101</b>
Security Design .....	101



Blackout Sensitive Data .....	102
Purging Sensitive Data.....	103
Authentication and Passwords.....	103
Windows PC, Server, Database, and Application Accounts .....	103
Logging and Auditing .....	104
Login Mode Configuration .....	104
SSL and TLS (Transport Security).....	105
Transport Security and PCI Compliance.....	106
HTTP/HTTPS Settings.....	107
<b>Appendix: Uptivity Discover Best Practices .....</b>	<b>108</b>
Disk Space Management .....	108
Plan for Growth.....	108
Remove Patches and Installers.....	108
Set Up Discover Disk Space Management Features .....	109
Delete Files from Content Management Upload Directory.....	109
Delete Temporary Files after Issues .....	109
Automatically Delete Temporary Files .....	109
Shut Down and Restart .....	110
Shut Down Discover Services.....	110
Anti-Virus Protection.....	111
Exclusion Guidelines .....	111
Common File Types .....	112
Additional Anti-Virus Considerations .....	113

## Introduction

### **Appendix: File Encryption in Uptivity Discover WFO..... 114**

Encryption Best Practices .....	115
About Thales Encryption vs. Standard Key Management.....	115
Verify File Encryption .....	116

### **Appendix: Uptivity Discover Screen Recording Administration..... 117**

Screen Recording Overview .....	117
Considerations .....	119
Security and PCI Compliance .....	119
About the Screen Recording Server .....	120
Screen Recording Server Settings.....	120
Configure Workstation Mapping.....	120
Import Workstations (Optional) .....	121
About the Screen Recording Client.....	122
Configure User Accounts for Screen Recording .....	122
Install the Screen Recording Client .....	123
About Silent Options for Client Installation.....	124
Configure the Screen Recording Client INI File .....	126
Screen Recording Troubleshooting.....	129
Laptops, New Monitors, Projectors, Changing Resolution .....	129
Multiple Monitors and USB Adapters.....	129
Desktop Background Images .....	130
System Events and Screen Recording .....	130
Troubleshooting Procedures.....	132

**Document Revision History ..... 135**

# Introduction

## Audience

This document is designed for users who will serve as administrators of Uptivity Discover WFO for their organizations. Readers should have a high level of familiarity with usage of a PC and its peripherals, the Windows operating system, their organization's ACD/PBX, and the business rules that affect both how Discover will be initially set up and how it will be used on a daily basis.

## Goals

The goal of this document is to provide knowledge, reference, and procedural information necessary to serve as an Uptivity Discover application administrator. The document is NOT intended as a specific system or network design document, nor is it designed to educate the reader on contact center and IT administration concepts or best practices.

## Assumptions

This document assumes that Uptivity Discover has been installed and integrated with your PBX if applicable.

## Need-to-Knows

The *Uptivity Discover Web Player Manual* contains general knowledge and procedures related to using the Web Portal, and may prove a helpful reference.

Depending on the components and modules used in your Uptivity Discover implementation, you may find these additional documents useful:

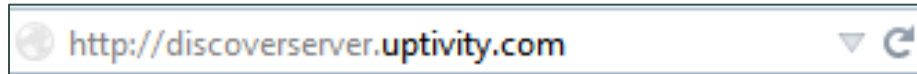
- Applicable *Customer's Guide* to your PBX/ACD integration
- *Uptivity Clarity WFM Administration Manual*
- *Uptivity Speech Analytics Administration Guide*
- *Uptivity Survey Administration Guide*
- *Uptivity Fusion Desktop Analytics Administration Guide*
- *Uptivity Discover On-Demand Administration Guide*

Several Discover features use pop-up menus and other windows that may be considered as “pop-ups” by some browsers. inContact recommends that you configure your browser to allow pop-ups for the Discover site.

Discover supports standard Windows methods for selecting multiple items in a list: press and hold the Shift key while clicking to select consecutive items or press and hold the CTRL key while clicking to select non-consecutive items.

## Discover Basics

Most administration tasks are performed in the Discover Web Portal, which you can access using a web browser. Internet Explorer, Firefox and Google Chrome have been tested and work well with Discover. Your Uptivity Discover Installation team will provide you with a web address for the portal. If your system topology calls for multiple Web Portals, each will have a unique hostname and IP address.



Uptivity Clarity WFM uses a different Web Portal than Uptivity Discover. If your installation includes both Clarity and Discover, your team will provide you with two web addresses. However, once you have logged into the Web Portal for either, you can switch back and forth between the two from within the applications.

Information visible in the Web Player portion of the Discover Web Portal is determined by user permissions and by Call List Settings. You can request a custom default setting configuration that is applied whenever you create a user account. Ask your Uptivity Discover team for additional information.

The version number for your Discover software appears in the upper-right corner of the login page. This version number can be useful for locating correct documentation for your software and obtaining support for your system.



Discover has a default account with system administrator level privileges. Your Installation team will provide you with the account username and password. You should change your password from the default as soon as possible. If your system is configured to use AD authentication, this application-level account will not be available to you. The Web Portal must be configured to allow either Database or Hybrid Mode authentication for application-level accounts to be used.

Discover allows you to customize field names and terminology in the Web Portal to fit your unique environment. Therefore, screen examples and field names used in this manual may differ from those seen in your implementation. For more information, see [About Terminology](#).

## Uptivity Discover Licensing

Uptivity Discover is a licensed product. Call recording and other functionality will not work if the Uptivity Discover software license file is not present, is invalid, has expired or is corrupt. The license is unique to your system and is created and loaded during installation.

Discover licenses are based on a MachineID that contains information about the hardware and software configuration of the Discover server. Therefore, making major changes to your Discover system (e.g., such as changing the Windows machine name, changing a motherboard, etc.) will cause your license to become invalid. The server will not function until a new license is created and applied to the system.

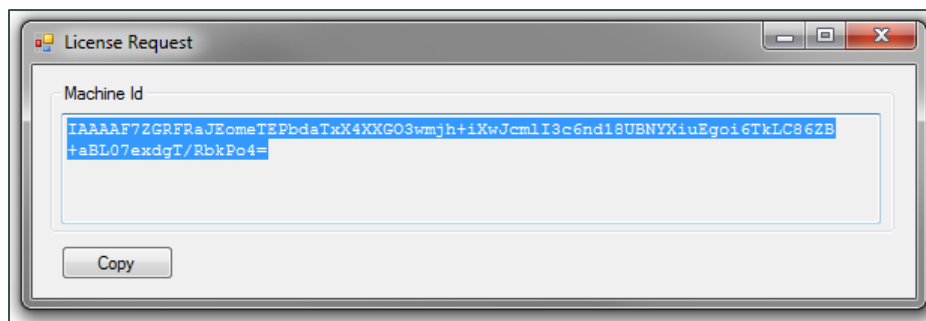
inContact recommends any such maintenance be scheduled for an approved maintenance time, as the system will be non-operational after the maintenance until a new license is applied. Contact your Uptivity Support team if any such maintenance is planned, so a new license can be issued immediately after system maintenance is completed.

In order to create a new license file, a new Machine ID must be generated on the server and supplied to Uptivity. This must occur **after** any maintenance is completed.

### Request a New License

To request a new license from Uptivity Support:

1. Open the Recorder directory on your Discover server.
2. Run the "LicenseRequest.exe" application to open a License Request window displaying the new Machine ID.



3. Click **Copy**.

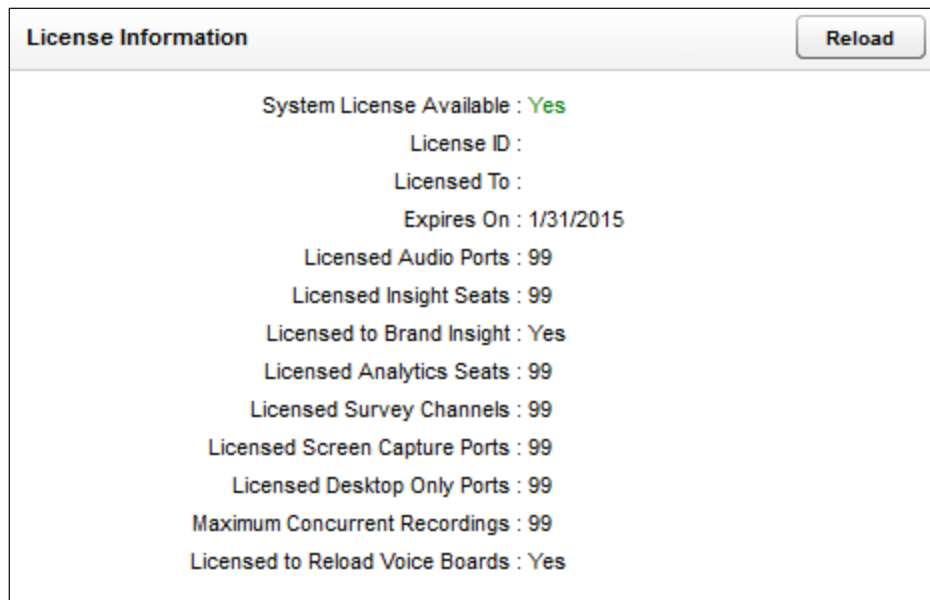
## Discover Basics

4. Paste the Machine ID into an email and send it to the Uptivity Support team, who will reply with a new license file.
5. Save the license file to the CallCopy directory on the Discover server.

## View License Information

To view license status:

1. Click the **Reporting** tab in the Discover Web Portal and expand **System Reports** in the left navigation menu.
2. Click **License Info**.
3. If **System License Available** is **Yes**, but no licenses are showing, click **Reload**.



If the license information looks correct, but call recording and other functions are not working, this may indicate problems with your license file. You may also see Windows server repeatedly attempting to start the Discover services and modules in Windows Task Manager. In this situation, contact Uptivity Support to investigate.



# Roles & Permissions

## About Roles & Permissions

**Permissions** and **Roles** work together to define what users can do in Discover. You will first create one or more roles and associate specific permissions with it. Then you will assign individual users and/or groups to the role(s) based on the permissions that user or group needs. Key facts about roles include:

- A role can be assigned to multiple users.
- A user can be assigned multiple roles.
- Role permissions are cumulative. For example, Role A has Permission 1, and Role B does not have Permission 1. If a user is assigned both Role A and Role B, that user will have Permission 1.
- Discover permissions do not conflict.
- Discover allows you to create an unlimited number of roles. Having more roles allows security to be more granular and targeted to the needs of specific users. But more roles can be confusing to administer, and users may not know what roles they need when they request access.

At the time of installation, Discover includes:

- One default role: `DiscoveryDefaultAgent`. You cannot delete this role but you can edit its permissions.
- A Superuser account with all permissions. The Superuser access level is not considered a role. You can grant Superuser access to individual users, but `inContact` recommends that you limit the number of superusers for security reasons.

Before creating users, develop a single plan that governs the use of groups and roles. The following two generic plans may help you decide the best plan for your organization.

### **Plan 1: Small Team**

In this scenario, a company has one location, and 30 agents are divided evenly to work three eight-hour shifts. Each shift has a supervisor who reviews call records and performs quality evaluations. The company owner and another employee administer the network and Discover. All calls are for the company's products.

The company could create:

- An Agent role and an Agent group. All agents are placed in the group, and the role allows them to review their own calls and evaluations.
- A Supervisor role and a Supervisor group. All supervisors are placed in the group, and the role allows them to review any agent's calls, perform evaluations, and live monitor agents.
- A system administrator role assigned to the company owner and administrator. These users can create users, change system settings, and also perform tasks that supervisors do.

### **Plan 2: Multiple Teams**

In this scenario, the company has three locations, and 120 agents who work a variety of shifts. All agents answer calls for the company's products. Some agents answer calls for a new Product X. Another group answers Spanish callers. This more complex organization could use the following role structure:

- An Agent role and an Agent group. All agents are placed in the group, and the role allows them to review their own calls and evaluations.
- A Supervisor role and a Supervisor group. All supervisors are placed in the group, and the role allows them to review any agent's calls, perform evaluations, and live monitor agents.
- Spanish Agent role and Spanish Agent group. Only certain agents are placed in this group. The role is assigned only to this group.
- Spanish Supervisor role and Spanish Supervisor group for those supervisors who evaluate Spanish-speaking agents.
- Product X role and Product X group. Any supervisor can evaluate these calls, so the Supervisor group is given permission to this group. Having a group for Product X allows users to search for and report on calls for this product.
- A system administrator role assigned to the company owner and administrators. These users can create users, change system settings, and also perform tasks that supervisors do.

Roles can also be created to fine-tune permissions for features like quality management and reporting. Creating specialized roles like QM Form Designer or Reporting Admin and assigning it to a few agents or supervisors maintains the base roles while allowing the flexibility to assign the feature-specific role.

## About the Roles List

Id	Name	Description	Last Modified
279	SurveyTest		11/25/2013 10:23 AM
1	DiscoveryDefaultAgent	This role contains the basic permissions normally available to all users. The role may be edited but may not be deleted.	2/10/2014 10:07 AM
280	ClarityUser		2/11/2014 11:25 AM
278	ClaritySuper		12/27/2013 2:53 PM
276	CCSuper	Typical permissions for a call center team lead or group supervisor	2/4/2014 9:31 AM
277	CCManager	Typical permissions for a call center manager	2/4/2014 9:30 AM

The **Roles** list shows the existing roles and when they were last modified. The system automatically generates the Role ID and uses this to track the role. This enables you to change the name of a role if necessary.

## Create a Role

To create a role:

1. Click the **Administration** tab and expand **Permissions** in the left navigation menu.
2. Click **Roles** and then click **Add Role**.
3. Enter a name for the role and, optionally, a description.
4. Select the check box(es) for the permission(s) needed for the role. For more information, see [About Permissions](#).
5. Associate the role with one or more Discover Groups, ACD Groups and/or ACD Gates if desired. For more information, see [Configure Permissions for Discover Groups](#) and [Configure Permissions for ACD Groups and/or ACD Gates](#).
6. Click **Save**.

### Edit a Role

To edit a role:

1. Click the **Administration** tab and expand **Permissions** in the left navigation menu.
2. Click **Roles** and then double-click the name of the desired role.
3. Make any desired changes and then click **Save**.

### Copy a Role

Copying a role assures consistent permissions assignment. For example, you might have one role for a group and want to create a group that will perform the same actions in Discover but handle a different type of call. Copying the role and giving it a different name assures that the agents have exactly the same permissions.

1. Click the **Administration** tab and expand **Permissions** in the left navigation menu.
2. Click **Roles** and then click the role to be copied.
3. Click **Copy Role**.
4. Enter a name for the role and then click **Save**.

### Delete a Role

Deleting roles removes permissions from users to which the role was attached, but does not delete the users themselves.

1. Click the **Administration** tab and expand **Permissions** in the left navigation menu.
2. On the Roles page, click **Delete Roles**.
3. Select one or more of the Available Roles.
4. Click the **right arrow**.
5. Click **Delete** and then click **Back**.

## About Permissions

Permissions in Discover can be very granular, allowing you to restrict users to only those tasks, groups, agents, and recordings to which they need access to perform their jobs. This section lists all of the Discover permission and provides a brief description of each.

Uptivity Clarity permissions are best understood in the context of the tasks to which they relate. Very few Clarity tasks require only a single permission. This section provides only a list of the Clarity permissions you will see in the Web Portal. For a full discussion of Clarity permissions, see the "Permissions, Roles & Accounts" section of the *Uptivity Clarity WFM Administration Manual*.

### General Administration Permissions

**Allow User Administration:** Allows users to add, edit, and delete other system users. This is an administrator-level permission.

**Allow Password Changes:** Allows users to modify their own password in Discover. If unchecked, a system administrator will have to modify the password for the user. Users cannot use the "Forgot Password" functionality in Discover unless they have this permission.

### System Permissions

**Note:** System Permissions should typically be limited to administrator roles.

**Allow System Configuration:** Allows users to modify system configuration settings.

**Allow Recording Record and File Deletes:** Allows users to delete records from Discover.

**Allow Archive Administration:** Allows users to create and edit Archives.

**Allow Group Administration:** Allows users to create and edit Discover Groups. While administering these groups, users with this permission can see all users to facilitate adding new group members.

**Allow Scheduling:** Allows users to set system-wide schedules. Recordings based on system schedules are not governed by the disk quota of the user who created the schedule.

**Allow API Authentication:** This permission is not used.

### Coaching Permissions (for use with Uptivity Discover Quality Management)

**Note:** Coaching permissions for performing, editing and deleting evaluations are affected by the Player permission "Allow Viewing All Call Records and QA Evaluations". Users with this permission could potentially view QA reports for all groups and agents, evaluate any agent, edit any evaluation, and/or delete any evaluation.

**Allow Viewing of QA Evaluations:** Allows users to view and access evaluations for any group(s) to which they have permission, including their own evaluations. Selecting this option automatically selects the other Coaching permissions. If those permissions are not appropriate for a role, clear them individually.

**Allow Deletion of Completed QA Evaluations:** Allows users to delete completed QA evaluations for groups to which they have permission, including their own evaluations. This allows for a disputed score to be deleted, and then reissued when appropriate. This permission does not apply to in-progress evaluations.

**Allow Manage Achievements:** Allows users to add a new achievement type for any agent or group. Also allows users to view and edit added achievement types, view a list of achievements awarded to agents, and upload custom icons displayed when achievements are awarded. Achievements can be awarded to specific groups or agents based on either QA evaluation scores or as an *ad hoc* achievement. To award ad hoc achievements, users must have the **Allow Award Ad Hoc Achievements** permission.

**Allow Editing of Completed QA Evaluations:** Allows users to edit the score or responses of a completed QA evaluation for groups to which they have permission, including their own evaluations. This permission does not apply to in-progress evaluations. To edit completed evaluations, users must also have the **Allow Performing QA Evaluations** permission.

**Allow Performing QA Evaluations:** Allows users to issue an evaluation upon an agent in any group to which they have permission. Users with this permission may also serve as arbitrators for dispute resolution involving agents they have access to evaluate. Also allows users to edit or delete an in-progress evaluation for an agent in any group to which they have permission.

**Allow Award Ad Hoc Achievements:** Allows users to award an existing ad hoc achievement type to any agent or group to which they have permission. To add or edit achievement types, users must also have the **Allow Manage Achievements** permission.

**Allow QA Form Administration:** Allows users to build and edit a QA form for any group.

**Allow Content Library Management:** Allows users to upload and manage files in the Content Library.

### Reporting Permissions

**Allow Viewing Call Reports:** Allows users to run reports based on call detail data.

**Allow Viewing QA Reports:** Allows users to run reports based on QA data (requires Uptivity Discover Quality Management).

**Allow Viewing Analytics Reports:** Allows users to run analytics reports (requires Uptivity Speech Analytics).

**Allow Viewing Audit Reports:** Allows users to run audit reports to monitor actions taken by other users in the system. This is an administrator-level permission.

**Allow Viewing System Reports:** Allows users to perform system-level reporting. This is an administrator-level permission.

**Allow Discover Ad Hoc Reporting:** Allows users to view the Ad Hoc Reporting menu, create ad hoc reports using the Report Builder page, and view/edit any ad hoc report that has been saved. This permission does not provide access to any report data and does not change the ability to save report search criteria as public or private. These reporting category permissions control the data fields users see in the ad hoc report builder: **Allow Viewing Call Reports**, **Allow Viewing QA Reports**, **Allow Viewing Survey Reports**, **Allow Viewing Audit Reports**. For example, to create/edit an ad hoc report on QA evaluations, a user needs both the **Allow Viewing QA Reports** and **Allow Discover Ad Hoc Reporting** permissions.

**Allow Report Subscriptions:** Allows users to set a specific report to run at a scheduled time, and provide the results to multiple users via email.

**Allow Viewing Survey Reports:** Allows users to run survey reports (requires Uptivity Discover Survey)

### Player Permissions

**Allow Viewing of User's Own Records:** Allows users to view calls recorded from their associated user account.

## Roles & Permissions

**Allow Viewing All Call Records & QA Evaluations:** Allows users to view all call recordings and QA evaluations regardless of group and/or gate settings. This permission should be granted to very few users. For related information, see [Coaching Permissions \(for use with Uptivity Discover Quality Management\)](#).

**Allow Live Monitoring of Calls:** Allows users to listen to audio of contacts in "real-time."

**Allow Downloading of Export:** Allows users to export recordings from Discover to their workstation using the Web Portal.

**Allow Emailing of Export:** Allows users to export and send recordings to an email address using the Web Portal.

**Allow Bookmarking:** Allows users to attach public or private bookmark comments to call records.

**Allow Viewing of Video:** Allows users to view video screen recordings associated with call records. Also allows live monitoring of video (where available) and video for timed schedules (i.e., screens recorded without associated calls). Requires Uptivity Discover Screen Recording.

### **Survey Permissions (for organizations using Uptivity Discover Survey)**

**Allow Viewing Surveys:** Allows users to view completed Survey results.

**Allow Survey Administration:** Allows users to manage Survey server configuration.

**Allow Editing Surveys:** Allows users to create, delete, and manage Survey forms.

**Allow Deleting Surveys:** This permission is not used.

### **Analytics Permissions (for organizations using Uptivity Speech Analytics)**

**Allow Analytics View:** Allows users to view Analytics data.

**Allow Analytics Administration:** Allows users to manage Analytics configuration.



**On-Demand Permissions (for organizations using Discover On-Demand)**

**Note:** If you change permissions while a user is logged into On-Demand, the changes will not take effect until the next time the user logs into the On-Demand client.

**Allow Recording by Device ID:** Allows users to record using the physical device extension.

**Allow Call Updates:** Allows users to update the call recording with additional information which is stored in Discover's user-configurable database fields. You control which fields the users can update using the On-Demand module. For more information, see the *Uptivity Discover On-Demand User Guide*.

**Prevent Setting Changes:** Prevents users from changing the IP address and port used to connect to the On-Demand server, as well as which of the On-Demand servers is the primary server.

**Allow Web On Demand:** This setting is not used.

**Allow Recording by Device Alias:** Allows users to record using a device alias (a device ID that does not physically exist, but is mapped to an existing physical device). Supports environments where agents use different physical devices but keep the same extension.

**Allow Recording Stop:** Allows users to stop call recordings that they initiate or that are already in progress. This allows users to stop the recording even if your system is set to always record. For related information, see [Scheduling](#).

**Prompt for Device at Login:** Prompts users to input their physical Device ID/extension/voice port each time they log in. This setting cannot be used if the **Prevent Device ID Changes** permission is selected.

**Notify On Demand Recordings Only:** Allows notifications to be displayed only for recordings initiated through the On-Demand client. Users with this permission can stop and/or blackout **only** those recordings they started with the On-Demand Client; the options will be grayed out at all other times.

**Allow Desktop Recording:** Allows users to start and stop screen recording if the Uptivity Screen Recording client is installed on their workstation.

**Prevent Device ID Changes:** Prevents users from setting or changing their device ID/extension/voice port from the On-Demand client. When this option is selected, you must manually maintain the association of device IDs to workstations. For

## Roles & Permissions

related information, see [Configure Workstation Mapping](#). This setting cannot be used if the **Prompt for Device ID** permission is selected.

**Allow Blackout Start and Stop:** Allows users to start/stop blackouts of audio recordings using the On-Demand client.

### Dashboard Permissions

**Allow Widget Administration:** Allows users to configure widgets or perform restricted tasks in widgets. This permission is not for granting users access to data. For example, users must have this permission to post items to the News widget, but not to see the News widget on their dashboard.

**Note:** The following three permissions apply only to organizations using Uptivity Clarity WFM.

**Allow View Forecast Actual Data:** Allows users to view, in the Discover Web Portal, forecasted call volume data and actual call volume data created and maintained through Clarity.

**Allow View Service Level Data:** Allows users to view, in the Discover Web Portal, Service Level data created and managed through Clarity.

**Allow View Snapshot Data:** Allows users to view, in the Discover Web Portal, call data and agent status information created and maintained through Clarity.

### Discover Toolbar Permissions

**Note:** Uptivity Discover WFO does not use the Discover Toolbar module.

### Uptivity Clarity WFM Permissions (requires Uptivity Clarity WFM)

For a full discussion of Clarity permissions, as well as sample role/permission configurations, see the "Permissions, Roles & Accounts" section of the *Uptivity Clarity WFM Administration Manual*.

All of the Clarity-specific permissions are listed here in alphabetical order. Some permission names are slightly different in standalone Clarity; where applicable, the permission name in the Discover Web Portal is shown in parentheses.

**Add Leave Request All**

**Add Leave Request Team**

**Allow Change Password** (Allow Password Changes)

**Allow User Admin** (Allow User Administration)

**Call Off**

**Configuration Section**

**Edit News Widget**

**Employee Create**

**Employee Profile All View**

**Employee Profile Team View**

**Employee Schedule All Edit**

**Employee Schedule All View**

**Employee Schedule Self Edit**

**Employee Schedule Self View**

**Leave Request Approval Team**

**PTO Page Self Edit**

**PTO Page All View**

**PTO Page Team View**

**Real Time Widgets**

**Report Subscription** (Allow Report Subscriptions)

**Reports Clarity Ad Hoc** (Allow Clarity Ad Hoc Reporting)

**Reports Historical**

**Reports Processes**

**Reports Real Time**

**Reports Section**

**Roster All**

Roles & Permissions

**Roster Team**

**Schedule Bidding**

**Schedule Create**

**Schedule Load**

**Schedule Publish**

**Schedule Section**

**Swap Request Approval All**

**Swap Request Approval Team**

### **User Edit Field Permissions**

Discover provides fifteen (15) fields that you can customize to contain data relevant to your organization. These fields can be populated automatically via custom API integrations or manually by your agents using the On-Demand module. You can assign individual permissions to edit each of these fields. For related information, see [About Terminology](#).

## **Configure Permissions for Discover Groups**

Group permissions give a user access to call records and other items created by members of a Discover Group. The user also needs relevant Player Permissions, such as Allow Viewing of Video. Assigning permission to a Discover Group does not make a user with that permission a member of the group. For details, see [Discover Groups](#). A role has access permissions to all Discover Groups shown in the **Attached Group** list.

To assign Discover Group permissions to a role:

1. Follow the procedure to [Create a Role](#) or [Edit a Role](#).
2. In the **Associated Discover Group** section, select the desired group(s) under **Unattached Discover Group**.
3. Click the right arrow to move the selected group(s) to **Attached Discover Group** and then click **Save**.

To remove Discover Group permissions from a role:

1. Follow the procedure to [Edit a Role](#).
2. In the **Associated Discover Group** section, select the desired group(s) under **Attached Discover Group**. Hold the Shift key and click to select multiple consecutive groups, or hold the CTRL key and click to select multiple non-consecutive groups.
3. Click the left arrow to move the selected group(s) to **Unattached Discover Group** and then click **Save**.



## Configure Permissions for ACD Groups and/or ACD Gates

Most PBX/ACD systems offer one or more means of grouping agents. Depending on the system, terminology may vary: labor groups, hunt groups, skills, gates and queues are just a few of the naming conventions.

Group and ACD Gate permissions give users access to call records and other items created by members of these types of groups. The users also need any relevant [Player Permissions](#). Assigning user permission to a Group or ACD Gate does not make that user a member of the group, gate or queue. Those memberships must be assigned on the PBX.


If no groups are specified, users with this role will be able to view all ACD groups. If groups are specified in the role, all groups still appear in the Call List Quick Filter Menu, but only calls for the specified groups will be available. This behavior is consistent with how Discover Group and Agent quick filters work in the Web Player.

To provide a role with access to recordings from an ACD Group or Gate:

1. From your PBX, identify the desired ACD Group(s) and/or Gate(s).
2. Follow the procedure to [Create a Role](#) or [Edit a Role](#).
3. Under **Group**, enter any ACD Group name(s) in the text field under the list, exactly as they appear in your PBX/ACD, and then click the **Add**  icon.
4. Under **ACD Gate**, enter any ACD Gate name(s) in the text field under the list, exactly as they appear in your PBX/ACD, and then click the **Add**  icon.
5. Click **Save**.

## Roles & Permissions

To remove a role's access to recordings from an ACD Group or Gate:

1. Follow the procedure to [Edit a Role](#) and then select the desired ACD Group(s) from the **Group** list.
2. Click the **Delete**  icon and then click **Save**.

## Edit Role Assignments for Multiple Users

You can assign roles to individual users when you create the user (see [Add a User](#)), and add/remove roles by editing the user (see [Edit a User](#)). To edit role assignments for multiple users at once:

1. Click the **Administration** tab and expand **Permissions** in the left navigation menu.
2. Click **Roles** and then click **Assign Users to Roles**.
3. Click the desired role.
4. Move users from **Available Users** to **Attached Users** to assign the role; move users from **Attached Users** to **Available Users** to remove the role assignment.
5. Click **Save**.

# Users

**Users** are individuals who have access to Discover and who can perform tasks. Users may include agents, supervisors, system administrators, and others. Users must have a user account in order to log in to Discover. The tasks a user can perform are defined by their assigned role(s). For related information, see [About Roles & Permissions](#).

## About User Accounts

**Note:** User account data can be added to or extracted from Discover via the Uptivity API. For details, see the *Uptivity Discover WFO API Manual*.

Discover allows you to store a variety of information about each user, but only five user account fields are mandatory:

- **Username.** Usernames must be unique. If you try to save a new user account with a Username that already exists, you will receive an error. Discover has no restrictions on characters and spacing in the Username.
- **Password.** There are no default restrictions for passwords.
- **First Name**
- **Last Name**
- **Email Address.** Email addresses must be unique; they are used to automatically email completed evaluation forms to employees.

Other available fields include:

- **Grant Superuser Access.** In most instances you will leave this check box unselected. Superuser access should be granted only in very rare circumstances and is not required to administer the application.
- **Account Locked.** Select this check box if you want to control when the user account becomes usable. For details, see [Lock a User Account](#).

## Users

- **Agent.** Select this check box if the user will be recorded (audio only, desktop only, or both) and should be tracked as an agent in reporting. If you enter an extension for a user, Discover selects this check box for you. Clearing this option allows the user to log into Discover, but the system will not record their calls or include them in reporting. Existing calls can still be evaluated for users whose agent status has been deactivated. For reporting purposes, an agent is Active if the Agent check box is selected. An agent is Inactive if the Agent check box was selected at one point but the check box has been cleared.

**Note:** Several additional tasks must be performed in order for an agent's audio to be recorded. For details, see [Set Up an Agent to Be Recorded](#).

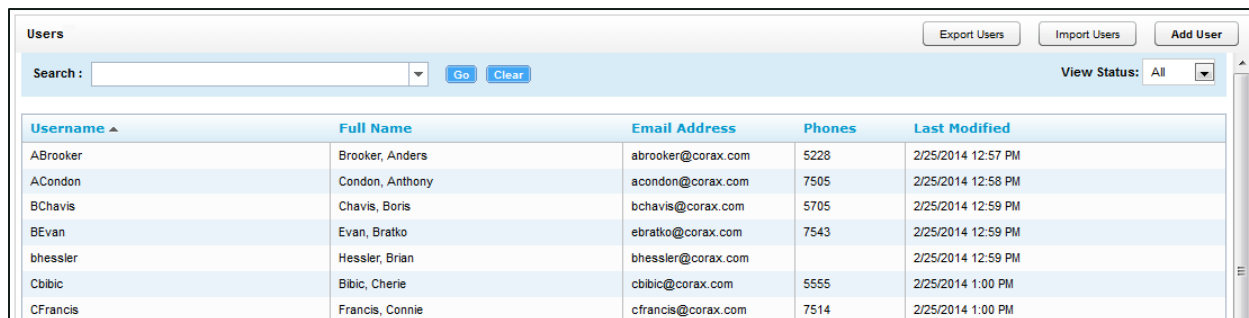
- **System Username.** This is the Windows username that the agent uses to log in to the network. This field is **mandatory** if your organization uses Uptivity Screen recording. Discover uses it to locate an agent's desktop via the Screen Recording client. Each agent must have a unique username, even if the agents are on different Windows domains, and must log in to their desktop with that username.
- **System Domain**
- **Active Directory Username.** This field is required if your organization uses the Active Directory login method. This field will be auto-populated when you select "Auto Create User on Login" or when you import users, provided all information is supplied in the import file.
- **Active Directory Domain.** This field is required if your organization uses the Active Directory login method. This works independently of the System Domain field above, which is primarily required for screen recording. This field will be auto-populated when you select "Auto Create User on Login" or when you import users, provided all information is supplied in the import file.
- **Employee ID.** This is typically used as a unique numbering system to identify employees, often mirroring some form of internal employee identification system.
- **CRM Username.** This field is typically used only when Discover is integrated with a CRM application via a custom API.
- **Location:** This field only appears if "Allow Lookup by Agent/Workstation" was enabled. It allows manual designation of a specific site/location for an agent for proper local routing of Screen Recording and Live Monitoring traffic. This setting is not set by default, but you cannot edit or save an agent without choosing a specific Location. For details, see [About Workstations Settings](#).
- **Quota:** This field is has been deprecated.



- **Shift Times to User's Timezone.** By default, Discover displays time by the time zone of the recording server. Selecting this check box allows time to be displayed using each user's time zone. For example: An agent works in the Eastern US zone and the agent's manager works in the Pacific US zone. The Shift Time option is set on the agent's and manager's accounts. The agent records a call at 8 AM Eastern time, and it appears in Discover to him as 8 AM. However, the call record appears to his manager as if the agent took the call at 5 AM. For this reason, it's important that your users know whether this setting is being used.
- **Time Display Format:** This field specifies whether to display time based on 24-hour (military) or 12-hour time.
- **Phones:** The login(s) and/or extension(s) associated with the user. For fixed-seating environments, enter the physical telephone extension(s). For free-seating environments, enter the agent number(s)/login(s). Consider the following when you enter information in the Phones field:
  - When you enter an extension, the Agent check box is automatically selected. If you clear the Agent check box, Discover will prompt you to remove all associated extensions when you attempt to save your changes.
  - You cannot assign an extension to more than one Agent. For example, extension 1234 cannot be assigned to Sally Smith and Jenny Jones, even if they sit at the same extension on different shifts.
  - You can assign multiple extensions to the same Agent. For example, Sally Smith may take incoming calls on extension 1234 and make outbound calls on extension 4321.
  - You can assign the same Agent to different Groups based on the contents of the Phones field. For more information, see [Add/Remove Agents in a Discover Group](#).
  - You cannot reassign an extension that is still attached to a user, even if that user has been deactivated. For more information, see [Deactivate a User](#).
  - When you remove an extension from an Agent's account, you must also manually remove that Agent from any Groups where membership was based on that extension. For more information, see [Add/Remove Agents in a Discover Group](#).
  - When you lock, deactivate, or delete a User account, you must first remove the associated extensions from that account if you wish to make them available for assignment to other users.

## Users

### About the Users List



Username	Full Name	Email Address	Phones	Last Modified
ABrooker	Brooker, Anders	abrooker@corax.com	5228	2/25/2014 12:57 PM
ACondon	Condon, Anthony	acondon@corax.com	7505	2/25/2014 12:58 PM
BChavis	Chavis, Boris	bchavis@corax.com	5705	2/25/2014 12:59 PM
BEvan	Evan, Bratko	ebratko@corax.com	7543	2/25/2014 12:59 PM
bhessler	Hessler, Brian	bhessler@corax.com		2/25/2014 12:59 PM
Cbibic	Bibic, Cherie	cbibic@corax.com	5555	2/25/2014 1:00 PM
CFrancis	Francis, Connie	cfrancis@corax.com	7514	2/25/2014 1:00 PM

The Users list allows you to see all users in your Discover system.

To access the Users list:

- Click the **Administration** tab and expand **Permissions** in the left navigation menu, then click **Users**.

To locate specific users:

- Enter all or part of a user's name in the Search field, select the desired user from the list of possible matches, and click **Go**.

To filter the list by agent status:

- Select **Users, Agents** (i.e., users who have the Agent option selected on their accounts), or **All** (i.e., both) from the drop-down **View Status** list.

## Add a User

**Note:** If you have a hybrid Discover/Clarity system, creating user accounts in Clarity will also create them in Discover. This is the preferred method. If you create the user account in Discover, you must perform the Mass Update Incomplete Users procedure before the user will be available in Clarity. See the *Uptivity Clarity WFM Administration Manual* for more information.

To add a user:

1. Click the **Administration** tab and expand **Permissions** in the left navigation menu.
2. Click **Users** and then click **Add User** at the top of the User List.
3. Enter information in all mandatory fields. For more information, see [About User Accounts](#).
4. Complete additional fields as desired. For more information, see [About User Accounts](#).
5. Select a time display format.
6. Enter the extension(s) and/or login(s) associated with the agent in the lower field under **Phones** and click the green **Add** icon.
7. Move one or more roles from **Unattached Roles** to **Attached Roles** to assign them; move roles from **Attached Roles** to **Unattached Roles** to remove the assignment.
8. Click **Save**.

## Edit a User

To edit a user:

1. Click the **Administration** tab and expand **Permissions** in the left navigation menu.
2. Click **Users** and then double-click the desired user record.
3. Make the necessary changes and then click **Save**.

Users

## Lock a User Account

By default, users can log into Discover and view the **Home** tab and, if your organization uses Uptivity Discover QM, the **Coaching** tab's **Content Library**. In the library, they can only see documents that have been assigned to them.

Locking a user account prevents the user from logging in to Discover. All other functionality is unaffected, including recording and the account information used for reporting. If the account is needed again, it can be unlocked and will function normally. Users whose accounts have been locked receive a locked account message if they attempt to log in.

Accounts should be locked if a user leaves your organization, transfers to another job role and no longer needs access to Discover, or is prohibited from accessing the system for other reasons. If an account is locked, the extensions/logins can be removed from the account and assigned to another user.

To lock a user account:

1. Click the **Administration** tab and expand **Permissions** in the left navigation menu.
2. Click **Users** and then double-click the desired user record.
3. Select the **Account Locked** check box and then click **Save**.

## Deactivate a User

Deactivating a user/agent is slightly more involved than simply locking the account, but not as permanent as deleting a user altogether. Locking an account would suit someone who has changed positions or is on extended leave. Deactivating would be appropriate in a scenario where a user has left the company altogether or a user's extension has been reassigned, but that user still needs to appear in reports and the user list.

To deactivate a user:

1. Click the **Administration** tab and expand **Permissions** in the left navigation menu.
2. Click **Users** and then double-click desired user record.
3. Select the **Account Locked** check box.
4. Clear the **Agent** check box.
5. Remove the assigned phone extension(s) under **Phones** and then click **Save**.

**Note:** Extensions cannot be reassigned if still attached to a user. If you clear the Agent check box and attempt to save changes without removing the extension(s), you will receive an error message.

## Delete a User

You can delete a user account if the user should no longer be accessible via the Web Portal. The account information and call data will still be in the Discover database, but will no longer be seen by Web Portal users.

To delete a user:

1. Click the **Administration** tab and expand **Permissions** in the left navigation menu.
2. Click **Users**.
3. Double-click the account on the User list.
4. Click **Delete** in the top-right corner and then click **OK**.



## Import Users

You can import users in batches using the CSV (Comma Separated Value) file import function. If you have a database or Excel spreadsheet of agents, you may be able to generate a CSV data file that you can then import into Discover, saving time by minimizing data entry tasks.

The CSV file must be in the following format: username, password, locked, first\_name, last\_name, email, active\_agent, system\_username, system\_domain, employee\_id, site\_id, phone1;phone2;phone3, roleId(role name);roleId(role name);roleId(role name) [optional], ActiveDirectoryDomain (for AD/Hybrid authentication), ActiveDirectoryUsername (for AD/Hybrid authentication)

The locked value is **Y** or empty. Roles are optional. If **Allow Lookup by Agent/Workstation** is enabled in the Web Portal Settings, importing the agent's Location is not supported. You may need to configure this separately for each agent after the import is completed. For more information on Location settings, see [About Workstations Settings](#).

Discover will verify the data is in the correct format and the file does not contain any existing agent names or phone IDs. Discover will also check for existing AD usernames on the same domain if you are using Hybrid or AD authentication. If duplicates are detected, you must correct the file and then try the import again.

## Users

To import users from an existing CSV file:

1. Click the **Administration** tab and expand **Permissions** in the left navigation menu.
2. Click **Users** and then click **Import Users**.
3. Click **Select**.
4. Browse to locate and open the file.
5. If the CSV file has a header row with column labels, select the check box for **Import file has a header**.
6. Click **Upload File** and then click **Import**.

## Export Users

Discover allows you to export a file of the user configuration data stored in its database. You may use this list as a backup or to import user information into other applications.

To export a CSV file of user information:

1. Click the **Administration** tab and expand **Permissions** in the left navigation menu.
2. Click **Users** and then click **Export Users**.
3. Download the file to your local system.

## Set Up an Agent to Be Recorded

The following tasks must be performed in order for an agent's audio to be recorded. The specifics of these tasks may vary somewhat depending on your organization and telephony integration. This list does not include tasks associated with screen recording and live monitoring.

- Create a user account for the agent in Discover and select the Agent option. For details, see [Add a User](#).
- Set the agent's Location if you are using lookup by agent/workstation. For details, see [About Workstations Settings](#).
- In the Phones section of the user account, specify telephone extension(s) for assigned-seating environments or agent number(s)/login(s) for free-seating environments. Discover will record audio without this step, but will not associate the audio with the agent.

- Add the user account to one or more Discover Group(s) if the user will be evaluated and monitored. Group membership is not required for the agent to be recorded. For details, see [Add/Remove Agents in a Discover Group](#).
- Create a new schedule if you use schedules for specific users. Alternatively, you can use an existing schedule to record multiple agents (i.e., those in a group or a range of ANIs). Review the business rules for the schedule and add the new user's extension, ANI, agent number, or other information as applicable. For details, see [Scheduling](#).
- Some telephony systems require that the user's phone be configured to forward call audio or perform in other ways. Review the customer's guide to your integration for requirements and configure the phone as needed.
- Some telephony systems require that the user's extension or device ID be added to a Discover voice board's channel settings. Review the customer's guide to your integration for requirements and configure the voice board channel settings as needed.
- Some telephony systems require that the user's extension or device ID be added to a Discover Core's CTI module. Review the customer's guide to your integration for requirements and configure the CTI Module settings as needed.
- Occasionally, the Discover script will not be able to register user phones in environments using passive VoIP recording. In these cases, administrators may have to add the user's extension to Discover's IP Phones list. For details, see [IP Phones](#).

## Discover Groups

**Discover Groups** are collections of users that you define in a way that makes sense for your organization. For example, Discover Groups could be based on:

- Skills on your ACD/PBX,
- Departments (sales, service, billing, etc.),
- Teams in your contact center (John's Team, Legends Team)
- Clients (for an outsourcer), or
- Geographic locations.

Supervisors and managers of these groups are then given a Discover user account with specific permissions to access records, evaluations, and reports for agents in the groups they manage. Several quality assurance reports are based on Discover Group assignments. Users do not have to be placed in a Discover Group. On the other hand, one user can belong to multiple Discover Groups.

Users can only be added to groups if they have the Agent box selected and at least one phone extension is registered on their user profile. This is because Discover manages group membership based on the agent's phone ID. You can see this in the Discover Group list shown below.

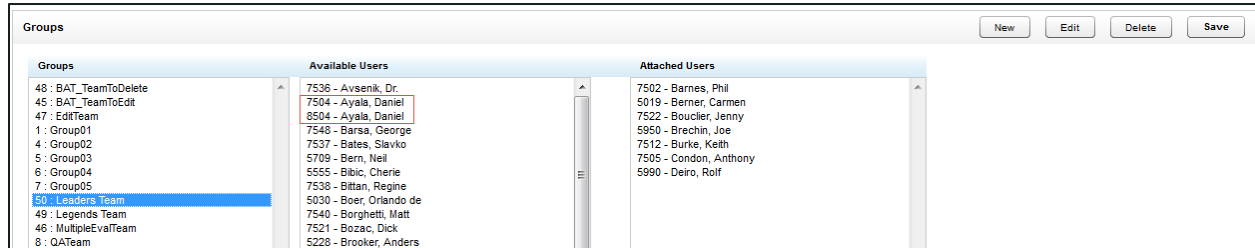
This approach gives you greater flexibility when it comes to associating calls with Discover Groups. For example, if an agent has several extensions and you want all calls for that agent associated with the same group, you will need to add all of the agent's extensions to that group. On the other hand, if the agent has three extensions, and takes a different type of call on each, you can associate each extension with a different group.

**Note:** Throughout this manual, you will see "Discover Groups" used to differentiate between these groups and ACD/PBX Skill groups.



## About the Discover Groups List

The **Groups** page displays a list of current Discover Groups, available users, and users attached to a group. Click any group to see attached users.



## Create a Discover Group

To create a Discover Group:

1. Click the **Administration** tab and expand **Permissions** in the left navigation menu.
2. Click **Groups**.
3. On the Group page, click **New**.
4. Enter a unique name for the new group and then click **Save**.

If a Discover Group already exists with the name you have chosen, the following error will be generated: "That group name already exists! Change the group name and try again."

## Delete a Discover Group

Deleting Discover Groups is not recommended. It will affect historical reporting because the deleted group will not be available as a filter. Also, deleted groups cannot be recovered. Deleting groups does not delete the users in those groups.

To delete a group:

1. Click the **Administration** tab and expand **Permissions** in the left navigation menu.
2. Click **Groups** and then click the group name.
3. Click **Delete** and then click **OK**.

## Discover Groups

### Add/Remove Agents in a Discover Group

To add agents to or remove agents from a Discover Group:

1. Click the **Administration** tab and expand **Permissions** in the left navigation menu.
2. Click **Groups** and then click the desired group.
3. Move users from **Available Users** to **Attached Users** to assign them to the group; move users from **Attached Users** to **Available Users** to remove the group assignment.
4. Click **Save**.

# Scheduling

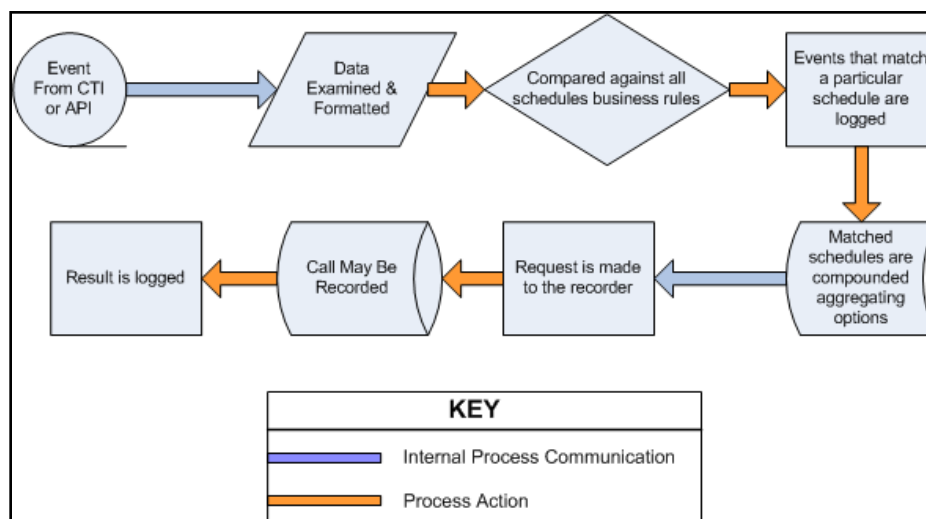
**Note:** Typically, you should create Archive Actions before schedules. For details, see [About Archive Actions](#).

Administrators create schedules based on business rules to control which calls are recorded. The Scheduler is flexible enough to allow for 1% to 100% recording and other types of recording such as time-based blocks or a set number of calls that match a particular schedule.

Schedules can be set up across any combination of call variables. All requests, including CTI messages and API requests related to call or agent information, are routed to the Scheduler for processing.

If your implementation uses multiple recording Cores, you can, if desired, relate schedules to a specific Core. If no schedules are related to a Core, the Core uses all schedules. If one or more schedules are related to a Core, the Core uses only the related schedules. For more information on this strategy, ask the Uptivity Discover Support team.

## About the Scheduling Process Flow



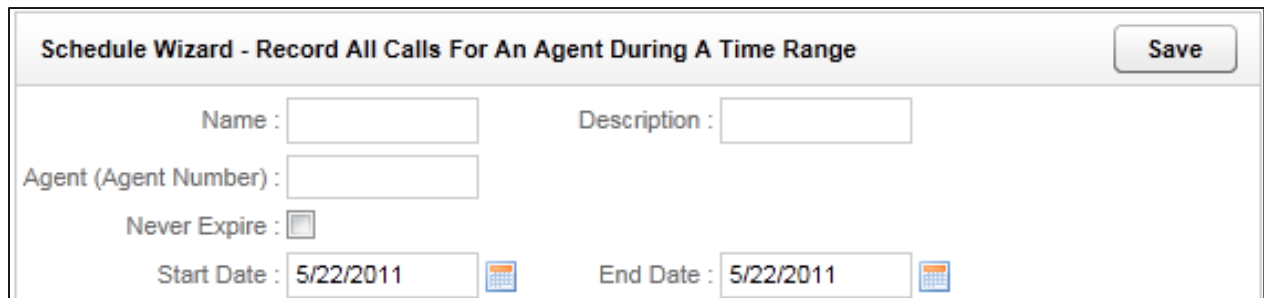
Every event received by the Scheduler is compared against the business rules of all active schedules. An event may match any number of schedules or none at all. When an event matches one or more schedules, an entry is logged for each individual match.

## Scheduling

Schedule options are aggregated, meaning that as an event matches schedules the least restrictive values are assigned to the event. These values include minimum and maximum recording lengths, priorities, retention & archiving, etc.

### About Time-Based Agent Schedules

A time-based schedule records all calls for an agent within a specified date range. Schedules created using this procedure use default values for Retention Days and other settings. For details, see [Custom Schedule Criteria Fields](#).



The screenshot shows a web form titled "Schedule Wizard - Record All Calls For An Agent During A Time Range" with a "Save" button in the top right corner. The form contains the following fields and controls:

- Name :** A text input field.
- Description :** A text input field.
- Agent (Agent Number) :** A text input field.
- Never Expire :** A checkbox.
- Start Date :** A date selector showing "5/22/2011" with a calendar icon.
- End Date :** A date selector showing "5/22/2011" with a calendar icon.

### Create a Time-Based Agent Schedule

To create a time-based agent schedule:

1. Click the **Administration** tab and expand **Scheduling** in the left navigation menu.
2. Click **Create Schedule**.
3. Click **Record All Calls For An Agent During A Time Range**.
4. Enter a **Name** for the schedule and a **Description** if desired.
5. Enter the **Phone ID** to be recorded in the **Agent Number** field.
6. Select the **Never Expire** check box if the schedule should remain in effect indefinitely, or use the date selectors to enter **Start Date** and **End Date**.
7. Click **Save**.

## About Number-of-Calls Based Agent Schedules

A call-based schedule records a specified number of calls for an agent, optionally within a given date range. Schedules created using this procedure use default values for Retention Days and other settings. For details, see [Custom Schedule Criteria Fields](#).

The screenshot shows a web form titled "Schedule Wizard - Record The Next 'N' Calls For An Agent". The form includes the following fields and controls:

- Name :** [Text input field]
- Description :** [Text input field]
- Agent (Agent Number) :** [Text input field]
- Number of calls :** [Text input field]
- Never Expire :**
- Start Date :** [Date selector showing 5/22/2011]
- End Date :** [Date selector showing 5/22/2011]
- Save** button

## Create a Number-of-Calls Based Agent Schedule

To create an agent schedule based on a specific number of calls:

1. Click the **Administration** tab and expand **Scheduling** in the left navigation menu.
2. Click **Create Schedule**.
3. Click **Record the Next *n* Calls for an Agent**.
4. Enter a **Name** for the schedule and a **Description** if desired.
5. Enter the **Phone ID** to be recorded in the **Agent Number** field.
6. Enter the **Number of calls** to be recorded.
7. Select the **Never Expire** check box if the schedule should remain in effect indefinitely, or use the date selectors to enter **Start Date** and **End Date**.
8. Click **Save**.

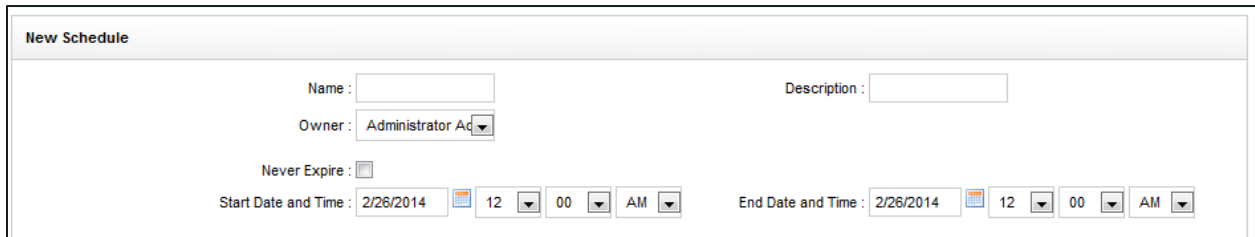
## Scheduling

### About Custom Agent Schedules

Custom schedules provide greater flexibility to meet your organization's needs. All custom schedule types can incorporate random probability if desired. In other words, when a call is delivered and the schedule is at or above its target percentage, the system generates a random number for the call, between 0 and 100. If the random number is equal to or less than the **Random Probability** value, the call is recorded. Otherwise, the call is skipped.

#### Custom Schedule Criteria Fields

The following fields can be used to create custom schedules. Many of these fields are also used in time-based and call-based schedules as well.



The screenshot shows a 'New Schedule' form with the following fields and values:

- Name: [Empty text box]
- Description: [Empty text box]
- Owner: Administrator Ad (dropdown menu)
- Never Expire:
- Start Date and Time: 2/26/2014 (calendar icon), 12 (hour dropdown), 00 (minute dropdown), AM (period dropdown)
- End Date and Time: 2/26/2014 (calendar icon), 12 (hour dropdown), 00 (minute dropdown), AM (period dropdown)

- **Name:** This field is required. Names do not have to be unique, as each schedule is given an internal ID number by Discover.
- **Description:** This field is optional. It allows you to provide additional information about the schedule in the Schedule List.
- **Owner:** This field is required. From the drop-down list, select the person who should be contacted regarding changes to the schedule. Select Administrator if no specific owner exists.
- **Never Expire:** This setting is optional. Select this check box if the schedule should remain in effect until the specified number of calls is reached.
- **Start/End Date/Time:** This setting is optional. Use the date and time selectors if the schedule should only be effective within a range of dates.

- **Type:** This setting is required. Other fields in this section will change depending on the type of schedule you choose. Select from the following options:
  - **Set Number:** This schedule type records a set number of calls matching the business rules you apply. For example, if you need to record the next five calls for a specific phone extension, you would use this schedule type. These fields display for this schedule type:
    - **Minutes Between:** If set, the schedule will prevent another recording from starting if the previous call was recorded within the value set here.
    - **Target Calls:** The total number of calls to be recorded by this schedule.
    - **Calls Between:** If set, the schedule will prevent another recording from starting if the previous call was recorded within the value set here.
    - **Random Probability**
  - **Percentage:** This schedule type gives you the flexibility to create randomized schedules as well as schedules for complete call logging. Enter the percentage of calls you would like to record. Use a percentage below 100% for randomized recording for quality assurance. Set a schedule to 100% for complete call logging. These fields display for this schedule type:
    - **Target Percent:** The percentage of calls to be recorded out of the total number delivered.
    - **Random Probability**
  - **API Initiated:** This schedule type only runs if the call delivered was triggered by a third-party application via the Uptivity Discover API. This is useful for defining different rules for these calls vs. internally-generated calls via CTI or passive methods. These fields display for this schedule type:
    - **Target Percent:** The percentage of calls to be recorded out of the total number delivered to an agent.
    - **Random Probability**
  - **On-Demand.** This schedule type only runs if a delivered call was triggered via the Discover On-Demand Client. These fields display for this schedule type:

## Scheduling

- **Target Percent:** This value is ignored. The call start/stop from the On-Demand client determines recording.
- **Random Probability**
- **Agent Percentage:** This schedule type allows you to enter a percentage of calls (1-100) you would like to record for every agent. This percentage will apply to each agent, so if you set the percentage to 50%, then 50% of each agent's calls will be recorded. These fields display for this schedule type:
  - **Days:** Select the check boxes for days of the week this schedule will be in effect.
  - **Target Percent:** The percentage of calls to be recorded out of the total number delivered to an agent.
  - **Random Probability**

Direction : both	Priority : 50
Min Record Length (Sec) : 10	Max Record Silence(Sec) : 600
Max Record Length (Sec) : 6000	Retention Days : 365
Screen capture wrap length (Sec) : 0	Archive Action : Purge
Stop screen capture wrap on call start : No	
Audio Capture : Yes	Screen Capture : No
Speech Analytics : Yes	
Disk Location : C:\Recordings	Comparison : AND
Blackout Remote Audio : <input type="checkbox"/>	

- **Direction:** This setting is optional. If the data is available, you can tell Discover to record only inbound calls, only outbound calls, or both.
- **Priority:** This setting is optional. You can give schedules a priority rating from 1 (lowest) to 100 (highest). If a call is delivered that matches multiple schedules, the schedule with the highest priority is used. If all matching schedules have equal priority, then the schedule with the oldest creation date is used.
- **Min Record Length (sec):** This setting is optional. It specifies the minimum length, in seconds, for records matching that schedule. You can use this setting to avoid recording hang-ups.
- **Max Record Length (sec):** This setting is optional. It specifies the maximum length, in seconds, for records matching that schedule. Longer calls require more disk space, so some organizations prefer to cap the recording length to prevent long calls from depleting system resources.



- **Max Record Silence (sec):** This setting is optional. It specifies the maximum length, in seconds, for silence in the call before recording is automatically stopped.
- **Screen Capture Wrap Length:** This setting is optional and only applies if your organization uses Uptivity Discover Screen Recording. It specifies the duration (in seconds) to keep recording an agent's screen after a call has ended.
- **Stop Screen Capture Wrap on Call Start:** This setting is optional and only applies if your organization uses Uptivity Discover Screen Recording. You can choose whether screen recording for agents in wrap time should stop when a new call is detected, or should continue until the Screen Capture Wrap Length time has been reached. If set to Yes, a new call or chat will trigger the end of the current capture and initiate a new one, even if the wrap time limit has not yet been reached.
- **Retention Days:** This setting is optional. It specifies the number of days you would like calls matching that schedule to be saved before being purged (deleted) or archived.
- **Archive Action:** This setting is optional. You can select from a drop-down list of available Archive Actions. The default action is "Purge," which means that the system will purge records when they reach the specified number of retention days. For details, see [About Archive Actions](#).

**Note:** Retention Days and Archive Actions are applied when the call is recorded. Changing this value in a schedule only applies to calls made **after** applying the schedule change, not to calls that have already been recorded.
- **Audio Capture:** This setting is optional. If set to Yes, audio/voice will be captured for this record if available.
- **Screen Capture:** This setting is optional and only applies if your organization uses Uptivity Discover Screen Recording. If set to Yes, screen activity will be captured for this record if available.
- **Speech Analytics:** This setting is optional and only applies if your organization uses Uptivity Speech Analytics. If set to Yes, the audio recording will be processed by Uptivity Speech Analytics.
- **Disk Location:** This setting specifies the location (UNC path or local disk) to which recorded audio/video files for this schedule will be written.
- **Blackout Remote Audio:** This setting is optional. Select the checkbox if remote audio should be subject to black out.
- **Comparison:** Select **AND** or **OR** to define schedule requirements using simple business rules. Select **Expression** to engage advanced business logic using a

## Scheduling

free-form expression. For more information, see [Schedule Requirements: Simple Business Rules](#) or [Schedule Expression: Advanced Business Rules](#).

### Schedule Requirements: Simple Business Rules

	Value Type	Comparison	Value	Case Sensitive
1				<input type="checkbox"/>
2				<input type="checkbox"/>
3				<input type="checkbox"/>
4				<input type="checkbox"/>
5				<input type="checkbox"/>

You can create simple schedules by matching up to five variables within a schedule, using the **Comparison** type selected previously. When you use the **AND** comparison, each rule set in the editor must match for a call to begin recording. When you use the **OR** comparison, only one of the rules must match the call in order to start a recording. If no schedule requirements are entered and the **Comparison** is **AND** or **OR**, the schedule can apply to all calls depending on other factors.

The Value Type variables include:

- **DeviceID:** The physical device on which the call was taken.
- **Agent ID:** The agent login or phone number.
- **ACD Group**
- **ACD Gate:** May also be called VDN, Queue, Application, etc., depending on your PBX.
- **Number Called:** The number on which the call came in (i.e. DNIS).
- **CallerID**
- **User Fields:** These are the fifteen (15) fields that contain data relevant to your organization. For further information see [About Terminology](#) and/or the *Uptivity Discover WFO API Manual*.

For each of these variables, the system can use the following comparison operators:

- Equal to or Not equal to
- Less than (<) or Greater than (>)
- Starts with or Ends with
- Contains or Does not contain

For non-numeric values, you can also perform a case sensitive match.

## Schedule Expression: Advanced Business Rules

When you select the **Expression** value from the **Comparison** setting, you can enter a free form expression (64,000 characters max) for more complicated decision-making. If **Comparison** is set to **Expression**, you must enter an expression or **no** calls will record.

Variables used in schedule expressions must reference the database field name, which can differ from the label for that field in the Web Portal. You can use any of these variables in creating an expression:

- **DeviceID:** The voice port/extension that receives or places the call.
- **Devicealias:** The ACD number for the agent who receives or places the call.
- **SGroup:** For inbound-routed ACD calls, this is the Hunt Group or Skill value (typically labeled **Group** in the Web Portal).
- **Gate:** For inbound-routed ACD calls, this is the ACD Queue or Group to which the call was delivered.
- **ANI:** The calling party for the call (i.e. CallerID).
- **DNIS:** The called party for the call.
- **User1 - User15:** These are the fifteen (15) fields that contain data relevant to your organization. For more information see [About Terminology](#) and/or the *Uptivity Discover WFO API Manual*.
- **CallID:** The Call ID assigned by the PBX/ACD to identify the call.
- **Calldirection:** Inbound or Outbound.
- **Callinstancediscriminator:** An internal variable assigned to the call by the Discover system for tracking purposes.
- **Initiatedby:** Identifies how the recording was started. Possible values are: cti, agent, supervisor, api, timed, apichat, agentchat.
- **Month:** Numeric value for the month (use leading zero for months 01- 09).
- **Day:** The numeric day of the month (use leading zero for months 01- 09).
- **Year:** The 4 digit year.
- **Time:** Time of day, formatted as 24-hour time, 00:00 to 23:59. When entering data in the Schedule Expression field, put single standard quotes (not "smart" or curly quotes) around the time values. For example, for time between 6 A.M. and 7 P.M., the expression would read: **time > '06:00' || time < '19:00'**.
- **Weekday:** Possible values are: mon, tue, wed, thu, fri, sat, sun.

## Scheduling

- **Date:** Format as yyyy-mm-dd.
- **Pvalue:** A random number from 0 to 99 that can be used for cases where a certain percentage must be met.

These operators can be used against the variables:

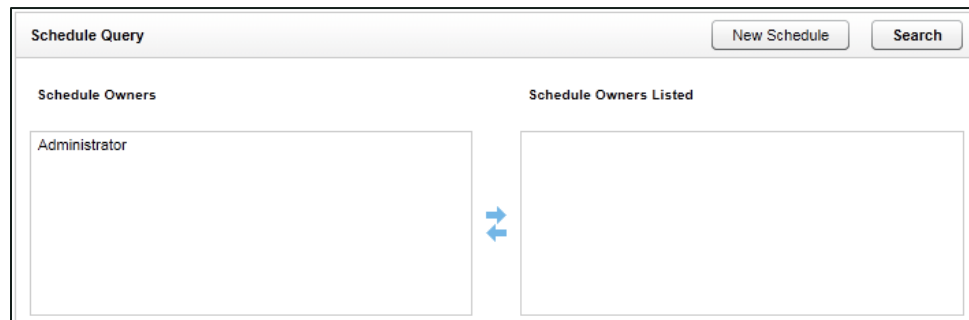
==	Equal to
!=	Not equal to
>	Greater than
<	Less than
>=	Greater than or equal to
<=	Less than or equal to
=~	Match a Regular Expression (Perl Formatted)
!~=	Does not match a Regular Expression (Perl Formatted)
'	Both single and double quotes can be used to signify strings in expressions.
c'	Prefixing quotes with a c indicates case-insensitive matching. This applies to normal string comparisons, IN, !IN, =~ and !=~ operators.
IN	Test if an identifier is in a bar separated list of values.
!IN	Test if an identifier is not in a bar separated list of values.
&&	Boolean AND operator.
	Boolean OR operator.
()	Parenthesis used for grouping and precedence.

**Note:** Boolean && operators are evaluated before || operators. Put parentheses around groups to override the default precedence.

## Create a Custom Agent Schedule

1. Click the **Administration** tab and expand **Scheduling** in the left navigation menu.
2. Click **Create Schedule** and then click **Create a Custom Schedule (Advanced)**.
3. Enter information in the desired fields (see [Custom Schedule Criteria Fields](#)).
4. Enter any desired schedule requirements and then click **Save Schedule**. For related information, see [Schedule Requirements: Simple Business Rules](#) and/or [Schedule Expression: Advanced Business Rules](#).

## Find a Schedule





















To search for a schedule:

1. Click the **Administration** tab and expand **Scheduling** in the left navigation menu.
2. Click **Find Schedule**.
3. To narrow your search to schedules created by or assigned to specific users, move users from **Schedule Owners** to **Schedule Owners Listed**; move users from **Schedule Owners Listed** to **Schedule Owners** to exclude them from your search. To retrieve all schedules, do not select an owner.
4. Click **Search** to display the Schedule list.

## Scheduling

### About the Schedule List


	ID	Name	Description	Complete	Created	Owner
  	1	RecordAll	Record 100% of calls	N/A	2/27/2014	Administrator, Administrator
  	2	OnDemand	Record supervisory calls	N/A	2/27/2014	Administrator, Administrator
  	3	NoScreenCap	No Screen Cap	100%	4/30/2012	Administrator, Administrator
  	4	Sales	Sales and marketing dept calls	100%	2/27/2014	Administrator, Administrator
  	6	ScreenCapWrap	Post-Call Processing Review	100%	2/27/2014	Administrator, Administrator
  	7	LegendsSchedule	Team schedule	N/A	2/27/2014	George, Gina

The Schedule List provides the following information about each schedule:


- **ID:** The unique internal identifier Discover uses for the schedule.
- **Name**
- **Description**
- **Complete:** If a schedule is set to expire, this value compares start date, end date, and today's date to get a percentage of completion. If a schedule is set to record a number of calls, the percentage of recordings completed is displayed. Schedules that do not expire are marked N/A.
- **Created:** The date the schedule was created.
- **Owner**

Several routine tasks can be performed from the Schedule List page.


To edit a schedule:

- Click the Edit  icon. Changes made to a schedule do not affect calls that have already been recorded.

To copy the rules from a schedule into a new schedule:

- Click the Copy  icon.

To delete a schedule:

- Click the Delete  icon. Previously recorded calls are not affected when you delete a schedule.

## About Timed Schedules

Timed schedules are used to record in environments where there is no phone event to trigger recordings, such as with chat or email agents. Timed schedules let you record an agent's desktop for a specified time period, dividing the recordings up incrementally according to your organizational needs. For example, recording could be scheduled from 8 AM to 5 PM, and each record could last 15 minutes. The desktop will be recorded provided the workstation is powered on and the Screen Recording Client is running, whether the agent is actively using the workstation or not.

**Note:** This feature will not work properly if you use the Workstations List. Unique usernames are required.





### Licensing for Timed Schedules

The ability to use timed schedules is licensed separately from voice and screen recording. Consult your Uptivity Discover Account Manager for more information.

### About the Timed Schedule List

To access Timed Schedules:

- Click the **Administration** tab, expand **Scheduling** in the left navigation menu, and then click **Timed Schedule**. Click a schedule to see additional information about it.

Timed Schedules						New Schedule
ID	Name	Start Time	End Time	Date Created		
  1	Timed Schedule 1	12:00 AM	12:00 AM	5/22/2011		
  2	Timed Schedule 2	12:00 AM	12:00 AM	5/22/2011		


The **Timed Schedules** list displays the following information for each schedule:

- **ID:** The unique internal identifier Discover uses for the schedule.
- **Name**
- **Start/End Time:** The time of day the schedule will begin and end recordings.
- **Date Created**


## Scheduling

Several routine tasks can be performed from the Timed Schedules list.

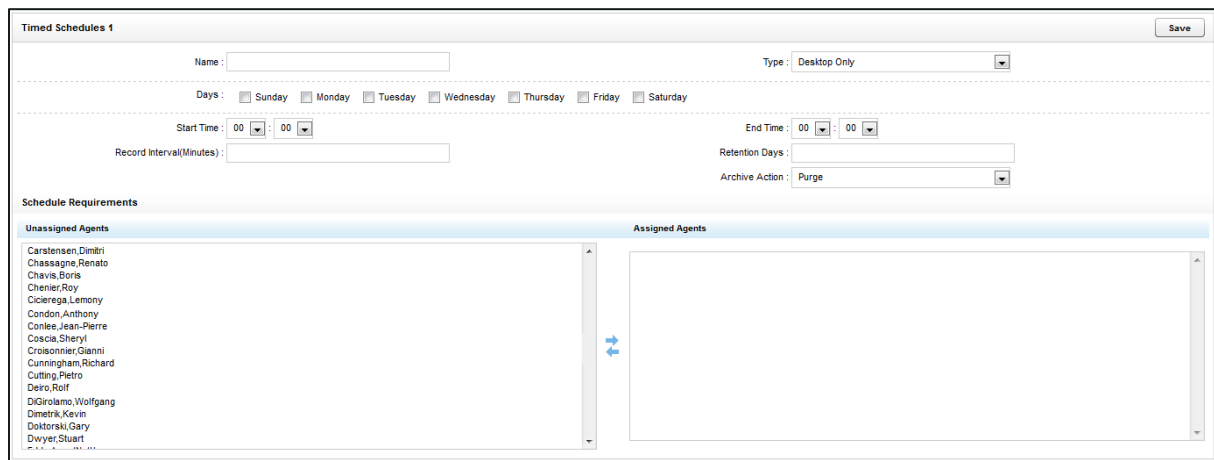
To edit a schedule:

- Click the Edit  icon. Changes made to a schedule do not affect calls that have already been recorded.

To delete a schedule:

- Click the Delete  icon. Previously recorded calls are not affected when you delete a schedule.

## Create a Timed Schedule



To create a Timed Schedule:

1. Click the **Administration** tab and expand **Scheduling** in the left navigation menu.
2. Click **Timed Schedules** and then click **New Schedule**.
3. Enter a **Name** for the schedule.
4. Select **Desktop Only** from the **Type** drop-down list.
5. Select the check boxes for the **Days** of the week the schedule will be in effect.
6. Enter the length for each individual recording in **Record Interval (Minutes)**.
7. Enter the number of days for which recordings should be saved in **Retention Days**.



8. Select the desired **Archive Action** from the drop-down list. For details, see [About Archive Actions](#).
9. Move agents from **Unassigned Agents** to **Assigned Agents** to assign them to the schedule; move agents from **Unassigned Agents** to **Assigned Agents** to remove the schedule assignment.
10. Click **Save**.

# Tools

## About the Service Manager

The **Service Manager** is used to centrally manage all Discover application services located on different machines. In order for the Service Manager to load and control application services, the [About CometDaemon](#) and Service Manager modules must be installed, configured, and running on each Discover system server, also called a Server Node. Otherwise, the Service Manager will show that it is not connected to that Server Node, (for example, the Analytics Server II in the image below).

Service Manager configuration is initially performed at the time your system is installed. Changes may be required later if services are added or moved to a different physical or virtual server. This level of change should only be completed by or under the supervision of Uptivity Discover Support. This section will help you understand the Service Manager display and learn how to start/stop services through the Service Manager.

The screenshot shows the Service Manager interface. At the top, there are buttons for 'Check All', 'Uncheck All', 'Start Selected', 'Stop Selected', and 'Remove Selected Applications'. Below these are two server nodes listed:

- Server: Analytics Server II - Not Connected** (IP: 172.186.325.4) with Edit and Remove buttons.
- Server: Main Recorder** (IP: 192.168.109.128) with Edit and Remove buttons.

The 'Main Recorder' server is expanded to show a table of services:

Application	Status	Last Started	CPU %	Memory	Auto-Restart	Stop	Edit	Remove
CallCopyArchiverService	Running	3/28/2012 2:25 PM	0%	168MB	Yes	Stop	Edit	Remove
CC_APIServer.exe	Running	3/28/2012 2:24 PM	0%	30MB	Yes	Stop	Edit	Remove
cc_cticore.exe	Running	3/28/2012 2:24 PM	0%	46MB	Yes	Stop	Edit	Remove
cc_insightServer.exe	Running	3/28/2012 2:25 PM	0%	25MB	Yes	Stop	Edit	Remove
cc_loggerService.exe	Running	3/28/2012 2:24 PM	3%	45MB	Yes	Stop	Edit	Remove
cc_ondemandServer.exe	Running	3/28/2012 2:24 PM	0%	23MB	Yes	Stop	Edit	Remove
CC_ScreenCapServer.exe	Running	3/28/2012 2:24 PM	0%	21MB	Yes	Stop	Edit	Remove
cc_transcoder.exe	Running	3/28/2012 2:25 PM	0%	27MB	Yes	Stop	Edit	Remove
cc_webMediaServer.exe	Running	3/28/2012 2:25 PM	0%	44MB	Yes	Stop	Edit	Remove

At the bottom of the table, there is an 'Add Application' button.

The Service Manager displays the Server Node name and IP address. Expand a Server Node to see data for each service:

- **Application:** The name of the Discover service. This value is case sensitive and is usually the name of the .exe file in Windows Explorer. Some legacy services may have a different name. You can verify the name by viewing the service's properties in Windows.
- **Status:** Indicates whether the service is **Running**, **Stopped**, or **Unknown**.

- **Last Started:** Indicates the time and date the service was last started.
- **CPU %:** Indicates the percentage of CPU being used by the service. This information is useful for determining why a service or server is running slowly.
- **Memory:** Specifies the service's current usage of server memory. Services like the Transcoder and Archiver use more memory as they process files.
- **Auto-Restart:** If set to 'Yes', Service Manager will attempt to restart the service if it stops on the host machine due to a non-critical error. The service cannot be stopped on the Windows machine if it is set to Auto-Restart. If the host server is rebooted, the service should restart because it was registered as a service during the installation process.

## Start/Stop Discover Services

To stop a running service:

- Click the **Stop** button next to the service you wish to shut down. The service status will switch to **StopPending**. Once the service is stopped, the status will display as **Stopped** and the **Start** button will be activated.

To start a stopped service:

- Click the **Start** button on the right side of the service listing. The service status will switch to **StartPending**. Once the service is started, the status will display as **Running** and the **Stop** button will be activated.

To start or stop multiple services at once:

1. Select the check boxes for all of the services you wish to control from the Service Manager list.

Alternative: Use the **Check All** or **Uncheck All** buttons to quickly select or de-select all services.

2. Click the **Start Selected**, **Stop Selected**, or **Remove Selected Applications** buttons to perform the specified action on all of the selected services.

## About the Archiver Console

Archiver								
Archive Actions			<a href="#">Refresh List</a>	<a href="#">Refresh Settings</a>	<a href="#">Run File Purge</a>	<a href="#">Delete Empty Directories</a>		
ID	Name	Run Now	Storage Type	Location	Restriction	Archive Type	Next Archive	Next Archive Days
1	Two Year Retention	<a href="#">Run Now</a>	Disk	C:\Archive	Archive Everthing	Normal	Purge	730
2	Standard Archive	<a href="#">Run Now</a>	Disk	c:\Standard Archive	Archive Audio Only	Normal	Purge	365
3	Back Up to NAS	<a href="#">Run Now</a>	SMB	\nas-server\archive	Archive Everthing	Normal	Purge	365
Optical Drives								
<a href="#">Load Archived Files</a>			<a href="#">Refresh Disk Status</a>	<a href="#">Update Drive Letter</a>				
Drive	Model	Erase Disk	Volume	Status	Media			
D	VMware IDE CDR10	<a href="#">Erase Disk</a>		Error Reading Disc	No media detected			
Output - File Archiving Completed.								
10:38:54 AM - File Archiving Completed.								

The Archiver Console provides manual control for many module functions. To access the console:

- Browse to the **Administration** tab, expand **Tools** in the left navigation menu, and click **Archiver Console**.

The following tasks can be accomplished with the Archiver Console:

- **Refresh List:** Forces a refresh of the list of active Archive Actions from the database. The list automatically refreshes every 5 minutes.
- **Refresh Settings:** Manually reloads the Archiver settings page options. For more information on configuring automatic refresh of these settings, see [About the Archiver](#).
- **Run File Purge:** Forces immediate processing of the File Purge queue.
- **Delete Empty Directories:** Immediately runs a job to clear out any empty folders that are managed by the Archiver.
- **Run Now:** Forces any listed Archive Action to run immediately.
- **Load Archived Files:** Causes any queued calls to be burned immediately to disk. Once this operation occurs, the disk must be replaced with a new one, as only one archive job can be executed per disk.
- **Refresh Disk Status:** Refreshes the status of disks in all drives.
- **Update Drive Letter:** Scans the server for any added/removed DVD drives and updates the Drive List.

The results of any commands issued will be displayed in the Output window.

# Recorder Settings

Recorder Settings control Discover Call Recording, which in turn uses three key features to record audio: a CTI Core, a [Transcoder](#), and one or more [Voice Boards](#). Depending on your system architecture, you may have more than one CTI Core and Transcoder.

## About CTI Cores

The CTI Core component integrates with your PBX/ACD and makes call recording decisions based on customer-defined Schedules. This component tells Discover **when** to record. At least one CTI Core is required for most integrations.

Discover supports multiple Cores, both on an individual Discover server and within a multi-server Discover system. Different Cores may be used for different integrations, to provide for failover recording as part of continuity and recovery planning, or for implementations with different geographic sites. The Core topology is created during the discovery process by the Uptivity Discover Sales Engineer.

The CTI Cores List displays all configured CTI Core modules in the system. A CTI Core is the module that provides the PBX/ACD integration, and makes call recording decisions based on [Scheduling](#) business logic. The CTI Core is also responsible for recording the raw audio files used for playback.

The configuration of a CTI Core is dependent on your ACD/PBX. Contact the Uptivity Discover Support team if you need a copy of the customer's guide to your integration.

CTI Cores can be viewed in the Web Portal, but should only be edited or removed by Uptivity Discover Installation or Support. If Core settings must be changed, and you are doing so with the Support team's direction, only open one Core at a time for editing. Do not open multiple Cores in separate browser tabs or, when saving one Core, another Core's settings may be overwritten.

## About Buddy Cores

Buddy Cores are used in a method of high availability and redundancy where only one Core is recording at a given time, as opposed to a system where a redundant recorder is always recording. Since only one Core is recording at a time, it can save space and resources. For instance, integrations using Avaya TSAPI/DMCC would require only one set of DMCC stations since the Buddy Cores will share the stations.

## Recorder Settings

Buddy Cores should always run on different machines (including VM clusters) to avoid having a single point of failure. There are two ways to configure Buddy Cores: Primary/Secondary and Active/Inactive.

### About Primary/Secondary Buddy Cores

In Primary/Secondary topology, the secondary Core will not record unless instructed to by the primary.

When the Primary Core starts up, it waits a configurable amount of time for the Secondary Core to start. If a timeout occurs, the Primary Core starts recording. When connection is made to the Secondary Core, the Secondary Core informs the Primary of its recording state (Recording, NotRecording, or Deciding). If the Secondary Core's state is NotRecording or Deciding, the Primary Core starts recording. If the state is Recording, the Primary Core goes into warm standby. All modules configured for warm standby start, but no recording occurs. If the Secondary Core drops off while the Primary is in standby, the primary Core starts recording.

The Secondary Core's function is different. When it starts up, it immediately goes into warm standby mode. When a connection is established to the Primary Core and then fails, the secondary Core starts recording. If no connection is ever made to the Primary Core, the secondary Core will wait indefinitely in warm standby mode.







### About Active/Inactive Buddy Cores

In Active/Inactive topology, the secondary Core will record unless instructed *not* to by the primary.

Both Cores function the way the Primary Core does as described in Primary/Secondary. If both Cores start up at the same time and neither is recording (both are in the Deciding state), the Core that would be considered the Primary Core (i.e., the Core not configured with a broadcast receiver) from above will take precedence and start recording, and the other Core goes into warm standby mode. If both Cores start up and cannot connect to one another, then they will both start recording.

Not all integrations are suitable for Buddy Cores. If you are interested in exploring this system architecture, contact Uptivity Discover Sales Engineering.

## Custom Lookups

Custom Lookup List				Import Lookup	Add New Lookup
Lookup Value	Match Value		Lookup Key		
1234	Customer X		Account		
520123	Customer A		DNIS		
7501	Special Customer		DNIS		


Pages : 1      Go To Page : 1 of 1      [Go](#)

The **Custom Lookup** feature lets you add a value to a call record based on the record's ANI (i.e. Caller ID) or DNIS (dialed number). For example, if calls for one customer always go to a 1-800/DNIS, this feature can add the customer name to every call record for that DNIS, making it easier to search for and report on that customer.



Custom scripting is required but once the script is in place, you can edit entries as needed. Contact Uptivity Discover Support for scripting assistance. Editing or deleting the custom lookup does not affect existing call records.

### Configure Custom Lookups

To add a custom lookup:


1. Click the **Administration** tab and expand **Recorder Settings** in the left navigation menu.
2. Click **Custom Lookup** and then click **Add New Lookup**.
3. In the **Lookup Value** field, enter the ANI or DNIS value for calls in question. Only one ANI or DNIS can be entered. The system will interpret 123,456 or 123 456 as single search values.
4. In the **Match Value** field, enter the replacement value to be added to the call record.
5. For the **Lookup Key**, select either DNIS or Account if your Lookup Value is based on ANI.
6. Click the Save  icon.

To edit a custom lookup:

1. Click the **Administration** tab and expand **Recorder Settings** in the left navigation menu.
2. Click **Custom Lookup** and then click the Edit  icon for the desired lookup.
3. Edit the desired values and then click the Save  icon.

## Recorder Settings

To delete a custom lookup:

1. Click the **Administration** tab and expand **Recorder Settings** in the left navigation menu.
2. Click **Custom Lookup** and then click the Delete  icon for the desired lookup.

### Import Multiple Custom Lookup Values

Multiple custom lookup values can be imported at once using a comma separated values (CSV) file. Each entry must be added to the file using this format: Lookup Value, Match Value, Lookup Key.





To import a file of custom lookup values:

1. Click the **Administration** tab and expand **Recorder Settings** in the left navigation menu.
2. Click **Custom Lookup** and then click **Import Lookup**.
3. Click **Browse**, locate the CSV file and select it.
4. Click **Upload File**.
5. Click **Import Now**.

During the import process, the system verifies that the entries are formatted correctly and displays an error message if they are not. You will need to correct the entries and repeat the import procedure.



## IP Phones

IP Phone List			Import	Add	Save
Extension	IP Address				
1234	10.100.8.20				
5555	10.100.8.22				



The **IP Phone List** allows you to register an extension with an IP Address manually. This list is only used in passive VoIP recording configurations where a phone cannot be automatically registered to the desired extension number. In most configurations, the use of this list is not necessary.

### Configure IP Phone Settings


To add a phone to the IP Phones List:

1. Click the **Administration** tab and expand **Recorder Settings** in the left navigation menu.
2. Click **IP Phones** and then click **Add**.
3. Enter the **Extension** and **IP Address**.
4. Click **Save**.

To edit an entry in the IP Phone List:

1. Click the **Administration** tab and expand **Recorder Settings** in the left navigation menu.
2. Click **IP Phones**.
3. Click the Edit  icon for the desired entry.
4. Change the extension and/or IP Address and then click the Save  icon.

To delete an entry from the IP Phone List:

1. Click the **Administration** tab and expand **Recorder Settings** in the left navigation menu.
2. Click **IP Phones** and then click the Delete  icon.

### Import Multiple IP Phones

Multiple IP phones can be imported at once using a comma separated values file (CSV). Each entry must be added to the file using this format: Extension, IP Address.

To import a file of IP phone information:

1. Click the **Administration** tab and expand **Recorder Settings** in the left navigation menu.
2. Click **IP Phones** and then click **Import**.
3. Click **Browse**, locate the CSV file and select it.
4. Click **Upload File**.
5. Review the preview of your data as displayed below **Perform Import**.
6. Click **Import Now**.

### On-Demand

These settings are available only if the Discover On-Demand module has been purchased. The On-Demand module is a client/server application that allows users to control recording of their calls from a desktop button. It also enables users to manually add data to the Discover call record. See the *Uptivity Discover On-Demand User Guide* for more information.

### Transcoder

The Discover **Transcoder** module converts raw audio files recorded by the system into compressed, .wav formatted audio files that are optimized for storage and playback retrieval. Transcoder module(s) configuration is initially done by the Uptivity Discover Installation team. This section provides you with a reference for the various Transcoder settings. However, Transcoder changes can have serious repercussions on recording and should be performed by or under the supervision of Uptivity Discover Support.

## Transcoder Settings

Each Transcoder has these settings:

- **Identity:** Discover-generated integer value used as an internal identifier. In distributed transcoding environments, this ID is used in the corresponding Transcoder module INI file.
- **Name:** Meaningful name to aid you in identifying and referencing the specific Transcoder instance.
- **Max Retries:** Number of times the module will attempt to process a file before it is considered unreadable. Value is stored in the Transcoder table of the Discover database. Increasing this value will not cause the Transcoder to retry files that have already reached the maximum retries.
- **Minutes between Retries:** Number of minutes to wait to retry a failed transcoding operation.
- **Number of Threads:** Number of concurrent transcoding sessions. Raising this value may increase Transcoder module performance, but can cause performance issues with other modules if the system cannot process more concurrent threads in parallel. Default number of sessions is five (5).
- **Priority:** System CPU priority assigned to Transcoding processing threads. Increasing this value can increase performance, but may degrade any other components on the same server. Possible settings are provided in a drop-down list; the default is **Low**.
- **Temp Directory:** Local directory where temporary conversion files are stored. Final file is stored with the original CCA file. For related information, see [Common File Types](#).
- **Create CCP File:** Creates a custom graphical representation of the audio waveform from a recorded call and stores it as a CCP file along with the audio file. When enabled, results in faster playback times as the waveform will not need to be recomputed for each playback.
- **CCP Interval:** Time interval (in milliseconds) between waveform data points in the graphical display. Increasing intervals can improve performance, but will create a less precise waveform display. Possible settings are provided in a drop-down list.
- **Store Original File Size in Field:** Inserts original file size of a VoIP recording in a selected user-defined field. Useful for diagnosing and troubleshooting network issues. Possible settings are provided in a drop-down list.

## Recorder Settings

- **Delay (minutes):** Delay between conversion attempts for audio files. Increasing this value may be needed for systems under heavy load, but causes a delay in making the recording available for. May also need increased to two to three minutes if Screen Recording and Desktop Analytics are used with call recording. Screen Recording and Desktop Analytics applications must complete and update their files in order for the Transcoder to process both the audio and video. If the Transcoder starts processing the audio file before the video files are complete, video blackouts may not appear on the processed file.
- **Format:** Audio format for storing audio. The following format choices are provided in a drop-down list:
- **CSA:** (~1KB/s) Compresses to smaller files. Highest quality of all available formats. Requires CSA format license from Uptivity for use. Files cannot be played in standard media players.
- **GSM610:** (~1.7KB/s) Compresses to smaller file, but can have lower playback quality. Can be played in standard media player.
- **VOX6K:** (~2.9KB/s) High-quality audio format, but audio files are 1.8 times larger than GSM.
- **VOX8K:** (~4KB/s) High-quality audio format but audio files are 2.5 times larger than GSM.
- **CSASTEREO:** (~2KB/s) Stereo version of CSA format. Creates files comparable in size to GSM, but allows additional per-channel post-processing options (per channel volume level and VAD). Requires CSA format license from Uptivity for use. Files cannot be played in standard media players.
- **Keep Days:** Value in days to keep original (raw) audio files after transcoding. Allows files to be recovered if there are errors in the transcoding process, but requires additional disk space to store the original files. Entering a value of '-1' will prevent the original file from being automatically deleted.
- **Create Analytics:** When enabled, the system creates an additional very high-quality stereo PCM .wav audio file to be used for speech analytics processing. Requires optional Uptivity Speech Analytics module for processing.
- **Analytics Keep Days:** Value in days to keep stereo (analytics) audio files after they have been created. Allows files to be stored for processing by a speech analytics engine, but requires additional disk space to store the stereo files. Entering a value of '-1' will prevent the original file from being automatically deleted.

- **Normalize:** Enables audio normalization, equalizing volume levels between PBX/Customer side and extension/agent side of a recorded call. This setting should never be enabled when Ai-Logix cards are used for audio acquisition.
- **Sample Rate (ms):** Sample rate passed to the conversion module. Higher rates usually result in higher quality audio files, but cause audio files to use more disk space in storage. Possible settings are provided in a drop-down list.
- **Look for Code:** Record codes reserved for this specific Transcoder. If the CTI Core setting **Transcode by Board** is enabled, each Voice Board in the Core has its own identifier (voice board ID+1, ex. '31' for Voice Board 3).
- **Perform Duplicate Packet Checks:** When enabled, the Transcoder checks for duplicate packets in recordings. Duplicate packets cause the recording to appear to be skipping, and can indicate configuration issues in passive VOIP recording integrations.
- **Purge Record from Transcoder Table After Completion:** When disabled, system keeps a record in the Transcoder queue after it has been successfully processed. Useful for troubleshooting if reprocessing of files may be needed, but over time can cause the Transcoder table to grow significantly and impact the performance of the entire database. Unless you are troubleshooting, should always be enabled.
- **VAD Packet Count Trigger:** Number of RTP packets with audio needed to trigger Voice Activity after a period of silence. Lower setting may avoid choppy calls or calls where agent/customer audio overlaps. Setting to 0 turns this off. Possible settings are provided in a drop-down list.
- **Analytic Storage Path:** Hardcoded UNC or disk path that all Analytic .wav files are written to. Useful if files are being analyzed by a third party product.
  - Note:** If this setting is used, Discover leaves management of the created files to the third party product or destination storage system.
- **Minimum Hold Duration (milliseconds):** Amount of silence before Transcoder inserts a Hold event in a recording.
- **Check Video Valid:** When enabled, system checks to see if a screen recording has at least one valid video frame. If that one frame does not exist, the file is still transcoded, and a record for it is created. But when the user attempts to play the screen recording video, the Web Player displays this message: "Unable to play call: The call does not have audio or video."
- **Minimum Audio Duration (seconds):** For audio recording files shorter than the minimum duration, the Web player displays this message: "Unable to play call: The call does not have audio or video."

## Recorder Settings

- **Enable Silence/Cross-talk Detection:** When disabled, remaining settings are grayed out and Transcoder will not detect silence/cross-talk. Default setting is **Yes**.
- **Cross-talk Threshold:** Gain level from 0.00 baseline that must be met on both channels to trigger cross-talk detection. Default value is 0.01, with a valid range from 0.01 to 1.00.
- **Cross-talk Minimum Duration (milliseconds):** Minimum time that audio must stay above the threshold in order for cross-talk period to be displayed during call playback. Default value is 1000, with a valid range from 1000 to 65535.
- **Silence Threshold:** Gain level from 0.00 baseline that audio needs to stay below in order to trigger silence detection. Default value is 0.01, with a valid range from 0.01 to 1.00.
- **Silence Minimum Duration (milliseconds):** Minimum time that audio must stay below the threshold in order for silence period to be displayed during call playback. Default value is 3000, with a valid range from 1000 to 65535.
- **Fragmentation Prevention (milliseconds):** Prevents momentary noise in audio from fragmenting silence/cross-talk into multiple periods. If two periods are detected within the specified duration, they are combined into a single period. Default value is 2000, with a valid range from 1000 to 65535.





## Voice Boards

As a Discover administrator, you should have a general understanding of Voice Boards and know how to configure individual channels, since you may need to modify these from time to time. However, you should never make any other Voice Board changes unless you are under direct supervision from Uptivity Discover Support. Done incorrectly, Voice Board modifications can have serious negative impact to your system. In addition, altering the hardware configuration of your system may void your warranty.

Voice Boards provide Discover with configuration information specific to your PBX/ACD. For more detailed reference information on Voice Boards and their configuration, refer to the customer integration guide for your system. If you cannot locate your integration guide, contact Uptivity Discover Support to obtain a copy.

Voice boards are licensed components of the Discover software. The software allows for adding an unlimited number of Voice Boards to the system, but will deny usage of any unlicensed components.

## Configure Voice Board Channels

Voice Boards List			
		<input type="button" value="Add Board"/>	<input type="button" value="Clear Boards"/>
<input type="button" value="Save Configuration"/>			
#	Name	Channels	
1	VOIPSNIFFER	25	 
2	CISCODMS	5	 

Channel configuration associates the licensed software channels on the Voice Board with the audio sources that will be recorded. To configure a Channel:

1. Click the **Administration** tab and expand **Recorder Settings** in the left navigation menu.
2. Click **Voice Boards**.
3. Click the **Edit** icon for the Voice Board you wish to configure.
4. Under Channel Configuration, enter the **Number of Channels** to be added (if applicable).
5. Configure the settings for the new channel or reconfigure settings for an existing channel, as desired.
6. Click the **Save** button.

When you are finished, you can click the **Back** button to return to the Voice Boards list, or navigate to another part of the Web Portal. Unless your system is licensed for the Voice Board Reloading feature, you will need to restart the Recorder service (cc\_cticore.exe) after any Voice Board and/or Channel changes. For more information, see [Start/Stop Discover Services](#).

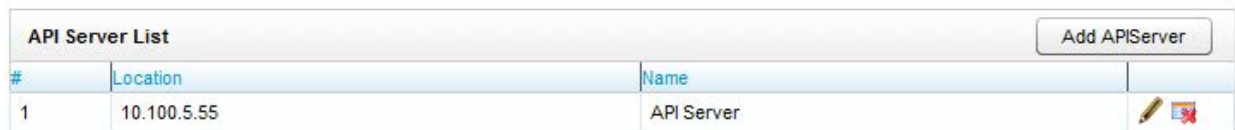
## Channel Configuration Settings



**Channel Configuration** settings will also vary depending on your specific integration, as different integration types support different options. Refer to the customer's guide to your specific PBX/ACD integration for detailed information on channel configuration fields and settings.

# System Settings

System Settings are typically configured during the installation process by the Uptivity Discover Deployment team. This topic is designed to give you a basic understanding of the settings and what they mean for your system. Do not change any System Settings without consulting Uptivity Discover WFO Support.

## About the Uptivity API Service



#	Location	Name	
1	10.100.5.55	API Server	 

The **API Server** module handles connections from any application that uses the Uptivity API service. The API can be used for such tasks as call control, management functions, and event streaming. Uptivity Discover uses the API Server for Live Monitoring and Call Exporting. For more information on Uptivity API Services, see the *Uptivity API Manual*.

The API Server List (shown above) displays the following:

- **#:** Internal identifier generated by Discover for the specific API Server. This identifier is an integer value, and is needed for configuring distributed API environments.
- **Location:** Hostname/IP Address of the server running the API Server.
- **Name:** Meaningful name that can help you distinguish between API Servers in a distributed API environment.

## About Archive Actions

Typically, disks on a local Discover server only have enough space to store audio and video recordings for a short time. By establishing archives, additional drives can be configured so that recordings can be stored indefinitely. Rules governing how long recordings remain in the system are configured during installation. If you need to change rules, or set up new rules, to govern when recordings are purged from your cloud storage, you can do so later by means of **Archive Actions**.

Recordings can be archived to attached disks or to Windows Network File Shares (SMB). Archived recordings are still available for playback, providing that the local disk is attached or the network file system is properly configured and available.



Be aware that if a call is deleted from the server by an Archive Action, any QA Evaluations performed on that call will remain in the database for historical searching and review. However, if a call is manually deleted, QA Evaluations performed on the call are deleted. If there are database entries for duplicate or missing files, the Archiver will continue trying to archive these files unsuccessfully (and logging errors) until the invalid database entries are removed.

*Archive Actions* are established to control archiving for types of calls. For example, Client A requires calls to be retained for one year, while Client B requires calls to be retained for two years. A one-year action and a two-year action can be created to archive the calls by client.

*Schedules* control when and what calls are recorded as well as how many days a recording is retained. Archive Actions are attached to Schedules to control whether recordings are purged once they exceed their retention days. Archive Actions should be configured before you create the Schedule in which they are used.

If a recording belongs to more than one schedule, the Archive Action for the schedule with the highest priority takes precedence. If priorities are equal, the earliest created schedule takes precedence.

Retention Days and Archive Actions are applied when the call is recorded. Changing this value in a Schedule only applies to calls made *after* applying the schedule change, not to calls that have already been recorded.

You will need to communicate archive settings to users so that they understand how long recordings are retained by the system. Schedules should be audited on a monthly basis to ensure all necessary information is being archived.

### About the Archive Actions List

The Archive Action List provides the following information about each Archive Action:

- **Identity:** Internal identifier generated by Discover for the specific Archive Action.
- **Name**
- **Location:** File path used by disk-based Archive Actions or DVD drive letter for DVD-based Archive Actions.
- **Status:** **A** for Active or **I** for Inactive.

## Archive Action Settings

Cancel Save

Name: Sales Dept Archives

Storage Type: Disk

Location: f:\Recordings\Disk

Archive Restriction: Archive Everything

Archive Type: Normal

Status: Active

Next Archive Action: <None>

Days Until Next Archive: 5

Use Schedule: Yes

Start Time: 01 : 00 AM

End Time: 03 : 00 AM

Number of schedules that are set to use this archive action: 4

Number of recordings in archive queue with this archive action: 1686

Name	Description	Owner	Date Created
RecordAll	Record 100% of calls	1	2/27/2014 3:20:50 PM -05:00
OnDemand	Record supervisory calls	1	2/27/2014 3:21:40 PM -05:00
Sales	Sales and marketing dept calls	1	2/27/2014 3:22:44 PM -05:00
ScreenCapWrap	Post-Call Processing Review	1	2/27/2014 3:28:27 PM -05:00

Each Archive Action has a number of configurable settings. The settings displayed change depending on the Storage Type you select. The following settings apply to every Storage Type:

- **Name:** Name of the Archive Action. This name will appear in the list of available **Archive Actions** in **Scheduling** and in the drop-down list for **Next Archive Action**.
- **Archive Restriction:** Specifies whether archived recording files are saved with audio, video (screen recording), and analytics (speech or screen) data, or if only a single component will be archived with the recorded audio. Choose one from the drop-down list:
  - **Archive Everything:** Archives audio, video and analytics data.
  - **Archive Audio Only:** Archives only the audio.
  - **Archive Audio & Analytics Only:** Archives audio and analytics data.
  - **Archive Audio & Video Only:** Archives audio and video data.

- **Archive Type:** Determines how the files will be moved from the original location to the archive location. Choose one from the drop-down list:
  - **Normal:** Files are moved to the archive location and then deleted from the original location. Discover database call records are updated with the new file location. If you want users to have access to the archived file from Discover, the location must be accessible. If the recording was archived to DVD, Discover notifies an administrator to load the disk and also notifies the user when the file is available.
  - **Copy:** Files are copied to the archive location, and files in the original location remain untouched. If files are later purged from the original location, they must be manually restored for Discover to access them.
  - **Backup:** Files are copied to the archive location and the original files are left alone. Call records are copied to a backup table in the Discover database and updated with the address of the backup location. When the original file and call record are purged, the backup call record is moved into the live database, making the file retrievable from the backup location.
- **Status:** Shows whether the action is available for use (Active) or unavailable (Inactive). Does not affect the operation of the action or how it is attached to any recording schedules. Only Active actions appear in the **Next Archive Action** list.
- **Next Archive Action:** Select the next desired action to be taken against the archived data from the drop-down list. If multiple Archive Actions are created, another action can be selected. This allows chaining actions together to move data between multiple archive locations. **Purge** can also be selected to delete data when the next Archive Action is performed. If no changes are to be taken on the files after the Archive Action completes, select **<None>**.
- **Days until Next Archive:** Number of days between successful execution of the current Archive Action against the record, and the execution of the **Next Archive Action**. This is a required field.

## System Settings

The **Disk** Storage Type lets you specify a local drive path for archiving. Discover must have read/write access to this drive. The following settings apply to the Disk Storage Type:

- **Location:** Enter a direct file path or a custom file mask for the archive destination (see [Customize the Location File Mask](#)).
- **Use Schedule:** When enabled, the Archive Action only runs during the specified time of day.
- **Start Time/End Time:** In conjunction with **Use Schedule**, the time of day restriction for the action.

The **SMB** Storage Type lets you specify CIFS/SMB network file storage share for archiving. If Discover is unable to write to the file share, the Discover Notification System generates an alert. The following settings apply to the SMB Storage Type:

- **User ID:** If the storage location requires credentials, enter the username here.
- **Password:** If the storage location requires credentials, enter the password here.
- **Location:** Enter a direct file path or a custom file mask for the archive destination (see [Customize the Location File Mask](#)).

The **DVD** Storage Type lets you use removable media for archiving. DVD+R, DVD-R, DVD+RW, and DVD-RW single-layer are supported. Archive Actions using the DVD storage type only execute once per day. DVD media must be manually removed and new media inserted on a daily basis. The following settings apply to the DVD Storage Type:

- **DVD Drive:** Archiver auto-detects any compatible DVD drives on the system and uses the first one that has a blank disk in it.
- **Archive Time:** Time of day the Archiver will start creating the DVD archive. Uptivity recommends you set this to the lowest period of system usage, as creating archives requires high system resources.

The **XAM** Storage Type lets you use the fixed-content access method associated with the Centera content-addressable storage platform for archiving. The following settings apply to the XAM Storage Type:

- **Retention Period (days):** Number of days the Centera server will retain archived files. This setting is used instead of the **Next Archive Action** setting.

- **PEA File:** Required only if security authentication is needed to access the Centera storage server. This is the full path name of the Pool Entry Authorization file for accessing the server.
- **Server IP Address:** Centera server IP address, or multiple addresses, comma-separated.

At the bottom of the **Edit Archive** window, an informational section shows the schedules which are configured to use this **Archive Action** as well as some statistics about the action's usage.

## Customize the Location File Mask

For the Disk and SMB storage types, you can create a file mask to customize the UNC path for the archive location and/or the types of files archived to that location. file names can be customized using file masks (see Disk and SMB storage types only). This table below shows the variables that can be used in file masks.

Variable	Value	Variable	Value
%Y	Four-Digit Year	%A	Agent Number (ID)
%y	Two-Digit Year	%R	Record ID
%M	Two-Digit Month	%C	Counter
%m	Month Name (three-letter abbr. – Jan, Feb, May, Dec)	%F	Filename without path
%D	Two-Digit Day	%P	path minus root (see additional explanation below)
%d	Day Of Week (Name)	%P<-1>	path minus root remove 1 bottom directory
%H	Hour	%P<1>	path minus root remove 1 top directory
%N	Minute	%U<1> through %U<15>	user fields
%S	Second		

## System Settings

For example, for the path "C:\recordings\test\device10\10-100-100.wav" these are the variables that would be used and what they represent:

%P<-1>	test\device10
%P<1>	recordings\test
%P	recordings\test\device10
%F	10-100-100

If no mask is specified, Archiver defaults to "%P\%F"; if only "C:\recordings\" or "C:\recordings" is entered, Archiver defaults to "C:\recordings\%P\%F".

If %P is not used in the file mask, the Archiver will determine one on its own using the following process:

- Archiver checks the Core where the file was recorded and obtains the default file mask if possible.
- Archiver tries to match the filename to the default file mask. If it matches, Archiver removes the rest of the path that does not match.
- If the filename does not match, Archiver removes the drive letter only.
- The path is put at the end of the archive location, forming the new path.

The file is then archived using the generated mask.

## Configure Archive Actions

To create a new Archive Action:

1. Click the **Administration** tab and expand **System Settings** in the left navigation menu.
2. Click **Archive Actions** and then click **Add**.
3. Configure the needed settings and click **Save**.

After you create an Archive Action, you must attach it to a schedule. For details, see [Scheduling](#).

To edit an existing Archive Action:

1. Click the **Administration** tab and expand **System Settings** in the left navigation menu.
2. Click **Archive Actions** and then click the action you wish to edit.
3. Configure the settings as needed and click **Save**.

## About the Archiver

The **Archiver** module is used to control disk and network usage by Archive Actions, preventing the actions from overwhelming local system resources or network bandwidth. The Archiver settings page controls the overall performance of the software.

Archiver settings are divided into several sub-categories: General, System Purge Action, Removable Media, and MSSQL Database Backup. These settings are typically configured by the Uptivity Discover Installation team and rarely need to be changed. This section provides an overview of settings for reference.

### General Archiver Settings

- **Archiver Server Host:** IP address or hostname of the server running the Archiver service.
- **Archiver Server Port:** TCP Port on which the Archiver service is configured to listen. The default is 5639.
- **Purge Limit:** Throttles the number of records purged from the local Discover system per Purge job. A setting of 0 (zero) means unlimited: the system will purge all records ready to be purged in the database.
- **Purge Interval:** Time interval in minutes between one Purge job and the next.
- **Archive Limit:** Number of records sent to the archive per Archive job. A value of zero (0) causes no recordings to be archived, so the value should typically be set to greater than zero.
- **Archive Interval:** Time interval in seconds between one Archive job and the next. The system default is 60 seconds, which is typically sufficient.
- **Enable Settings Reload:** When set to **Yes**, settings on this page automatically reload on the **Settings Reload Interval**. When set to **No**, the service must be restarted for the settings to take effect.

## System Settings

- **Settings Reload Interval:** Time in seconds that the module will reload its settings from the database. Any changes made to the settings on this page will not take effect until this interval has completed. Works in conjunction with **Enable Settings Reload**.
- **Hash Filename:** When set to **Yes**, files are renamed at archiving as the SHA-1 hash of the original storage path for the record. This is to prevent possible duplicate filenames in the archive location. Not normally needed unless original recording files have the potential of being named the same.
- **Enable Empty Directory Purge:** When set to **Yes**, Archiver periodically scans all directories in any recording locations and removes any folders that have no files inside.

## System Purge Action



The screenshot shows a form titled "System Purge Action". It contains the following fields:

- Use Schedule :** A dropdown menu with "No" selected.
- Start Time :** A time selection field with "12" for the hour, "00" for the minutes, and "AM" for the period.
- End Time :** A time selection field with "12" for the hour, "00" for the minutes, and "AM" for the period.

**System Purge Action** settings can be used to restrict the time period during which Discover purges recordings.

- **Use Schedule:** When set to **Yes**, Purge jobs will only run between the specified **Start Time** and **End Time**. Helps prevent system overload or excessive I/O operations in connected environments during peak hours.
- **Start Time/End Time:** Purge jobs will only run between these hours if **Use Schedule** is enabled.



## Removable Media Settings

**Removable Media**

Removable Media - Playback Temp File Location :

C:\RecordingsTemp\

Removable Media - Temp File Retention(days) :

30

Send Users Email Alert :

Yes

**Removable Media** settings are used when recordings are archived to DVD.

- **Playback Temp File Location:** Records restored from DVD are copied to this location for playback.
- **Temp File Retention:** Number of days a restored recording will be available for playback before it must be restored from DVD again.
- **Send Users Email Alert:** When set to **Yes**, Archiver sends an email notification to the user who requested a record be restored when that record is available for playback.

## MSSQL Database Backup Settings

**MSSQL Database Backup**

Enable MSSQL Database Backup :

No

Database Name :

Backup Filename :

Database Backup Time :

08 : 00 AM

MSSQL Database Backup settings allow you to back up the Discover database. This is useful for sites with SQL Express that cannot use scheduled backups.

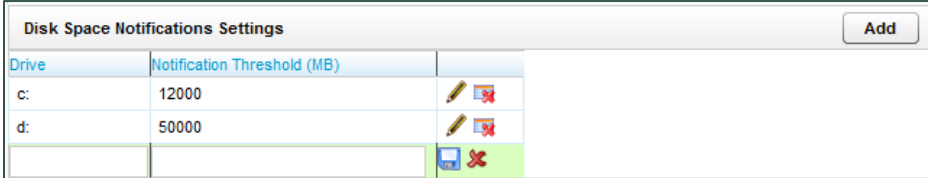
- **Enable MSSQL DB Backup:** When set to **Yes**, Archiver initiates a daily backup of ONE of the Discover databases.
- **Database Name:** Name of the database to be backed up.
- **Backup Filename:** Location of the backup file to use, determined during Discover installation.
- **Database Backup Time:** Time of day that the backup job will run. Uptivity highly recommends this time be set to the lowest usage period of the day.







## System Settings

### About Custom Extensions

If Professional Services development was included for your installation, this section may be used. Otherwise, it can be disregarded. Contact Uptivity Support if you have any questions regarding settings listed on this page.


### About Disk Space Notifications






Drive	Notification Threshold (MB)	
c:	12000	 
d:	50000	 
		 

Disk Space Notifications can be used to monitor free space on any local or mapped network drives the Archiver tool can access. Archiver manages disk usage for original recordings, archives, and SQL databases. If a specified drive drops below the Notification Threshold, Archiver can send a notification message to any email addresses in the **Notifications** list that have the **Disk Alert** notice type selected.

To add a drive entry to the list:

1. Click the **Administration** tab and expand **System Settings** in the left navigation menu.
2. Click **Disk Space Notifications** and then click **Add**.
3. In the **Drive** column, enter the drive letter followed by a colon.
4. In the **Notification Threshold** field, enter the minimum free space (in megabytes) to remain available.
5. Click the Save  icon.

To edit or delete an existing entry:

1. Click the **Administration** tab and expand **System Settings** in the left navigation menu.
2. Click **Disk Space Notifications**.
3. Click the Edit  icon for the desired entry, edit the fields in that row as needed and then click the Save  icon OR click the Delete  icon and then click **OK**.

## About Info Broker

The Information (Info) Broker service is required only in environments using Live Monitoring. It is started, and typically configured, during the installation process. Info Broker settings rarely need to be changed. This section provides an overview of settings for reference.

### Info Broker Settings

Settings for this service are:

- **Host:** IP address of the server running the Info Broker service.
- **Port:** Communications port on the server running the Info Broker service. Default is 50817.
- **HTTP Timeout Seconds:** Timeout for individual communication requests between Info Broker and the Screen Recording Server, Core, and Live Monitor. If Info Broker does not receive communication from Core within the specified time, it assumes it is not running and all calls on devices it was recording have ended. The default value is 5 seconds.
- **Live Monitor Client Timeout Seconds:** Time that can pass without Info Broker hearing from a connected Live Monitor client before a timeout occurs. The default value is 30 seconds.
- **Media Timeout Seconds:** Timeout for the connection to Cores and Screen Recording Clients. The default value is 30 seconds.
- **Excessive Debugging:** When checked, adds detailed logging for Info Broker which can be useful for troubleshooting.

## About Locations

**Locations** are part of your Discover system topology and are typically developed by Uptivity Discover Sales Engineering. Locations allow for easy grouping of Cores, Screen Recording Servers, and Web Media Servers for customers with multiple sites that are geographically or logically separate. Changes to Locations settings should only be made by or under the supervision of Uptivity Discover Support.

## About Logging

**Logging** settings specify the level of events the application sends to the Logger. Logging levels correspond to the subscription types described in [About Notifications](#). These settings are configured during initial installation and should only be changed by or under the supervision of Uptivity Discover Support.

## About Discover Mail

**Discover Mail** allows multiple Discover features to communicate with users via email. To take advantage of this, an email account must be created in your email system for Discover to use. This account is generally created prior to installation, and Discover Mail settings are configured at that time.

This section explains the Discover Mail settings for your reference.

### Discover Mail Settings

The following are in **Server Settings**:

- **Mail Server Host:** The hostname or IP address of the SMTP mail server Discover will use to export recordings via email.
- **Mail Server Port:** The SMTP port that will be used.
- **From Address:** This can be any email address, real or fake, and does not have to be an address tied to the account's username and password.
- **Display Name:** This name appears on the emails sent from the account, and does not have to match the email account username.

The following are in **Secure Settings**:

- **Username:** The username for authentication to the SMTP server.
- **Password:** The Password for authentication to the SMTP server.
- **Confirm Password**

The following are in **Forgot Password Mail Settings**:

- **SMTP Host Email Server:** The hostname or IP address of the SMTP mail server Discover will use to respond.
- **"Send From" Email Account:** The email account Discover will use to respond.
- **"Send From" Username:** The username for this email account.
- **"Send From" Password:** The password for this email account.

## About Notifications

**Notifications** allow you to adjust how long Discover retains information in its log files, and also let you configure audible and/or email maintenance alerts. Be sure to consider disk size when deciding how long to retain log files.

Discover offers different types and levels of alert subscriptions to help you effectively manage your system. While these subscriptions are configured during installation, you may need to make adjustments later as your personnel and/or needs change.

### About Alert Subscriptions

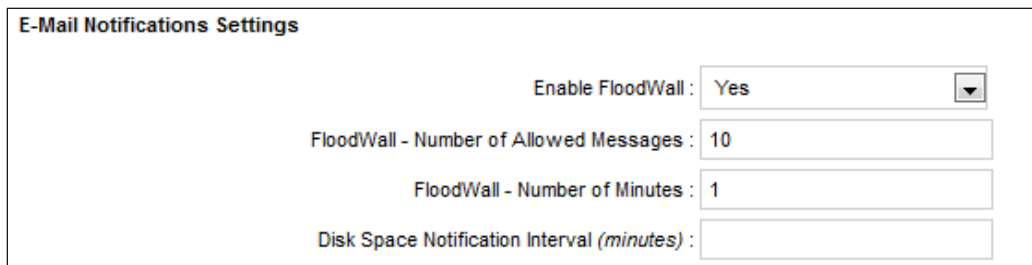
You can set up alerts based on the following event levels:

- **Critical:** A service or system has stopped functioning completely due to an error. You should have at least one email subscription notified of any critical alerts.
- **Emergency:** A service or system has stopped functioning completely due to a configuration or resource issue. You should have at least one email subscription notified of any emergency alerts.
- **License:** The system is reaching a license limitation or someone is attempting to use an unlicensed feature. You should have at least one email subscription notified of any license alerts. These license events are logged and generate notifications:
  - License Expired
  - License Corrupted
  - License Invalid (no license for an accessed feature)
  - Avaya licenses exceeded (Avaya integrations only; may result in loss of recording)
- **Error:** A system error has occurred that caused a single operation or transaction to fail. You should have at least one email subscription notified of any error alerts.
- **Security:** A security event, such as multiple password failures, has occurred. You should have at least one email subscription notified of any security alerts.
- **Warning:** An event occurred that could be related to further errors. This event type is mainly used in troubleshooting and should only be enabled as needed.

## System Settings

- **Info:** General system information. This event type should only be enabled as needed.
- **Notice:** An informational notice regarding system events. This event type should only be enabled as needed.
- **Testing:** Enhanced debugging and development information enabled for troubleshooting. This event type should only be enabled as needed.
- **Debug:** Highest volume/detail output for all modules. This event type should only be enabled as needed.
- **Archive:** All events and messages related to archiving. For example, if a user requests a recording that has been archived to DVD, users subscribed to this alert would receive an email telling them which disk to insert into the server. Archiver error alerts are not included in this subscription, but are in the **Error** and **Critical** alert types. This is an email-only subscription.
- **Disk:** Alerts subscribers when the amount of free space on a disk has dropped below the specified level. See [About Disk Space Notifications](#).

### About E-Mail Notifications Settings



The screenshot shows a dialog box titled "E-Mail Notifications Settings". It contains four settings:

- Enable FloodWall:** A dropdown menu set to "Yes".
- FloodWall - Number of Allowed Messages:** A text input field containing the number "10".
- FloodWall - Number of Minutes:** A text input field containing the number "1".
- Disk Space Notification Interval (minutes):** An empty text input field.

Email notifications can be sent from Discover any time a log message is generated. You can set up subscriptions for multiple email addresses so that different alerts can be sent to specific users. These settings govern email notifications.

- **Enable Floodwall:** Some conditions can generate an enormous number of alerts within a short period of time. When set to **Yes**, the floodwall throttles email alerts to prevent overloading your mail server.
- **Floodwall - Number of Allowed Messages:** Works with **Enable Floodwall** to specify the number of email messages the server sends per interval. Any further messages of the same type will be blocked until the interval expires.
- **Floodwall - Number of Minutes:** Works with **Enable Floodwall** to define the number of minutes per interval.
- **Disk Space Notification Interval:** Specifies the interval in minutes between sending low disk space email alerts.

## About SNMP Notifications Settings

**SNMP Notifications Settings**

Enable SNMP Notifications : No

SNMP Community :

SNMP Enterprise : 26393

SNMP Gen Trap :

SNMP Version : SNMPv2

Discover can send SNMP traps when a log message is generated. SNMP trapping requires use of a Management Information Base (MIB) file that can be loaded in a third-party SNMP management application to define trap types. This file can be obtained from Uptivity Support. These settings govern how Discover uses SNMP.

- **Enable SNMP:** When set to **Yes**, allows Discover to send SNMP traps.
- **SNMP Community:** This is an optional value, although some SNMP management applications require this value to allow Discover access.
- **SNMP Enterprise:** Identifier for Discover-generated SNMP events. Discover is IANA-registered as 26393.
- **SNMP Gen Trap:** This optional setting is a generic type value that can be used to distinguish between multiple Discover systems.
- **SNMP Version:** Discover can generate both SNMPv1 and SNMPv2 traps. Set to the type supported by your SNMP management application.

## Configure Notifications

To configure log file retention and/or Discover alerts:

1. Click the **Administration** tab and expand **System Settings** in the left navigation menu.
2. Click **Notifications**.
3. Enable **Audible Alerts** if desired and then check each condition that should trigger an audible alert.
4. Enter the number of days you want Discover to retain log files.
5. Configure **E-mail Notifications Settings** as desired.
6. For each email subscription, click **Add E-mail** and enter the email address, then select the check box for each alert that should be sent to that email address.
7. Configure **SNMP Notifications Settings** as desired.

## System Settings

8. For each SNMP subscription, click **Add SNMP** and enter the SNMP address, then select the check box for each alert that should be sent to that SNMP address.
9. Click **Save**.

### Test Alerts

This feature sends a message to all users who are set up to receive any notifications. It enables users to confirm that they are receiving the correct notifications. To send a test alert:

1. Click **Save** to record any changes.
2. Select a **Subscription Type** from the drop-down list.
3. Enter text explaining that the message is a test and what type of notification is being tested.
4. Click **Test**.
5. Confirm with each user who should have received the test message.

## About Server Nodes

**Server Nodes** are the machines (physical or virtual) that run Discover software modules. A separate Server Node is created for each machine running modules. Server Nodes are configured by Uptivity at the time of installation. For related information, see [About the Service Manager](#).

Changes may later be required if services are added to your system or moved to different servers. These changes require configuration in multiple locations within Discover and should only be performed by or under the supervision of Uptivity Support.

## Web Media Server

**Web Media Server** (WMS) is a Discover module that manages both playback of recordings and streaming for Live Monitoring. The WMS service is set up during installation. If additional configuration is needed, it should be performed by or under the supervision of Uptivity Support. There can be only one Web Media Server per website (Web Portal) for playback, but Discover supports multiple Web Media Servers for Live Monitoring if this functionality is widely used in your environment.

This section provides an overview of WMS settings for reference.



## Web Media Server Settings

- **Host:** IP address of the Web Media Server.
- **Silverlight Port:** Port used to play recordings and stream live audio.
- **Media Port:** Port used for messaging traffic with Core and Screen Recording Server. The default value is 5630.
- **HTTP Port:** Port used for messaging traffic with Info Broker. The default value is 2015.
- **Allow Live Monitor:** When the check box is selected, the Web Media Server will be used for Live Monitoring.
- **Excessive Debugging:** When the check box is selected, detailed logging will be collected for Info Broker (useful for troubleshooting).
- **API Host:** IP address of the API Server. Used only for exporting recordings via email.
- **API Port:** Port used to communicate with the API Server.
- **API Reconnect Milliseconds:** Frequency with which the WMS attempts to connect to the API server via TCP.
- **API Connect Timeout Milliseconds:** Connection timeout for API server connection attempts. When timeout expires, Discover "sleeps" until the next reconnection attempt.
- **API Response Timeout Milliseconds:** Timeout for API server responses before Discover considers the request to have timed out.
- **SSL Certificate Name:** SSL certificate file name (no path required) if SSL is required for data in transit.
- **SSL Certificate Pass:** SSL certificate password if SSL is required for data in transit.
- **Location:** Location with which this Web Media Server is associated.
- **Mapped Drives:** Sets an internal drive map so if the filename says f:\recordings, but for WMS the path is Z:\recordings, the f: becomes Z: on the WMS side. Unless otherwise specified, default settings are used.

## System Settings

### About Web Server

Several Discover services, such as call playback, utilize **Web Server** services. These settings are configured during the initial installation. If configuration changes are needed later, these should be performed by or under the supervision of Uptivity Support.

As explained on the page itself, these settings do not configure IIS. If the manual override is not used, the settings may be changed by other processes.

### About Workstations Settings

Core uses the Workstations List to determine the Screen Recording Server with which it should communicate. The list is not used in all installations. For more information, see [Configure Workstation Mapping](#) in the Screen Recording Appendix.

# Web Portal Settings

## About CometDaemon

When a Server Node is created, a corresponding **CometDaemon** is created in the Web Portal. CometDaemon runs in the background and manages connections to and between Discover software modules on its corresponding Server Node and other services (e.g. Service Manager). CometDaemons are configured by Uptivity at the time of installation. If configuration changes are needed later, these should be performed by or under the supervision of Uptivity Support. This section provides an overview of CometDaemon settings for reference.

### About CometDaemon Settings

- **HTTP Port:** Specifies the port on which HTTP communication takes place between the CometDaemon and the Service Manager.
- **HTTP Address:** If the server on which the Web Portal is installed is assigned multiple IP addresses, this field can be used to restrict access to only one of those addresses. Using 0.0.0.0 uses all of the addresses.
- **HTTP Session Time Out Minutes:** If the CometDaemon does not receive a message from the Service Manager within the time specified here, it ends the session.
- **Allowed Subnets Client:** This setting is no longer used.
- **Allowed Subnets System:** This setting is no longer used.
- **Allowed Subnets Session:** Specifies valid IP address of the Web Portal used to access the Server Node for this CometDaemon; controls IP addresses from which sessions can be initiated. The client can start the session in one subnet range. Once the session is started, it will continue the session using the client subnet. This subnet can use CIDR notation and be comma-separated.
- **Site IP:** Displays the IP address of the Server Node on which the Service Manager resides.
- **Status Timer Interval:** Time in milliseconds for "heartbeat" polling with the CometDaemon.
- **Configuration Timer Interval:** Time in milliseconds for reloading the module's settings.
- **Search Directory:** Specifies the location of the Discover Install directory. CometDaemon knows what services are available based on directory contents.




### About Security

To enhance system security, Discover lets you control **Security** settings related to forgotten passwords and PCI security for the Web Portal. These settings are configured by Uptivity at the time of installation. If configuration changes are needed later, these should be performed by or under the supervision of Uptivity Support. This section provides an overview of the settings configured on the Security screen for reference.

#### Site Settings

**Site Settings** allow you to specify the IP address or hostname where users will access Discover and, if applicable, Clarity. These settings must be configured for users to be able to switch back and forth between Discover and Clarity from within the applications.

IP address entries must be in the format "http://1.1.1.1." If the "http://" is left off, the URL validator will not receive a response from the supplied IP/port. You will see one of the following icons next to the field after you enter the IP or hostname.

-  indicates a valid IP or hostname.
-  indicates an invalid IP or hostname. You will not be able to save changes to the page if the one of the URL fields contains an invalid value.
-  indicates the system is currently attempting to resolve the IP or hostname

#### Forgot Password Settings

Discover can be configured to allow users to reset their own passwords. **Forgot Password Settings** let you specify:

- **Password Max Length**
- **Password special characters length:** Number of special characters the password must contain.
- **Mail Subject:** Subject line of the email users receive when they click the "Forgot Your Password?" link.
- **Mail Body:** Body of the email users receive when they click the "Forgot Your Password?" link.

## Active Directory Settings

Discover can be set up to let users authenticate via a Discover user account and password (database mode) or via their Windows network/Active Directory credentials (AD mode). They can also be given a choice of database or AD authentication at the time of login (hybrid mode). The login mode is typically configured by Uptivity at installation.

In multiple domain environments, Discover maintains a separate user account for each user on each domain (this also works with the "Auto Create User on Login" feature). For example, if Joe Smith works at two different locations, each with its own domain, user jsmith would be created twice in Discover, with one account assigned to each unique domain. Reporting and other features treat the accounts as unique individual users.

Users must be placed in one or more AD groups that have access to Discover. You can relate Discover Roles to Active Directory group names, allowing Discover Groups, Roles, and Permissions to be synchronized at each login. Discover can even remove any Roles that are not linked to an AD group when a user logs in. This feature is called AD Group Role Synch.

**Active Directory Settings** apply to organizations using AD or hybrid mode for authentication:

- **Auto Create User on Login:** When the check box is selected, allows creation of a user account in the Discover database the first time a user logs into the system using Windows credentials. The user account is populated with the AD account's login name, first name, last name, and email address.
- **If Using AD Group Role Synch, Delete User's Roles That Do Not Match an AD Group on Login:** When the check box is selected, automatically updates each User's Groups, Roles, and Permissions accordingly upon login. Otherwise, Groups, Roles, and Permissions must be changed manually.
- **Domain:** Name of your AD domain. Multiple domains can be configured.
- **LDAP String:** Active Directory LDAP string (the "LDAP://" portion must be capitalized). Consider the following when configuring LDAP, particularly if logging in with AD credentials is not working properly:
  - **Case Sensitivity:** If a user logs into Windows with "Username" but their AD account is "username", the login attempt may not pass through LDAP.
  - **Idle States.** If a computer enters an idle state (e.g. sleep, standby, or hibernation) that turns off the network interface card based on power management settings, users may experience intermittent login issues when

## Web Portal Settings

using AD authentication. To avoid this, configure power management settings to keep the system and network card awake during work hours.

- **Password Special Characters.** Certain special characters may not work properly with LDAP, resulting in a failed login attempt. Avoid using #, @, \*, ", &, and %. The characters (, ), ^, \$, and ! should be fine.
- **Secure Sockets:** When the check box is selected, enables/requires the use of SSL.
- **Signing:** When the check box is selected, enables LDAP security; enabling it here and in Windows Server encrypts the connection between them.

## Login Settings

**Login Settings** govern other factors associated with the login mode your system uses:

- **Access Type:** Specifies your system login mode (Hybrid, Database, or Active Directory).
- **User Token Expire Time:** User tokens monitor activity for a user ID within the site. The system refreshes the timestamp and expiration of the token every time a user clicks on something. Once the token expires, the user's next action will log them out and bring them back to the login screen. The default expiration time is five minutes.
- **Login Token Expire Time:** Login tokens are passed to the database when a user clicks the login button. Once the session is established, the token is expunged from the database. If something interrupts the transaction or the process encounters an error, the token may be left behind, and this timeout triggers it to be automatically deleted. The threshold should be set to only a few seconds.
- **Integration Token Expire Time:** Integration tokens are similar to login tokens, but are created when a user transitions from Discover to Clarity, or vice versa. As soon as this transaction is complete, the token is removed from the database. If something interrupts the transaction or the process encounters an error, the token may be left behind, and this timeout triggers it to be automatically deleted. The timeout threshold should be set to only a few seconds.

## PCI Settings

**PCI Settings** are optional settings that control password policy for Discover user accounts, based on the PCI Security Standards Council's Data Security Standard v2.0 (viewable at their website). Passwords are automatically "salted" by Discover, and password changes are tracked through both the Audit Log and the System Activity Summary Report.

Changing these PCI password security settings in the Web Portal does not automatically force users to change their passwords. The settings do not affect users until their passwords are changed, either by the user or an administrator. If you want to enforce PCI settings, you must force users to change their passwords or change the passwords for them.

These settings apply **only** to Discover database user accounts and do not impact Windows accounts used with hybrid or AD authentication:

- **Password Strength Enforcement:** When the check box is selected, forces all new passwords to be a minimum of eight characters in length and contain at least three of the following character types:
  - lowercase letters
  - UPPERCASE letters
  - Numbers
  - Special characters
- **Prompt user to change password before expiration:** When the check box is selected, controls how long a password can remain active. You can set the **Number of days before password expires** (cannot be zero) and the **Number of days of warning before password expires**. This applies to all Discover accounts, including the superuser account.

## Web Portal Settings

- **Prevent Re-use of Passwords:** When the check box is selected, password changes are checked against a password history to prevent re-use. You can set the **Number of previous passwords to check** (for example, password cannot be the same as the last 5 used) and/or the **Number of days between password change** (for example, password cannot be the same as one used in the last 60 days). Discover does not trace passwords unless this feature is enabled, so the re-use look-back will not consider or compare passwords used before enablement.

**Note:** Administrative users can manually change a user's password to anything that meets the complexity requirements in force, including previously used passwords. This setting affects only users changing their own passwords.

- **Limit Failed Login Attempts:** When the check box is selected, user accounts are locked after the **Maximum number of failed login attempts to allow** has been reached. Locked accounts must be unlocked by an administrative user before the user may attempt another login. This setting does not apply to the Superuser account unless the **Lock out Superuser after limit reached?** Check box is selected.

## HTTP/HTTPS Settings

When the **Force the site to use HTTPS** check box is selected, secures Web browser cookies (ASP.NET\_SessionID) by setting the **secure** flag. This prevents cookies from being sent across non-https connections and is a PCI-compliant feature.

## About Terminology

The Discover Web Portal can be customized with terminology used in your operating environment. For example, if you don't use the term agents, but instead refer to "reps" or "CSRs", Discover can be configured to show your terminology in its user interface.

Terminology Settings are typically discussed during the discovery phase and configured at the time your system is installed. You can change them later if necessary.

If you make changes to Terminology Settings, it may take some time for the changes to appear in the ad hoc reporting pages. Terminology changes affect only Discover and do not carry through to Clarity Web Portal.



## Terminology Settings

- **Switch Type:** Drop-down list of common ACD/PBX hardware manufacturers (eOn, Alcatel, Aspect, Avaya, and Custom). Select from this list and Discover will auto-populate the terminology names with terms common to that ACD/PBX. You can overwrite these defaults as needed.
- **Agent:** Employees who staff your contact center (e.g., Agent, CSR, TSR, Associate, etc.).
- **Group:** Group setting in your ACD/PBX (for example: Hunt Group, Skill Group, or Labor Group). This does not refer to the Discover Group.
- **ACD Gate:** Call gate or queue setting in your ACD/PBX (for example: Application, Split, Gate, etc.).
- **Called Number (DNIS):** For inbound calls, this would be the number the caller dialed to reach you. For outbound calls, it would be the number your agent dialed.
- **CallerID (ANI):** For inbound calls only, this is the number of the calling party as provided from the telecommunications carrier.
- **Device/Port ID:** "Hardware" identifier in your ACD/PBX (for example, Position ID, Phone Port, DN, or Extension).
- **Agent Number (Device Alias):** Agent-associated identifier in your ACD/PBX (for example, extension, agentID, etc.).
- **Group Name:** Discover Group. For details, see [Discover Groups](#).
- **User 1- User 15:** Custom data fields. If your system includes custom API integrations, it is common for data received from third party IVR, CRM, or ACD platforms to be inserted into these fields. If you use Discover On-Demand, agents can enter information in these fields via the On-Demand client. You can rename them to be more descriptive regarding the data contained within the field.

## Configure Terminology

To configure Discover to use customized terminology:

1. Click the **Administration** tab and expand **Web Portal Settings** in the left navigation menu.
2. Click **Terminology**.
3. Edit any settings as needed and click **Save**.

### About Web Portal

**Web Portal** allows you to configure settings for the Discover Web Portal and Web Player. The majority of these are set by Uptivity during installation. If configuration changes are needed later, these should be performed by or under the supervision of Uptivity Support. This section provides an overview of Web Portal settings for reference.

#### Web Portal Settings

- **Content Management Upload Directory:** Disk or UNC path on the Discover server where files uploaded to the Content Library are stored.
- **Fusion Script Settings Upload Directory.** If the Uptivity Fusion Desktop Analytics component was purchased, the scripts used to manage Desktop Analytics clients are loaded into this directory.
- **Location Settings: Allow Lookup by Agent/Workstation:** This check box is selected ONLY if your environment is segmented in a way that inhibits standard agent lookup by Location. An example might be if all your telephony hardware and call routing is done from one Location but agents, Screen Recording servers, and Web Media servers are set up at other Locations and agents cannot be grouped logically into the primary Location for audio recording. In that scenario, enabling this setting would ensure that agents at the Locations apart from the telephony system will have Screen Recording and Live Monitoring traffic kept local to their site. Enabling this setting requires the Location setting to be configured for each agent in the system. Screen recording will not take place for agents who do not have a specific, valid Location. For more information on assigning agents to specific Locations, see [Add a User](#).
- **Call Segment Settings: Allow Call Segments:** Applies only to specific telephony environments where Call Segments can be generated and related for viewing in the Call List. Refer to the *Uptivity Discover Web Player Manual* for details on Call Segments.
- **Call List Quick Filters:** Selecting the check box next to an item causes it to appear as a filtering option on the Web Player tab for all users.
- **Number of Items to Display:** Sets the number of rows to display per page, except on Printable Reports and the Call List.
- **Display data value when building ad hoc reports:** When set to **Yes**, data for a field appears or disappears on the Report Builder preview each time the user moves a field to/from the Structure area. The database is queried upon each of these changes.

## About Home Tab Widgets

You can administer which widgets are available to users for dashboard configuration on their Home tab. This includes adding new widgets, editing existing widgets and deleting widgets from those available. For specific information on individual widgets, refer to the *Uptivity Discover Web Player Manual*.

Adding or deleting a widget cycles the application pool in IIS, and requires a page refresh and new login to see changes. **This will force a logout for all connected users and should be performed outside of regular business hours.**

### About the Home Tab Widgets List

Home Tab Widgets <span>Upload</span>		Title	File Name	Description	Date	Actions
News	NewsWidget	The News Widget allows for Administrative based Users to push quick, one line information to groups of agents and other users.			Feb 28 2014 6:52PM	<a href="#">Edt</a>   <a href="#">Delete</a>
Forecast vs. Actual	ForecastVsActual	The Forecasted vs. Actual Widget allows for Users to compare actual call volume against that of forecasted call volume.			Feb 28 2014 6:52PM	<a href="#">Edt</a>   <a href="#">Delete</a>
KPI Performance	KPIPerformance	The News Widget allows for Administrative based Users to push quick, one line information to groups of agents and other users.			Feb 28 2014 6:52PM	<a href="#">Edt</a>   <a href="#">Delete</a>
Live Snapshot	LiveSnapshot	The Live Snapshot widget allow for Users to view call data, staffing information and service levels.			Feb 28 2014 6:52PM	<a href="#">Edt</a>   <a href="#">Delete</a>
Service Level Snapshot	ServiceLevelSnapshot	The Service Level Snapshot Widget allows for Users to view Service Level percent for various Labor Units and CallCopy Groups.			Feb 28 2014 6:52PM	<a href="#">Edt</a>   <a href="#">Delete</a>
Assignment Inbox	AssignmentInbox	The Assignment Inbox widget allows Users to view items in their Assignment Inbox.			Feb 28 2014 6:52PM	<a href="#">Edt</a>   <a href="#">Delete</a>
QA Benchmark	QaBenchmark	The QA Benchmark widget enables users to compare QA score averages for agents, CallCopy groups, and forms.			Feb 28 2014 6:52PM	<a href="#">Edt</a>   <a href="#">Delete</a>
Achievement	Achievement	The Achievements widget enables users to view the available achievements			Feb 28 2014 6:52PM	<a href="#">Edt</a>   <a href="#">Delete</a>

The **Home Tab Widgets** list shows the widgets that are currently available in your system. The widgets shown in the screenshot above are default widgets in every Discover installation.

The Date column shows when the widget was uploaded or last updated. You can upload new versions of existing widgets if they become available. If the file names are identical, Discover will prompt for confirmation to overwrite the existing widget. Uploading a new version resets the widget's date to the current day.

## Manage Widgets

While Home Tab Widgets are managed in the Web Portal, the underlying widget files reside on the Discover server. Therefore, widget management tasks must be performed on the server itself.

To upload a new Widget:

1. Click the **Administration** tab in the Discover Web Portal and expand **Web Portal Settings** in the left navigation menu.
2. Click **Web Portal**.

## Web Portal Settings

3. In the Home Tab Widgets section, click **Widget Upload** and then click **Upload**.
4. Navigate to the directory on the Discover server where widgets are stored (typically \Program Files (x86)\CallCopy\WebPortal\bin).
5. Select the desired widget .dll file and click **Open**. If you are uploading a new version of an existing widget, click **Overwrite File**.

You can modify a widget's Title and Description. Changes take effect immediately, do not require clicking Save, and will not affect login status of connected users. To edit a widget:

1. Click the **Administration** tab in the Discover Web Portal and expand **Web Portal Settings** in the left navigation menu.
2. Click **Web Portal**.
3. In the Home Tab Widgets section, click **Edit** for the desired widget.
4. Enter a new **Title** (25 character max) and/or **Description** (200 character max) as desired.
5. Click **Save**.

Deleting a widget removes the widget from the system *and* removes the corresponding DLL from the server. Removing a widget from the system also removes it from any user dashboards where it was displayed. Widget .dll files should be backed up to protect against accidental deletion. To delete a widget:

1. Click the **Administration** tab in the Discover Web Portal and expand **Web Portal Settings** in the left navigation menu.
2. Click **Web Portal**.
3. In the Home Tab Widgets section, click **Delete** for the desired widget.

The maximum number of widgets that will be listed per page is determined by the **Number of Items to Display** setting, found above the Home Tab Widgets section of Web Portal Settings. If more widgets than that are uploaded, pagination will be used to view the rest.

## Manage Dashboards

Once widgets are configured on the Administration tab, you can create custom dashboards for your organization and users can access them from their Home tab. Users can also create their own dashboards using the widgets you make available. For more information on managing dashboards, see the *Uptivity Discover Web Player Manual*.

## Appendix: System Security in Discover

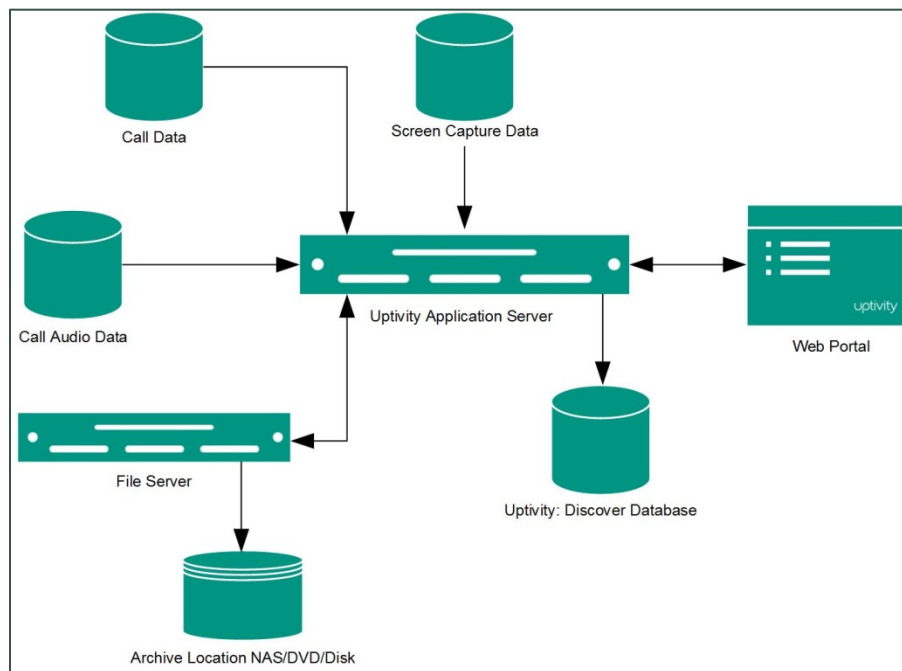
This section offers a high-level overview of security-related concerns related to Uptivity Discover WFO, so that network, system, and Discover administrators understand how different features work together. Additional details may be available in sections specific to a Discover feature.

### Security Design

As a general rule, Discover receives call audio from the PBX or agent telephone. Call data comes from the PBX. Screen recording data is received from the agent's PC over the LAN/WAN.

The Uptivity Discover applications capture the audio and screen data and write it to files on the File Server. Files can optionally be encrypted. Files can initially be stored on the local server and later written to another server based on schedules and available bandwidth. The temporary local files are deleted. Records for each recording are created in the Discover Database for file and quality management. Recordings can be archived in a variety of ways if needed. Records and archives can be configured with retention periods and automated purging.

The audio and video files can be listened to and viewed from the file server via the Web Portal's Web Player by users with appropriate permissions.



## Appendix: System Security in Discover

Interactions between Uptivity Discover components (e.g., servers, Web Portal), file servers, and archive devices can use SSL if that feature is enabled. If users are recorded from remote locations or access recordings from remote locations, a VPN must be established for PCI certification.

### Blackout Sensitive Data

inContact recommends blanking audio and screen recording when sensitive data is being referenced or collected by any Uptivity Discover system. This feature is referred to as a "blackout."

Blackouts in Discover can be triggered in two ways:

- Manually using the "Start Blackout" and "Stop Blackout" options from the On-Demand client menu. This allows an agent to apply blackouts to a captured call.
- Automatically using Uptivity Fusion Desktop Analytics or a similar third-party application, which sends a scripted call to the API server. The API server in turn issues BLACKOUTSTART and BLACKOUTSTOP, or AGENTBLACKOUTSTART and AGENTBLACKOUTSTOP, commands to the recording Core.

AGENTBLACKOUT is the preferred method, and the default in Discover. While BLACKOUT is based on call instance, AGENTBLACKOUT will blackout all call and screen data for a specific time range for the specified agent. The time period is user-specified in the CTI Core settings. The system can be configured by inContact to use BLACKOUT if you prefer.

Blackouts do not stop the recording; they simply prevent reviewers from hearing/seeing the blacked out information. When the call and screen data is processed by the Transcoder, these start/stop events tell it when to blank the screen and audio to protect sensitive information. The Transcoder deletes the recorded content and replaces it with blank audio or video.

A blackout is applied to an agent's entire call. If an agent's call has multiple instances, the blackout criteria apply to all instances of that call. For example, if an agent answers a call, puts the call on hold, calls a supervisor, ends the supervisor call, and returns to the original call, the blackout criteria are applied to the entire original customer call and the supervisor call. The blackouts are inserted by the Transcoder once the entire call is completed, so the number of activities performed during the call does not impact this.

Blackouts are effective during call "wrap" periods. The amount of wrap time allocated after a call is determined by the associated schedule, which also tells Uptivity Discover Screen Recording to keep recording. API server calls for blackout starts/stops are still being recorded and are applied during transcoding.

API-triggered blackouts can be used with On-Demand recordings.

Screen-only recording based on [About Timed Schedules](#) rather than call events cannot apply blackouts. Without call start/stop events from the device, Discover cannot associate blackout events. However, if timed and non-timed events happen concurrently, blackouts can still be applied to the non-timed events.

In individual cases where this process fails and sensitive data is recorded to an audio or video file, these files must be securely removed from the server using Discover and a tool such as sdelete or Eraser.

### **Purging Sensitive Data**

If your business process requires recording and then deleting sensitive data after a period of time, Discover supports doing this either manually or automatically.

Uptivity Discover WFO Support can manually move files and their corresponding database records to the Discover Purge Queue. You can then delete the files by running a file purge as described in [About the Archiver Console](#).

Automatic purging of data is controlled by schedules and Archive Actions in Discover. Discover cannot purge data from devices or disks that are not currently connected to the network (such as archived files on DVD media).

### **Authentication and Passwords**

Users can authenticate via a Discover user account and password or their Windows network/Active Directory credentials. If authentication is done via Active Directory, password length and other security measures are configured in AD. See [About Security](#) for additional information.

### **Windows PC, Server, Database, and Application Accounts**

Appropriate security measures must be used on any PCs, servers, applications, or databases included in recording and storage of recording files and data. This is especially true in contact centers that are concerned with PCI compliance. Consider:

## Appendix: System Security in Discover

- One or more Windows file servers may be used for storing recording files with cardholder data.
- Servers, network attached storage devices, removable media, or other devices may be used in archiving recording files with cardholder data.
- Uptivity Discover Screen Recording servers may be used, resulting in video files that are stored in a different location from the associated audio files.

The accounts and passwords used to manage these files should also comply with overall security measures. inContact recommends the following:

- As a precaution, any account used to manage the Windows server and IIS server hosting Discover should be secured in order to prevent anyone from tampering with Discover's operations.
- Discover uses an SQL database to store recording "records" (i.e., metadata about recording files), audit tables, and configurations. For SQL servers, NT Authority\System for SQL Server Database Engine, NT Authority\Network Service for SQL Server Reporting Services, and NT Authority\Local Service for the SQL Server Browser should be used. Talk to your Uptivity Discover Installation and/or Support teams for more information.
- When separate Uptivity Discover Screen Recording servers are used, Discover must be provided with a UNC path for the location and a user account and password with Write permission for the location. This account should also be secured.

## Logging and Auditing

For details, see [About Logging](#). Additional logging information appears in administration manuals for Uptivity Clarity WFM, Uptivity Speech Analytics, etc. Auditing information is discussed in the *Uptivity Discover Reporting Manual*.

## Login Mode Configuration

Discover supports three login modes:

- **Database Mode:** Utilizes Discover's internal user database that has been populated from entered user accounts and passwords. This mode is used by default.
- **Active Directory Mode:** Uses Kerberos authentication to validate that an Active Directory user is logged in and a member of the proper AD group to access the Discover system.



- **Hybrid Mode:** Allows users to log in using their Discover user accounts or their Windows AD account. On the Discover login page, user must select either Database or Active Directory mode.

The login mode is set during Discover installation. If hybrid or AD mode is used, additional settings must be configured. For additional information, see [Active Directory Settings](#) and [Login Settings](#).

When users log in using AD authentication, a message is sent from Discover to AD. This event is logged, as is the result, which can be:

- Discover receives a response from AD. Authentication succeeds and the user is logged in.
- Discover receives a response from AD. If authentication fails, a specific message identifying the cause is logged.
- Discover fails to receive a response. In this case, a "Directory Entry Failed" error is logged, as AD could not be reached. There is no timeout associated with this; it either succeeds or fails. On the Discover login screen, the following message is displayed: "Login failed. No response was received from Active Directory or Active Directory could not be contacted."

## SSL and TLS (Transport Security)

Interactions between Discover suite components (e.g., servers, Web Portal), file servers, and archive devices can use SSL (Secure Socket Layer) and TLS (Transport Layer Security) for data in transit. **Customers must obtain their own SSL certificate(s).**

For transport security to be effective, all communication starting and ending points should be secured. Endpoint configuration details are explained in the next few sections. Bear in mind that SSL/TLS are all-or-nothing solutions. If you enable SSL/TLS on the Screen Recording or Web Media Server but not on the client modules that rely on them, the modules will not be able to communicate.

If users are recorded or access recordings from remote locations, they must go through a VPN for this level of security.

If transport-level security was not included with your system at installation, and you would like to add this feature to your system, contact Uptivity Discover Support.

## Appendix: System Security in Discover

Transport-level security is typically used in conjunction with optional Discover Encryption. For more information, see [Appendix: File Encryption in Uptivity Discover WFO](#).

The following table summarizes the impact of encryption and TLS on a Discover system.

Encryption	TLS	What is Encrypted
ON	ON	All supported file formats on disk. All Web Player and Live Monitoring communications.
ON	OFF	All supported file formats encrypted on disk. No Web Player or Live Monitoring communications.
OFF	ON	No supported file formats on disk. All Web Player and Live Monitoring communications.
OFF	OFF	No supported file formats on disk. No Web Player or Live Monitoring communications.

### Transport Security and PCI Compliance

From the standpoint of PCI compliance, Discover On-Demand, API Server, and Fusion Desktop Analytics are considered secure regardless of encryption usage. When sensitive information is communicated, Uptivity Fusion Desktop Analytics triggers the API Server to stop recording, ensuring that no such data is recorded or flowing through the application or network. Payment data is not at risk because it is not communicated over networks via Discover, but rather through the your payment application. On-Demand is not affected either way by encryption being on or off; it triggers call recording, and as long as that component is encrypted, then the activity is secured.

Coalfire Systems, a Payment Application Qualified Security Assessor (PA-QSA) company, has determined that Uptivity Discover WFO is not "payment aware" at any time. Analysis of network transmissions and examination of the hard drive of the system running Discover using industry-standard forensic tools/techniques confirmed that no cardholder data was accessible. Blackout techniques within the software render cardholder data inaccessible through call/screen recordings.

In short, when properly implemented following best practices, Discover will not negatively impact your organization's PCI-DSS compliance status.

## **HTTP/HTTPS Settings**

Discover can be configured to support HTTPS. For configuration details, see [About Security](#). This setting affects only Discover. Other Discover components that communicate with the Discover server must be configured separately to use SSL.

# Appendix: Uptivity Discover Best Practices

This section provides high-level guidelines and suggestions network, system, and Discover administrators, based on the experience of the Uptivity Discover Installation and Support teams as well as the hundreds of customers successfully using Uptivity Discover WFO.

## Disk Space Management

If Discover servers do not have adequate disk space, call recording and other functions will stop. This section explains common disk space management issues and how you can address them.

### Plan for Growth

During the sales and installation processes, Uptivity Discover sales engineers use your data to recommend the amount of disk space needed. Estimating future growth and changes is difficult. These common changes alter the need for disk space:

- Adding voice channels
- Adding screen recording
- Changing desktop resolution
- Increasing call volumes

If your organization is or will be experiencing any of these or similar changes, contact Uptivity Support so that the needed disk space can be recalculated.

### Remove Patches and Installers

Files used during installation and maintenance may not need to remain on the server. Examples include Uptivity software patches, downloaders, and installers. Uptivity Install and Support engineers attempt to remove all unnecessary Uptivity files. Be sure to remove any unnecessary software when you do maintenance work, such as changes to the server operating system.

## Set Up Discover Disk Space Management Features

Disk space management is affected by settings on several Discover features. The default settings are adequate for most environments, but changes or specific situations may require setting adjustments. If disk space is a recurring issue, talk to Uptivity Support for a review of the following settings:

- **Disk Space Notifications:** see [About Disk Space Notifications](#).
- **Logging:** Make sure the system is not logging excessively and that files are not being saved longer than necessary. See [About Logging](#) for details.
- **Archiver and Archive Actions:** Confirm files are being purged after they are no longer needed.
- **Scheduling:** Confirm schedules do not have excessive retention days and are tied to Archive Actions or purging.
- **Transcoder**

## Delete Files from Content Management Upload Directory

Files uploaded to the Content Library through the Discover Web Portal are stored on the Discover server (for details, see [Web Portal Settings](#)). When a file is deleted from the Content Library on the Web Portal, only the entry in the Web Portal is deleted. The actual file remains stored on the server with the filename updated to the timestamp of the deletion.

If disk space becomes an issue, you may want to manually delete these files from the server after they have been deleted through the Web Portal. Contact Uptivity Support for assistance if needed.

## Delete Temporary Files after Issues

During service issues, log files grow significantly. After an issue is resolved, clear disk space by manually deleting or editing files that are no longer needed. If an application was configured for excessive or debug logging, reset it to the normal logging level.

## Automatically Delete Temporary Files

Windows and IIS generate many temporary files that are retained indefinitely. These log files are mainly for troubleshooting and reviewing security. If neither of those issues is of immediate interest to you, the files can be deleted periodically. Contact Uptivity Discover Support for assistance.

## Shut Down and Restart

This information applies to planned shutdowns/restarts and unplanned Windows server outages.

Microsoft server updates (patches, hot fixes, etc.), which usually cause system restarts, typically do not affect Discover. However, there is no guarantee that this statement is always true.

Points to consider:

- Discover applications and modules are typically installed as Windows services that auto-start when the server starts. Archiver does not auto-start; it can be started from the Service Manager. Uptivity Survey is not registered as a service, and the way it starts depends on how it was configured.
- If calls are being recorded when the system is shut down, those calls are lost. A file of the recorded audio is retained, but no call record is created, and the audio file is not transcoded.
- The system does not restart calls that were in the recording process at the time of the shutdown.
- If the Transcoder is processing a call when the system is shut down, the Transcoder will reprocess that call after the restart unless the maximum number of attempts has already been reached.
- If a call is being analyzed, the speech analytics engine will reprocess that call. Uptivity Speech Analytics is installed on a different server from other Uptivity applications and modules, so the only effect of work on the Discover server should be an interruption in calls available for processing.
- If users are performing evaluations or creating evaluation or survey forms, all unsaved changes are lost.
- Scheduled processes (e.g., archiving, report generation) can be affected by shutdowns. Administrators need to be aware of when these processes occur and may want to schedule shutdowns accordingly or reschedule the processes.
- The sequence in which Uptivity Discover applications and modules are started/stopped does not matter.

### Shut Down Discover Services

To shut down Discover applications and services prior to a scheduled server shutdown or restart:

1. Follow the procedures for stopping services as described in [Start/Stop Discover Services](#).
2. If any Uptivity Discover applications were not run as services or are not managed from **Service Manager**, log onto the desired server through Windows and use Task Manager to stop them.
3. Shut down the server, or perform desired tasks (e.g. Windows updates) that will require a server restart.

When the server is restarted, the Discover applications and modules should restart and function normally. After any server restart:

1. Open a command prompt and start any desired services that are not managed from **Service Manager**.
2. Follow the procedures for starting services as described in [Start/Stop Discover Services](#).
3. Confirm that call recording and all other functions are operating normally.

## Anti-Virus Protection

inContact recommends anti-virus exclusions be configured in any system where anti-virus scanning is installed. These guidelines will assist with ensuring the reliability and performance of the Uptivity Discover system, while still providing for a secure environment. A lack of exclusions can cause system performance issues and possibly contribute to service outages.

These guidelines apply to both memory-resident and on-demand scanning.

### Exclusion Guidelines

The table below lists recommended exclusions for each service or application. Any paths or ports shown in this document are the installation defaults only. Actual paths or ports may vary depending on configuration options set during installation.

Service/Application	Process	File, Extension, or TCP/IP Port	Default Folder
<b>Logger Service</b>	cc_loggerservice.exe	*.log	C:\Program Files\CallCopy\Logs\
<b>CTI Core</b>	cc_cticore.exe	*.cca, *.wav, *.vox, *.vox8, *.xml	C:\default_rec

## Appendix: Uptivity Discover Best Practices

<b>Transcoder</b>	cc_Transcoder.exe	*.cca, *.vid, *.wav, *.vox, *.vox8, *.csa, *.ccp	C:\temp\Transcoder-temp
<b>Speech Analytics</b>	cc_analytics.exe	*.wav, *.idx	
<b>Screen Recording</b>	cc_screencapsrv.exe	*.vid	C:\temp\

### Common File Types

Below are many of the common file types associated with Discover.

File Type	Description
<b>.cav</b>	Uptivity Discover proprietary combined audio/video format generated only when a file is exported. Requires a special player, which is included with every Uptivity Discover installation and which can be copied to a shared location for general access.
<b>.cca</b>	Discover raw audio pre-transcode, typically deleted after transcoding and compressed into .wav.
<b>.ccp</b>	Waveform that accompanies playback in the web player. Does NOT contain bookmarks; those are inserted at time of playback via stored database records. Blackouts are represented in the waveform as flat segments with no audio present.
<b>.csa</b>	Discover stereo audio, typically deleted after transcoding and compressed into G729 .wav format.
<b>.idx</b>	Phonetic index of the recorded call created and used by the speech analytics engine. This is an Aurix proprietary format.
<b>.log</b>	Log files where system activities and errors are recorded. Useful in troubleshooting system issues.
<b>.vid</b>	Screen recording data for playback.
<b>.vox</b>	Compressed audio format for playback. Higher quality than .wav, but also larger file size. Mostly a legacy format now.
<b>.vox8</b>	Compressed audio format for playback. Higher quality than .wav, but also larger file size. Mostly a legacy format now.
<b>.wav</b>	Compressed audio format for playback.
<b>.xml</b>	Used to store call metadata or API responses to clients.



## Additional Anti-Virus Considerations

The exclusion guidelines listed above are product-specific for the applications shown. For other applications it is often necessary to determine exclusions on a case-by-case basis. The section below provides some guidance in this area.

Files should typically be excluded based on the following criteria:

- **Locked Files:** Includes any files permanently locked open by a legitimate server process. Examples: databases such as DHCP and SQL Server, the Windows Pagefile, etc.
- **Large Files:** Any files manipulated often by a legitimate server process and typically large in size. Example files and processes: copying CD/DVD images (.iso), offline maintenance of Virtual Machine Files (.vhd), offline maintenance on Exchange Server databases.
- **Temporary Files:** Any temporary files written to disk by a legitimate server process.

## Appendix: File Encryption in Uptivity Discover WFO

This appendix provides an overview of encryption, an optional feature in Uptivity Discover. If encryption was not included with your system at installation, and you would like to add this feature to your system, contact Uptivity Discover Support.

Discover can support file level encryption for almost all audio and video data files (the exceptions are noted below). Files are encrypted as they are written to disk using AES-256-bit encryption. This provides full end-to-end protection, as files are never left on disk in an unencrypted format.

Encryption is based on a unique key generated for each individual system, typically by the Uptivity Discover installation team. If encryption is enabled on an existing system, enabling it only encrypts new files as they pass through the transcoder. Existing recording files can be encrypted using a tool available to Uptivity Discover Support personnel. Contact Support for more information.

Encryption exceptions include:

- ShoreTel TAPI/WAV recording generates unencrypted .wav files. Since Discover relies on a third-party library to generate these files, the application cannot encrypt them while they are writing. However, the Discover Transcoder module will convert the files to an encrypted format if/when they are transcoded.
- XML files that contain call metadata are not encrypted. However, these files are not required. To turn off .xml file generation, contact Uptivity Discover Support.

If the database becomes unavailable while a Core service is running, encryption will continue operating. However, Core services that utilize encryption cannot be started or restarted without a connection to the database. For security reasons, encryption keys cannot be stored locally to allow for this.

## Encryption Best Practices

- **Never** delete keys from the database.
- If a key is lost, any files encrypted with that key will be completely inaccessible.
- Whenever you generate a new key, export it using the `cc_crypt.exe` utility. Keep the exported file in a secure location that is backed up regularly. This will help guard against possible loss of data.
- To disable encryption, consult Uptivity Discover Support to deactivate all active encryption keys via `cc_crypt.exe` commands or database manipulation. All audio and video files generated thereafter will not be encrypted. However, audio and video files generated while encryption was enabled can no longer be played unless the appropriate encryption key is reactivated. Attempting to play such a recording results in an error.
- Do not deactivate keys when there are active files using those keys. Wait until any files with that key have been removed due to archiving.

## About Thales Encryption vs. Standard Key Management

Discover can integrate with Thales Encryption Key Management, a system that provides similar functionality to Discover Encryption key management. For a more detailed explanation on the hardware, software, and configuration of the Thales platform's functionality, see the *Uptivity Discover Thales Encryption Technical Brief*.

When determining whether to use Thales or the built-in functionality of Discover, consider the structure of the encryption system:

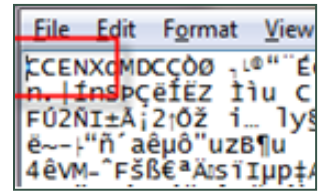
- In Discover, the Primary Key is stored in either a DLL or ASCII text file. In Thales, the Primary Key is in a data store attached to a Thales box. This key is used to decrypt...
- The Database Key(s), stored in the Discover database, which are used to decrypt...
- The File Key, stored in the header of the encrypted file.

If the Primary Key becomes corrupt or lost, it can be easily replaced or changed if in the Thales or ASCII text file format. If the key is stored as a DLL, the file will have to be decompiled, updated, recompiled, and replaced in the system. Both Thales and the Discover ASCII text file option offer a similar level of flexibility. The main difference is the extra hardware, cost, and configuration required when integrating Thales into the Discover environment.

## Verify File Encryption

To determine whether a particular recording file is encrypted, open the file in Notepad. If the file is encrypted, the letters "CCENX" will appear right at the beginning.

If the file is not encrypted, those characters will be missing.



# Appendix: Uptivity Discover Screen Recording Administration

This section contains knowledge and procedures related to the optional Uptivity Discover Screen Recording component. If screen recording was not included with your system at installation, and you would like to add this feature to your system, contact Uptivity Discover Support.

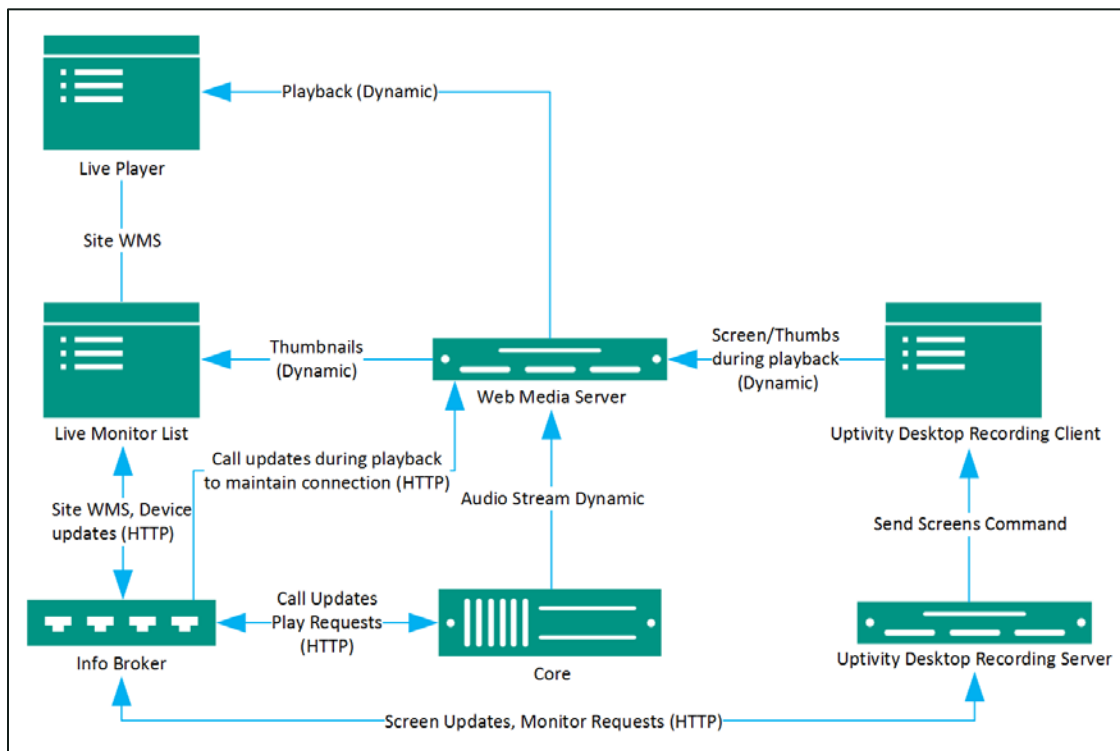
## Screen Recording Overview

Uptivity Discover Screen Recording is a client/server system application that:

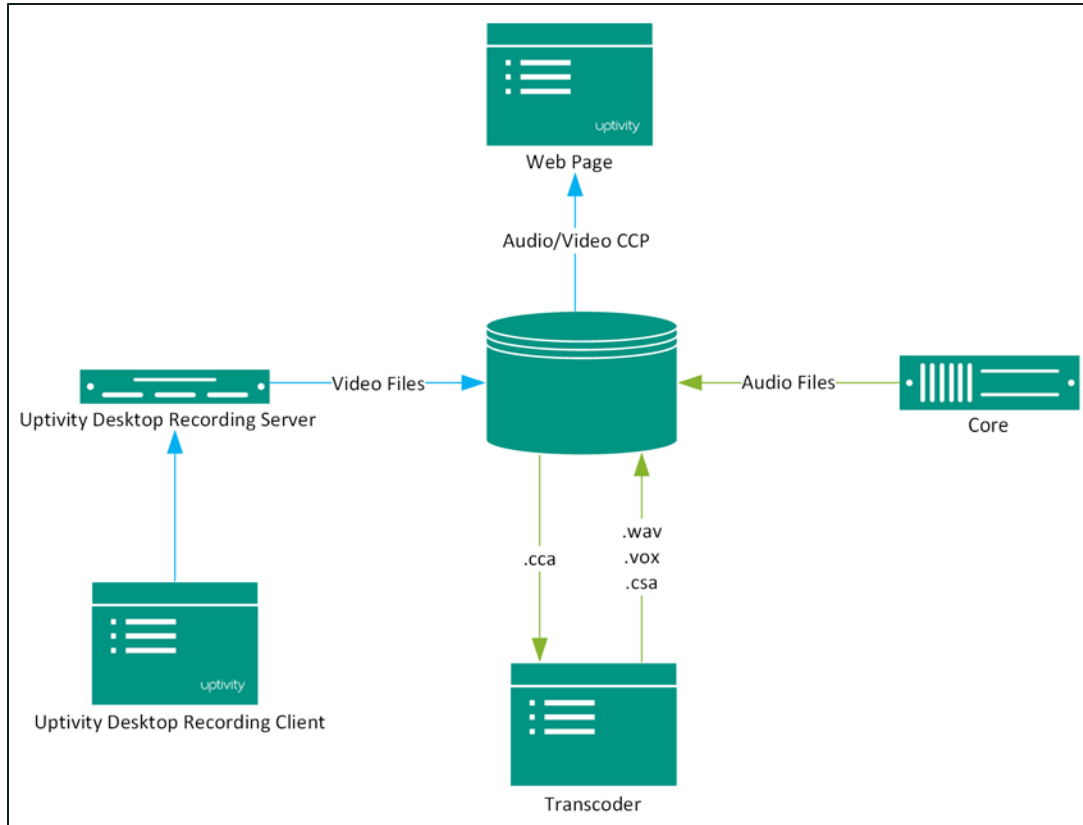
- Captures video and application-window data from Windows workstations and collects video data into VID files that can be played back along with recorded audio for a call.
- Enables live monitoring of user desktops.

These diagrams illustrate the system components involved in the functions stated above. The table that follows provides additional details.

### Live Monitoring of User Desktops



### Screen Recording of User Workstations



Component	Function
<b>Screen Recording Client</b>	Installed on the agent's computer. Sends desktop images and other information to Web Media Server and Screen Recording Server.
<b>Web Media Server (WMS)</b>	The client must connect to the WMS. WMS works with other components to deliver images and agent status information. Used for live monitoring and other features.
<b>API Server</b>	Provides initial state of the client to the WMS.
<b>Information Broker</b>	Manages traffic and requests between components. Allows for load balancing of screen recording and live monitor processes.
<b>Discover Database</b>	Provides WMS with the list of agents used to determine who can and should be monitored.
<b>Discover Core</b>	Delivers call audio, which the WMS matches with the desktop images.

## Appendix: Uptivity Discover Screen Recording Administration

<b>Web Portal Live Monitor List</b>	Displays list of agents that can be monitored. Plays audio and desktop images.
<b>Screen Recording Server (SRS)</b>	Captures video from the client and writes it to the file system. Manages connection to the client.
<b>File System/Disk</b>	Storage location for video files and audio files.
<b>Transcoder</b>	Converts that raw audio files (.cca) to WAV file formats.
<b>Web Player</b>	Discover Web Portal page used by supervisors and agents to review recorded call audio and video.

### Considerations

During the sales process, an Uptivity Discover sales engineer works with your organization to determine the best way to implement the software. The number of users/agents is a key issue. Growth in the number of agents affects performance and may necessitate changes to the implementation design.

Determining the number of users that can connect to the WMS(s) and SRS(s) is complicated due to the different combinations of Discover services that can be run from a single server. In a standalone configuration, where the WMS or SRS is the only Discover service installed (except for the Loader and Logger services which are standard on every server), there can be a *maximum* of 750 simultaneous connections and 300 active concurrent screen recording or playback sessions.

### Security and PCI Compliance

Interactions between Discover suite components (e.g., servers, Web Portal), file servers, and archive devices can use SSL and TLS for data in transit, and the data can be encrypted to disk when written. For more information, see [Appendix: System Security in Discover](#) and [Appendix: File Encryption in Uptivity Discover WFO](#).

## About the Screen Recording Server

**Screen Recording Server**(s) are typically configured as part of the installation process. This section will help you understand the settings that govern its operation. Do not change these settings without contacting Uptivity Support.

### Screen Recording Server Settings

- **Host:** IP address of the Screen Recording Server.
- **Port:** Communication port used by the Screen Recording Server.
- **HTTP Port:** Port used for messaging traffic with Info Broker. The default value is 2014.
- **Write to Temp:** Enabled when the Screen Recording Server is not local to the recording location.
- **Default Temp Location:** Location for temporary video files written by the server.
- **Raise Error on Start Fail:** When enabled, an error level notification is generated every time the server cannot initiate a recording with a client.
- **SSL Certificate Name:** Enter the certificate filename.
- **SSL Certificate Pass:** Enter a password if the certificate is not in the IIS store and Discover needs to load it.
- **Screen Capture Path:** Enter the path where screen captures will be stored.
- **Location:** Location with which this Screen Recording Server is associated.

## Configure Workstation Mapping

In most cases, you do not need to take special steps to ensure Discover records the correct workstation for each user. By default, Discover looks at the system username (i.e. the Windows login) in a user's profile, compares it to logged-in usernames reported by Screen Recording clients, and matches the workstation to the user accordingly.

In situations where this lookup fails or cannot be used (e.g., Windows usernames are not unique for each agent or the software fails to report the correct username), Discover supports an alternate method of statically mapping a phone extension (Device ID) to a Windows workstation name. However, if usernames are not unique, the following features will not work correctly:



- Live Monitoring
- Screen Recording Reporting
- Timed Schedules
- Screen Recording Desktop Analytics
- System Status – Screen Recording Agent Report
- "Current application" reporting based on user, seen in Clarity's real-time display and the System Status page

To enable static workstation mapping:

1. Click the **Administration** tab and expand **System Settings** in the left navigation menu.
2. Click **Workstations Settings** and then click **Add**.
3. In the **Device ID** field, enter the phone extension associated to the workstation.
4. In the **Station** field, enter the Windows workstation name or its IP (if static).
5. Click **Save**.

To delete a single entry from the list:

- Select the station and click the  icon.

To delete all entries from the list

- Click the **Delete All** button at the top right.

### Import Workstations (Optional)

You can add multiple workstations simultaneously by importing them. This function appends a list of workstations to the end of the current Workstations list.

To import a workstation list, you must create a Comma Separated Value (.csv) file in the following format:

```
Workstation, Port
```

**Note:** The on-screen instructions state that the format should be "Workstation, Port, LocationID". LocationID is needed only if "Allow Lookup by Agent / Workstation" is enabled. If this setting is not enabled, do not include LocationID in your file.

## Appendix: Uptivity Discover Screen Recording Administration

An example of this file would be:

```
Wkstation01,1234
Wkstation02,2222
Wkstation03,2345
Wkstation04,4321
```

To obtain Location IDs:

- Click the **Administration** tab and expand **System Settings** in the left navigation menu, then click **Locations Settings**.

To import a CSV file containing workstation data:

1. Click the **Administration** tab and expand **System Settings** in the left navigation menu.
2. Click **Workstations Settings** and then click **Import Workstations**.
3. Click **Browse**, then locate and select your CSV file.
4. Click **Upload File** and then click **Import Now**.

### About the Screen Recording Client

The Screen Recording Client must be installed on every workstation to be recorded.

If you are upgrading from a previous version of Discover, Screen Recording Server v5.5 will not be backward-compatible with installed screen recording clients older than v5.4. In addition, Screen Recording Clients v5.4.x.1339 or higher are labeled "Uptivity Screen Capture" in Add/Remove Programs, and are installed to Uptivity instead of CallCopy directories.

For these reasons, uninstall any earlier version of the Screen Recording Client before installing a new version. You can do this through the Windows Add/Remove Programs functionality in the Control Panel. The software will be labeled "CallCopy ScreenCapture Client Software".

### Configure User Accounts for Screen Recording

Users running Screen Recording must have their Windows network ID in the System Username field of their Discover user accounts. Each user must have a unique username, even if the users are on different Windows domains.

See the *Discover by Uptivity Administration Manual* for explanation of these fields.

## Install the Screen Recording Client

The Uptivity Screen Recording Client installer can be obtained from any Discover server by browsing to the C:\Program Files (x86)\CallCopy\Installers\ folder. The application installer is named "Screen Capture Client Installer.msi".

To install the screen recording client on a user workstation:

1. Copy the installer to the workstation and double-click the installation MSI file.
2. Click **Next**.
3. Select the check box to accept the License Agreement and click **Next**.
4. On the Custom Setup page, set the directory where the client software will be installed by clicking the **Browse** button and selecting a folder. To verify the workstation has enough disk space to install the software, click the **Disk Usage** button.
5. Click **Next**.
6. Enter the IP addresses of all Screen Recording servers for the Location where the client will reside and then click **Next**. If more than 10 servers exist in a Location, more can be added via the Screen Recording Client's INI file.

Screen Capture Server	IP Address
Screen Capture Server 1:	10.100.10.40
Screen Capture Server 2:	Not Configured
Screen Capture Server 3:	Not Configured
Screen Capture Server 4:	Not Configured
Screen Capture Server 5:	Not Configured
Screen Capture Server 6:	Not Configured
Screen Capture Server 7:	Not Configured
Screen Capture Server 8:	Not Configured
Screen Capture Server 9:	Not Configured
Screen Capture Server 10:	Not Configured

7. Click **Install**.
8. Click **Next** when the **Status** bar indicates installation is complete and then click **Finish**.

## Appendix: Uptivity Discover Screen Recording Administration

The client will not run until either the user's workstation is restarted or the client is manually started.

To manually start the client:

- Navigate to the directory in which it was installed and double-click the file **CC\_ScreenCapClient.exe**.

### About Silent Options for Client Installation

The client installer also has options to install silently, with no user intervention required or allowed. The installer uses standard Windows Installer options available by running the "**msiexec.exe**" application.

```
Install Options

</package | /i> <Product.msi>

    Installs or configures a product

/a <Product.msi>

    Administrative install - Installs a product on the network

/j<u|m> <Product.msi> [/t <Transform List>] [/g <Language ID>]

    Advertises a product - m to all users, u to current user

</uninstall | /x> <Product.msi | ProductCode>

    Uninstalls the product

Display Options

/quiet

    Quiet mode, no user interaction

/passive

    Unattended mode - progress bar only

/q[n|b|r|f]

    Sets user interface level
```

## Appendix: Uptivity Discover Screen Recording Administration

```
n - No UI

b - Basic UI

r - Reduced UI

f - Full UI (default)

/help

Help information

Restart Options

/norestart

Do not restart after the installation is complete

/promptrestart

Prompts the user for restart if necessary

/forcerestart

Always restart the computer after installation
```

Using these parameters, you can install the software automatically and require the computer to be restarted after. An example command for that configuration would be:

```
Msiexec.exe /i "C:\CallCopy ScreenCap Client Installer.msi" /passive /forcerestart
```

This command must be run from the command prompt to process properly. If the silent install is used with default settings, the configuration settings will not be set to connect to any server. The configuration files must be modified afterwards, or the MSI package will need to be extracted and the configuration file replaced. Ask your Uptivity Discover WFO installation team for assistance.

## Configure the Screen Recording Client INI File

The client settings are stored and read from a configuration file that is stored in the client installation directory. The file is named **CC\_ScreenCapClient.ini**. The INI filename should always match the name of the executable it configures. This file contains the settings configured during installation, and advanced settings used for adjusting screen capture performance in different environments.

In most cases, you will not need to make any changes to the INI file. However, there may be times when you are asked to do so under the supervision of Uptivity Support.

For reference, Screen Recording Client INI settings and their default values (if applicable) are shown on the left in this table, with additional explanation of the settings detailed on the right.

[app-settings]	
<b>delay=0</b>	Specifies the delay in seconds before the client begins recording.
<b>log_level=info</b>	Specifies the application logging level. The "debug" level gathers more client information but may cause performance issues.
<b>use_logging=1</b>	Specifies whether to use client application logging. Set to 1 to enable, 0 to disable.
<b>priority=belownormal</b>	Specifies the priority for the client process. Possible settings, from highest to lowest are: realtime, high, abovenormal, normal, belownormal, low. Increasing priority may result in better screen recording performance, but will utilize more system resources.
<b>create_form=0</b>	When enabled, a console window is displayed when the client runs. This should only be enabled during active debugging or troubleshooting. 1 = Enabled, 0 = Disabled.
[server-settings]	
<b>Number_screencap_servers=1</b>	Specifies the number of Screen Capture Servers to which the client will connect.

## Appendix: Uptivity Discover Screen Recording Administration

Screencap_host1=127.0.0.1	IP address of first Screen Recording server. If more than one is present, add a setting for host2=, host3=, etc. Multiple hosts may be needed for redundancy or load balancing.
screenap_port1=5633	TCP Port used to connect to first Screen Recording Server. If more than one is present, add a setting for tcp-port2=, tcp-port3=, etc.

## Appendix: Uptivity Discover Screen Recording Administration

[capture-settings]	
<b>Custom_capture=0</b>	Optional setting that allows capturing a fixed resolution portion of the screen, the values for which are specified in the settings below. Useful in certain environments where issues persist with capturing specific resolutions. For example, if the settings are configured as left = 0, right = 1024, bottom = 768, top = 0, the top left 1024x768 pixels of the screen would be captured. For this setting, 1 = Enabled, 0 = Disabled.
<b>custom_capture_left=0</b>	Specifies the left border setting in pixels if using custom capture.
<b>custom_capture_right=0</b>	Specifies the right border setting in pixels if using custom capture.
<b>custom_capture_bottom=0</b>	Specifies the lower border setting in pixels if using custom capture.
<b>custom_capture_top=0</b>	Specifies the upper border setting in pixels if using custom capture.
<b>capture_frequency=1000</b>	Specifies the time in milliseconds between screen captures. Increasing this value results in smaller screen capture files. Do not set below 1000.
<b>livemon_capture_frequency=5000</b>	Specifies the time in milliseconds between Live Monitor screen captures. Decreasing frequency improves performance but provides screen updates less often.
<b>width_slices=1</b>	Settings used to determine how portions of screen data are collected. If width is set to 1 and height is set to 10, data is captured as 10 vertical slices and 1 width slice. Generally these settings do not need to be changed.
<b>height_slices=10</b>	
<b>use_mirror=0</b>	When enabled, this setting forces the client to use a mirror driver as opposed to the standard bitblt driver for capturing screens. Only enabled if drivers for bitblt are not used or available in your environment. 1 = Enabled, 0 = Disabled.



## Screen Recording Troubleshooting

This section outlines a variety of considerations and procedures that can be helpful in troubleshooting screen recording issues.

### Laptops, New Monitors, Projectors, Changing Resolution

Changes such as plugging in additional monitors/projectors, changing the screen resolution, and docking/undocking a laptop affect the Screen Recording Client's performance. When a user's computer starts, the client is initialized, and the screen recording area including the number of display devices is detected. Changes to the capture area are not detected automatically. Problems can be minimized by following these recommendations:

- If a new display device (monitor, projector, etc.) is plugged into a computer, the computer must be restarted.
- If a laptop uses a docking station and monitor, it must be docked before it is started in order for the client to detect the monitor.
- If a laptop is undocked without powering down and then docked later, it must be restarted.

### Multiple Monitors and USB Adapters

Uptivity Discover Screen Recording supports capturing from computers using video cards and monitors in these configurations:

- Monitors using portrait and landscape layouts.
- Multiple monitors placed side-by-side horizontally.
- Multiple monitors stacked vertically.
- Multiple monitors arranged both horizontally and vertically (e.g., two vertical rows of three monitors).
- Multiple monitors connected to multiple video cards.

There is no limit to the number of monitors that can be recorded. For monitors connected via a USB adapter, the Screen Recording Client does not support vertically stacked monitors.

### **Desktop Background Images**

inContact strongly recommends that user desktop backgrounds be one solid color. Background patterns, logos, themes, and pictures dramatically increase the size of the video file. Larger files consume disk space and make call playback slower and choppy.

### **System Events and Screen Recording**

Screen recording behavior can be affected by system events like starting screen savers, locking desktops, and logging on or off the system. This section explains how screen recording reacts to these scenarios. Behavior is the same for Windows 7 and Windows XP except where specifically noted.

#### **General Operation**

The Screen Recording Server always keeps track of the time of its last communication with each client. If a client stops sending data, the Screen Recording Server repeats the last frame it received until the client starts sending new data again.

If the Screen Recording Server has not received any communication from a client for two minutes, it stops the video recording and unlocks the video file. It also marks the Screen Capture field for that recording as "Closed Due To Inactivity," meaning that the video is assumed to be erroneous and the Web Player will not attempt to play the video, though the video itself is intact. Live Monitoring is not affected by this timeout.

#### **Logging Off, Restarting, and Shutting Down**

When a user shuts down, restarts, or logs off their computer, the client stops sending data. When this happens, the Screen Recording Server inserts the last frame it received into the video until the two-minute timeout is reached.

If the call ends before this timeout is reached, the video for the recording is marked as valid. If the timeout is reached before the call ends, the screen capture is stopped and the video file is closed and marked "Closed Due To Inactivity." The timeout causes the Screen Recording Client to lose its state, meaning that even if the call is still active, screen capture will not resume until the machine is restarted or the user logs in again.

### Switching Users

While the second user account is active, screen capture data is not sent. If the user switches back to the first account, data transmission resumes. If the timeout occurs because no data is sent for two minutes, the video file is closed and marked "Closed Due To Inactivity".

### Screen Saver – Without Login Required

When a screen saver is displayed, the video of the screen saver itself will be displayed in the video file. Screen recording continues working normally, sending the screen shots as they appear to the user.

### Screen Saver – With Login Required

In Windows 7, when a locking screen saver is displayed, the user desktop will continue to be displayed in the video, regardless of the fact that the user cannot see their desktop. This event has no noticeable effect on screen capture, but is still subject to standard timeout parameters.

In Windows XP, while the machine is locked by a screen saver, data is not sent. If the machine is unlocked, data transmission resumes. If the timeout occurs because no data is sent for two minutes, the video file is closed and marked "Closed Due To Inactivity".

### Sleep Mode

While the machine is asleep, data is not sent. If the machine is woken up, data transmission resumes. If the timeout occurs because the Screen Recording Server receives no data for two minutes (including Sleep time), the video file is closed and marked "Closed Due To Inactivity".

### Hibernation

While the machine is hibernating, data is not sent. If the machine is woken up, data transmission resumes. If the timeout occurs because the Screen Recording Server receives no data for two minutes (including Hibernation time), the video file is closed and marked "Closed Due To Inactivity".

### Screen Lock

In Windows 7, when the machine is locked, the user desktop continues to be displayed in the video, regardless of the fact that the user cannot see their desktop.

## Appendix: Uptivity Discover Screen Recording Administration

Essentially, locking the screen has no effect on screen recording, but is still subject to standard timeout parameters.

In Windows XP, while the machine is locked, data is not sent. If the machine is unlocked, data transmission resumes. If the timeout occurs because no data is sent for 2 minutes, the video file is closed and marked "Closed Due To Inactivity".

### Troubleshooting Procedures

If a workstation that has the Screen Recording Client software installed is not being recorded, there are specific troubleshooting steps that can be performed before contacting Uptivity Support.

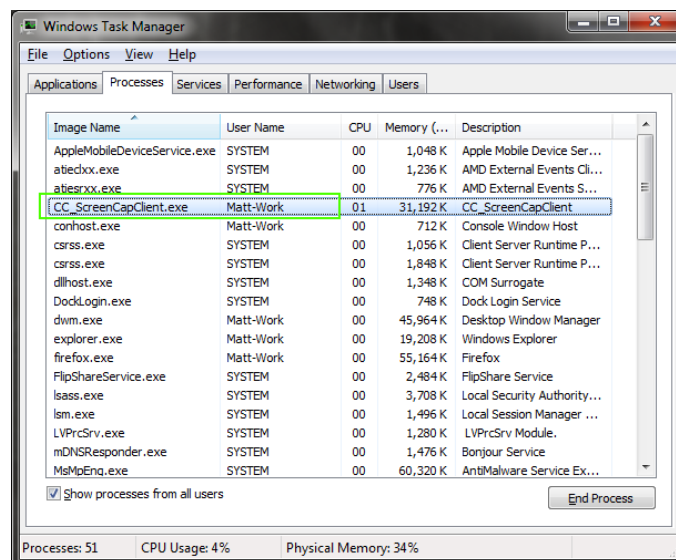
#### Confirm the User Account Configuration

The user's account must be correctly configured to support screen recording. For details, see [Configure User Accounts for Screen Recording](#).

#### Verify the Client is Running

To verify the Screen Recording Client is running on the agent's workstation:

1. Open **Windows Task Manager** on the workstation.
2. On the **Processes** tab, verify the **CC\_ScreenCapClient.exe** process is listed.
3. Verify the process is running under the **User Name** that is currently logged into the computer. Two clients can run under the same user name; this situation commonly occurs in terminal services.



### Check the System Status Report

If the Screen Recording Server is running, the Screen Recording Client status can be viewed from the **System Status** report on the Web Portal. The Agent Status section of the report lists all Screen Recording Clients that are successfully connected to the system.

You must have the **Allow Viewing System Reports** permission to be able to view the report.

To access the System Status report:

1. Click the **Reporting** tab in the Discover Web Portal and expand **System Reports** in the left navigation menu.
2. Click **System Status**.
3. Scroll to the **Agent Status** section at the bottom of the report.

Agent Status						
Status	Last State Change	Computer	Username	IP Address	Port	Version
AVAILABLE	Sep 8 2010 5:01PM	BKNACK-LAPTOP	bknack	10.100.5.12	0	4.3.1.0
AVAILABLE	Sep 8 2010 2:32PM	KKRESS-NEWLAPTO	kkress	10.100.5.232	0	4.3.1.0
AVAILABLE	Sep 8 2010 5:30PM	NSOWERS-LAPTOP	nsowers	10.100.5.20	0	4.3.1.0
AVAILABLE	Sep 7 2010 9:42AM	SEDDY43	Administrator	10.100.5.59	0	4.3.1.0
AVAILABLE	Sep 8 2010 11:42PM	TURBOBEAST	Matt-Work	192.168.1.70	0	4.3.1.0
AVAILABLE	Sep 8 2010 11:42PM	TWILLIAMS-LAPTO	twilliams	10.100.5.41	0	4.3.1.0

4. Verify the desired workstation name is listed in the **Computer** column.
5. Verify the correct user is listed in the **Username** column.
6. Verify the value in the **Status** column is **AVAILABLE**.

If this information is not present for an agent's computer, the client is not communicating to the Screen Recording Server and you will need to investigate and resolve the network/communication issue.

### Obtain Screen Recording Client Logs

If the client is available according to the steps listed above, it may be necessary to contact Uptivity Discover WFO Support for further assistance. Before contacting Support, you should collect the Screen Recording Client log files for use in troubleshooting.

To obtain these logs from the agent workstation:

- Navigate to %APPDATA%\CallCopy\CC\_ScreenCaptureClient\.

The client log files are listed inside, with one log file listed for each date the Screen Recording Client was running. The log files follow a '*yyyymmdd.log*' format (e.g. 20100901.log). Copy these log files so you can forward them to inContact Support for analysis.

## Document Revision History

Revision	Change Description	Effective Date
0	Initial release for this version	2015-02-13