uptivity

an inContact. company

DISCOVER BY UPTIVITY ADMINISTRATION MANUAL, V5.4

April 2014

Reference Guide

www.uptivity.com

Security Classification: Uptivity Confidential.

Distribution: Approved internal Uptivity staff only and licensed Uptivity customers.

Note: Applicable non-disclosure agreements must be in force for authorization.

Revision History		
Revision	Change Description	Effective Date
0	Re-branded for v5.4. Reorganized information where possible for clearer separation of procedures, knowledge and reference information. Added examples and supporting information to cc_Crypt Commands table. Added information on deactivating encryption keys to Encryption Best Practices. Added new Clarity permissions. Clarified relationship between agent PhoneID and Discover Group membership. Added Windows 2012 information to Login Mode Configuration. Corrected Scheduling Operators changing to "IN Test if an identifier is in a bar separated list of values."	2014-04-30

Table of Contents

Introduction

Discover by Uptivity is a workforce optimization (WFO) suite that interfaces with your existing ACD/PBX technology and personal computers. It enables organizations to maximize customer satisfaction by leveraging call recording, quality management, desktop recording, speech analytics, and performance management capabilities.

This manual is for system administrators, application administrators and managers who will be performing the tasks outlined in the table of contents.

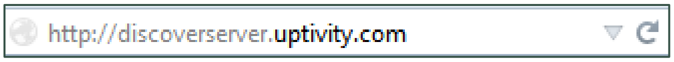
This manual assumes you are familiar with:

- The ACD/PBX configuration relative to the Discover and all relevant settings and identifiers for their location.
- Basic Windows PC usage such as right- and left-clicking the mouse.
- Basic computer networking.

Administrators should also be familiar with information in Discover's guides for installation, reporting, and integration. The *Discover by Uptivity Web Player Manual* covers basic tasks such as navigation and logging into the system.

Most administration tasks are performed in the Discover Web Portal. This portal is deployed during the installation process and can be accessed using either Internet Explorer or Firefox.

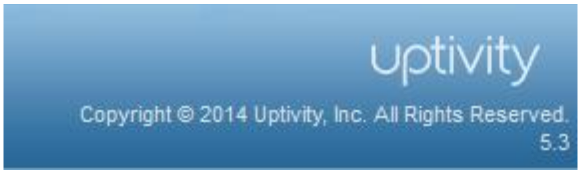
A hostname or IP address for the server will be established so that you may access the Discover Web Portal. If multiple Web Portals are installed in a network, each will have a unique hostname and IP address.



http://discoverserver.uptivity.com

Discover has a default account with system administrator level privileges. The Uptivity Installation team will provide you with the account username and password. It is recommended you change your password from the default provided as soon as possible. If your system is configured to use AD authentication, this account will not be available to you; the Web Portal must be configured to allow either Database or Hybrid Mode authentication.

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



uptivity

Copyright © 2014 Uptivity, Inc. All Rights Reserved.
5.3

Discover allows administrators 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.

Roles & Permissions

Permissions are associated with Roles that are assigned to either users or groups. They define what users can do in the Discover system. **Roles** are attached to users or groups, and specify permissions for those users. 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. Most permissions allow users to do things, but a few On-Demand product permissions prevent a user from doing something.
- 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: DiscoverDefaultAgent. This role cannot be deleted, but its permissions can be edited.
- Roles migrated from earlier versions of Discover (if applicable).
- A Superuser account with all permissions. The Superuser access level is not considered a role. You can grant Superuser access to individual users, but Uptivity 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. Below are two generic plans.

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 that 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 agents' 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

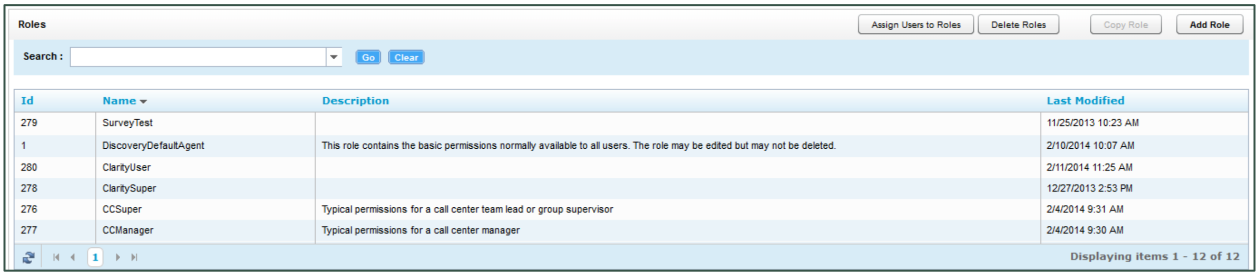
In this scenario, the company now has three locations, and 120 agents who work a variety of shifts. All agents answer calls for the company's products. Some agents answer calls for a new Product X. Another group answers Spanish callers.

- 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 agents' 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 that evaluates 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 the group allows calls for this product to be searched for and reported on in Discover.
- 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 for Discover modules such as On-Demand and Toolbar. Some agents may use these applications while other agents do not. In this situation, creating an On-Demand or Toolbar agent role and assigning it to a few agents maintains the base agent role and allows the flexibility to assign the module-specific role. Similarly, some supervisors may need access to certain reports but not others. Creating one or more supervisor reports roles addresses this need for granularity.

Roles

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.



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

Create a Role

To create a role:

1. Click the **Administration** tab and expand **Permissions** in the left navigation menu.
2. Click **Roles**.
3. Click **Add Role**.
4. Enter a name for the role and, optionally, a description.
5. Select the check box(es) for the permission(s) needed for the role. For more information, see Permissions Definitions.
6. Associate the role with one or more Discover Group(s), ACD group(s) and/or ACD gate(s) if desired. For more information, see Assign Permission to Discover Groups and Assign Permission to a Group or ACD Gate/Queue.
7. 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**.
3. Double-click the name of the desired role.
4. Make any desired changes
5. Click **Save**.

Copy a Role

Copying a role assures consistent permissions assignment. For example, you 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**.
3. Click the role to be copied.
4. Click **Copy Role**.
5. Enter a name for the role.
6. 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**.
6. Click **Back**.

Permissions Definitions

General Administration

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

Allow Password Changes: Allows the user to modify their own password in Discover. If unchecked, a system administrator will have to modify the password for the user.

System Permissions

Allow System Configuration: Allows the user to modify system configuration settings. This is an administrator-level permission.

Allow Recording Record and File Deletes: Allows the user to delete records from the system. This is an administrator-level permission.

Allow Archive Administration: Allows the user to create and edit Archives. This is an administrator-level permission.

Allow Group Administration: Allows the user to create and edit Discover Groups.

Allow Scheduling: Allows the user to set system-wide schedules. Recordings based on system schedules are not governed by the disk quota of the user who created the schedule. This is an administrator-level permission.

Allow API Authentication: This permission is not used.

Coaching Permissions

> **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 to which that user has permission, including their own evaluations. Selecting this option automatically selects the other Coaching permissions. If those permissions are not appropriate for a role, they must be cleared individually.

Allow Deletion of Completed QA Evaluations: Allows users to delete completed QA evaluations for groups to which that user has 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 the specified groups or agents based on either QA evaluation scores or as an *ad hoc* achievement. To award ad hoc achievements, the user 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 that user has permission, including their own evaluations. This permission does not apply to in-progress evaluations. To edit completed evaluations, the user 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 that user has permission. Users with this permission may also serve as arbitrators for dispute resolution involving the 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 that user has permission.

Allow Award Ad Hoc Achievements: Allows users to award an existing ad hoc achievement type to any agent or group to which that user has permission. To add or edit achievement types, the user 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.

Allow Viewing Analytics Reports: Allows users to run analytics reports (requires optional Analytics product).

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 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 optional Survey product)

Player Permissions

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

Allow Viewing All Call Records & QA Evaluations: Allows users to view all call recordings and QA evaluations regardless of Group and/or Gate settings. Uptivity strongly recommends assigning this permission to very few users. For related information, see Coaching Permissions.

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

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

Allow Emailing of Export: Allows users to export and send them to an email address by 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 desktop recordings associated with call records. Also allows live Monitoring of video and video for timed schedules (i.e., screens recorded without associated calls).

Survey Permissions (Survey product required)

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 (Analytics product required)

Allow Analytics View: Allows users to view Analytics data in the Web Portal.

Allow Analytics Administration: Allows users to manage Analytics configuration.

On-Demand Permissions (On-Demand module required)

> **Note** If permissions are changed 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. The additional information 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 *On-Demand Administration Guide*.

Prevent Setting Changes: Prevents users from changing any other settings beside the Logging Level and Device ID/Extension/Voice Port.

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 the user 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.

Allow Desktop Recording: Allows users to start and stop the desktop recording product if it 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 maintain the association of device IDs to workstations. For related information, see Workstations Settings. 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.

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

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

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

Discover Toolbar Permissions (Discover Toolbar module required)

Allow Access Through Desktop: Allows users to load and access the Desktop Discover Toolbar application.

Clarity by Uptivity Permissions

> **Note** These permissions are listed in alphabetical order. They appear only when Clarity is installed along with Discover. In this type of hybrid environment, all roles are managed through Discover. For related information, refer to the "Roles, Permissions, and Accounts" section of the *Clarity by Uptivity Administration Manual*.

Call Off: Allows users to record call offs for themselves or others in Clarity.

Can Be Supervisor: Allows users to be assigned as Supervisors for Clarity Teams. Additional permissions are needed to perform tasks such as approving swaps. Removing this permission causes the user to immediately be removed as a supervisor from all Teams.

Configuration Section: Allows users to do all tasks on the Clarity Configuration tab.

Edit News Widget: Allows users to add, update, and remove items from the Clarity Home page’s News widget.

Employee Create: Allows users to create user accounts in Clarity. Users created in Clarity will appear in Discover when both applications are installed together, even if the creating user does not have Discover's Allow User Administration permission. However, any Discover-related settings (for example, the Agent check box) must be configured in Discover.

Employee Profile All View: Allows users to view Clarity profile information for any user.

Employee Profile Team View: Allows users to view Clarity profile information for employees who are members of a Team for which they are a Supervisor. Also causes those employees to be visible on Schedule Search screen.

Employee Schedule All Edit: Allows users to edit any employee’s schedule.

Employee Schedule All View: Allows users to view any employee’s schedule.

Employee Schedule Team Edit: Allows users to edit the schedules of employees who are members of a Team for which they are a Supervisor.

Employee Schedule Team View: Allows users to view the schedules of employees who are members of a Team for which they are a Supervisor.

Employee Search: Allows users to search for any employee and see those search results. Search results can include Name, Labor Unit, Location, Title, and Team memberships.

Employee Section: Allows users to access the Employees tab in Clarity but not do anything on it. This permission is required in order to have other Employees tab permissions.

Employee Self Edit: Allows users to edit their profile's email account and change their Clarity/Discover password in Clarity.

Forecast Acquire: Allows users to load call history data to create a forecast data set.

Forecast Predict: Allows users to generate a forecast.

Forecast Section: Allows users to access the Forecast tab but not do anything on it. This permission is required in order to have other Forecast permissions.

Forecast Trend: Allows users to create an historical trend line when creating a forecast.

Historical Widgets: Allows the user to add and view historical reporting widgets.

Home Page Widgets: Allows users to add/remove/view widgets from the Clarity Home page.

Leave Request Approval All: Allows users to approve leave requests for any employee.

Leave Request Approval Team: Allows users to approve leave requests for employees who are members of a Team for which they are a Supervisor.

Real Time Widgets: Allows users to add and view real-time reporting widgets on the Real-Time Reports page.

Reports Historical: Allows users to access the Historical Reports page but not add or see the historical widgets.

Reports Processes: Allows users to access the Processes page.

Reports Real Time: Allows users to access the Real-time Reports page but not add or see the real-time widgets.

Reports Section: Allows users to access the Reports tab but not do anything on it. This permission is required to have other Reports permissions.

Roster All: Allows users to view the Real-Time Roster for any Labor Unit or Skill group.

Roster Team: Allows users to view the Real-Time Roster for any Team of which they are a Supervisor.

Schedule Bidding: Allows users to manage agent ranking criteria, bidding schedules, and bidding periods.

Schedule Create: Allows users to create a schedule from loaded forecast data.

Schedule Load: Allows users to load a forecast data set to create a schedule.

Schedule Publish: Allows users to publish a schedule.

Schedule Section: Allows users to access the Schedule tab but not do anything on it. This permission is required to have other Schedule permissions.

Swap Request Approval All: Allows users to approve shift swap requests for any employee.

Swap Request Approval Team: Allows users to approve shift swap requests for employees who are members of a Team of which they are a Supervisor.

Allow Clarity Ad Hoc Reporting: Allows users to view the Ad Hoc Reporting button in Clarity, create ad hoc reports using the Report Builder page, view/edit any ad hoc report that has been saved, and save ad hoc report search criteria as public or private. This permission provides access to all Clarity report data. A user must have permission to the following in order to use the Clarity ad hoc reporting feature: **Reports Section**, **Reports Real Time**, **Reports Historical**, **Reports Processes**. Clarity ad hoc reports can only be accessed through Clarity; they are not available from the **Reporting** tab in Discover.

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 Terminology.

Assign Permission to 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. Groups may be moved from the **Attached** to **Unattached** list, and vice versa, to provide or remove permissions.

Assign Permission to a Group or ACD Gate/Queue

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/queue permissions give a user access to call records and other items created by members of these types of groups. The user also needs relevant Player Permissions, such as Allow Viewing of Video. Assigning permission to a group or ACD gate/queue does not make a user with that permission 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 here, all groups will 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 a group or ACD gate/queue:

1. From your ACD or PBX, identify the desired groups.
2. Follow the procedure to Edit a Role.
3. Enter the group names, exactly as they appear in your PBX/ACD, in the text field below either the **Group** or **ACD Gate** list.
4. Click the ⊕ button and then click **Save**.

To remove a role's access to recordings from a group or ACD gate/queue:

1. Follow the procedure to Edit a Role.
2. Select the desired group or gate from the **Group** or **ACD Gate** list.
3. Click the ✖ button.
4. 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**.
3. Click **Assign Users to Roles**.
4. Click the desired role.
5. 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.
6. 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 the assigned role(s). For related information, see Roles.

User Accounts

Discover allows you to store a variety of information about each user, but only five of the 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. If your system integrates with Active Directory (AD), check with your AD administrator to see if any AD restrictions exist.
- **Password.** There are no default restrictions for passwords. For other password restriction considerations, see PCI Settings under Login, Password and AD Integration Settings.
- **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.
- **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 will select this check box for you. Clearing this option will allow 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.

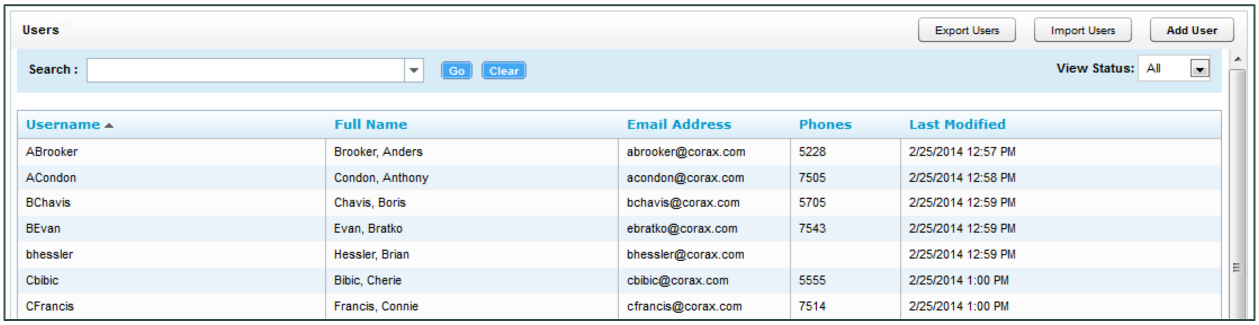
  > **Note** Several additional tasks must be performed in order for an agent's audio to be recorded. For details, see Set Up an Agent to Be Recorded.

- **System Username.** This is the Windows username that the agent uses to log in to the network. This field is required for desktop recording, as Discover uses it to locate an agent's desktop via the Desktop 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.** Required if using Active Directory login method. This field will be auto-populated when using "Auto Create User on Login" or importing users, provided all information is supplied in the import file. For related information, see Login Mode Configuration.

- **Active Directory Domain.** Required if using Active Directory login method. This works independently of the System Domain field above, which is primarily required for desktop recording. This field will be auto-populated when using "Auto Create User on Login" or importing users, provided all information is supplied in the import file. For related information, see Login Mode Configuration.
- **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:** Only appears if "Allow Lookup by Agent/Workstation" is enabled. Allows manual designation of a specific site/location for an agent for proper local routing of Desktop Recording and Live Monitoring traffic. This setting is "Not Set" by default, but an agent cannot be edited and saved without choosing a specific Location. For details, see Workstations Settings.
- **Quota:** This field is no longer used.
- **Shift Times to User's Timezone.** By default, Discover displays time by the time zone of the server on which the system is installed. 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. Discover is installed on a server in the Central US zone. 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.

User List

To see the users in your Discover system, click the **Administration** tab and expand **Permissions** in the left navigation menu, then click **Users**. If your system includes multiple Discover Web Portal servers, this list is relative to the server (i.e., URL) you are logged onto.



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

Use the **Search** field to locate specific users. You can enter all or part of the user's name, and the field will display a list of possible matches.

The **View Status** drop-down list lets you limit your view to Users (i.e. only Users who are not configured as Agents), Agents (i.e., only Users who have the Agent option selected on their accounts), or All (i.e., both).

> **Note** For more information on Discover Agent Sync in Cisco environments, refer to the *Cisco UCCE Integration Guide* or the *Cisco UCCX Integration Guide*, whichever is appropriate for your environment.

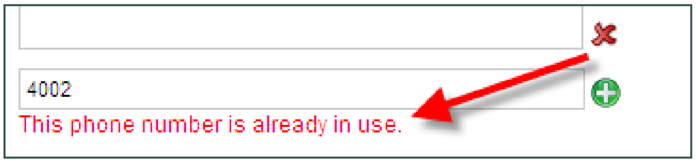
Add a User

> **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 will then have to import the account using the Mass Update Incomplete Users function in Clarity. See the *Clarity Administration Manual* for more information.

To add a user:

1. Click the **Administration** tab.
2. Expand **Permissions** in the left navigation menu and click **Users**.
3. Click **Add User** at the top of the User List.
4. Enter information in all mandatory fields. For more information, see User Accounts.
5. Complete additional fields as desired. For more information, see User Accounts.
6. Select a time display format.
7. Enter the extension(s) and/or login(s) associated with the agent in the lower field under **Phones** and click the green button.
8. 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.
9. Click **Save**.

> **Note** A phone number can be assigned to only one agent. If you attempt to assign a number that is already assigned to another agent, an error message appears beside the Phones box.


4002

This phone number is already in use.

Edit a User

To edit a user:

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

Lock a User Account

By default, users can log into Discover and view the **Home** tab and 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 the company, transfers to another role in the company and no longer needs access to Discover, or is prohibited by the company 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**.
3. Double-click the desired user record.
4. Select the **Account Locked** check box.
5. 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**.
3. Double-click desired user record.
4. Select the **Account Locked** check box.
5. Clear the **Agent** check box.
6. Remove the assigned phone extension(s) under Phones.

   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.

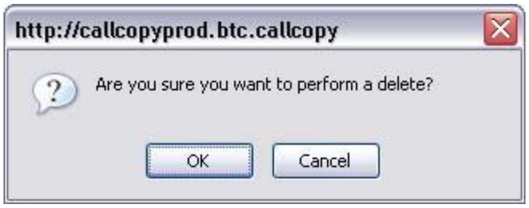
7. Click **Save**.

Delete a User

Users can be deleted from the Web Portal. The account information and call data is retained in the Discover database but cannot be seen in the portal.

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 the **Delete** button in the top-right corner.
5. Click **OK**.



http://callcopyprod.btc.callcopy

Are you sure you want to perform a delete?

Import Users

Users can be imported 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 information can then be imported into Discover, saving time by minimizing data entry tasks.

A 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. This may need to be configured separately for each agent after the import is completed depending on the customer's environment. For more information on Location settings, see Workstations Settings.

Discover will verify the data is in the correct format and the file does not contain any existing agent names, phone IDs, or AD usernames on the same domain if using Hybrid or AD authentication. If duplicates are detected, the file will need to be corrected before attempting the import again.

Notes

- User data can be added or extracted via the Uptivity API. For details, see the *Uptivity API Manual*.
- If agents are being assigned to Locations manually, this data cannot currently be imported through a CSV. Locations must be set manually for agents in that specific configuration.

To import users:

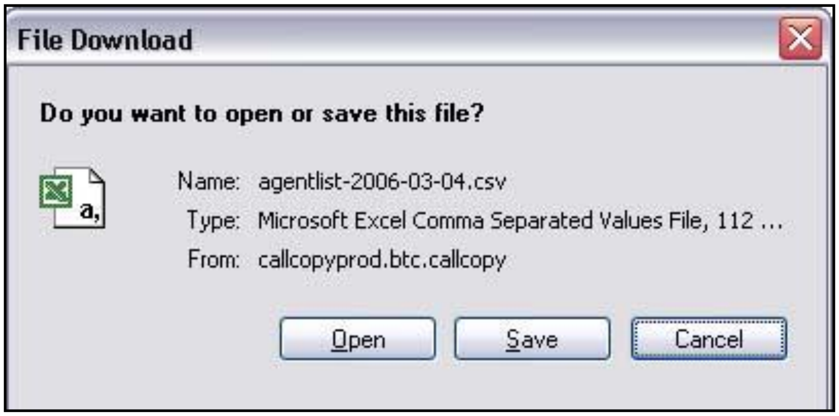
1. Create the CSV file and store it on a local or network drive.
2. Click the **Administration** tab and expand **Permissions** in the left navigation menu.
3. Click Users.
4. Click **Import Users**.
5. Click **Select**.
6. Browse to locate and open the file.
7. If the CSV file has a header row with column labels, select Import file has a header.
8. Click **Upload File**.
9. Click **Import** to create the agents, or review the error message and make the necessary corrections.

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**.
3. Click **Export Users**.
4. Download the file to your local system.


File Download

Do you want to open or save this file?

Name: agentlist-2006-03-04.csv
Type: Microsoft Excel Comma Separated Values File, 112 ...
From: callcopyprod.btc.callcopy

Set Up an Agent to Be Recorded

Several tasks must be performed in order for an agent's audio to be recorded. The specifics of those tasks vary greatly depending on your telephony system and workforce organization. The list below will give you an idea of the required tasks, but is not integration-specific. It also does not include tasks associated with desktop 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 using lookup by agent/workstation. For details, see 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. Audio will be recorded even if there is no extension or agent number specified, but will not be associated with the agent.
- Add the user account to one or more 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.
- If schedules are created for specific users, a new schedule must be created. If an existing schedule is used to record multiple agents (i.e., those in a group or a range of ANIs), review the business rules for the schedule. The new user's extension, ANI, agent number, or other information may need added to the schedule's rules. 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 PBX-specific Discover integration guide 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 PBX-specific Discover integration guide and implement any necessary voice board channel settings.
- Some telephony systems require that the user's extension or device ID be added to a Discover Core's CTI module. Review the PBX-specific Discover integration guide and implement any necessary CTI module settings.
- 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:

- Labor/hunt/skill groups 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 group assignments. Users do not have to be placed in a Discover Group. On the other hand, one user can below to multiple Discover Groups.

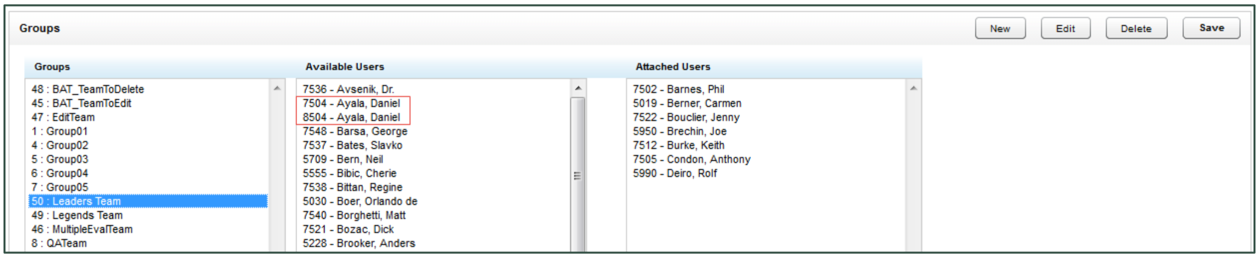
Users can only be added to groups if they have the Agent box selected and at least one phone extension is registered on their user profile. This is because Discover manages group membership based on the agent's phone ID. You can see this in the Discover Group list shown below.

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 groups.

Discover Group List

The Group page displays a list of current groups, available users, and users attached to a group. Click any group to see attached users.



Groups	Available Users	Attached Users
48 : BAT_TeamToDelete	7536 - Avsenik, Dr.	7502 - Barnes, Phil
45 : BAT_TeamToEdit	7504 - Ayala, Daniel	5019 - Berner, Carmen
47 : EditTeam	8504 - Ayala, Daniel	7522 - Bouclier, Jenny
1 : Group01	7548 - Barsa, George	5950 - Brechin, Joe
4 : Group02	7537 - Bates, Slavko	7512 - Burke, Keith
5 : Group03	5709 - Bern, Neil	7505 - Condon, Anthony
6 : Group04	5555 - Bibic, Cherie	5990 - Deiro, Rolf
7 : Group05	7538 - Bittan, Regine	
50 : Leaders Team	5030 - Boer, Orlando de	
49 : Legends Team	7540 - Borghetti, Matt	
46 : MultipleEvalTeam	7521 - Bozac, Dick	
8 : QATeam	5228 - Brooker, Anders	

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.
5. Click **Save**.

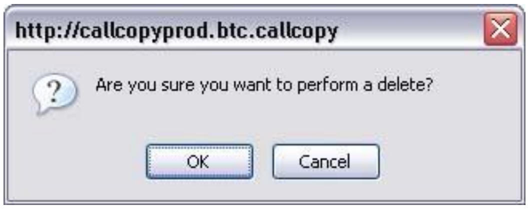
If a Discover Group already exists with the name you have chosen, the following error will be generated: "That group name already exists! Change the group name and try again."

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**.
3. Click the group name.
4. Click **Delete**.
5. Click **OK**.



Are you sure you want to perform a delete?

Add/Remove Agents in a Discover Group

1. Click the **Administration** tab and expand **Permissions** in the left navigation menu.
2. Click **Groups**.
3. Click the desired group.
4. 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. Use the Control or Shift keys to select more than one user at a time.
5. Click **Save**.

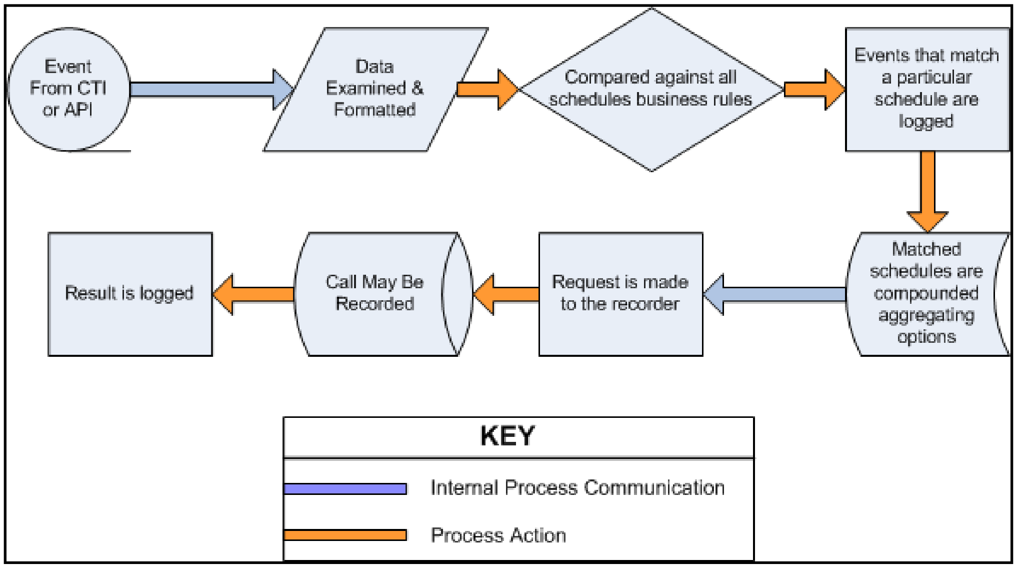
Scheduling

> **Note** Typically, Archive Actions should be created before schedules are created.

Schedules control which calls are recorded. Administrators create schedules based on business rules. 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.

Scheduling Process Flow


Event From CTI or API
Data Examined & Formatted
Compared against all schedules business rules
Events that match a particular schedule are logged
Matched schedules are compounded aggregating options
Request is made to the recorder
Call May Be Recorded
Result is logged
KEY
Internal Process Communication
Process Action

Every event that is 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.

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. The call is then sent to the recorder with the aggregated values assigned to it, and the recording is then written to the system disk.

> **Note** Schedules operate inside the constraints of the configured Voice Boards. When you configure schedules, keep factors such as recording capacity (fixed or concurrent) in mind.

Schedules and Recording Cores

Schedules can be related to a Recording Core but do not have to be. If no schedules are related to a Core, that Core will use all schedules. If one or more schedules are related to a Core, that Core will use only those schedules. Relating schedules to one or more Cores can be useful if:

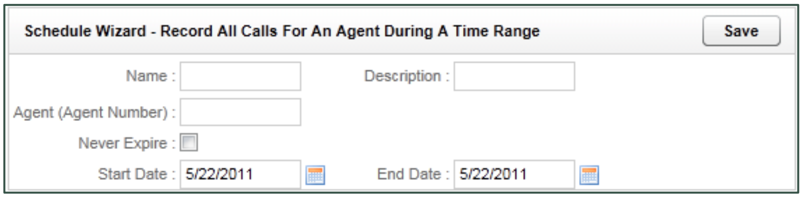
- You want a specific Core(s) to record specific agents' calls, such as agents dedicated to a customer or language.
- You want to balance the load of calls recorded by each Core.
- If in a Syntellect environment and use Schedule States see KB# 000002078.

Initial Core and Schedule configuration is done by the Uptivity Installation Team. See the Discover integration guide for your specific PBX for information on configuring the Core and relating a schedule.

Agent Schedules – Time-Based

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

To create a time-based agent schedule:



Schedule Wizard - Record All Calls For An Agent During A Time Range

Start Date : 5/22/2011

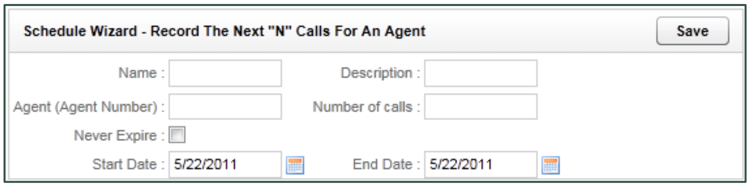
End Date : 5/22/2011

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**. The schedule begins recordings on the entered start date.

Agent Schedules – Number-of-Calls Based

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

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



Schedule Wizard - Record The Next "N" Calls For An Agent

Name :

Description :

Agent (Agent Number) :

Number of calls :

Never Expire : □

Start Date : 5/22/2011

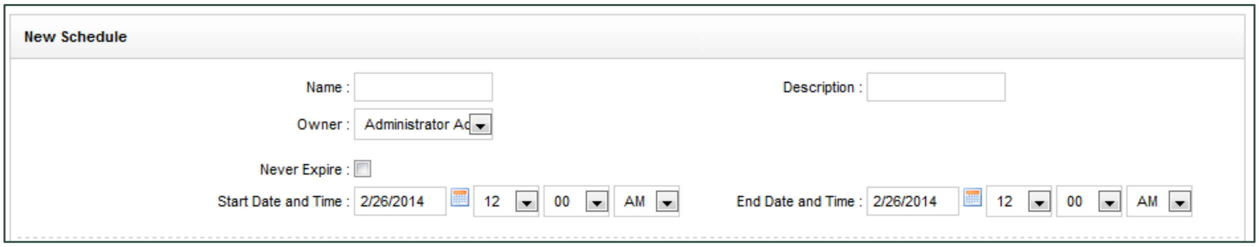
End Date : 5/22/2011

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**. The schedule begins recordings on the entered start date.

Custom Agent Schedules

A custom schedule enables you to create diverse sets of schedules based on a wide variety of criteria to meet your business needs. All of the 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 will be recorded. Otherwise, the call is skipped.

Custom Schedule Criteria Fields



New Schedule

Name :

Description :

Owner : Administrator Ad

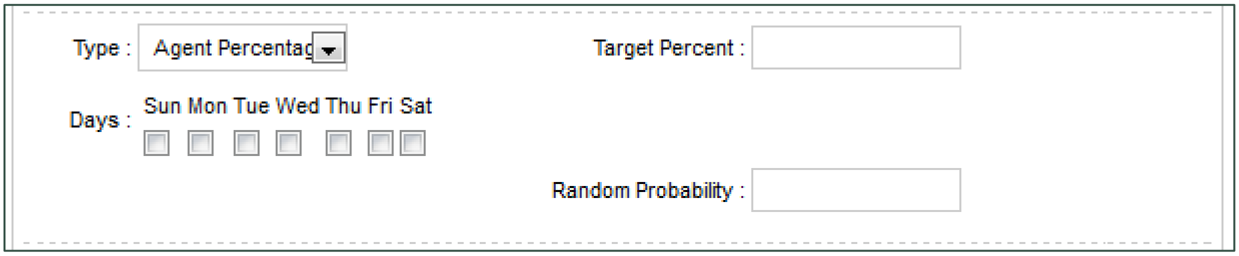
Never Expire : □

Start Date and Time : 2/26/2014 12 00 AM

End Date and Time : 2/26/2014 12 00 AM

- **Name.** Schedule names do not have to be unique, as each is given an internal ID number. Required.
- **Description.** Allows you to provide additional information about the schedule in the Schedule List. Optional.
- **Owner.** From the drop-down list, select the person who should be contacted regarding changes to the schedule. Select Administrator if no specific owner exists. Required
- **Never Expire.** Select this check box if the schedule should remain in effect until the specified number of calls is reached.

- **Start/End Date/Time:** Use the date and time selectors if the schedule should only be effective within a range of dates.



Type : Agent Percentag ▾

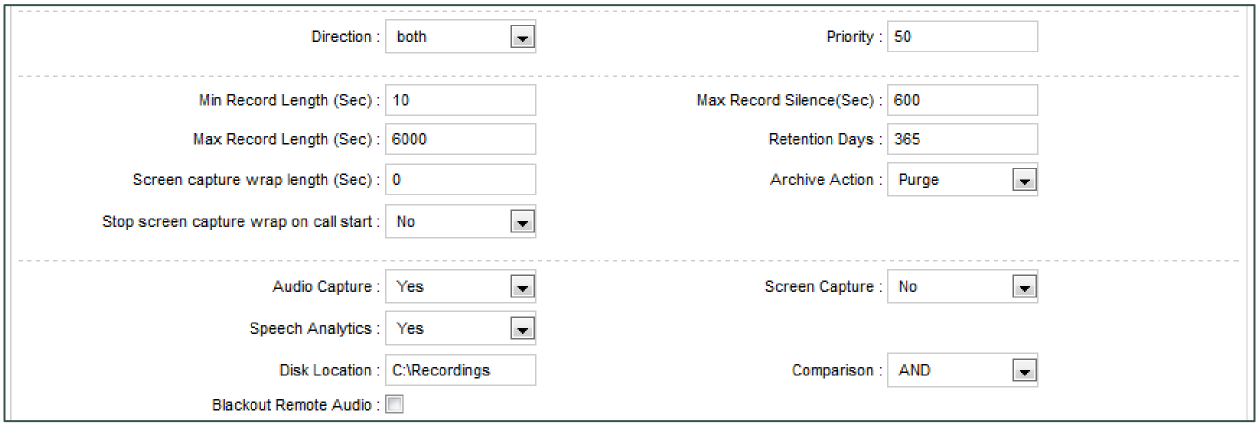
Target Percent :

Days : Sun Mon Tue Wed Thu Fri Sat
□ □ □ □ □ □ □

Random Probability :

- **Schedule Type.** 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. Options specific to this schedule type are:
    - **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. Simply enter the percentage of calls that you would like to record. Use a number below 100 for randomized recording for quality assurance. Set a schedule to 100% for complete call logging. Options specific to this schedule type are:
    - **Target Percent**: The percentage of calls to be recorded out of the total number delivered.
    - **Random Probability.**
- **API Initiated.** This schedule type will only be run if the call delivered was triggered by a 3rd Party application via the Uptivity API. This is useful for defining different rules for these calls vs. internally generated calls via CTI or passive methods. Options specific to this schedule type are:
    - **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 will only be run if a delivered call was triggered via the Discover On-Demand Client. Options specific to this schedule type are:
    - **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 record a percentage of every agent's calls. Simply enter the percentage of calls that you would like to record (1-100). 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. Options specific to this schedule type are:

- **Days.** Select the check boxes for the 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 :	□		

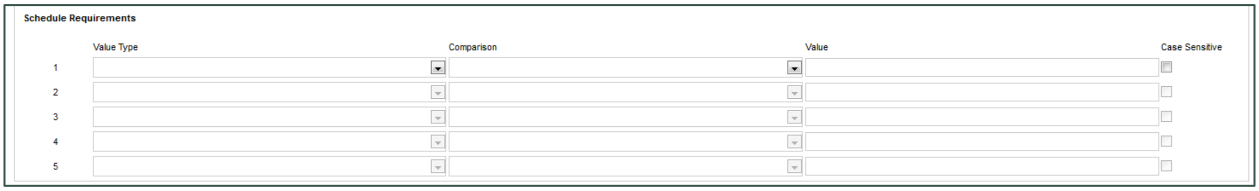
- **Direction.** If the data is available, you can specify to record only inbound/outbound calls, or both.
- **Priority**. Schedules can be given a priority rating from 1 (lowest) to 100 (highest). If a call is delivered that matches multiple schedules, the schedule with the highest priority will be used. If all matching schedules have equal priority, then the schedule with the oldest creation date will be used.
- **Min Record Length (sec).** The minimum length, in seconds, for records matching that schedule. You can use this setting to avoid recording hang-ups.
- **Max Record Length (sec).** The maximum length, in seconds, for records matching that schedule. Longer calls require more disk space, so some companies prefer to cap the recording length to prevent long calls from depleting system resources.
- **Max Record Silence (sec).** The maximum length, in seconds, for silence in the call before a recording is automatically stopped.
- **Screen Capture Wrap Length.** The duration (in seconds) to keep recording an agent's screen after a call has ended. Only available if the optional Uptivity Desktop Recording product is installed on the system.
- **Stop Screen Capture Wrap on Call Start.** You can choose whether desktop 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**. The number of days you would like calls matching that schedule to be saved in the system before being purged (deleted) or archived.
- **Archive Action.** 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 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. Changing this value DOES NOT apply to already recorded records.

- **Audio Capture**. If set to Yes, audio/voice will be captured for this record if available.

- **Screen Capture.** If set to Yes, screen activity will be captured for this record if available. This setting is ignored if Uptivity Desktop Recording software is not licensed for your system.
- **Speech Analytics.** If set to Yes, the audio recording will be processed by the Uptivity Speech Analytics application. This setting is ignored if the Analytics software is not licensed for your system.
- **Disk Location.** Location (UNC path or local disk) to which audio/video files for the record will be written.
- **Blackout Remote Audio.**
- **Comparison.** Select **AND** or **OR** to define schedule requirements using simple business rules. Select Expression to engage advanced business logic using a free-form expression.

Schedule Requirements: Simple Business Rules



Schedule Requirements

	Value Type	Comparison	Value	Case Sensitive
1				□
2				□
3				□
4				□
5				□

You can create simple schedules by matching up to five variables within a schedule. Utilizing the **AND** comparison, each rule set in the editor must match for a call to begin recording. Using 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 is 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 Variables.** There are 15 user-defined fields available for values received by your Discover application server from other applications. For further information see the *Uptivity API Manual*.

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

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

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

Schedule Expression: Advanced Business Rules

Selecting the **Expression** value from the **Comparison** setting lets you to enter a free form expression up to 64,000 characters in length. This allows for much more complicated decision-making to be available for the recorder. If **Comparison** is set to **Expression**, an expression must be entered or ***no*** calls will be recorded.

The variables that can be matched in a schedule include:

- **DeviceID.** The voice port/extension receiving or placing the call
- **Devicealias.** The ACD agent number for the person receiving or placing the call.
- **Group.** For inbound-routed ACD calls, this is the Hunt Group or Skill value
- **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.** There are 15 user-defined fields available for values received by your Discover application server from other applications. For further information see the *Uptivity API Manual*.
- **CallID.** The Call ID assigned from the PBX/ACD to identify the call
- **Calldirection.** Inbound or Outbound
- **Callinstancedescriminator.** An internal variable assigned to the call by the CTI Core for tracking purposes.
- **Initiatedby.** Possible values are: cti, agent, supervisor, api, timed, apichat, agentchat
- **Month.** Numeric value for the month (numbers less than 10 must have the leading zero, e.g. 09)
- **Day.** The numeric day of the month (numbers less than 10 must have the leading zero, e.g. 09)
- **Year.** The 4 digit year
- **Time.** The time of day, formatted as 24-hour time, 00:00 to 23:59. When entering data in the Schedule Expression field, put single 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'**

  Note If copying/pasting from Microsoft Office or other word processing software that uses Smart (a.k.a., "curly") Quotes, you must replace the Smart Quotes with standard quotes in the Schedule Expression field or it will generate an error when you save the schedule.

- **Weekday.** Three-letter day codes - mon, tue, wed, thu, fri, sat, sun
- **Date.** Format as yyyy-mm-dd
- **Pvalue.** A random number from 0 to 99 that can be used for cases where a certain percentage needs to be met.

These are the available operators to be used against the variables:

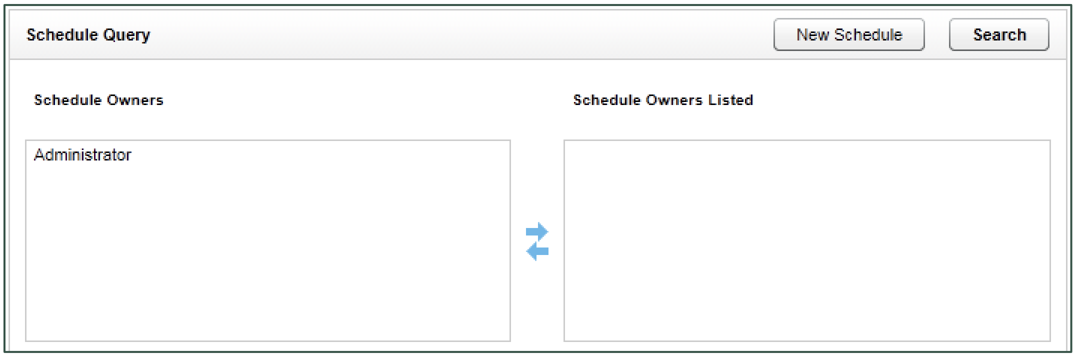
==	Equal to
!=	Not equal to
>	Greater than
<	Less than
>=	Greater than or equal to
<=	Less than or equal to
=~	Match a Regular Expression (Perl Formatted)
!=~	Does not match a Regular Expression (Perl Formatted)
'	Both single and double quotes can be used to signify strings in expressions.
c'	Prefixing 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. Parenthesized groups can be used to override the default precedence.

Create a Custom Schedule

1. Click the **Administration** tab and expand **Scheduling** in the left navigation menu.
2. Click **Create Schedule**.
3. Click **Create a Custom Schedule (Advanced)**.
4. Enter information in the desired fields. For details, see Custom Schedule Criteria Fields.
5. Enter any desired schedule requirements. For related information, see Schedule Requirements: Simple Business Rules and/or Schedule Expression: Advanced Business Rules.
6. Click **Save Schedule**. The schedule begins recording on the entered start date.

Find a Schedule


Schedule Query

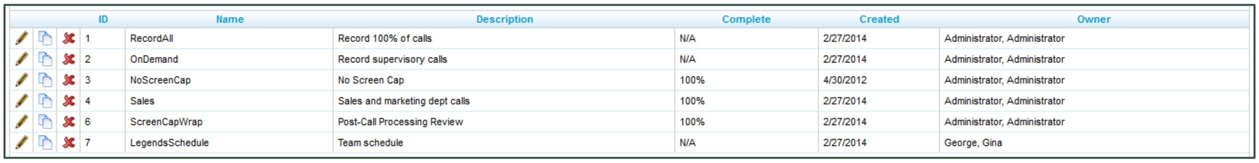
Schedule Owners

Administrator

Schedule Owners Listed

1. Click the Administration tab and expand Scheduling in the left navigation menu.
2. Click Find Schedule.
3. If you want to search for 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. Use the Control or Shift keys to select more than one user at a time. To retrieve all schedules, do not select an owner.
4. Click **Search** to display the Schedule list.

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 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**

From the Schedule List, you can perform the following operations:

- **Edit:** To edit a schedule, click the (✎) icon. Changes made to a schedule do not affect calls that have already been recorded.
- **Copy:** To copy the schedule rules into a new schedule, click the (⧉) icon.
- **Delete:** To delete a schedule, click the (✖) icon. Previously recorded calls are not affected by deleting a schedule.

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 Desktop Recording Client is running, whether the agent is actively using the workstation or not.

Note This feature will not work properly if the Workstations List is utilized. Unique usernames are required.

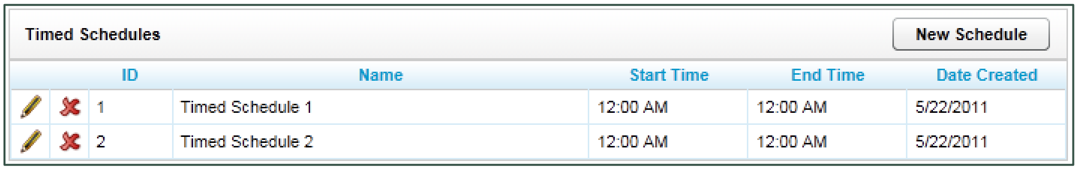
Licensing

The ability to use timed schedules is licensed separately from voice and desktop recording. These schedules require a **Desktop Only** license seat for each agent scheduled. Consult your Uptivity Account Manager for more information.

Timed Schedule List

To access Timed Schedules:

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



		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

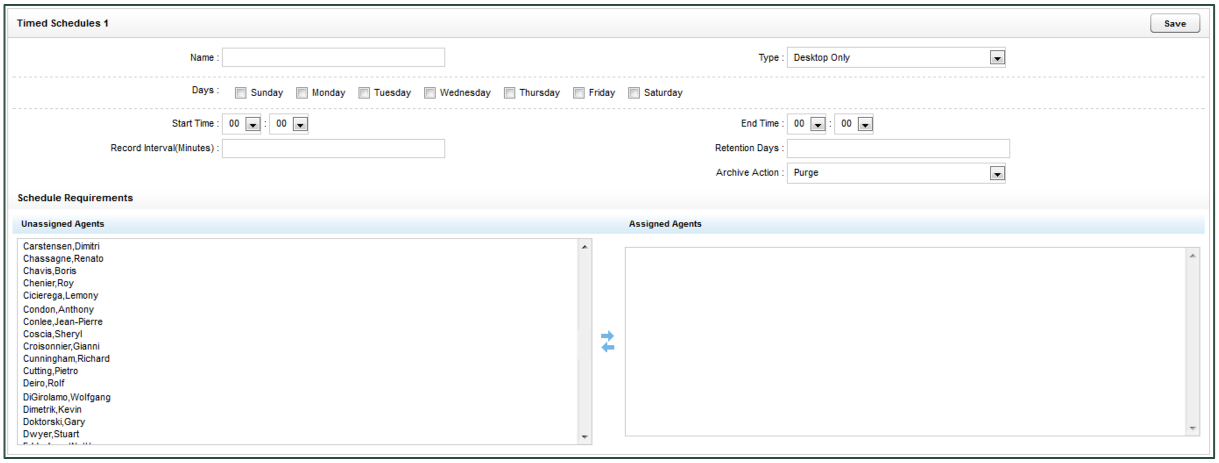
The Timed Schedule List displays the following information for each schedule:

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

From the Timed Schedule List, you can perform the following operations:

- **Edit:** To edit a schedule, click the (✎) icon. Changes made to a schedule do not affect calls that have already been recorded.
- **Delete:** To delete a schedule, click the (✖) icon. Previously recorded calls are not affected by deleting a schedule.

Create a Timed Schedule



Timed Schedules 1

Name :

Type : Desktop Only

Days : □ Sunday □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday

Start Time : 00 : 00

End Time : 00 : 00

Record Interval(Minutes) :

Retention Days :

Archive Action : Purge

Schedule Requirements

Unassigned Agents

Carstensen,Dimitri
Chassagne,Renato
Chavis,Boris
Chenier,Roy
Cicierega,Lemony
Condon,Anthony
Conlee,Jean-Pierre
Coscia,Sheryl
Croisonnier,Gianni
Cunningham,Richard
Cutting,Pietro
Deiro,Rolf
DiGirolamo,Wolfgang
Dimetrik,Kevin
Doktorski,Gary
Dwyer,Stuart

Assigned Agents

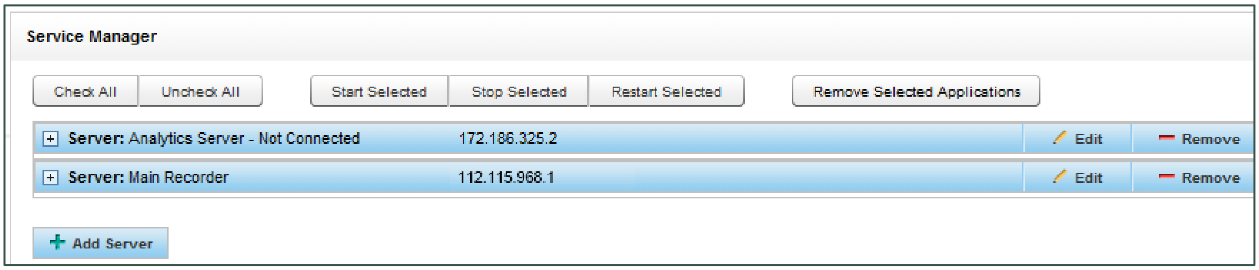
1. Click the Administration tab and expand Scheduling in the left navigation menu.
2. Click Timed Schedules.
3. Click **New Schedule**.
4. Enter a **Name** for the schedule.
5. Select **Desktop Only** from the **Type** drop-down list.
6. Select the check boxes for the **Days** of the week the schedule will be in effect.
7. Enter the length for each individual recording in **Record Interval (Minutes)**.
8. Enter the number of days for which recordings should be saved in **Retention Days**.
9. Select the desired Archive Action from the drop-down list. For details, see Archive Actions.
10. 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. Use the Control or Shift keys to select more than one agent at a time.
11. Click **Save**.

Tools

Service Manager

The Service Manager is located under the Tools menu on the Administration Tab.

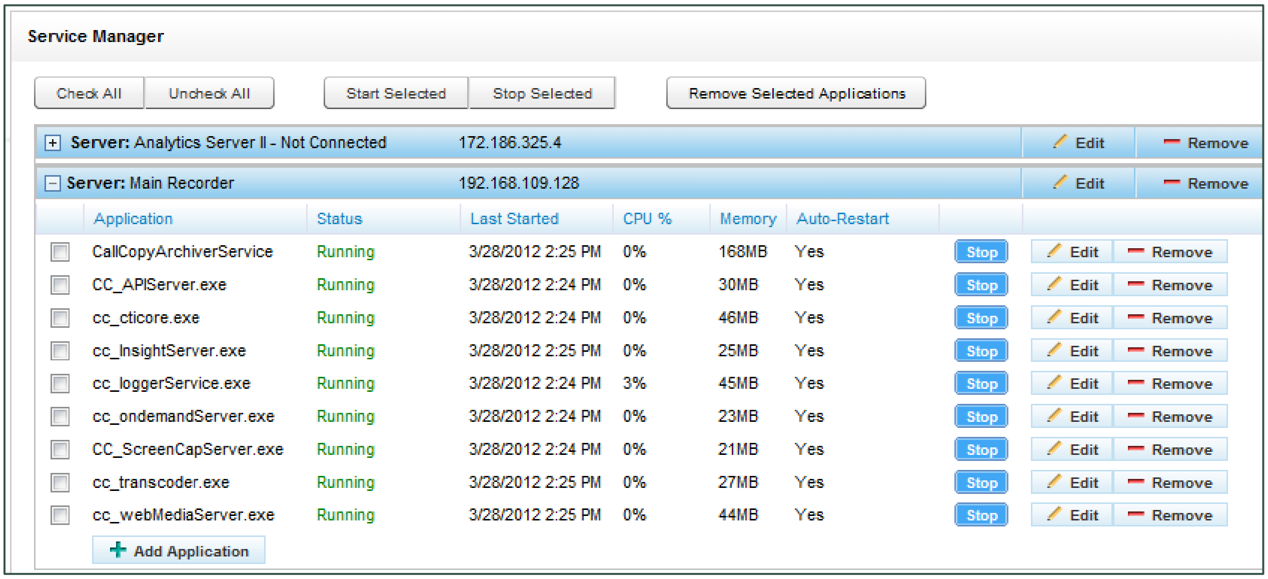
The Service Manager is used to centrally manage all Discover application services located on different machines (i.e., Server Nodes). In order for the Service Manager to load and control application services, the CometDaemon and Service Manager modules must be installed, configured, and running on each Discover system server. Otherwise, the Service Manager will show that it is not connected to that Server node, as shown below.



Service Manager

⊞	**Server:** Analytics Server - Not Connected	172.186.325.2	Edit	Remove
⊞	**Server:** Main Recorder	112.115.968.1	Edit	Remove

The Service Manager displays the Server Node name and IP address, as well as all Uptivity application services on the node and their current statuses.



Service Manager

⊞	**Server:** Analytics Server II - Not Connected	172.186.325.4	Edit	Remove
⊟	**Server:** Main Recorder	192.168.109.128	Edit	Remove

	Application	Status	Last Started	CPU %	Memory	Auto-Restart			
□	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

The Manager displays the following data for each service:

- **Application.** The name of the service installed. This value is case sensitive and is usually the name of the.exe 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** time and date.
- **CPU %.** This information is useful to determine why a service or server is running slowly.
- **Memory.** 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.

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 service 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 service status will display as 'Running' and the **Stop** button will be activated.

To start or stop multiple services at once, select the check boxes for all of the services you wish to control from the Service Manager list. You may also use the **Check All** or **Uncheck All** buttons to quickly select or de-select all services. You can then click the **Start Selected**, **Stop Selected**, or **Remove Selected Applications** buttons to perform the specified action on all of the selected services.

Add/Edit/Remove a Server Node

Server Nodes can be added, edited, and deleted from the Service Manager. Adding nodes requires the corresponding CometDaemon to be configured. Editing and removing nodes will affect your ability to manage the services on those nodes and the services themselves. Carefully plan changes to IP addresses and removal of nodes.

To add a Server Node:

1. Click **Add Server**.
2. Enter the server name and IP address.
3. Click **Save**.

To edit a node, click **Edit**. Make the needed changes and click **Save**.

To remove a node, click **Remove**.

Add/Edit/Remove a Service Application

To add a service application to a Server Node:

1. Click the **Administration** tab and expand **Tools** from the left navigation menu.
2. Click **Service Manager**.
3. Expand the desired Server Node and click **Add Application**.
4. Enter the name of the service under **Application**. This must exactly match the name of the EXE file as it appears in Windows Explorer. The name is case sensitive.
5. Select **Yes** or **No** from the **Auto-Restart** drop-down list.
6. Enter any parameters that must be set for the application. If the ident for a service was not set when the service was originally installed from command line, it can be added here. For example, for the Web Media Server using ident 1, the following would go in the parameters field:

   ```
   -web_media_server=1
   ```

   For details on whether a given service uses the ident parameter and the ident name format, refer to the section of the *Discover by Uptivity Installation Guide* that covers installing the service or the administration manual specific to that feature.

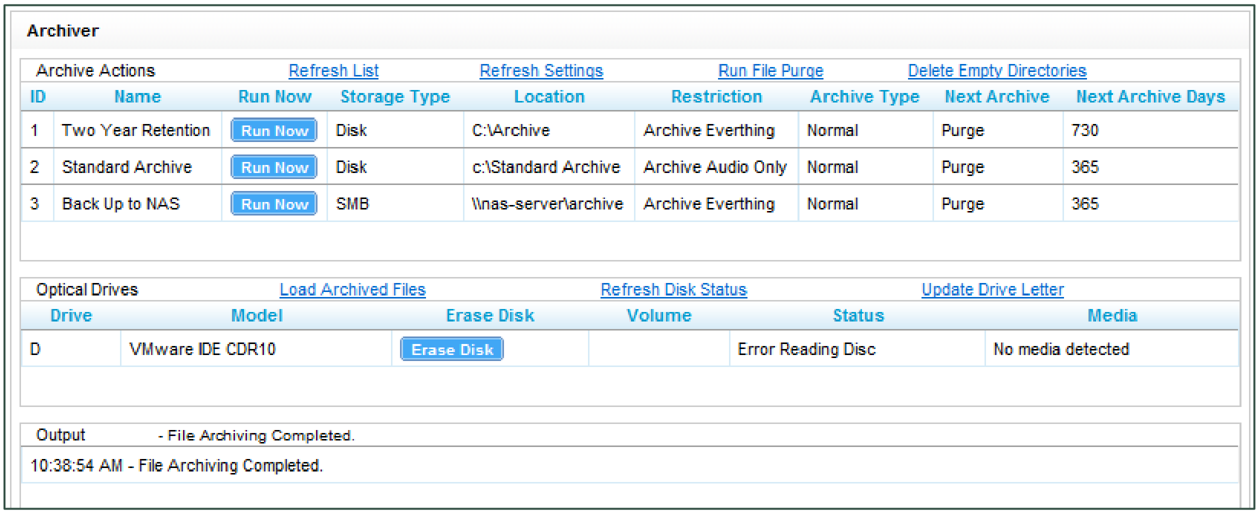
7. Click **Save**.

To edit a service application, click **Edit** after step 3. Make the needed changes and click **Save**.

To remove a service application, click **Remove** after step 3, then click **Yes**.

Archiver Console

The Archiver Console provides manual control for many Archiver module functions. To access the manager, browse to the **Administration** tab, expand **Tools** in the left navigation menu, and click **Archiver Console**.



Archiver

Archive Actions　Refresh List　Refresh Settings　Run File Purge　Delete Empty Directories

ID	Name	Run Now	Storage Type	Location	Restriction	Archive Type	Next Archive	Next Archive Days
1	Two Year Retention	Run Now	Disk	C:\Archive	Archive Everthing	Normal	Purge	730
2	Standard Archive	Run Now	Disk	c:\Standard Archive	Archive Audio Only	Normal	Purge	365
3	Back Up to NAS	Run Now	SMB	\\nas-server\archive	Archive Everthing	Normal	Purge	365

Optical Drives　Load Archived Files　Refresh Disk Status　Update Drive Letter

Drive	Model	Erase Disk	Volume	Status	Media
D	VMware IDE CDR10	Erase Disk		Error Reading Disc	No media detected

Output　- File Archiving Completed.

10:38:54 AM - File Archiving Completed.

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 Archiver Settings.
- **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:** Force any listed Archive Action to run immediately by clicking the button.
- **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 the actions of the Discover Voice Recorder component, 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 also have more than one CTI Core and Transcoder.

CTI Cores

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 the customer's ACD/PBX. Uptivity publishes integration guides to detail the required configuration for each supported PBX/ACD platform. If you need the integration guide for your system, contact Uptivity Support.

To access the CTI Cores list in the Web Portal, click the **Administration** tab, expand **Recorder Settings** in the left navigation menu, and click **CTI Cores**.

> **Note** If Core settings changes are required, 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.

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. Buddy Cores should always run on different machines (including VM clusters) to avoid having a single point of failure. Not all integrations are suitable for Buddy Cores. Contact Uptivity Solution Engineering for details.

Types of Configurations

There are two ways to configure Buddy Cores: Primary/Secondary and Active/Inactive. The main difference is in how the secondary Core behaves.

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

Primary/Secondary

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.

Active/Inactive

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.

Configure Buddy Cores

You will need the following information to get started:

- Settings of the Primary Core via Web Portal.
- List of CTI modules and settings for each in the Primary Core.
- IP address of the server that will be running the Secondary Core.

Set Up Core and Voice Board

After installing Discover on a second server using the standard installation process, set up a dedicated CTI Core and Voice Board for the Secondary Core. Follow the instructions for **Voice Boards**, **CTI Core Configuration**, and **CTI Core Service** in the integration guide that corresponds to your environment. Generally speaking, the Secondary Core's settings should mirror the Primary Core's.

Additionally, during Core configuration:

- Relate the Secondary Core to the Primary Core, and vice versa.
- Add a **Broadcast Receiver** module to the Secondary Core.
- Customize **Switch Over Delay** as needed. This determines how long the Secondary Core waits without receiving an update from the Primary Core before the Secondary Core takes over recording. The default value (in milliseconds) is 3000 (three seconds).

If you are working with a dual-AES configuration where one Core is associated with an individual AES, within the TSAPI module, set the number of AES connection attempts to mirror the Primary Core's setting. This is the number of times it will try to reconnect before shutting down the Primary Core and activating the Secondary Core. Entering 0 disables the reconnection option. The Core verifies AES connectivity every 10 seconds.

Configure Settings

The settings that determine Primary/Secondary vs. Active/Inactive behavior as well as how long Cores attempt to read each other's state when starting up must be configured for proper operation. Refer to knowledge base article # 000001508 for information on these settings and their values.

Set Cores to Automatically Restart

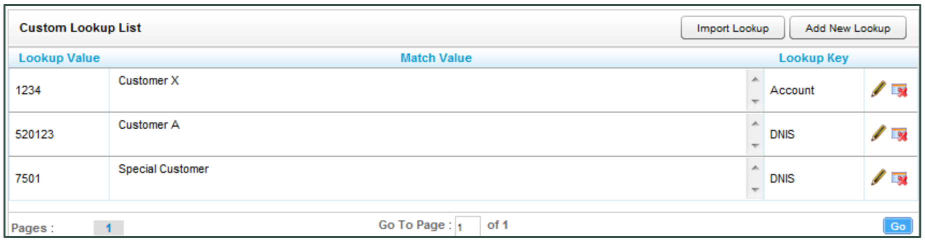
If the cause of the Buddy Core activation is a power outage, network problem, or other server fault beyond just a Core failure, that issue will need to be resolved first.

Once the server is back online, perform the following steps during a time that will not affect service, depending on your configuration:

1. Click the **Administration** tab and expand **Tools** in the left navigation menu.
2. Click **Service Manager**.
3. Expand the applicable **Server Nodes**.
4. Verify that **Auto-Restart** for both the Primary and Secondary Cores is set to **Yes**.
5. Save any configuration changes.

If an event causes a Core to stop and restart, it will go through the same determination process described at the beginning of this section.

Custom Lookup



Custom Lookup List

Lookup Value	Match Value	Lookup Key	
1234	Customer X	Account	✎ ✖
520123	Customer A	DNIS	✎ ✖
7501	Special Customer	DNIS	✎ ✖

Custom Lookup 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. Once the script is in place, you can edit entries as needed. Contact Uptivity Support for scripting assistance.

To edit a custom lookup, click the ✎ icon; to delete a lookup, click the ✖ icon. Editing or deleting the custom lookup does not affect existing call records.

Add a Custom Lookup

To add a custom lookup:

1. Click the **Administration** tab and expand **Recorder Settings** in the left navigation menu.
2. Click **Custom Lookup**.
3. Click **Add New Lookup**.
4. 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.
5. In the **Match Value** field, enter the replacement value to be added to the call record.
6. For the **Lookup Key**, select either DNIS or Account if your Lookup Value is based on ANI.
7. Click the 💾 icon.

Import Multiple Custom Lookup Values

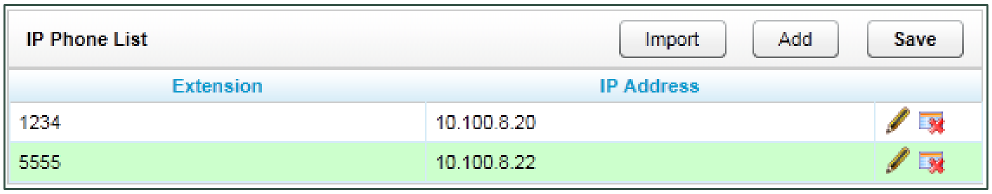
Multiple custom lookup values can be imported at once using a comma separated values (CSV) file. Each entry must be added to the file using this format: Lookup Value, Match Value, Lookup Key.

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**.
3. Click **Import Lookup**.
4. Click **Browse**, locate the CSV file and select it.
5. Click **Upload File**.
6. Click **Import Now** to complete the task.

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



Extension	IP Address	
1234	10.100.8.20	✎ ❌
5555	10.100.8.22	✎ ❌

The **IP Phones** settings allow 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.

To edit an entry, click the ✎ icon. Change the extension and/or IP Address and then click the 💾 icon. To delete an extension, click the ❌ icon.

Add Phones

To add a phone:

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

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**.
3. Click **Import**.
4. Click **Browse**, locate the CSV file and select it.
5. Click **Upload File**.
6. Review the preview of your data as displayed below **Perform Import**.
7. Click **Import Now** to complete the task.

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 *Discover On-Demand Administration Guide* for more information.

Transcoder

A Transcoder converts raw audio files recorded by the system into compressed, .wav formatted audio files, optimized for storage and playback retrieval. There are three options for relating Transcoders, Voice Boards, and CTI Cores:

- **One Transcoder for all Cores.** This is the default setup.
- **One Transcoder per Voice Board.** In this case, the Core's **Transcode by Board** option is set to 'True', and the Transcoder's **Look for Code** field includes the Voice Board's number.
- **One Transcoder per one or more Cores.** In this case, each Core's **Transcode by Board** option is set to 'True'. Each Core's cc_cticore.ini file has to have a Transcoderprefix value set, and this value has to be added to the Transcoder's **Look for Code** field. The Transcoderprefix can be any arbitrary number.

If both Transcoder-per-voice-board and Transcoder-per-Core are used, be careful to use Transcoderprefix numbers that do not conflict with Voice Board numbers.

The best option depends on several factors, including the number of calls, the duration of those calls, the size of the call files, and the distribution of calls during a day. If two Cores are on the same machine, using one Transcoder is usually acceptable. Transcode per board or per Core(s) is useful for distributing work. If Cores are distributed over a network, pulling large, unprocessed call files over the network can be avoided by using the per-Core option with a Transcoder on each network branch with a Core. The best option is determined and configured during installation of your system. However, as call volumes and networks change, you should be aware of which option you use and how it may affect transcoding.

Note Transcoder scripts support file names up to 260 characters, including the file extension.

Transcoder Settings

Each Transcoder has these settings:

- **Identity:** Auto-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.

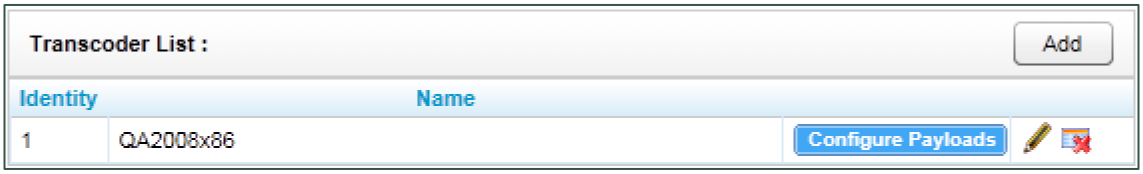
- **Create CCP File:** Creates a custom graphical representation of the audio waveform from a recorded call and stores it as a CCP file along with the audio file. When enabled, results in faster playback times as the waveform will not need to be recomputed for each playback.
- **CCP Interval:** Time 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.
- **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 Desktop Recording and Desktop Analytics are used with call recording. Desktop 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.
- **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). For related information, see Transcoder.
- **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 desktop 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 desktop 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."
- **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.

Configure Transcoders



Transcoder List : Add

Identity	Name		
1	QA2008x86	Configure Payloads	✎ ☒

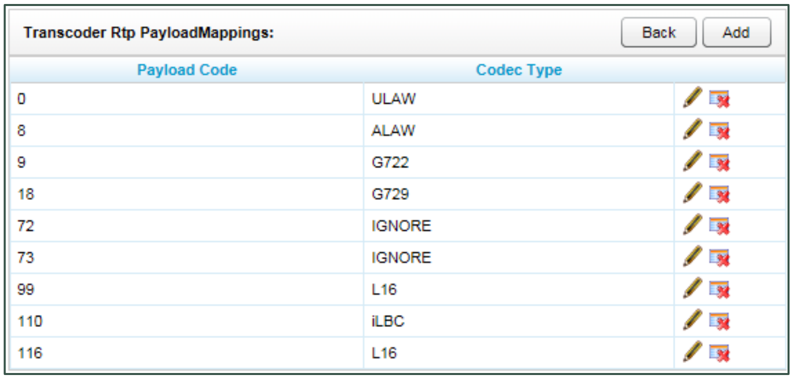
To add a Transcoder:

1. Click the **Administration** tab and expand **Recorder Settings** in the left navigation menu.
2. Click **Transcoder**.
3. Click the **Add** button.
4. Configure Transcoder settings.
5. Click **Save**.

To view or edit Transcoder settings, click the ✎ icon.

To remove a Transcoder, click the ☒ icon. Do NOT delete a Transcoder if files are being processed, and/or before a new Transcoder is ready to process files.

Configure Payload



Transcoder Rtp PayloadMappings: Back Add

Payload Code	Codec Type	
0	ULAW	✎ ☒
8	ALAW	✎ ☒
9	G722	✎ ☒
18	G729	✎ ☒
72	IGNORE	✎ ☒
73	IGNORE	✎ ☒
99	L16	✎ ☒
110	iLBC	✎ ☒
116	L16	✎ ☒

In order for a Transcoder to properly read recorded audio files, it needs to know which audio codec is being used for the file, which for VoIP recording is stored in the RTP Payload Type. The RTP Payload should match with the types defined in Network Working Group RFC 3551.

By default, the Transcoder module is configured to follow the specified RTP. Some PBX vendors specify Payload Types that do not follow the RFC. When this occurs, the audio files cannot be properly transcoded, and the audio codec must be manually configured.

To manually configure a Payload Type:

1. Click the **Configure Payload** button for the desired Transcoder.
2. Click the ✎ icon on the right side of the row.

To remove a Payload Type:

- Click the ☒ icon on the right side of the row.

Transcoder Configuration

The preferred method of configuring the Transcoder is via command line. Refer to the Transcoder configuration section of the *Discover by Uptivity Installation Guide* for more information.

Configure INI

Use of an INI file to configure the Transcoder should **only** be done when advised by a developer. The INI file used by the Transcoder is located at **Recorder\Transcoder\cc_Transcoder.ini.** The INI filename should always match the name of the executable it configures. This is an example output of a configuration file, with important settings detailed in the table to the right:

[app_settings]	
[value_storer]	If you need the possible values for this INI file, copy the key you need from below and paste under the [app_settings] section.
Transcoder_ident=1	For configuring distributed transcoding environments, this ID needs to be configured in the corresponding Transcoder module INI file. Identity number is in Discover Web Portal for a Transcoder.
external_process=0 (or 1)	Allows Transcoder to encapsulate conversion in external process. Should rarely be used.
reverse_channels=0 (or 1)	Allows Transcoder to swap inbound and outbound streams for analytic and CCP purposes. Do not activate unless told to by a Uptivity developer.
debugexcess=false	Set to True to enable. Logs out the most available information, useful for troubleshooting.

Transcoder Troubleshooting

These issues may affect transcoding (for related information, see the Transcoder Status report in the *Discover by Uptivity Reporting Manual*):

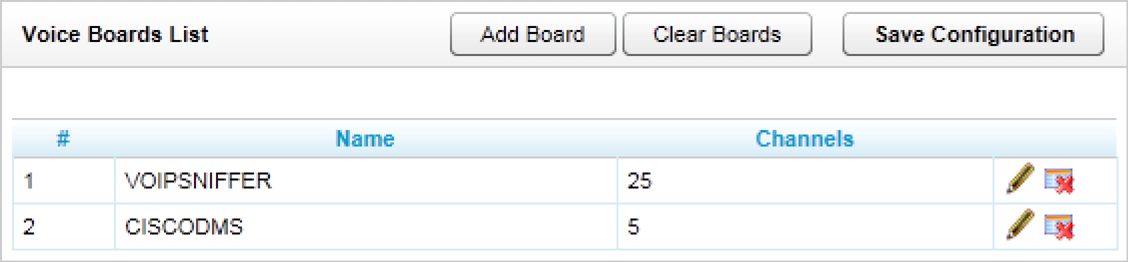
- **No connection to SQL database:** The Transcoder must access the database to determine whether there are audio files to transcode. A connection failure (i.e., timeout) should be recorded in the SQL server logs.
- **Inadequate permissions:** Can occur if the recorder and Transcoder are located on different servers and the Transcoder does not have read/write permissions to the directory where raw CCA and compressed files are located or where the Transcoder's temporary files are stored.
- **Network latency:** The Transcoder may time out if the recorder and Transcoder are on different servers and the network is slow to copy files to the Transcoder's temp directory.
- **Inadequate disk space**
- **Large number of files awaiting transcoding:** Increasing the number of threads used by the Transcoder reduces this number but also affects performance of other processes. If there are periods during the day or week when CPU usage is lower, this number of threads can be increased and then lowered.

Voice Boards

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 integration guide for your system. If you cannot locate your integration guide, contact Uptivity Support to obtain a copy. This topic contains a general overview of Voice Boards and the configuration options for individual channels, since you may need to modify these from time to time.

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. Contact Uptivity Support before adding or removing Voice Boards to prevent any negative impact on your system.

Voice Board & Channel Configuration



#	Name	Channels	
1	VOIPSNIFFER	25	✏ ✖
2	CISCODMS	5	✏ ✖

To manage Voice Boards:

- Click the **Administration** tab of the Web Portal, expand **Recorder Settings** in the left navigation menu, and click **Voice Boards**.

To add a Voice Board:

- Click the **Add Board** button; refer to your integration guide for additional steps.

To view or edit Voice Board settings, including Channel Configuration settings:

1. Click the ✏ icon.
2. Edit any desired settings.
3. Click **Save**.

To remove the configuration for that individual Voice Board:

- Click the ✖ icon.

To clear all Voice Board entries from the system:

- Click the **Clear Boards** button.

  Notes

  If you make any changes to these settings, the recorder process must be restarted.

  Contact your Uptivity support provider prior to adding or removing any hardware components from your Uptivity system. ***Altering the hardware configuration may void your warranty.***

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

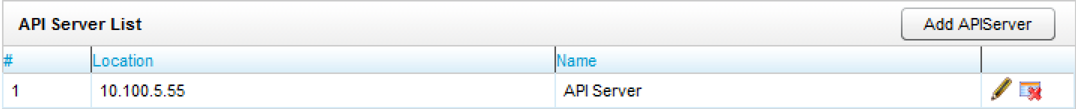
Regardless of integration, each channel entry includes the **Assign** field, which defines that type of recording will take place on that channel. Possible assignment types include:

- **Not in Use**
- **Anything:** Allows channel to be used for all recording and playback events, as determined by schedule priorities.
- **Playback Anything:** Limits channel to playback of recordings via telephone.
- **Record Anything:** Allows channel to be used for any scheduled or API-triggered recording.
- **Instant Record:** Dedicates channel to instant recording requests from the API.
- **Dedicated Record ACD Group:** Limits channel to recording only the specified ACD/PBX group (not the Discover Group, independently of any schedules.
- **Dedicated Record ACD Gate:** Limits channel to recording a specific ACD queue type.
- **Dedicated Record Device/PortID:** Limits channel to recording a specific hardware resource (e.g., voice port or DN) on the ACD/PBX. This option may be worded differently depending on your Terminology settings.
- **Dedicated Record Agent Number/Device Alias:** Limits channel to recording a specific agent number or extension. This option may be worded differently depending on your Terminology settings.
- **Dedicated Record Number Called DNIS:** Limits channel to recording a specific inbound number, such as an 800-number carrying traffic to your facility.
- **Dedicated Record CallerID ANI:** Limits channel to recording a specific ANI. Full or partial ANI matches may be used, e.g., limit to a matching area code.
- **Dedicated Record User 1-5:** Limits channel to recording a specific user-defined value as set by the API. Examples include Account and Case Number.
- **Playback and Instant Record:** Limits channel to playback and instant recording requests from the API.
- **Playback and Record:** Limit channel to scheduled recordings and playback.
- **Record and Instant Record:** Limit calls to recording only, but of any recording type.
- **Unlicensed:** Unlicensed channels are not used.

System Settings

System Settings are typically configured during the installation process by the Uptivity team. This topic is designed to give you a basic understanding of the settings and what they mean for your system. Contact your Uptivity support provider before making any changes to your System Settings.

API Servers



API Server List

#	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. API Servers are required for the Live Monitoring and Call Exporting features in the Discover software. For more information on Uptivity API Services, see the *Uptivity API Manual*.

> **Note** Install the application or service that will use the API server before adding the API server to this list. For example, a CTI Core must be installed and added to the CTI Core List before it can be added to an API server.

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

- **#:** Internal identifier 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 set by the user to aid in identifying API Servers.

Configure API Servers

To configure an API Server:

1. Click the **Administration** tab and expand **System Settings** in the left navigation menu.
2. Click **API Servers**.
3. Click **Add API Server** to add a new API Server to the list.
4. Click the ✎ icon on the right side of the new entry's row.
5. Edit the **API Server Settings** as necessary.
6. Click **Save**.

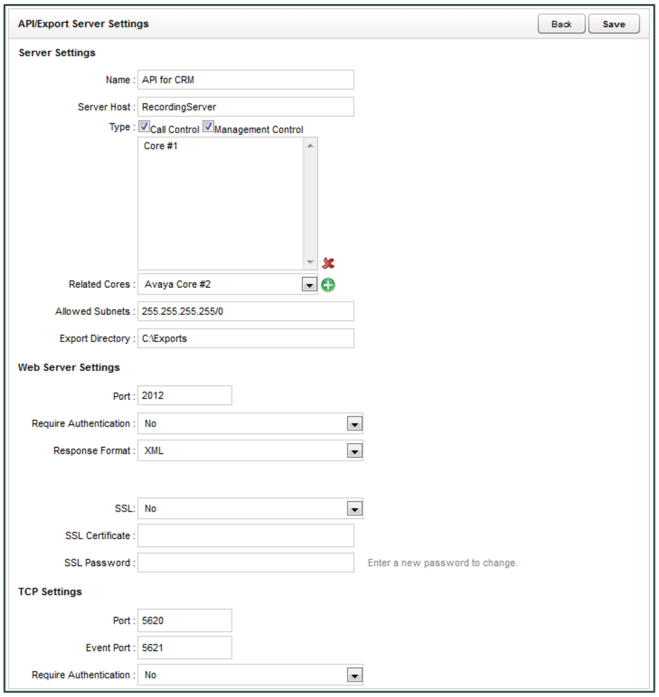
To edit an existing API Server:

- Click the ✎ icon on the row for the desired API Server.

To remove an API Server:

- Click the ✖ icon on the row for the desired API Server.

API Server Settings



API/Export Server Settings

Server Settings

Name : API for CRM

Server Host : RecordingServer

Type : ☑ Call Control ☑ Management Control

Core #1

Related Cores : Avaya Core #2

Allowed Subnets : 255.255.255.255/0

Export Directory : C:\Exports

Web Server Settings

Port : 2012

Require Authentication : No

Response Format : XML

SSL: No

SSL Certificate :

SSL Password : Enter a new password to change.

TCP Settings

Port : 5620

Event Port : 5621

Require Authentication : No

Each API Server has the following list of settings:

Name: A meaningful name given to the API server for reference.

Server Host: Hostname or IP address of the server on which the API module is running.

Type: Can use Call Control (recording functions, i.e. CALLSTART/CALLSTOP) and/or Management Control (management functions, i.e. IMPORTAGENT/GROUP).

Related Cores: CTI Core modules associated with this specific API Server instance. Multiple Cores can be associated to a single API Server. Select the desired Core from the drop down menu, and click the ⊕ button to add it to the list. To remove a CTI Core, select it from the list and click the ✖ button.

Allowed Subnets: The API Server can be limited to accept requests from specific subnets only. By default, requests from all addresses (255.255.255.255/0) are accepted.

Export Directory: Temporary location used for writing files that are requested for export in the Web Portal.

(Web Server) Port: TCP port on which the API Server will accept HTTP WebAPI requests. The default is 2012.

Require Authentication: If enabled, all HTTP requests must provide the credentials of a user in the Discover system (not Active Directory credentials) in HTTP Basic Authentication format. If authentication is required, other Discover components will not be able to authenticate to this server. For security purposes, some organizations choose to dedicate one API server to Desktop Analytics/On-Demand. This server would have only call control permissions, authentication would be disabled, and the server could not export. A second dedicated API server is used for exporting. This server would have management permissions and authentication enabled.

Response Format: Determines whether API responses are sent to clients in XML or SOAP format.

SSL: When enabled, all HTTP requests must utilize a secure SSL connection with a specified certificate.

SSL Certificate: Local path to the SSL certificate to use for encryption. Certificate must be in P12 format.

SSL Password: Password for the listed SSL Certificate.

> **Note** The server must be rebooted for changes to this configuration to be effective.

(TCP) Port: TCP port on which the API Server will listen for socket-based requests. The default is 5620.

Event Port: TCP port on which the API Server listens for Event Service calls from the CTI Core. The default is 5620. The system is designed to receive all Port and Event Port messages on the same port.

Require Authentication: If enabled, Discover user credentials must be passed on every connection to the API socket.

Archive Actions

Typically, disks on a local Discover system only have enough space to store audio and video recordings for a short time. By establishing archives, additional drives can be attached so that recordings can be stored indefinitely. Be aware that if a call is auto-archived and/or deleted from the server, the QA Evaluations performed on that call will remain on the database for historical searching and review. However, if a call is manually deleted from the server, the 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.

Recordings can be archived to local 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.

Archiving is controlled by:

- **Archive Actions:** Archive actions 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:** 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 the recordings are archived or purged once they exceed their retention days.

  Notes

  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 and DOES NOT apply to already recorded calls.

  Before you create a schedule that will require archived recordings, you should first configure the archive action. Typically, only administrators have permissions to create archives, so you will need to communicate archive settings to users. Schedules should be audited on a monthly basis to ensure all necessary information is being archived.

- **Archiver:** This software manages recording storage and backup of the Discover SQL database based on the Archive Action specified for a call and its call record. The Archiver settings page controls the overall performance of the software.

  Note Before Archiver can back up the SQL databases, an initial backup must be done manually through SQL Server Management Studio. See the *Discover by Uptivity Installation Guide*.

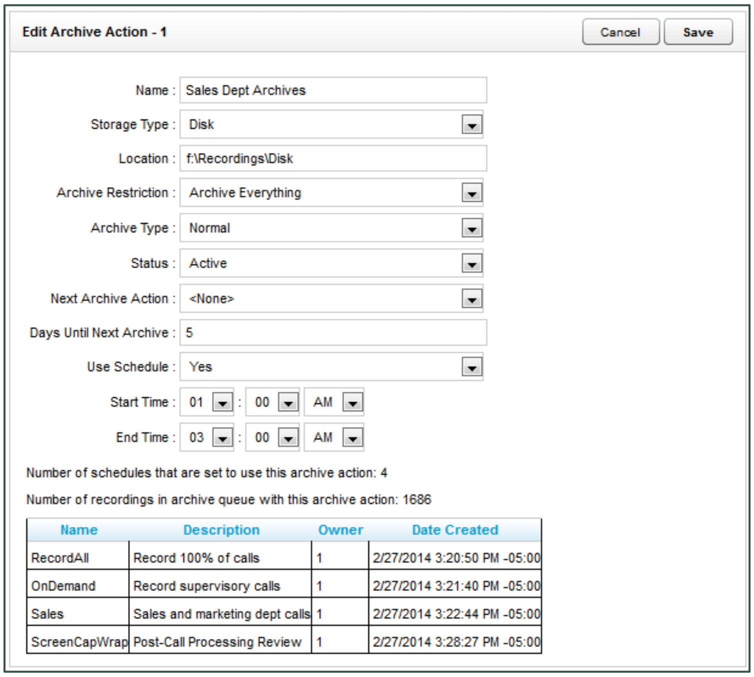
- **Archive Console:** This tool provides information on archive actions and some manual control over them.

  Note For details, see Archiver Console and Scheduling.

Archive Action Settings

Each Archive Action has a number of configurable settings.

Name: Name of the Archive Action. This name will also appear in the list of available **Archive Actions** in **Scheduling**.



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

Storage Type: Choose a storage type from the drop-down list:

- **Disk**: When selected, you must provide a local drive path in the Location field. The Archiver service must have read/write access to this drive.
- **SMB:** A SMB/CIFS network file storage share. When selected, the following options will appear:

- **User ID:** If the storage location requires credentials, enter the username here.
- **Password:** If the storage location requires credentials, enter the password here.
- **Location:** The UNC path to the CIFS storage location used for archiving.

  Note If Discover is unable to write to the file share, the Discover Notification System generates an alert.

- **DVD:** Recordable disk media (DVD+R, DVD-R, DVD+RW, DVD-RW single layer supported). If selected, the following options will appear:

- **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.

  Note Archive actions using the DVD storage type will only execute once per day. DVD media must be manually removed and new media inserted on a daily basis.

- **XAM:** Fixed content access method associated with the Centera content-addressable storage platform.

  - **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 Centera storage server. 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.

Location: Enter a direct file path for the archive destination. Path and/or file names can be customized using file masks (Disk and SMB storage types only). Available file masks are as follows.

%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*
%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		

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.

Archive Restriction: Specifies whether archived recording files are saved with audio, video (desktop recording), and analytics (speech or desktop) data, or if only a single component will be archived with the recorded audio.

- **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.

- **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: Indicator set by the administrator to show if the action is available for use (Active). Does not affect the operation of the action or how it is attached to any recording schedules.

> **Note** An archive action displays as active (i.e., Status equals A) even if an archive location is technically unavailable. If an archived location is unavailable, the system notification tool will issue an alert.

Next Archive Action: Sets the next desired action to be taken against the archived data. 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**.

Use Schedule: When enabled, the archive action only runs during the specified time of day. Helps prevent system overload or excessive I/O operations in connected environments during peak hours.

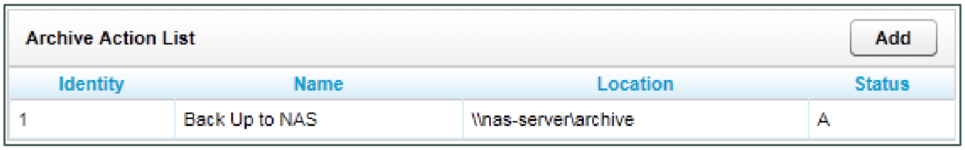
> **Note** Not available if DVDs are used.

Start Time/End Time: In conjunction with **Use Schedule**, the time of day restriction for the action.

> **Note** Not available if DVDs are used.

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.

Configure Archive Actions



Identity	Name	Location	Status
1	Back Up to NAS	\\nas-server\archive	A

To create a new Archive Action:

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

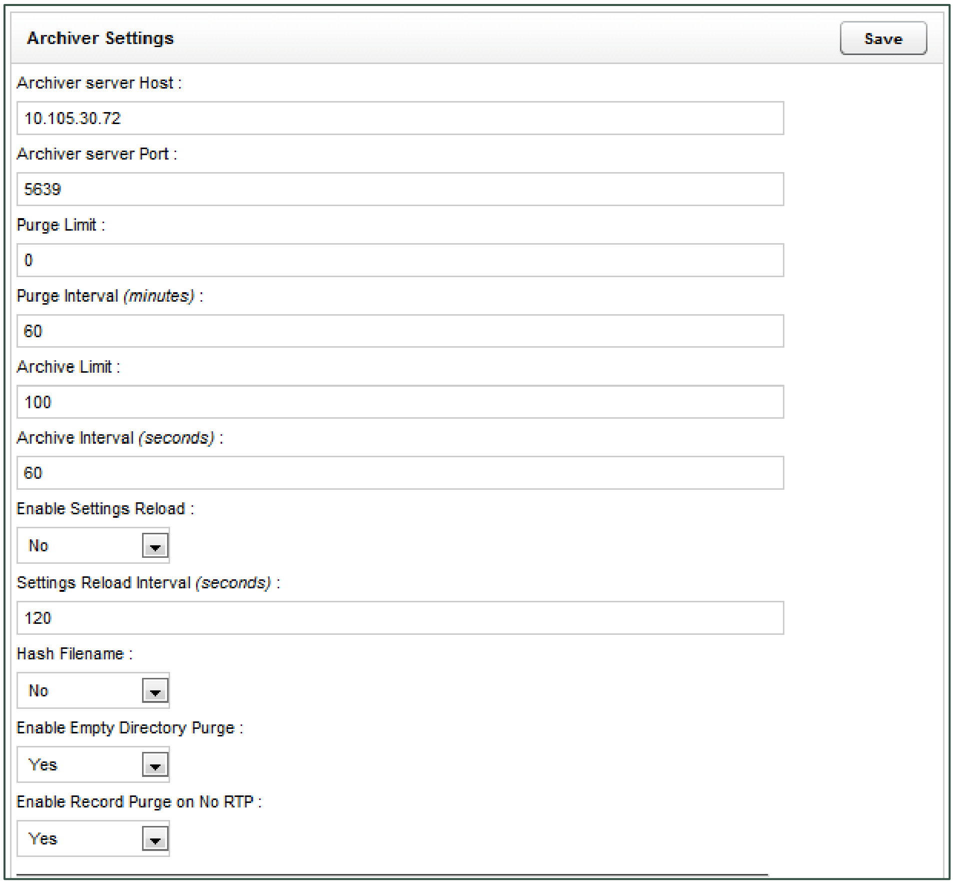
After you create an archive action, you must attach it to a schedule. For details, see Scheduling.

To edit an existing archive action:

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

Archiver

Archiver settings are used to control disk and network usage by Archive Actions, preventing the actions from overwhelming local system resources or network bandwidth. Settings are divided into several sub-categories: General, System Purge Action, Removable Media, and MSSQL Database Backup.



Archiver server Host : 10.105.30.72

Archiver server Port : 5639

Purge Limit : 0

Purge Interval *(minutes)* : 60

Archive Limit : 100

Archive Interval *(seconds)* : 60

Enable Settings Reload : No

Settings Reload Interval *(seconds)* : 120

Hash Filename : No

Enable Empty Directory Purge : Yes

Enable Record Purge on No RTP : Yes

Note Before configuring Archiver, review Archive Actions.

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 running Purge jobs.

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 running Archive jobs. System default is 60 seconds, which is typically sufficient.

Enable Settings Reload: When set to ‘Yes’, settings on this page automatically reload on an interval. When set to ‘No’, the service must be restarted for the settings to take effect.

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.

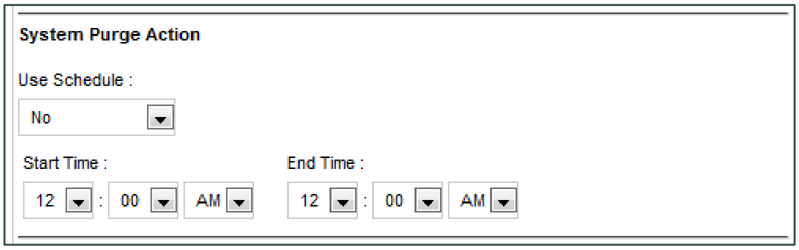
Hash Filename: When the record is archived, associated files are renamed as the SHA-1 hash of the original path the record was stored at. This is to prevent possible duplicate filenames in the archive location. Not normally needed unless original recording files have the potential of being named the same.

Enable Empty Directory Purge: When enabled, Archiver periodically scans all directories in any recording locations and removes any folders that have no files inside.

Enable Record Purge on No RTP: Removes records that are recorded when no audio is present on the line. Effective only in VoIP configurations, where it is mainly used to compensate for false positive recording triggers in passive installations.

System Purge Action

Use Schedule: If enabled, Purge jobs will only run between the specified hours of the day. Helps prevent system overload or excessive I/O operations in connected environments during peak hours.



System Purge Action

Use Schedule : No

Start Time : 12 : 00 AM

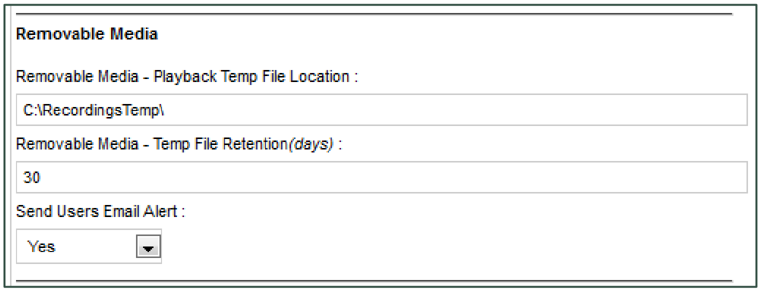
End Time : 12 : 00 AM

Start Time/End Time: The time of day restriction for the Purge job. The job will only run between these hours if **Use Schedule** is enabled.

Removable Media Settings

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.



Removable Media

Removable Media - Playback Temp File Location : C:\RecordingsTemp\

Removable Media - Temp File Retention*(days)* : 30

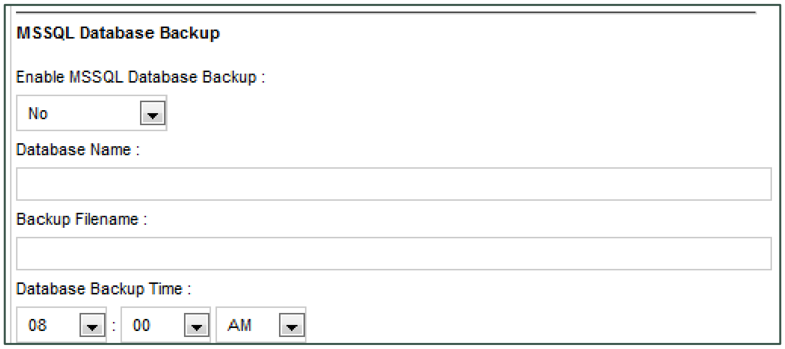
Send Users Email Alert : Yes

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

Enable MSSQL DB Backup: When enabled, Archiver initiates a daily backup of ONE of the Discover databases. Useful if your installation utilizes an SQL Express database that cannot use scheduled backups.

Database Name: Name of the database to be backed up.



MSSQL Database Backup

Enable MSSQL Database Backup : No

Database Name :

Backup Filename :

Database Backup Time : 08 : 00 AM

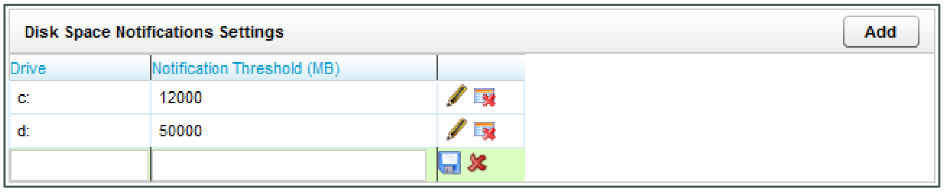
Backup Filename: Location of the backup file to use, determined during Discover installation. Refer to the "Backup the SQL Database" section in the *Discover by Uptivity Installation Guide* for more information.

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.

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.

Disk Space Notifications



Disk Space Notifications Settings

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 accesses. Archiver manages disk usage for original recordings, archives, and SQL databases. If a specified drive drops below the established free space threshold, Archiver will send out 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**.
3. Click **Add**.
4. In the **Drive** column, enter the drive letter followed by a colon.
5. In the **Notification Threshold** field, enter the minimum free space (in megabytes) to remain available.
6. Click the 💾 icon to add the entry to the list.

To edit an existing entry on the list, click the ✏ icon. Edit the fields in that row as needed and click the 💾 icon.

To delete an existing entry, click the ❌ icon and then click **OK**.

Info Broker Settings

Information (Info) Broker manages how system components communicate with one another, promoting greater scalability, resiliency, and compliance while reducing resource bottlenecks and potential break points. The Info Broker service allows for greater system growth, expandability, and scalability by splitting the Web Media Server's tasks between it and the Info Broker, allowing it to direct Live Monitor traffic and requests between components rather than sending all traffic to the Web Media Server.

The Info Broker service can be monitored by the existing Discover Service Manager and restarted as needed (see Service Manager). The only feature wholly reliant on Info Broker is Live Monitoring, so critical services will continue to operate in the event that Info Broker goes down or needs to be restarted.

When the Info Broker service starts up, it retrieves information from the Discover database about devices, modules, hosts, and ports. It then sends a message to Core(s) asking for the current state of all devices the core handles. Info Broker also identifies all Web Media Servers and maintains a list that it uses to direct data within a Location to specific servers. Info Broker does not actively communicate with the Desktop Recording Servers unless it receives messages from them.

The Info Broker service is required only in environments using Live Monitoring. It is started, and typically configured, during the installation process. Refer to the *Discover by Uptivity Installation Guide* for more information.

Configure Info Broker

To configure Info Broker:

1. Click the **Administration** tab and expand **System Settings** in the left navigation menu.
2. Click **Info Broker Settings**.
3. Enter the settings.
4. Click **Save**.

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 Desktop 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. Default 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. Default is 30 seconds.
- **Media Timeout Seconds:** Timeout for the connection to Cores and Desktop Recording Clients. Default is 30 seconds.
- **Excessive Debugging:** When checked, adds detailed logging for Info Broker which can be useful for troubleshooting.

Locations Settings

Locations allow for easy grouping of Cores, Desktop Recording Servers, and Web Media Servers for customers with multiple sites that are geographically or logically separate. This also allows for better distribution of work between Desktop Recording Servers and Web Media Servers within each Location, and reduces network traffic between locations by prioritizing and utilizing local resources. Storing and retrieving data locally also means customer locations are not isolated from their database or storage if a network outage occurs between remote offices.

The standard configuration for Info Broker and Locations assumes a Core is present at each Location. However, for environments where all calls come from only one Location and/or there is a single Core at one location that sends requests to Desktop Recording Servers at several locations, agents can be manually assigned to a Location in their user profiles. In a multi-Location environment, a Web Media Server must be configured for each Location where you will use live monitoring.

API Servers are still assigned to Cores directly and are unaffected by Locations.

A default Location is created during installation.

Configure Locations

To add a Location:

1. Click the **Administration** tab and expand **System Settings** in the left navigation menu.
2. Click **Locations Settings**.
3. Click **Add**.
4. Enter a name and description for the Location.
5. Click **Save**.

To edit an existing Location:

1. Click the **Administration** tab and expand **System Settings** in the left navigation menu.
2. Click **Locations Settings**.
3. Click the ✏ icon on the Location you wish to edit.
4. Make the necessary changes.
5. Click **Save** to commit changes.

Logging

Event logging is configured in the INI and configuration files of various Uptivity applications and on the Discover Web Portal's Logging Settings page. INI and configuration files specify the level of events the application sends to the Logger. Logging Settings specify where the Logger writes the log files and the level of events recorded to those files.

It is important to maintain consistency between the INI/configuration files and the Logging Settings. For example, if an application is configured to send Debug and Info events, and the Logger is configured to write only Critical and Emergency events, the Debug and Info events will not be written to the log files. Critical information may be lost due to this inconsistency. The number of days for retaining log files is configured in Notifications.

The default Log Directory path can be changed is configured during initial installation. If this setting is changed, make sure the new directory is large enough to store the log file.

Logging Levels correspond to the subscription types in Notifications, and these settings configure which logged events are passed on. Settings that specify logged events are configured during initial installation, but you may opt not to log certain events. Uptivity recommends leaving all **Logging Levels** selected. Refer to the "Logger Service" section of the *Discover by Uptivity Installation Guide* for more information.

Configure Logging Settings

To configure Logging Settings:

1. Click the **Administration** tab and expand **System Settings** in the left navigation menu.
2. Click **Logging Settings**.
3. Enter or edit the **Log Directory** path if desired.
4. Enter or change any desired **Logging Levels** settings.
5. Click **Save**.

Discover Mail

Multiple Discover features can use email to communicate to users. An email account will need to be created in your email system for Discover's use. Once that account is ready, you will need to configure the Discover settings for the email account. These are divided into two sections: **Server Settings** and **Secure Settings**. The settings for Discover's **Forgot Password** functionality are also configured in this area.

Discover Mail Settings

The following are in Discover Mail **Server Settings**:

- **Mail Server Host.** Enter the hostname or IP address of the SMTP mail server Discover will use to export recordings via email.
- **Mail Server Port.** Identify 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 Discover Mail **Secure Settings**:

- **Username.** Enter the Username for authentication onto the SMTP server.
- **Password.** Enter the Password for authentication onto the SMTP server.
- **Confirm Password.**

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

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

Configure Discover Mail

To configure **Discover Mail Settings**:

1. Click the **Administration** tab and expand **System Settings** in the left navigation menu.
2. Click **Mail Settings**.
3. Enter **Server Settings** as needed
4. Enter **Secure Settings** as needed.
5. Enter **Forgot Password Mail Settings** as needed.
6. Click **Save**.

    Note If you make changes to mail settings, you must restart the API server before calls can be exported via email from the Web Player call list.

Notifications

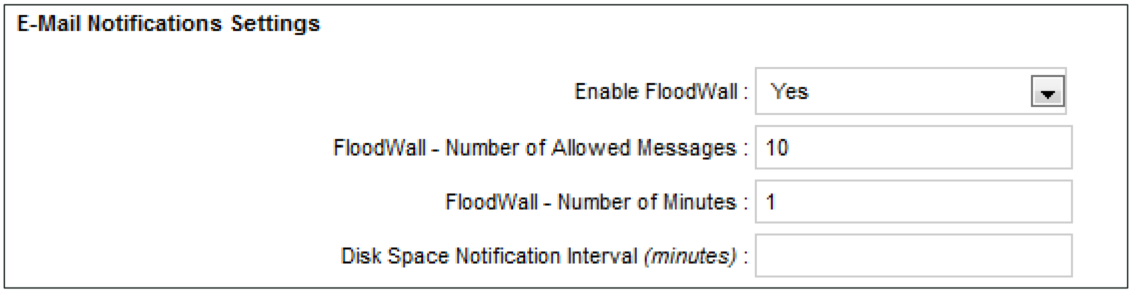
Notifications allow you to adjust how long Discover retains information in its log files, and also lets you configure audible and/or email maintenance alerts. Discover offers different types and levels of alert subscriptions to help you effectively manage your system.

> **Note** Be sure to consider disk size when deciding how long to retain log files.

Types of Alert Subscriptions

- **Critical:** A service or system has stopped functioning completely due to an error. Uptivity recommends you 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. Uptivity recommends you 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. Uptivity recommends you have at least one email subscription notified of any license alerts. License events that are logged and generate notifications are:
    - 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. Uptivity recommends you have at least one email subscription notified of any error alerts.
- **Security:** A security event, such as multiple password failures, has occurred. Uptivity recommends you 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. Uptivity does not recommend warning alerts be enabled by default.
- **Info:** General system information. Uptivity does not recommend info alerts be enabled by default.
- **Notice:** An informational notice regarding system events. Uptivity does not recommend notice alerts be enabled by default.
- **Testing:** Enhanced debugging and development information enabled for troubleshooting. Uptivity does not recommend testing alerts be enabled by default.
- **Debug:** Highest volume/detail output for all modules. Uptivity does not recommend debug alerts be enabled by default.
- **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.** Works with Disk Space Notifications to alert subscribers when the amount of free space on a disk has dropped below the specified level.

E-Mail Notifications Settings



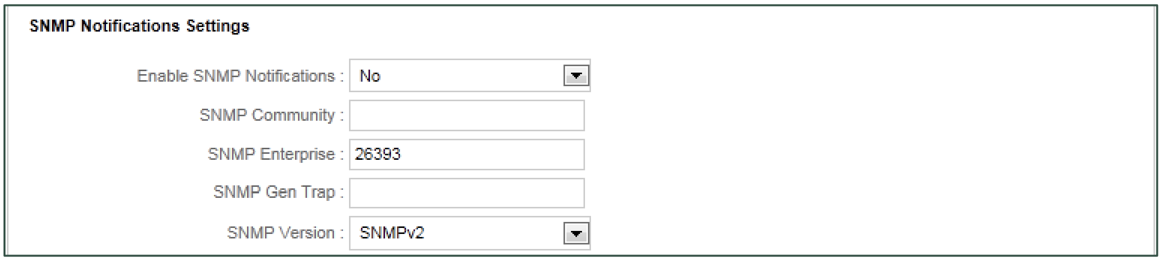
E-Mail Notifications Settings

Enable FloodWall :	Yes
FloodWall - Number of Allowed Messages :	10
FloodWall - Number of Minutes :	1
Disk Space Notification Interval *(minutes)* :	

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 enables, the floodwall will throttle email alerts to prevent overloading your mail server.
- **Floodwall - Number of Allowed Messages** Works with the floodwall setting to specify the number of email messages the server will send per interval. Any further messages of the same type will be blocked until the interval expires.
- **Floodwall - Number of Minutes.** Works with the floodwall setting to define the number of minutes per interval.
- **Disk Space Notification Interval** Interval in minutes between sending low disk space email alerts.

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.** Allows Discover to send SNMP traps.
- **SNMP Community.** Optional value. Some SNMP management applications require this value to allow the Discover system access.
- **SNMP Enterprise.** Identifier for Discover-generated SNMP events. Discover is IANA-registered as 26393.
- **SNMP Gen Trap.** Optional. This generic type value can be used to distinguish between multiple Discover systems.
- **SNMP Version.** Discover can generate both version 1 or 2 traps, depending on type are 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.
4. Check each type of condition that should trigger an audible alert.
5. Enter the number of days you want Discover to retain log files.
6. Configure **E-mail Notifications Settings** as desired.
7. For each email subscription, click **Add E-mail** and enter the email address, then select the check box for each type of alert which should be sent to that email address.
8. Configure **SNMP Notifications Settings** as desired.
9. For each SNMP subscription, click **Add SNMP** and enter the SNMP address, then select the check box for each type of alert which should be sent to that SNMP address.
10. Click **Save**.

Test Alerts

This feature sends a message to all users who have subscribed to 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 a message explaining that the message is a test and what type of notification is being tested.
4. Click **Test**.

Confirm with each user who was supposed to receive the test message.

Desktop Recording

Desktop Recording Servers are typically configured by Uptivity as part of the installation process. If Desktop Recording is used in your environment, this section will help you understand the settings that govern its operation. Do not change these settings without contacting Uptivity Support. To view the settings:

- Click the **Administration** tab and expand **System Settings** in the left navigation menu. Then click **Screen Capture Settings** and click the **Edit** icon for the server you wish to view.

Desktop Recording Server Settings

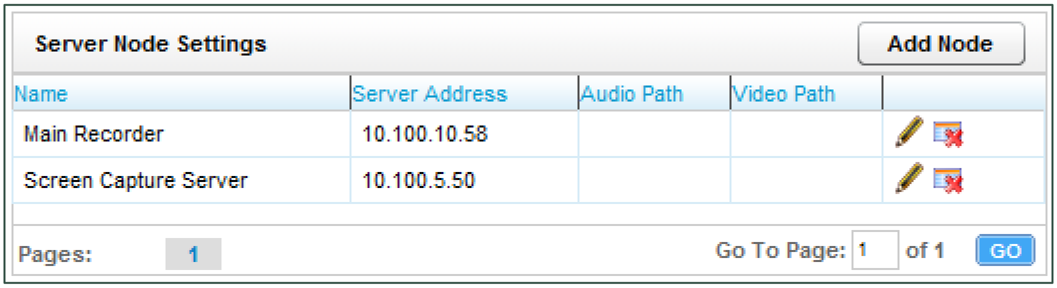
- **Host.** IP address of the Desktop Recording Server.
- **Port.** Communication port used by the Desktop Recording Server.
- **HTTP Port.** Port used for messaging traffic with Info Broker. Default is 2014.
- **Write to Temp.** Enabled when the Desktop Recording Server is not local to the recording 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 Desktop Recording Server is associated.

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, but there are occasions when a Server Node must be added or changed on a production system.

If services are added or moved to new machines, those services will need to be added to their new node after the service installation is complete. Delete the old node only after the new services are running correctly.

Adding, deleting, or editing a Server Node also adds, deletes, or changes a corresponding CometDaemon. If you change a Server Node, you must check the settings of its Comet Daemon and make any needed changes. You must also add, edit or delete the Server Node in the Service Manager. Do not delete a Server Node before removing all associated services in the Service Manager.



Server Node Settings

Name	Server Address	Audio Path	Video Path	
Main Recorder	10.100.10.58			✎ ✖
Screen Capture Server	10.100.5.50			✎ ✖

Configure Server Nodes

To add a Server Node:

1. Click the **Administration** tab and expand **System Settings** in the left navigation menu.
2. Click **Server Nodes**.
3. Click **Add Node**.
4. Enter a meaningful **Name** that will allow you to easily distinguish between Server Nodes.
5. In the **Address** field, enter either the hostname or IP address of the Server Node.
6. Click **Save Node**.

> **Note** The remaining settings on this page are no longer managed by Server Node and may be disregarded.

To edit or delete an existing Server Node:

1. Click the **Administration** tab and expand **System Settings** in the left navigation menu.
2. Click **Server Nodes**.
3. To change the settings for the Server Node, click the ✏ icon for the desired node; to delete the node, click the ❌ icon.
4. Click **Save Node** if applicable.

Web Media Server

Web Media Server (WMS) is a Discover module that manages both playback of recordings and streaming for live monitoring. The Web Media Server service is started during installation, but additional configuration can be performed in the Web Portal. 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.

Configure Web Media Server

To add a Web Media Server:

1. Click the **Administration** tab and expand **System Settings** in the left navigation menu.
2. Click **Web Media Server Settings**.
3. Click **Add**.
4. Enter the appropriate settings.
5. Click **Save**.

To edit or delete an existing Web Media Server:

1. Click the **Administration** tab and expand **System Settings** in the left navigation menu.
2. Click **Web Media Server Settings**.
3. To change the settings for the Web Media Server, click the ✏ icon for the desired server; to delete the server, click the ☒ icon.
4. Click **Save**.

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 Desktop Recording Server. Default is 5630.
- **HTTP Port:** Port used for messaging traffic with Info Broker. Default is 2015.
- **Allow Live Monitor:** Must be checked if the Web Media Server will be used for Live Monitoring.
- **Excessive Debugging:** Check to add detailed logging 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 TCP connection to API server attempts to reconnect.
- **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)
- **SSL Certificate Pass:** SSL certificate password
- **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.

Web Server

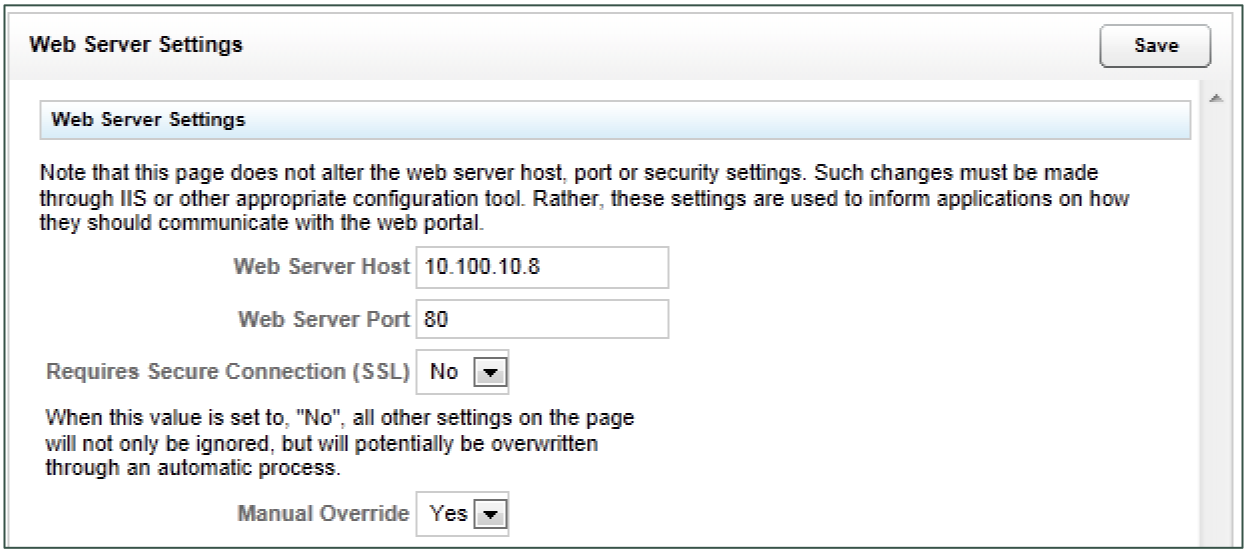
Several Discover services, such as call playback, utilize Web Server services. For example, when reviewing reports, users can click links in reports to play calls. Discover detects the Web Server IP address and port during startup. When Discover services are distributed on multiple machines and the machine hosting the Web Server has more than one network interface card, Discover may detect the wrong IP and port. In this case, the Reporting Server is provided the wrong information and is not able to access Web services. Users receive an access error message. Manually setting the Web Server settings avoids this problem. These settings should be configured during the initial installation.

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.

Configure Web Server Settings

To enter the settings:

1. Click the **Administration** tab and expand **System Settings** in the left navigation menu.
2. Click **Web Server Settings**.
3. Set **Manual Override** to **Yes**.
4. In the **Web Server Host** field, enter the IP address the IIS server hosting the Web Server.
5. In the **Web Server Port** field, enter the port on which the Web Server will communicate.
6. In the **Requires Secure Connection (SSL)** field, select **Yes** from the drop-down menu if SSL has been set up on IIS.
7. Click **Save**.



Note that this page does not alter the web server host, port or security settings. Such changes must be made through IIS or other appropriate configuration tool. Rather, these settings are used to inform applications on how they should communicate with the web portal.

Web Server Host: 10.100.10.8

Web Server Port: 80

Requires Secure Connection (SSL): No

When this value is set to, "No", all other settings on the page will not only be ignored, but will potentially be overwritten through an automatic process.

Manual Override: Yes

If Manual Override is disabled after having been enabled, the values in the Web Server Host and Web Server Port field will be blanked. If this happens, users will not be able to play back calls from links in reports until the values are restored. There are two ways to resolve this.

- Open the web.config file, add a blank line at the beginning or end, save it, delete the blank line you just entered, save it again, reopen the site and it will recompile the web.config and re-insert the default automatic values for these fields. This method requires a bit more time/care but is less invasive than #2 because it only affects Discover.
- Open IIS, restart the Application Pool for CCWeb, or restart the IIS service entirely. This method is perhaps easier, but if other sites at the company rely on IIS, restarting it as a whole could cause a brief interruption in service.

Once you apply your chosen fix, go back to Administration -> System Settings -> Web Server Settings and verify that the fields are now filled.

Workstations Settings

Core uses the Workstations List to determine the Desktop Recording Server with which it should communicate. The list is not used in all installations. For more information, see "Add Workstations" in the "Desktop Recording Server Configuration" section of the *Desktop Recording Administration Manual*.

Settings.ini

This file stores settings for a wide range of software components, including survey configuration, software modules, archiving, and settings and credentials for accessing the Discover databases. If you are interested in encrypting the credentials stored in this file, contact Uptivity Support and reference knowledge base article # 000001461. It is **strongly recommended** that customers **do not** attempt to modify the contents of this file. Doing so may cause components or even the entire system to stop working.

Web Portal Settings

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 primarily configured by Uptivity at the time of installation, but changes to a Server Node can require changes to its CometDaemon.

Configure CometDaemon

To edit a Comet Daemon:

1. Click the **Administration** tab and expand **Web Portal Settings** in the left navigation menu.
2. Click **CometDaemon** and expand a Server Node to view the settings for its CometDaemon.
3. Edit any settings as needed.
4. Click **Save**.

CometDaemon Settings

CometDaemon settings can be viewed and/or configured through the Discover Web Portal. Unless otherwise specified, the default settings should be used.

- **HTTP Port**: This value should not be changed.
- **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**: Specifies valid IP address ranges from which clients are allowed to communicate using Discover Toolbar Client. This subnet can use CIDR notation and be comma-separated.
- **Allowed Subnets System:** Specifies valid, secure IP ranges from which Service Manager can communicate with Discover Toolbar. For optimal security, this range should be limited so only administrators can access the server. In multi-server configurations, on the Web Portal Server Node, set this to the subnet/IP of the server. This subnet can use CIDR notation and be comma-separated.
- **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:** Informational only and cannot be changed.
- **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:** Discover Install directory. The module knows what Discover services are available based on the directory's contents. If Discover was installed to a different directory, this setting must be changed to that directory. This field is case sensitive.

Security

To enhance system security, Discover lets you control login and password settings for the Web Portal and specify certain parameters of its integration with Active Directory. Other security features, such as recording file encryption, SSL, TLS, and IIS settings for session and login security are addressed by different settings. For settings details, see System Security.

Login, Password and AD Integration Settings

These settings, which are configured on the Security page, include:

- **Site Settings.** Allow you to specify the IP address or hostname where users will access Discover and, if applicable, Clarity. IP address entries should 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. The following settings work in conjunction with the appropriate permissions and Discover Mail:
    - **Password Max Length.**
    - **Password special characters length.**
    - **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.** Users can 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.

Notes on AD Integration

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 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.

If your system uses AD or hybrid mode, the following settings are configurable:

  - **Auto Create User on Login.** 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 enabled, automatically updates each User's Groups, Roles, and Permissions accordingly upon login. If not enabled, 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).

    Note 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 all lowercase, 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 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.** Enables/requires the use of SSL.
  - **Signing.** Enables LDAP security; enabling it here and in Windows Server encrypts the connection between them.

- **Login Settings.** These settings govern other factors associated with the login mode your system uses.

  - **Access Type.** Specifies your system login mode.
  - **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. Default expiration 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**. 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.

  Note These settings apply *only* to Discover database user accounts. If you are using AD or hybrid authentication, the AD accounts and passwords are managed through Active Directory/group policy.

  - **Password Strength Enforcement:** When 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.** 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 accounts, including the superuser account.
  - **Prevent Re-use of Passwords.** When enabled, password changes are checked against a password history to prevent re-use. You can set the **Number of previous passwords to check** (e.g. password cannot be the same as the last 5 used) or the **Number of days between password change** (e.g. 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 enabled, user accounts are locked after the defined number of failed login attempts. 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 option is selected.

  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.
- **HTTP/**HTTPS **Settings.** When **Force the site to use HTTPS** is checked, 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.

Configure Login, Password and AD Integration Settings

To configure these settings:

1. Click the **Administration** tab and expand **Web Portal Settings** in the left navigation menu.
2. Click **Security**.
3. Configures any settings as needed.
4. Click **Save**.

Configure AD Group Role Synch

AD Group Role Synch is enabled simply by adding AD groups to your Active Directory settings. To add an AD group:

1. Click the **Administration** tab and expand **Web Portal Settings** in the left navigation menu.
2. Click **Security**.
3. Under **Active Directory Settings**, click **Add Group**.
4. Enter the name of the AD group (group names are case-sensitive).
5. To associate Discover Roles with the AD group, click **Add/Edit Roles** and move any desired Roles from the Uassigned to the Assigned column. Click **Apply**.
6. Click **Save**.

Depending on how your AD is configured, you may see a clickable link that allows you to test validation of the AD groups configured in Discover. When available, the test can return the following results:

> ✓ -- This indicates the Group checks out as valid in Active Directory.
>
> ✗ -- This indicates that the Group could not be validated with Active Directory. If validation fails, verify the spelling and case of the Group name, the LDAP string, and the presence of the Group in AD.

To remove an AD group and disassociate any Roles, delete the group from your Active Directory settings. Removing a group will cause members of that group to lose access to Discover.

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.

Available Fields

- **Switch Type.** This is a list of common ACD/PBX hardware manufacturers. When you choose one of these switch types, Discover will auto-populate the terminology names with commonly used descriptions for that type. 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).** Dialed Number Identification Service - call identifier from the telecommunications carrier. For inbound calls, this would be the number the caller dialed to reach you.
- **CallerID (ANI).** Number of the calling party as provided from the telecommunications carrier.
- **Device/Port ID.** Hardware identifier in your ACD/PBX (e.g., Position ID, Phone Port, DN, or Extension).
- **Agent Number (Device Alias).** Phone number/extension in your ACD/PBX to which calls are delivered. This is commonly an agent phone login or extension.
- **Group Name.** Discover Group. For details, see Discover Groups.
- **User 1 – 15.** Custom data fields not normally utilized in the Discover system. 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. You can rename them to be more descriptive regarding the data contained within the field.

  Notes

  The settings on this page can be automatically populated via the Uptivity API. Further documentation regarding the API can be found in the *Uptivity API Manual*.

  Angle brackets (i.e., < >), some special characters, and symbols may cause interactions with User fields not to work. System administrators using these fields with the Uptivity API must thoroughly test any calls they make. Discover On-Demand users should be trained to avoid use of these characters.

  Terminology page settings changes will not appear in the ad hoc reporting pages immediately. The Discover application pool in IIS must be recycled in order for the changes to appear.

  Terminology changes affect only Discover and do not carry through to Clarity in hybrid systems.

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**.

Web Portal

The Web Portal page allows you to configure settings for the Web Portal and Web Player. The majority of these are set by Uptivity during installation.

- **Content Management Upload Directory.** Disk or UNC path where files uploaded to the Content Library are stored. For typical installations, Discover runs under the IUSR/IIS_IUSRS account, which will not have permissions to this default directory.
- **Fusion Script Settings Upload Directory.** If the Uptivity Desktop Analytics (formerly known as Fusion) application was purchased, the scripts used to manage Desktop Analytics clients are loaded into this directory. Make sure the account under which the Desktop Analytics server runs has access to this directory.
- **Location Settings: Allow Lookup by Agent/Workstation.** Enable this setting ONLY if your environment is segmented in a way that inhibits standard agent lookup by Location. For example, if all your telephony hardware and call routing is done from one Location but agents, Desktop 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 Desktop 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. Desktop recording will not take place for agents who do not have a specific, valid Location. If this setting is enabled, every Core will connect to every Desktop Recording Server. For more information on assigning agents to specific Locations, see Add a User.
- **Call Segment Settings: Allow Call Segments.** Enabled in certain environments where Call Segments can be generated and related for viewing in the Call List. Refer to the *Discover by Uptivity 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.** Controls whether preview data appears on the Report Builder page in ad hoc reporting for both Discover and Clarity. If 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.

  Note In standalone Clarity systems, preview data is displayed by default and the setting cannot be changed.

Home Tab Widgets

> **Note** This content applies only to Home tab widgets. For specific information on configuring dashboards and individual widgets, refer to the *Discover by Uptivity Widget Administration Manual*.

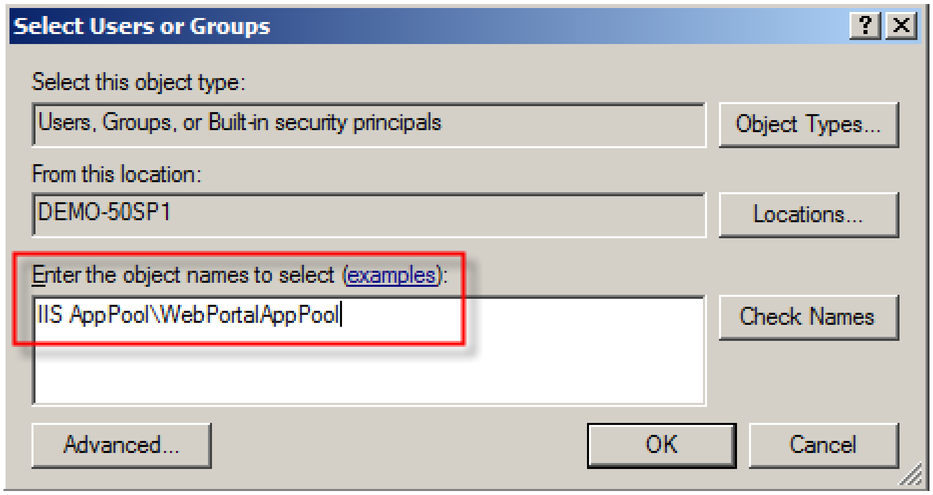
You can administer which widgets are available to users for dashboard configuration on their Home tab. This includes adding new widgets, editing existing widgets and deleting widgets from those available.

> **Important** 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.**

Configure Remote Widget Management

Widget DLLs are stored in "\Program Files (x86)\CallCopy\WebPortal\bin." If you manage widgets remotely, the Web Portal application pool in IIS will need Full Control permissions to this folder. To configure these permissions:

1. Browse to \Program Files (x86)\CallCopy\WebPortal\bin on your Web Portal server.
2. Right-click on the **bin** folder.
3. Click **Properties**.
4. Open the **Security** tab.
5. If the Web Portal application pool (typically named **WebPortalAppPool**) is not listed, click **Edit**. If it is already listed, skip to step 8.
6. Click **Add**.
7. Under "Enter the object name to select," enter "IIS AppPool\[Web Portal application pool name]."



Select Users or Groups

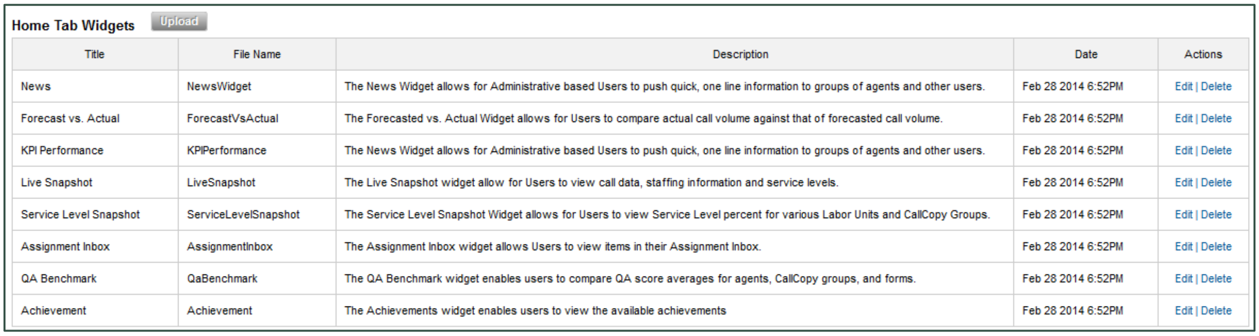
Select this object type:
Users, Groups, or Built-in security principals

From this location:
DEMO-50SP1

Enter the object names to select (examples):
IIS AppPool\WebPortalAppPool

8. Click **OK**.
9. With the application pool selected, select the check box for **Full Control** and click **OK**.

Widget List



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	Edit | Delete
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	Edit | Delete
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	Edit | Delete
Live Snapshot	LiveSnapshot	The Live Snapshot widget allow for Users to view call data, staffing information and service levels.	Feb 28 2014 6:52PM	Edit | Delete
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	Edit | Delete
Assignment Inbox	AssignmentInbox	The Assignment Inbox widget allows Users to view items in their Assignment Inbox.	Feb 28 2014 6:52PM	Edit | Delete
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	Edit | Delete
Achievement	Achievement	The Achievements widget enables users to view the available achievements	Feb 28 2014 6:52PM	Edit | Delete

The Widget 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.

Manage Widgets

Possible interactions with Home tab widgets include:

- **Upload:** New widgets can be added by clicking the Upload button and selecting the corresponding widget DLL. The Date column shows when the widget was uploaded or last updated. New versions of existing widgets can be uploaded as well. 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.
- **Edit:** Allows the Title (25 character max) and Description (200 character max) of the widget to be modified. Changes take effect immediately, do not require clicking Save, and will not affect login status of connected users.
- **Delete:** Removes a widget from the system and removes the corresponding DLL from the server. Removing a widget from the system removes it from any user dashboards where it was displayed.

> **Note** Uptivity recommends that widget DLLs be backed up before deletion in case they are needed again later. The following are included by default:
>
> - AssignmentInbox.dll
> - ForecastVsActual.dll
> - KPIPerformance.dll
> - LiveSnapshot.dll
> - NewsWidget.dll
> - QaPerformance.dll
> - ServiceLevel.dll

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.

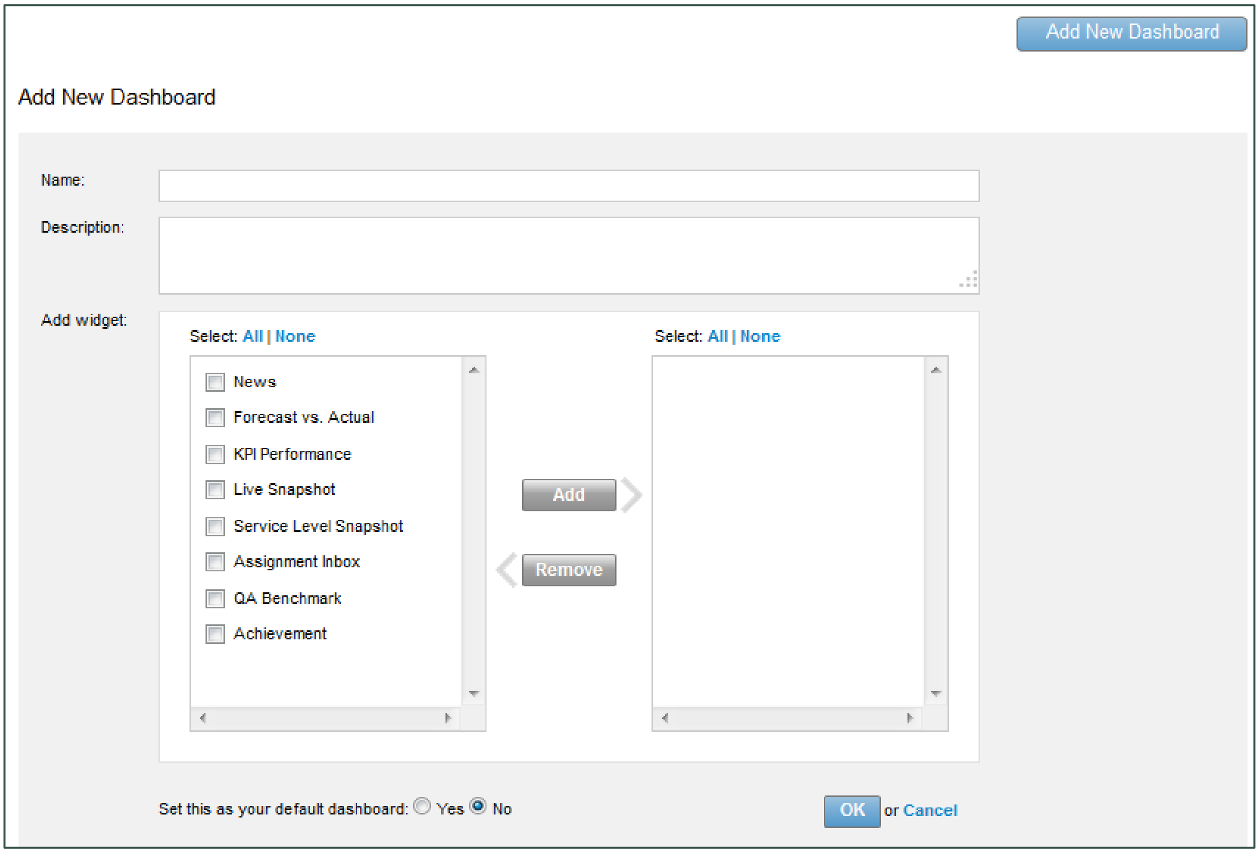
Manage Dashboards

Once widgets are configured on the Administration tab, custom dashboards can be created and managed from the Home tab. The News dashboard/widget is displayed by default, but can be reconfigured or removed.

1. Under Dashboard on the left navigation menu, click **Manage Dashboards**.
2. Click **Add New Dashboard**. The Add New Dashboard dialog opens under the Dashboard List.
3. Add a **Name** (must be unique, 25 characters max) and **Description** (200 characters max).
4. Select the check boxes next to the widgets to be displayed and click **Add**. The same widget can be displayed multiple times on the same dashboard. A maximum of 10 widgets can be displayed per dashboard (this is a browser performance constraint).
5. Choose whether to set this dashboard as the default.

   Note If you view another dashboard, the default setting is overwritten. When you log in again, the last dashboard viewed is displayed.

6. Click **OK** to commit changes or **Cancel** to close without saving changes.



Add New Dashboard

Name:

Description:

Add widget:

Select: All | None

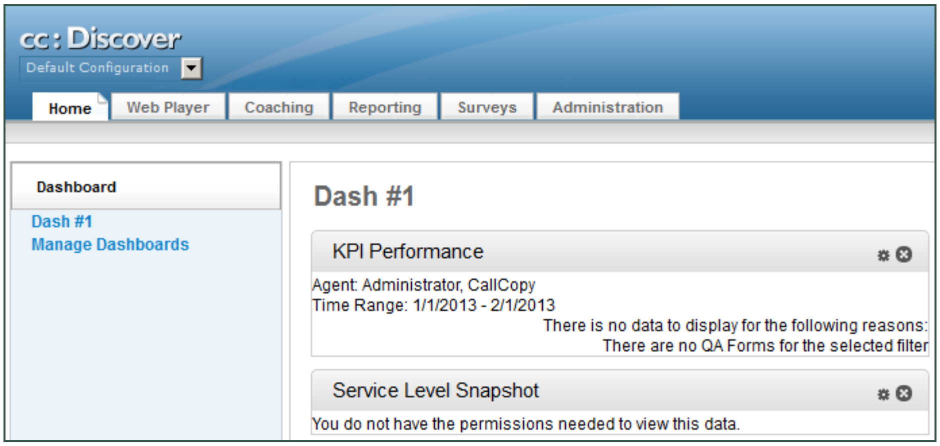
□ News
□ Forecast vs. Actual
□ KPI Performance
□ Live Snapshot
□ Service Level Snapshot
□ Assignment Inbox
□ QA Benchmark
□ Achievement

Select: All | None

Set this as your default dashboard: ○ Yes ● No

The name of the new dashboard will appear under Dashboard in the left navigation menu, sorted alphabetically with numbers first. Users can create an unlimited number of different dashboards. Click on the dashboard to view. From here, you can drag displayed widgets to rearrange as needed, and they will retain the specified order across subsequent logins. The last dashboard selected will persist when switching tabs.

Each widget can be configured by clicking on the **Gear** icon ⚙ on the widget title bar. Widgets can be removed by clicking the **Remove** icon ⊗. Additional dashboards can be configured by repeating this process, and will appear listed under Dashboards on the left navigation menu. Click a different dashboard to change between them. To edit or delete a dashboard, click **Manage Dashboards**, then click **Edit** or **Delete** under Actions for the corresponding dashboard.



Agent: Administrator, CallCopy
Time Range: 1/1/2013 - 2/1/2013
There is no data to display for the following reasons:
There are no QA Forms for the selected filter

You do not have the permissions needed to view this data.

Since widgets pull information from different products – some of which may not apply to your configuration – for information on configuring individual widgets and their settings and permissions, refer to the *Discover by Uptivity Widget Administration Manual*.

Web.config

This file stores settings for a variety of aspects of the Discover Web Portal, including debugging, logging levels, connection information for Live Monitoring and Web Media servers, and configurations for SSL, SMTP, and reporting services. Also stored here are connection strings with credentials for accessing the Discover databases. If you are interested in encrypting the credentials stored in this file, contact Uptivity Support and reference knowledge base article # 000001460.

It is **strongly recommended** that customers **do not** attempt to modify the contents of this file. Doing so may cause components or even the entire system to stop working.

System Security in Discover

Security Design

This section explains Discover's high-level security design so that system administrators understand how different features work together. Additional details may be available in sections specific to a Discover feature.

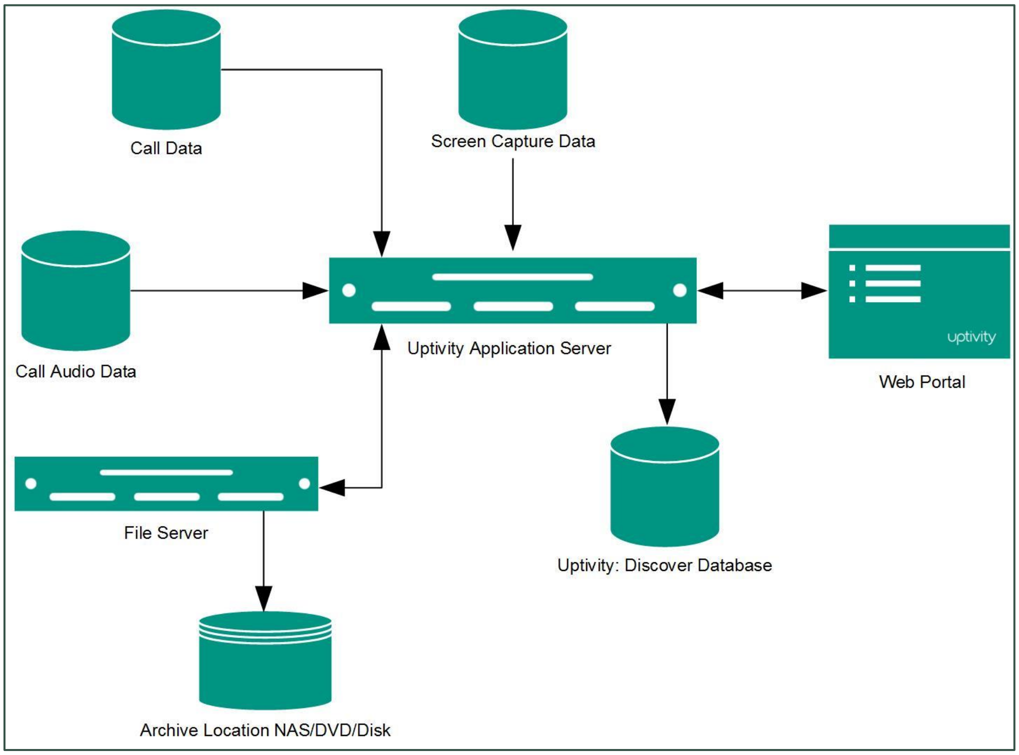
As a general rule, Discover receives call audio from the PBX or agent telephone. Call data comes from the PBX. Desktop recording data is received from the agent's PC over the LAN/WAN.

Discover recorders write the audio and screen data to files on the Windows File Server. Files can be encrypted if encryption keys are created. 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.

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.

Recordings can be archived, if needed, to network attached storage, DVDs, ENC Centera XAM, or disks.

Records and archives can be configured with retention periods and automated purging.


Call Data
Screen Capture Data
Call Audio Data
Uptivity Application Server
uptivity
Web Portal
File Server
Uptivity: Discover Database
Archive Location NAS/DVD/Disk

Interactions between the Discover suite 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

Uptivity recommends blanking audio and screen recording when sensitive data is being referenced or collected by any Discover system. This feature is referred to as a "blackout." Refer to the *Discover by Uptivity Installation Guide* for more information on configuring the API server to perform blackouts.

Blackouts in Discover can be triggered:

- 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 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 Uptivity 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 Desktop 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 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 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 Archiver Console.

Automatic purging of data is controlled by schedules and archive actions in Discover.

Files can be written and archived to network-attached storage (NAS) devices and DVDs. Discover cannot purge data from devices or disks that are not currently connected to the network.

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 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:

- 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 Desktop 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. Uptivity 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 database (SQL) – 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. See the *Discover by Uptivity Installation Guide* for specific instructions.
- When separate Uptivity Desktop 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 Logging. Additional logging information appears in administration manuals for each Uptivity application. Auditing information is discussed in the *Discover by Uptivity 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 details, see Login, Password and AD Integration 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."

IIS Site Settings for Hybrid Mode and AD Authentication

This task must be completed for both Hybrid Mode and AD authentication on the machine running Discover.

Windows Server 2008/IIS 7.x

1. Click the **Start** button and type **IIS Manager** in the **Search programs and files** box.
2. Click on **Internet Information Services (IIS) Manager**.
3. Expand **Sites**.
4. Click **CCWeb** to see the site properties in the center panel.
5. Under the **IIS section**, double-click **Authentication**.
6. If **Anonymous Authentication** is not enabled, right-click it and select **Enable**.

Windows Server 2012

1. Click **Server Manager** from the **Start** menu.
1. Click **IIS**.
2. Right-click the desired **Server Name** and select **Internet Information Services (IIS) Manager**.
3. Expand the desired Server Name in the Connections pane and then expand **Sites**.
4. Click **CCWeb** to see the site properties in the center panel.
5. Under the **IIS section**, double-click **Authentication**.
6. If **Anonymous Authentication** is not enabled, right-click it and select **Enable**.

Settings Changes for Former AD Auto-Login Environments

If you are upgrading from a previous version of Discover that allowed automatic login (i.e., single sign-on) with AD authentication, for security reasons, and **provided such changes do not conflict with the operation of any other existing applications**, your Uptivity installation team will modify the following settings as needed.

Windows Server 2008/IIS 7.x Win Login Settings

1. In IIS Manager, expand Web Sites > CallCopy web site.
2. In the Features View pane, open **Authentication**.
3. Right-click **Windows Authentication** and choose **Disable**.
4. Right-click **Anonymous Authentication** and choose **Enable**.
5. Right-click **Anonymous Authentication** again and choose **Edit**.
6. Configure to use a specific user account or application pool identity according to customer's environment.

Windows Server 2012

1. Click **Server Manager** from the **Start** menu.
2. Click **IIS**.
3. Right-click the desired **Server Name** and expand **Sites** in the **Connections** pane.
4. Click **CCWeb**.
5. In the center pane, double-click **Authentication**.
6. Right-click **Anonymous Authentication** and choose **Enable**.
7. Right-click **Anonymous Authentication** again and choose **Edit**.
8. Configure to use a specific user account or application pool identity according to customer's environment.

Internet Explorer Settings – Must Be Changed for Each User

1. In Internet Explorer, open **Tools** > **Internet Options** and click the **Security** tab.
2. Click **Local Intranet** > **Custom Level**.
3. In the Settings list, scroll to **User Authentication**. Set this to the mode required by the customer.
4. On the Advanced tab's Settings list, scroll to the **Security** section. If not required by any other customer applications, clear the check box for **Enable Integrated Windows Authentication**.
5. Click **OK**. Restart Internet Explorer for the settings to take effect.

Other than having to now log in manually to Discover/Clarity, there should be no change to the agent-side experience of using the software.

IIS Session Timeout

For Windows servers, session timeout is affected by several processes. You can configure an approximate session time setting using IIS Manager in Windows. The setting can also be adjusted via the Discover Web Portal configuration file. Changing it in one location automatically updates it in the other. For assistance in editing the Web Portal configuration file, contact Uptivity Support.

Windows Server 2008/IIS 7.x

1. On the server hosting Discover, click the **Start** button and type **IIS Manager** in the **Search programs and files box**.
2. Click on **Internet Information Services (IIS) Manager**.
3. Click on **Application Pools**. Right-click the application pool for the Discover site, then **Advanced Settings**.
4. Expand **Process Model** and update "Idle Time-out (minutes)" to 15 minutes.

Windows Server 2012

1. On the server hosting Discover, click **Server Manager** from the **Start** menu.
2. Click **IIS**.
3. Right-click the desired **Server Name** and select **Internet Information Services (IIS) Manager**.
4. Expand the server entry in the **Connections** pane.
5. Click on **Application Pools**. Right-click the application pool for the Discover site (typically WebPortalAppPool) and select **Advanced Settings**.
6. Expand **Process Model** and update Idle Time-out (minutes) to the desired time period.

Web Portal Configuration

To edit the Web Portal configuration file:

1. On the server hosting Discover, open Windows Explorer and navigate to C:\Program Files\CallCopy\WebPortal.
2. Open the Web.config file.
3. Find <sessionState timeout="60"/>. Change the value to 15.
4. Save changes.

   Note If you set the recycling interval on the site's application pool in IIS to a lower threshold than the timeout threshold in Discover, the site will recycle every 60 minutes, causing user sessions to time out unexpectedly and possible data loss. This is a bug with IIS. It is best to set the recycling interval greater than or equal to the session timeout threshold.

File Encryption

Discover supports file level encryption for almost all audio and video data files (the exceptions are noted below). To enable encryption, a system administrator must generate encryption keys. 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. The encryption is based on a unique key generated for each individual system. 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 Support personnel. Contact Support for more information.

While it is possible to encrypt existing recordings by reprocessing them with the transcoder after enabling encryption, it is not recommended because:

- All new calls to be transcoded would be queued up behind this work, meaning new calls cannot be reviewed or played back until the queue is cleared.
- A mass replace statement would need done to change the source type from CCA to WAV.
- A purge record in the transcoder database table would clear records, making it impossible to re-transcode any associated calls.

Encryption exceptions:

- 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 Transcoder will convert these files to an encrypted format if/when they are transcoded.
- Stereo .wav files generated by the Transcoder for speech analytics are not encrypted since the speech analytics engine cannot read encrypted files. Once analytics data has been captured, the calls can be encrypted when archived, or deleted during a file purge. If security of the stereo .wav files is a concern, they can be stored on an encrypted disk volume, though this will negatively impact performance of the speech analytics engine when reading the files.
- The .xml files that contain call metadata are not encrypted. However, the option exists to turn off .xml file generation. The XML file generation toggle is on the CTI Cores setting page under Administration > Recorder Settings > CTI Cores.

Generating Keys

Key generation activates encryption in Discover, and the databases have tables to store keys by default. Keys can be generated and managed using the cc_crypt.exe that is installed in the recorder directory. This is a command line tool that accepts various parameters to generate, list, deactivate and reactivate keys. Many commands will require you to type the database password to complete the operation.

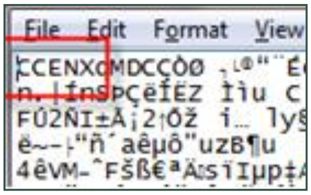
Any module that uses the encryption libraries will need to be able to query the database for the keys to encrypt/decrypt the files. If there are active keys in the database, the modules supporting encryption should automatically load and use them on startup. Modules will also periodically reload the keys to check for changes once every 15 minutes.

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, 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.

Encryption Status Verification

To determine whether a particular recording file is encrypted, use one of the following methods.

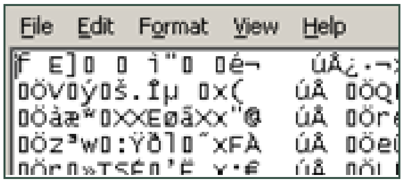


Check the File Header

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.

Validate Using cc_crypt's Master Key Command



Run the following command against the file(s) in question: cc_crypt masterkey [filename]

- If the file is encrypted, the output will read "Master key: [key ID]"
- If the file is not encrypted, the output will read " Command failed: Header doesn't match - file may not be encrypted."

For details, see cc_crypt Utility Commands.

Considerations

- 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.

cc_crypt Utility Commands

The cc_crypt utility can be used to execute the listed commands. It is executed from a command prompt on any Discover server. A correctly-formatted example is shown with each **Command** below, along with information specific to that command. You can also see additional information by using the **Get help** function.

Function	Command
Get help (list commands)	cc_crypt.exe help
Get help with a command	cc_crypt.exe help [command]
Generate a key	cc_crypt.exe genkey
List active keys	cc_crypt.exe list
List active and inactive keys	cc_crypt.exe list -inactive
Deactivate a key	cc_crypt.exe deactivate {fingerprint} Ex.: cc_crypt.exe deactivate -fingerprint=0032F242
Reactivate a key	cc_crypt.exe activate {fingerprint} Ex.: cc_crypt.exe activate -fingerprint=0032F242
Export keys to a password protected file	cc_crypt.exe export {keyfile} Ex.: cc_crypt.exe export keyfile -password=secret - keyfile: filename of encrypted export file with keys; can be anything with any file extension - password: the password used to encrypt the exported file, also required to import it back into the database. If password is not included, you will be prompted for it.

Include inactive keys	cc_crypt.exe export {keyfile} –inactive Ex.: cc_crypt.exe export keyfile -password=secret -inactive - keyfile: filename of encrypted export file with keys - password: the password used to encrypt the exported file, also required to import it back into the database. If password is not included, you will be prompted for it. - inactive switch (optional) includes inactive keys along with active keys
Import keys from a password protected file	cc_crypt.exe import {keyfile} Ex.: cc_crypt.exe import keyfile -password=secret -inactive - keyfile: filename of encrypted export file with keys - password: the password used to encrypt the exported file, also required to import it back into the database. If password is not included, you will be prompted for it. - inactive switch includes inactive keys along with active keys
Encrypt a file using the current master key	cc_crypt.exe encrypt {filename} {encrypted_filename} -Ex.: cc_crypt.exe encrypt UnencryptedFile EncryptedFile
Decrypt a file (must have appropriate master key in database)	cc_crypt.exe decrypt {encrypted_filename} {filename} Ex.: cc_crypt.exe decrypt EncryptedFile UnencryptedFile
Decrypt a file using a master key from an export file (database is not available)	cc_crypt.exe decrypt {encrypted_filename} {filename} -keyfile={keyfile} Ex.: cc_crypt.exe decrypt EncryptedFile UnencryptedFile -keyfile=[keyfile filename] -password=secret - Password is only required if keyfile is supplied; if password is not included, user will be prompted for it.
Encrypt a file with a password (anyone who wants to decrypt it will need to know the password)	cc_crypt.exe pencrypt {filename} {encrypted_filename} Ex.: cc_crypt.exe pencrypt UnencryptedFile EncryptedFile -password=secret - Encrypts a file with a password but does NOT use master keys.

Decrypt a file that was encrypted with a password	cc_crypt.exe pdecrypt {encrypted_filename} {filename} Ex. cc_crypt.exe pdecrypt EncryptedFile UnencryptedFile -password=secret - Password is only required if keyfile is supplied; if password is not included, user will be prompted for it.
Show the master key fingerprint that was used to encrypt a file	cc_crypt.exe masterkey {encrypted_filename} Ex.: cc_crypt.exe masterkey "F:\CallCopy\Recordings\Cisco MediaSense\Encrypted\20140226\3000\3000-15-43-51.cca" - Output response is "Master key: 0032F242"
Take an arbitrary setting value and encrypt it	cc_crypt.exe encryptsetting {value} Ex.: cc_crypt.exe encryptsetting Y - Generates encrypted equivalent for any setting value. For example, if you want to encrypt the "Y" value for the setting "preserve_raw_audio=", you would enter the above and it would respond with "E[U1JNfkzgDTjAKvrQEqYB4g==]". This can be used to encrypt IP addresses, passwords, network interfaces, and so on within INI files, etc.

For commands that accept passwords on the command line, the encryptsetting option can be used to generate an encrypted equivalent. For example, instead of using **cc_crypt.exe list -dbpassword=secret,** you can encrypt the password "secret" using the encryptsetting tag and then use the encrypted value instead:

```
Example: cc_crypt.exe list -dbpassword=E[hXk7v3zjuQCghVzVFoCORA==]
```

Thales Encryption vs. Standard Key Management

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

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 starting and ending points of communication 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 they are enabled on the Desktop 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 from remote locations or access recordings from remote locations, a VPN must be established for PCI certification.

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.

Enable Transport Security – Web Player and Live Monitoring

To enable secure communications in Silverlight (which encompasses both Web Player and Live Monitoring), verify that Discover's **web.config** file contains the following value:

```
<!--Silverlight Values-->
<add key="UseSilverlightSSL" value="1"/>
```

Enable Transport Security – Servers

At present, Desktop Recording Server and Web Media Server allow for TLS. Add the appropriate values for the corresponding SSL Certificate to the respective configuration screens under the Administration Tab > System Settings > **Screen Capture Settings** and **Web Media Server Settings**:

[server]	
ssl_certificate_name=	SSL certificate file name (path optional if in root of CallCopy directory)
ssl_certificate_pass=	SSL certificate password

The Web Media Server and Desktop Recording Server expect a file extension of .p12, which is the file type of certificates directly from the store. Thus, if the certificate loads from the certificate store, only the name (with or without file extension) as it is listed in the store is needed in the INI file. If the certificate loads from the module directory, the file name and extension need to be in the INI file name and you will need to rename the file to use a .p12 extension if necessary.

The settings INI needs to be present in the directory in which the module EXE resides. The certificate can be stored in the local certificate store and/or in the directory with the module. For example, for the Desktop Recording Server module, these would go in C:\Program Files (x86)\CallCopy\Recorder\CC_ScreenCapServer.

Enable Transport Security – Client Modules

The next step is to configure the client modules so that they will connect via a TLS method. Core and Desktop Recording Client can be enabled by configuring their respective INI files.

For Core, add the following to the cc_cticore.ini (in C:\Program Files (x86)\CallCopy\Recorder\CtiCore\):

[settings]	
use-TLS=1	Tells the module whether to use TLS (0 for no, 1 for yes).

For the Desktop Recording Client, add the following to the CC_ScreenCapClient.ini (in C:\Program Files (x86)\CallCopy\ScreenCaptureClient\):

[app-settings]	
use-TLS=1	Tells the module whether to use TLS (0 for no, 1 for yes).

The Desktop Recording Client INI file is configured when building the MSI package before deployment to agent computers. If the software is already in place prior to this configuration change, the INI files can be mass updated by the customer, or a new updated Desktop Recording Client package can be built by Uptivity that will mass uninstall the existing client and settings, then mass reinstall using the new settings.

Enable Transport Security – Web Portal

Configuring SSL for the Web Portal is handled through the settings in IIS. With the customer-provided SSL certificate required for this process, complete the steps below.

Configure Windows Server 2008/IIS 7.x

1. Open IIS. On the main page, open the **Server Certificates** section.
2. Import the SSL certificate.
3. Right-click **CCWeb** and click **Edit Bindings**. Select "**https**" and leave the other settings at default unless they create a conflict.
4. Under SSL Certificate, choose the SSL certificate. Click **OK**.
5. Back on the IIS page for the site, open **SSL Settings**. Check the option to require SSL and choose to Ignore, Accept, or Require client certificates based on the client's needs. Click **Apply**.

Transport Security and PCI Compliance

Interactions between the Discover suite components (e.g., servers, Web Portal), file servers, and archive devices can use SSL and TLS for data in transit.

On-Demand, API Server, and Desktop Analytics are considered secure regardless of encryption usage. When sensitive information is communicated, Uptivity 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 merchant's 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 the application is not "payment aware" at any time. When properly implemented following Uptivity best practices, Discover will not negatively impact a merchant’s PCI DSS compliance status.

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.

HTTP/HTTPS Settings

Discover can be configured to support HTTPS. For configuration details, see Security.

This setting affects only Discover. Other Discover modules, such as Discover Toolbar, communicate with the Discover server, and they must also be configured separately to use SSL. See each module or application's installation and administration guide for details.

Best Practices

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 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 desktop recording
- Changing desktop resolution
- Increasing call volumes

If your company is or will be experiencing any of these or similar changes, contact Uptivity 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, review these settings to confirm that they manage disk space usage efficiently:

- Disk Space Notifications
- Logging– Make sure that the system is not logging excessively.
- Types of Alert Subscriptions – Verify you are not saving log files longer than necessary.
- 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 – If you configured the Transcoder to retain files (Keep Days), lowering this setting can free disk space.

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). 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 delete these files from the server after they have been deleted through the Web Portal. Contact Uptivity 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. This section explains how to use a batch file and scheduled task to automatically delete IIS files that are more than 14 days old from the server running the Discover Web Portal.

> **Note** All Discover services should be stopped prior to running this file, as files cannot be deleted if they are in use by the application.

Get the cleanTempFiles.bat file from Uptivity support or save this code as a batch file.

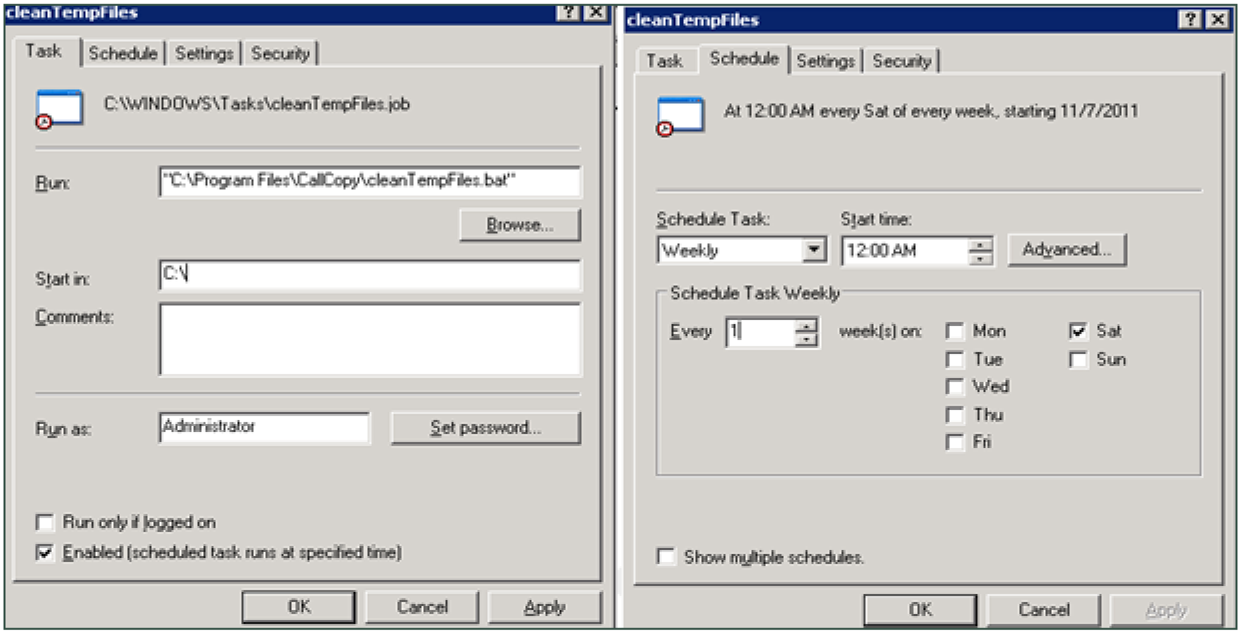
```
@echo off

del /f /s /q "%windir%\Temp\*.*"

del /f /s /q "%userprofile%\local settings\temp\*.*"

del /f /s /q "%userprofile%\local settings\temporary internet files\*.*"

Forfiles -p %systemroot%\system32\LogFiles\W3SVC1 -s -m *.log -d -14 -c "Cmd /C
DEL @File"
```

You will need to replace the path and filename in the last line of the batch file with the correct entries for your server. To check the directory your Windows 2008 or Windows 2012 IIS server uses, follow these steps:

1. In IIS Manager, expand **Web Sites**.
2. Double-click the Discover site (usually **CCWeb**)
3. In the center pane, under **IIS**, double-click **Logging** (make sure you are in **Features View**).
4. The log file directory and name appear in the **Log File** section.

To schedule the file to run automatically:

1. Copy the batch file to this directory: C:\Program Files\CallCopy
2. Click **Start** > **Settings** > **Control Panel**.
3. Double-click **Scheduled Tasks**.
4. Double-click **Add Scheduled Task** to start the wizard.
5. Click **Next** on the opening screen.
6. Click **Browse**. Navigate to the batch file location and select it.
7. Select **Weekly** and click **Next**.
8. Specify a **Start Time** when few users are in Discover, such as 12:00 AM.
9. Select a day to run the deletion.
10. Enter the name and password of the account that will run the deletion.
11. Select the option to open **advanced properties**. Click **Finish**.
12. Review the settings and click **OK**.



C:\WINDOWS\Tasks\cleanTempFiles.job

Run: "C:\Program Files\CallCopy\cleanTempFiles.bat"

Start in: C:\

Comments:

Run as: Administrator

☐ Run only if logged on

☑ Enabled (scheduled task runs at specified time)

At 12:00 AM every Sat of every week, starting 11/7/2011

Schedule Task: Weekly

Start time: 12:00 AM

Schedule Task Weekly

Every 1 week(s) on: ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☑ Sat ☐ Sun

☐ Show multiple schedules.

Control Database Size

This section explains two tasks for controlling database size using SQL Server 2008.

Task: Database Recovery Model

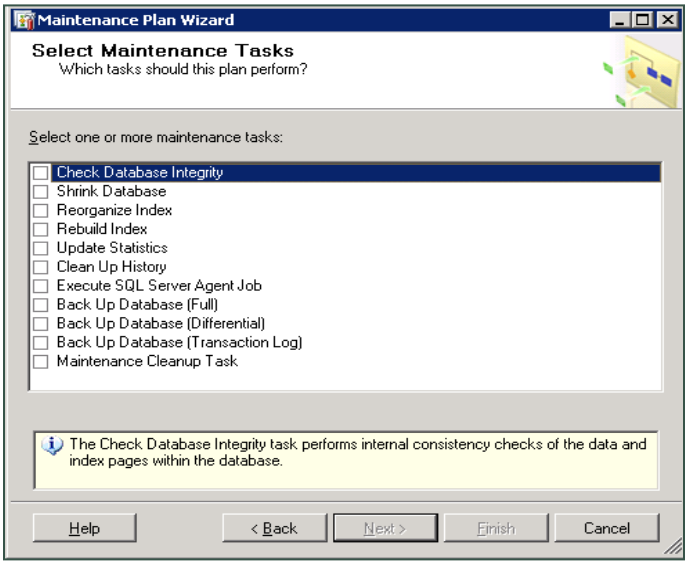
Set a database's recovery model to Simple in order to prevent oversized transaction logs:

1. In SQL Server Management Studio, expand Databases.
2. Right-click the Discover database and select **Properties**.
3. In the Database Properties dialog box, click **Options**.
4. In the Recovery Model setting, select **Simple**.

Task: Schedule Maintenance Plans

Maintenance plans can be used to automate the cleaning of unnecessary indexes and removal of multiple backup files.

1. In SQL Server Management Studio, expand the Management folder.
2. Right-click **Maintenance Plans** and select **Maintenance Plan Wizard**.
3. Select these tasks: Reorganize Index, Rebuild Index, and Backup Database (Full).



Maintenance Plan Wizard

Select Maintenance Tasks
Which tasks should this plan perform?

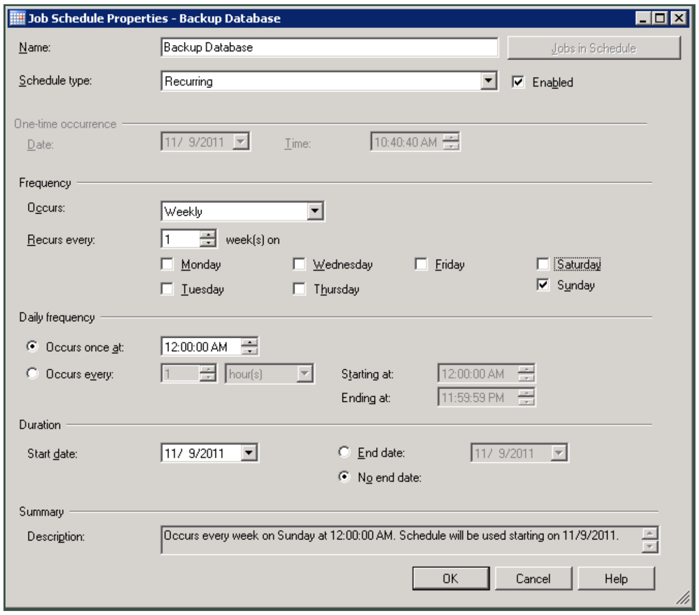
Select one or more maintenance tasks:

□ Check Database Integrity
□ Shrink Database
□ Reorganize Index
□ Rebuild Index
□ Update Statistics
□ Clean Up History
□ Execute SQL Server Agent Job
□ Back Up Database (Full)
□ Back Up Database (Differential)
□ Back Up Database (Transaction Log)
□ Maintenance Cleanup Task

The Check Database Integrity task performs internal consistency checks of the data and index pages within the database.

4. Configure each task as a recurring, once-weekly job.

   Jobs can be accessed in Management Studio > SQL Server Agent > Jobs. Right-click the appropriate job and select **Properties**. Click **Schedule**.



Job Schedule Properties - Backup Database

Name: Backup Database
Schedule type: Recurring ☑ Enabled

One-time occurrence
Date: 11/ 9/2011 Time: 10:40:40 AM

Frequency
Occurs: Weekly
Recurs every: 1 week(s) on
□ Monday □ Wednesday □ Friday □ Saturday
□ Tuesday □ Thursday ☑ Sunday

Daily frequency
● Occurs once at: 12:00:00 AM
○ Occurs every: 1 hour(s) Starting at: 12:00:00 AM
Ending at: 11:59:59 PM

Duration
Start date: 11/ 9/2011 ○ End date: 11/ 9/2011
● No end date:

Summary
Description: Occurs every week on Sunday at 12:00:00 AM. Schedule will be used starting on 11/9/2011.

Shut Down and Restart

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

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

Points to consider:

- The standard installation instructions call for registering Discover's applications as Windows services that auto-start when the server starts. Archiver does not auto-start; it can be started from the Service Manager. The Uptivity Surveys application 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, so the only effect of work on the Discover server should be an interruption in calls available for processing.
- If users are doing evaluations or creating evaluation or survey forms, all unsaved changes are lost.
- Scheduled processes (e.g., archiving, report generation) can be affected by shutdowns. Admins need to be aware of when these processes occur and may want to schedule the shutdown accordingly or reschedule the processes.
- The sequence in which Uptivity applications are started/stopped does not matter.

Shut Down Discover

1. Click the **Administration** tab and expand **Tools** in the left navigation menu.
2. Click **Service Manager**.
3. Expand the Server Node for the desired server.
4. Select all of the applications and click **Stop Selected**.
5. If any Uptivity applications were not run as services or not managed from **Service Manager**, log onto the desired server through Windows and use Task Manager to stop them.
6. Shut down the server, or perform desired tasks (e.g. Windows updates) that will require a server restart.

Restart Discover

When the server is restarted, the Discover applications should restart and function normally. To restart Discover applications/services manually:

1. Open a command prompt and start any desired services that are not managed from **Service Manager.**
2. Click the **Administration** tab and expand **Tools** in the left navigation menu.
3. Click **Service Manager**.
4. If a desired application is not running, click its **Start** button.
5. Confirm that call recording and all other functions are operating normally.

Anti-Virus

Uptivity 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 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
Logger Service	cc_loggerservice.exe	*.log	C:\Program Files\CallCopy\Logs\
CTI Core	cc_cticore.exe	*.cca, *.wav, *.vox, *.vox8, *.xml	C:\default_rec
Transcoder	cc_Transcoder.exe	*.cca, *.vid, *.wav, *.vox, *.vox8, *.csa, *.ccp	C:\temp\Transcoder-temp
Speech Analytics	cc_analytics.exe	*.wav, *.idx	
Desktop Recording	cc_screencapserver.exe	*.vid	C:\temp\

Common File Types

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

File Type	Description
.cav	Uptivity proprietary combined audio/video format generated only when a file is exported. Requires a special player to view.
.cca	Discover raw audio pre-transcode, typically deleted after transcoding and compressed into .wav.
.ccp	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.
.csa	Discover stereo audio, typically deleted after transcoding and compressed into G729 .wav format.
.idx	Phonetic index of the recorded call created and used by the speech analytics engine. This is an Aurix proprietary format.
.log	Log files where system activities and errors are recorded. Useful in troubleshooting system issues.
.vid	Desktop recording data for playback.
.vox	Compressed audio format for playback. Higher quality than .wav, but also larger file size. Mostly a legacy format now.
.vox8	Compressed audio format for playback. Higher quality than .wav, but also larger file size. Mostly a legacy format now.
.wav	Compressed audio format for playback.
.xml	Used to store call metadata or API responses to clients.

Additional 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.

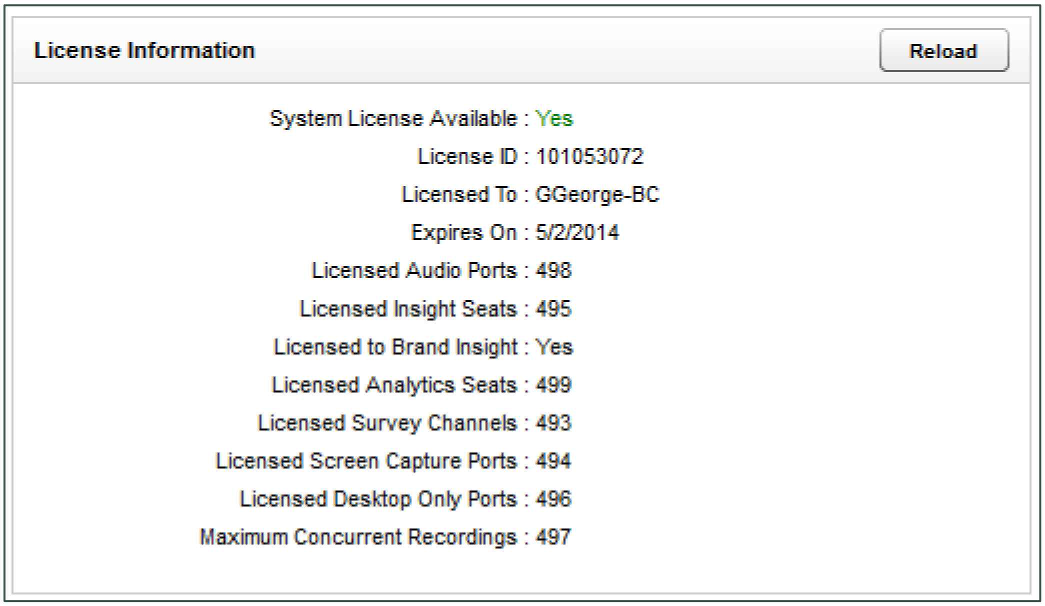
Files should typically be excluded based on the following criteria:

- **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 are 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.

Expired or Corrupt License File

Call recording will not work if the Uptivity software license file has expired or is corrupt. To view license status:

1. Click the Reporting tab 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**.



System License Available : Yes
License ID : 101053072
Licensed To : GGeorge-BC
Expires On : 5/2/2014
Licensed Audio Ports : 498
Licensed Insight Seats : 495
Licensed to Brand Insight : Yes
Licensed Analytics Seats : 499
Licensed Survey Channels : 493
Licensed Screen Capture Ports : 494
Licensed Desktop Only Ports : 496
Maximum Concurrent Recordings : 497

If call recording and other functions are not working, this may indicate your license file is expired, corrupt, or missing. 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.

License Requests

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 system to become unlicensed. The server will not function until a new license is created and applied to the system.

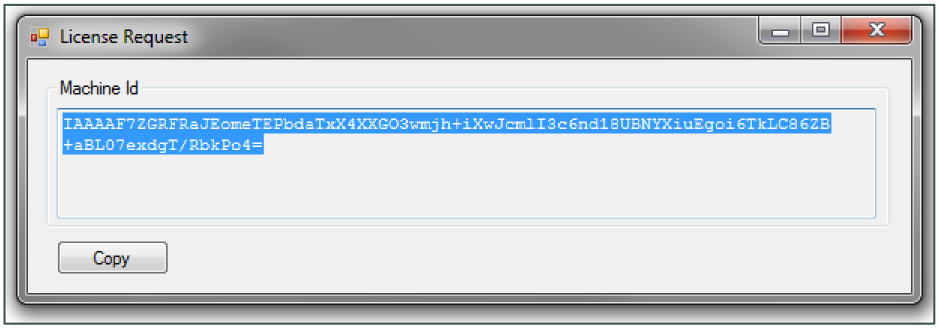
Uptivity recommends any such maintenance be scheduled for an approved maintenance time, as the system will be non-operational after the maintenance until a new license is applied. Contact your Uptivity Support team if any such maintenance is planned, so a new license can be issued immediately after system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



Machine Id

```
IAAAAF7ZGRFRaJEomeTEPbdaTxX4XXGO3wmjh+iXwJcmlI3c6nd18UBNYXiuEgoi6TkLC86ZB
+aBL07exdgT/RbkPo4=
```

3. Click **Copy**.
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.

About Uptivity

What boosts the bottom line for any company with a contact center? How about getting the best that every agent can deliver from their first day on the job and constantly optimizing contact center management and performance? Only Uptivity gives you the tools you need to continuously improve every aspect of each step of every agent's life cycle and enhance customer satisfaction. You get exactly what you need thanks to a modern, integrated, and easy-to-use suite of tools that offers a unified system for performance management, workforce management, speech analytics, and call recording. Unparalleled customer service and support from our in-house staff combine with a better bundle for a better value, and a lower total cost of ownership.

Headquartered in Columbus, Ohio, and on the Web at www.uptivity.com.