



## Service Account Manager

---

- [Service Account Management, on page 1](#)
- [Service Account Manager End User Interfaces, on page 3](#)
- [Service Account Manager GUI Dialog Boxes, on page 3](#)
- [Service Account Manager – Main Dialog Box, on page 4](#)
- [Service Account Manager – Edit Service Account dialog box, on page 10](#)
- [Command Line Interface for Service Account Manager, on page 11](#)
- [Service Account Manager, on page 12](#)

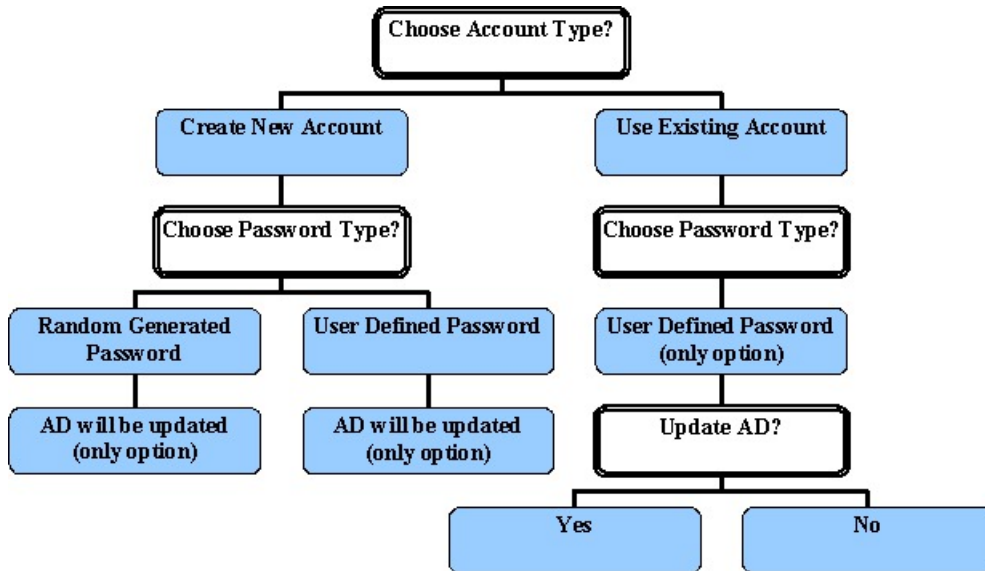
## Service Account Management

The Service Account Manager serves three purposes. It allows you to:

1. Create new accounts with random passwords.
2. Use existing AD accounts as Unified ICM service accounts.
3. Provide an interface to modify Unified ICM service account passwords.

The following diagram illustrates the basic workflow of the Service Account Manager.

Figure 1: Service Account Manager Application Workflow



## Other Considerations

### Permissions

You must have the correct privileges to create or modify the accounts in the domain. Typically, a Domain User with local administrator privilege performs this task.

### Domain Restriction

The service account must be in the same domain as the Unified ICM server and also the UPN login name of the Service When choosing an existing account, the account user should be same as NETBIOS pre-windows 2000 login name (SAM Account Name).

*Special Case:* If the distributor service Account and logger service account is different then add distributor service account in logger.

### AD Update Failures

If the Service Account Manager finds that a service is running, it first requests your permission; if you approve, it stops the service. If you choose not to stop the service, the Service Account Manager does not modify the service account information. If the Service Account Manager explicitly stopped the service before you edit the account information, it automatically starts the service. If the Service Account Manager fails to update the account in AD, due to either a noncompliant password policy or any connectivity error, the Service Account Manager warns you and logs the error. At that point, you can choose to fix the problem and retry, or cancel.

### Logging

The application maintains its own log file, when you invoke it as a standalone application. If you invoke it through the Web Setup tool, logs write to the Websetup log files only.

## Service Account Memberships Setup for CICM Replication

When the application is invoked from the standalone NAM's Logger servers (sides A and B), the command line is as follows:

```
ServiceAccountManager  
/SrcInstance<InstanceName>  
/DestDomain<DomainName>  
/DestFacility<FacilityName>  
/DestInstance<InstanceName>
```

## Service Account Manager End User Interfaces

The Service Account Manager has two user interfaces:

- The Graphical User Interface consisting of the following dialog boxes:
  - Main
  - Edit Service Account
- The Command Line Interface

### Related Topics

[Service Account Manager GUI Dialog Boxes](#), on page 3

[Service Account Manager – Main Dialog Box](#), on page 4

[Service Account Manager – Edit Service Account dialog box](#), on page 10

[Command Line Interface for Service Account Manager](#), on page 11

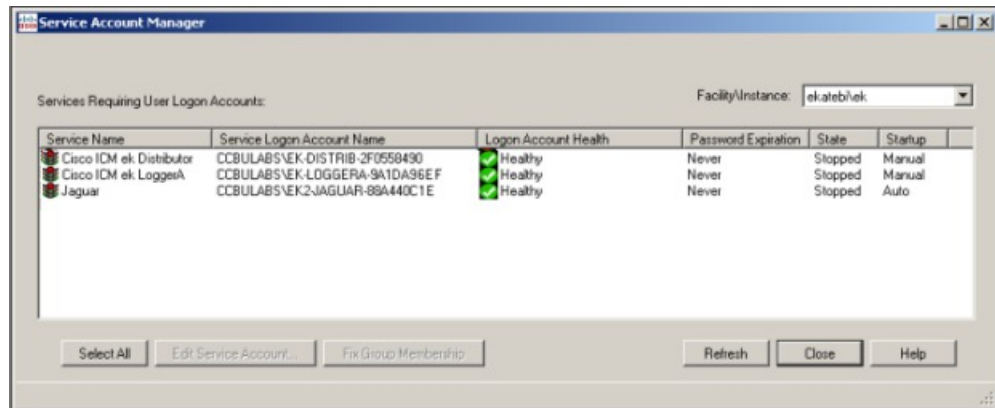
## Service Account Manager GUI Dialog Boxes

You can find a shortcut to the application in Windows **Start > Programs > Cisco Unified ICM-CCE-CCH Tools** folder.

The Service Account Manager has two dialog boxes:

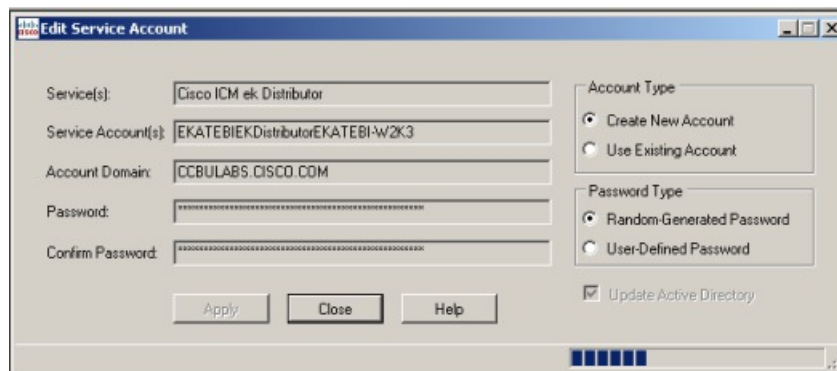
- Main

Figure 2: Main Service Account Manager Dialog



- Edit Service Account dialog box.

Figure 3: Service Account Manager - Edit Service Account Dialog



### Related Topics

[Service Account Manager – Main Dialog Box](#), on page 4

[Service Account Manager – Edit Service Account dialog box](#), on page 10

## Service Account Manager – Main Dialog Box

You can use the Service Account Manager as a standalone application for Cisco Unified ICM/CCE Installer.

The Main Service Account Manager dialog box is the application's primary interface. It consists of the *Services Requiring User Logon Accounts* section (which contains the *Service Name*, *Service Logon Account Name*, *Logon Account Health*, *Password Expiration*, *State*, and *Startup* fields), the **Facility/Instance** drop-down; and the **Select All**, **Edit Service Account**, **Fix Group Membership**, **Refresh**, **Close**, and **Help** buttons.

The following table provides a description for each field and button in this dialog box.

<b>Field/Button/ Drop-down</b>	<b>Description</b>
Service Name	A list of all relevant services. If there are no relevant services on the server, such as a Administration & Data Server, or Logger; the field displays the message “This instance does not have any service that requires a service account.”
Service Logon Account Name	Displays the service account name for the list of relevant services.

Field/Button/ Drop-down	Description
Logon Account Health	<p>The Service Account Manager has an account health check mechanism. When the application starts, it scans all relevant Unified ICM services and flags them as indicated below.</p> <ul style="list-style-type: none"><li>• Green<ul style="list-style-type: none"><li>• <i>Healthy Account</i>: the service account state is normal.</li></ul></li><li>• Yellow<ul style="list-style-type: none"><li>• <i>Password Warning</i>: the password is due to expire in less than 7 days.</li></ul></li><li>• Red<ul style="list-style-type: none"><li>• <i>Invalid Account</i>: service has an invalid account associated with it.</li><li>• <i>Password Expired</i>: service account password has expired.</li><li>• <i>Group Membership Missing</i>: service account is missing from the required local security groups.</li><li>• <i>Account not associated with service</i>: service account created but not replicated, hence not associated yet.</li></ul></li></ul>

Field/Button/ Drop-down	Description
	<p>The following messages could appear in the Health column.</p> <ul style="list-style-type: none"> <li>• Healthy <ul style="list-style-type: none"> <li>• Only applies to the service account, not the service itself.</li> <li>• The account is a member of the required UcceService local service and local adminUnified ICM/CCE/Unified CCH security groups.</li> <li>• The account has been validated to start a service.</li> <li>• If the account password is changed outside of the Service Account Manager application, <i>Healthy</i> would be displayed even though the service might not actually be healthy because this application cannot detect the change.</li> </ul> </li> <li>• Need to create service account <ul style="list-style-type: none"> <li>• The Service Account Manager must be used to create a service account for each service.</li> </ul> </li> <li>• Account not a member of the UcceService local group <ul style="list-style-type: none"> <li>• The Service Account Manager then places the account in the required UcceService local service group and local admin group, and sets the required permissions.</li> </ul> </li> <li>• Account Disabled <ul style="list-style-type: none"> <li>• In AD, an account can be enabled or disabled. This message indicates that the account is disabled in the domain.</li> </ul> </li> <li>• Password Expired</li> <li>• Service Group not a member of local Administrators group</li> <li>• Central Controller (sideA ) Domain name is unknown (Administration &amp; Data Server only) <ul style="list-style-type: none"> <li>• Administration &amp; Data Servers can be in a different domain than the Central Controller. When <b>Fixed Group</b> is selected, you are queried for the domain name of the Central Controller if it is different than that of the Administration &amp; Data Server.</li> </ul> </li> <li>• Central Controller (sideA ) Domain is not trusted or trust is not two-way (Administration &amp; Data Server only) <ul style="list-style-type: none"> <li>• There must be a two-way trust between the Central Controller and the Administration &amp; Data Server. SAM detects the lack of the trust relationship and displays this message. SAM might detect this issue, but is unable to fix it.</li> </ul> </li> <li>• Account not a member of LoggerA Domain Service Group (Administration</li> </ul>

Field/Button/ Drop-down	Description
	<p data-bbox="672 317 889 344">&amp; Data Server only)</p> <ul style="list-style-type: none"> <li data-bbox="708 365 1484 453">• If the Administration &amp; Data Server is on a different domain than the Central Controller, it applies the Administration &amp; Data Server's Domain Service Group to both itself and the Central Controller.</li> <li data-bbox="656 495 1484 554">• Central Controller (sideB ) Domain name is unknown (Administration &amp; Data Server only) <ul style="list-style-type: none"> <li data-bbox="708 575 1484 697">• Administration &amp; Data Servers can be in a different domain than the Central Controller. When <b>Fixed Group</b> is selected, you are queried for the domain name of the Central Controller if it is different than that of the Administration &amp; Data Server.</li> </ul> </li> <li data-bbox="656 739 1442 798">• Central Controller (sideB ) Domain is not trusted or trust is not two-way (Administration &amp; Data Server only) <ul style="list-style-type: none"> <li data-bbox="708 819 1468 907">• There must be a two-way trust between the Central Controller and the Distributor. SAM detects the lack of the trust relationship and displays this message. SAM might detect this issue, but is unable to fix it.</li> </ul> </li> <li data-bbox="656 949 1484 1008">• Account not a member of LoggerB Domain Service Group (Administration &amp; Data Server only) <ul style="list-style-type: none"> <li data-bbox="708 1029 1484 1117">• If the Administration &amp; Data Server is on a different domain than the Central Controller, it applies the Administration &amp; Data Server's Domain Service Group to both itself and the Central Controller.</li> </ul> </li> <li data-bbox="656 1159 1052 1186">• Account not associated with service <ul style="list-style-type: none"> <li data-bbox="708 1207 1468 1295">• When SAM associates an account with a service it might run into replication issues. Use <b>Edit</b> and select <b>Associate the account with a service</b> rather than selecting editing from the beginning.</li> </ul> </li> <li data-bbox="656 1337 1019 1365">• Service not validated for starting <ul style="list-style-type: none"> <li data-bbox="708 1386 1484 1444">• When SAM validates a service it might run into replication issues. Use <b>Validate</b> to successfully start the service.</li> </ul> </li> <li data-bbox="656 1486 961 1514">• Password About To Expire <ul style="list-style-type: none"> <li data-bbox="708 1535 1484 1623">• Check the <b>Password Expiration</b> option to determine the validity period of the password. The Service Account Manager can then be used to reset the password for this pre-existing account.</li> </ul> </li> </ul>



<b>Field/Button/ Drop-down</b>	<b>Description</b>
	<p>A service has an <i>Invalid Account</i> health state immediately after creation because no domain account is assigned to it yet. This is expected behavior.</p> <p>A service can have a <i>Missing Group Membership</i> problem due to a prior AD related failure. The Service Account Manager is capable of fixing this issue by providing an interface that re-attempts placing the account in the relevant local and domain security groups.</p> <p><b>Note</b> SAM health reporting might be inaccurate for the period of time while AD replication is in progress. The previous health state might be indicated during this time.</p>
Password Expiration	<p><b>Note</b></p> <ul style="list-style-type: none"> <li>• Any service with an account password that expires in seven (7) days is yellow flagged by the application.</li> <li>• You own the responsibility to refresh the passwords before they expire. If you do not, the system services fail to function.</li> </ul>
State	The current state of the service (Stopped, Start/Stop Pending, or Running).
Startup	Displays how the service is started (Manual or Automatic).
Facility/Instance	<p>Drop-down displaying the “Facility/Instance” name.</p> <p>In case of multiple instances, the default “Facility/Instance” selected in the drop-down is the last instance edited by Setup.</p> <p>Select a specific instance. The Service Account Manager lists all relevant services with their account information, account health, password expiration and startup state for the selected instance.</p> <p>If there are no relevant services on the server (such as a Administration &amp; Data Server, or Logger) the Service Account Manager displays the message: <i>This instance does not have any service that requires a service account.</i></p>
<b>Select All</b>	Click to select all listed services.
<b>Edit Service Account</b>	<p>To fix any account issues, edit one, a few, or all accounts at the same time by selecting them and clicking this button.</p> <p>When the dialog box appears, the Service Account Manager prompts you to try to use the account recently created, as it keeps track of it. If you agree to use the recently created account, the application tries to reuse the previously created account, thereby escaping from the recursive cycle of trying to create and use an account. If you chose random password, the application creates a new one, or prompts you to enter one. The application never stores the password.</p>
<b>Fix Group Membership</b>	Available ONLY if an account with the <i>Group Membership Missing</i> health state is selected.
<b>Refresh</b>	Refreshes all information in the Service Account Manager Main dialog box.
<b>Close</b>	Closes the Service Account Manager dialog box.

Field/Button/ Drop-down	Description
Help	Select to access the online help for the Service Account Manager.

## Service Account Manager – Edit Service Account dialog box

The **Edit Service Account** dialog allows you to create a new or use an existing account, and to choose a random or a user defined password. The status bar at the bottom of the dialog box displays status messages as needed.

The following table provides a description for each field, button, and check box for this dialog box:

Field/Button/check box	Description
Service(s)	Displays the name of the service to be edited.
Service account(s)	Displays the account name for the selected service.
Account Domain	Displays the server domain. (Read Only)
Password	<p>If the Password Type selected is <b>Random-Generated Password</b>, this field is populated with the generated password.</p> <p>If the Password Type selected is <b>User-Defined Password</b>, enter the password to be used for this account.</p> <p>Enter the password associated with the account name.</p>
Confirm Password	<p>If the Password Type selected is <b>Random-Generated Password</b>, this field is populated with the same generated password as the Password field.</p> <p>If the Password Type selected is <b>User-Defined Password</b>, re-enter the password to use for this account.</p> <p>Re-enter the password associated with the account name.</p>
Account Type	<p>Allows you to either create a new account or use an existing account by selecting the appropriate radio button.</p> <p><b>Create New Account</b> is the default if no domain account assigned yet.</p> <p><b>Use Existing Account</b> is the default if a domain account is already assigned.</p>
Password Type	<p>Allows you to choose a random-generated or a user-defined password by selecting the appropriate radio button.</p> <p><b>Random Generated Password</b> is the default if you are creating a new account.</p> <p><b>User Defined Password</b> is the default, and only, option when using an existing account.</p>

Field/Button/check box	Description
Update Active Directory	<p><b>Checked</b> is the default, and only, option if you are creating a new account.</p> <p><b>Note</b> By checking this check box, you are actually making changes to the Active Directory domain and any changes to passwords affect the password of the existing user.</p> <p><b>Unchecked</b> is the default if using an existing account.</p>
<b>Apply</b>	Click to apply any changes on this dialog box.
<b>Close</b>	<p>Click to close this dialog box.</p> <p>Whenever this dialog box is closed, the Service Account Manager determines if a valid domain account is associated with the services or not.</p> <p>If the Service Account Manager finds that you did not successfully associate a valid domain account with a service, it warns you that the service fails to function until you use the Service Account Manager to associate a valid domain account with the service.</p>
<b>Help</b>	Select to access the online help for the Service Account Manager.

## Command Line Interface for Service Account Manager

### Silent Setup for Default Service Accounts

Web Setup uses the command line interface to silently create service accounts.

Setup passes the following three arguments to the Service Account Manager:

/Instance <InstanceName>

- The InstanceName argument specifies the Unified ICM instance name for which the service is being setup.

/Service <ServiceType>

- The Service argument specifies the type of the service whose account name and password are being created.

For example: /Service Distributor

Service types to use are:

- Distributor
- LoggerA – Use when on Side A of the logger or for All-In-1 ICM/CCE
- LoggerB – Use when on Side B of the logger only

/Log <Path\LogFileName>

- The Log argument specifies the log file name and the path where the log is appended. Typically, Web Setup and Cisco Unified ICM/CCE/Unified CCH Installer passes their own log file name to append the logs. The Service Account Manager also maintains its own log file in the temp folder.

**Note**

- If any one of the arguments is missing or incorrect, the Service Account Manager returns an error to Setup.
- If Setup needs to create accounts for more than one service, it invokes the Service Account Manager multiple times using the command line interface.

## Service Account Memberships for CICM Replication Process

When upgrading the Unified ICMH to Unified ICM 9.0 (or later), the CICM replication process (CRPL) does not have proper permission to make configuration updates to customer instances without manually configuring the Active Directory.

This configuration entails adding the standalone NAM's logger service accounts to the service groups of the CICMs. Thus the standalone NAM's service account has the permissions necessary to update the database of the CICM.

One function the Service Account Manager provides is to automate the manual configuration steps (as described at <https://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-contact-center-hosted/70536-crpl-fails.html>). This functionality is exposed through the Service Account Manager command-line interface as described in the *Service Account Memberships for CICM Replication Process* section.

Typically this functionality is utilized through two batch files (one for the A side and the other for the B side) where there is an entry for each CICM as a destination (/Dest). Each time the Web Setup is executed, running the batch file enables you to configure the Active Directory permissions properly.

# Service Account Manager

## Create New Account for Single Service

### Procedure

- 
- Step 1** Select a single service from Main Service Account Manager dialog box.
- Step 2** Click **Edit Service Account**.  
The Edit Service Account dialog box opens.
- Step 3** Select **Create New Account**.  
If no domain account is associated with the service, then **Create New Account** is selected by default.
- Step 4** Enter a password or have one generated randomly.  
Random-Generated Password is selected by default.

**Step 5** Click **Apply**.

The Service Account Manager creates a new account in AD with a password.

If the account name exists, the Service Account Manager asks you to either recreate it, or update the password.

The application associates the account with the service on the server. The Service Account Manager places the account in required UcceService local service group and local admin group, and sets the required permissions. Service account is recreated, or just the password changes, based on your selection before you click **Apply**.

**Note** If the Service Account Manager fails to put the account in domain security group, it asks you to rerun the application 20 minutes later to give AD time to replicate the account.

---

## Update Existing Account for Single Service

### Procedure

---

**Step 1** Select a single service from Main Service Account Manager dialog box.

**Step 2** Click **Edit Service Account**.

The Edit Service Account dialog box opens.

**Step 3** Select **Use Existing Account**.

If a domain account is associated with the service, **Use Existing Account** is selected by default.

**Step 4** Enter a password.

**Step 5** Choose whether to update the password in AD.

**Step 6** Click **Apply**.

If previously selected, the Service Account Manager updates the password in AD. It updates the service on the server with the new account information.

The Service Account Manager places the account in required UcceService local group and local admin group, and sets the required permissions.

---

## Create New Accounts for More Than One Service

### Procedure

---

**Step 1** Select multiple services or click **Select All**.

**Note** Use the normal Windows conventions for selecting all or multiple services.

**Step 2** Click **Edit Service Account**.

The Edit Service Account dialog box opens.

The Service Name column lists all services. Because multiple services are selected, **Use Existing Account** is selected by default.

**Step 3** Click **Create New Account**.

A separate service account is created for each service.

**Step 4** Enter a password, or have one generated randomly.

If you choose to enter a password, then the same password is shared across all accounts.

If you choose to randomize the password, a separate random password is generated for each account.

**Step 5** Click **Apply**.

The Service Account Manager creates multiple accounts in AD with the password. The application associates each account with the respective service on the server. The Service Account Manager then places the account in the required UcceService local service group and local admin group, and sets the required permissions.

**Note** If the Service Account Manager fails to put the account in domain security group, it asks you to rerun the application 20 minutes later to give AD time to replicate the account.

## Update existing account for more than one Service

### Procedure

**Step 1** Select multiple services or click **Select All** on the Main Service Account Manager dialog box.

**Step 2** Click **Edit Service Account**.

The Edit Service Account dialog box opens.

The Service Name column lists all services. Because multiple services are selected, **Use Existing Account** is selected by default.

**Step 3** Enter an account name.

**Step 4** Enter a password.

**Step 5** Choose whether to update the password in AD.

**Step 6** Click **Apply**.

If previously selected, the **Service Account Manager** updates the password in AD. It updates the service on the server with the new account information.

The Service Account Manager then places the account in the required UcceService local group and local admin group, and sets the required permissions.

## Fix Account Displaying Adverse Health State

**Fix Group Membership** is only enabled when an account that is in an adverse health state, is selected. The health state is displayed by a message such as “Group Membership Missing” or

### Procedure

---

**Step 1** Select the unhealthy accounts displaying a state such as the "Group Membership Missing" state.

**Step 2** Click **Fix Group Membership**.

If any of the selected account is not in the “Group Membership Missing” state, **Fix Group Membership** is disabled.

**Step 3** Click **Apply**.

The Service Account Manager then places the account in required domain security group and local security group, and sets the required permissions.

**Note** If the Service Account Manager fails to place the accounts in the groups, it provides an appropriate error.

---

