

Installing Cisco Unity 3.0: "Password Rejection" and "User Doesn't Have the Rights to Install Unity" Error Workaround

Document ID: 9158

Introduction

Prerequisites

Requirements

Components Used

Conventions

Give Rights to an Installation Account

Member Server Step-by-step Instructions

Domain Controller Step-by-step Instructions

Verify the Procedure

Related Information

Introduction

Cisco Unity 3.0 contains a caveat in which the password for the installation account is not accepted. This occurs only during the configuration setup of Cisco Unity version 3.0. Setup part two prompts the installer to type the password and account used for the installation. The password that is entered is rejected even though it is a valid password.

The reason for this caveat is that the Syscheck component no longer verifies the proper rights for the account. Cisco bug ID [CSCdv37418](#) addresses this situation, and can be found in the Release Notes for Cisco Unity Release 3.0(2).

This document provides a workaround that describes how to give the Act as Part of the Operating System and Log On as a Service rights to the installation account. Thus, it completes the configuration setup.

Note: Another symptom can also occur: When an attempt is made to install Cisco Unity, the setup program can complain that the user does not have the rights to Act as part of the Operating System.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on this software version:

- Cisco Unity 3.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Give Rights to an Installation Account

These sections explain how to give Act as Part of the Operating System and Log On as a Service rights to the installation account in order to complete the configuration setup.

There are two different scenarios for this workaround, depending on whether the Cisco Unity server is used as:

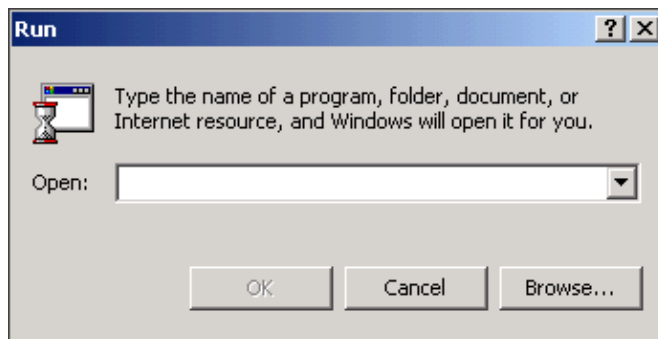
- A Member Server in a Windows 2000 Active Directory domain
- A Domain Controller of the Windows 2000 Active Directory domain (This is the typical scenario of an all-in-one-box installation.)

Member Server Step-by-step Instructions

Complete these steps:

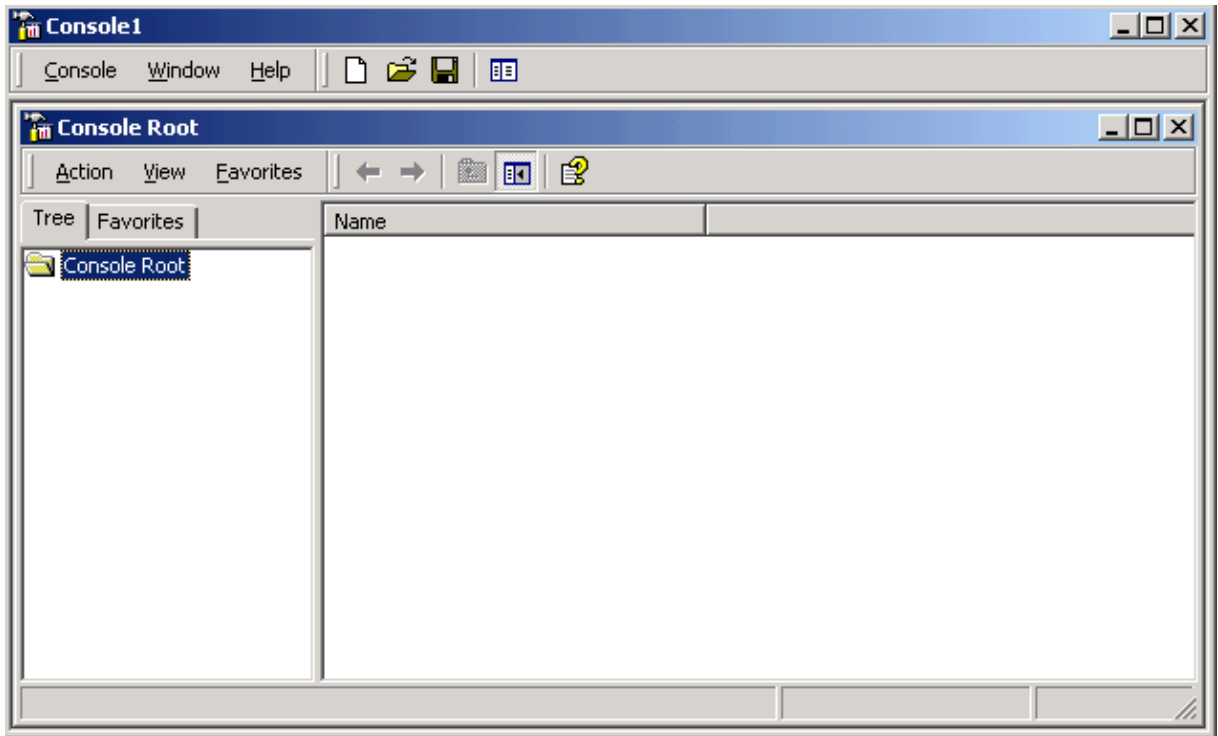
1. From the Windows desktop, select **Start > Run**.

This window appears:



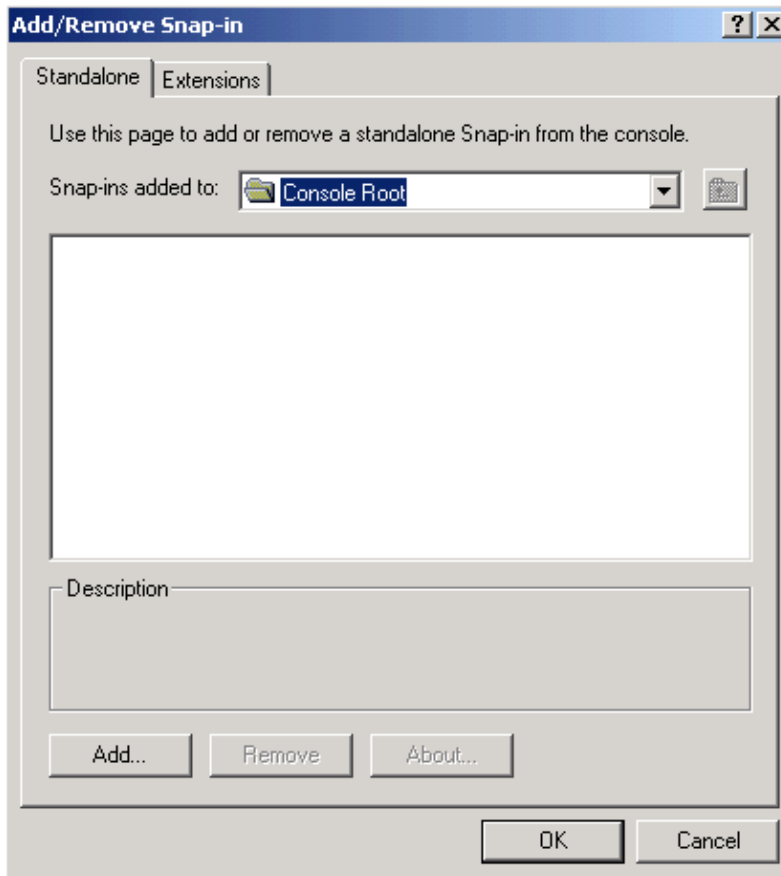
2. Type **mmc**, then click **OK**.

The Console window appears:



3. From the Console pull-down menu, select **Add/Remove Snap-in**.

The Add/Remove Snap-in window appears:



4. Verify that the Standalone tab is the active tab, and click the **Add** button at the bottom of the window.

The Add Standalone Snap-in window appears.

5. From the list of Available Standalone Snap-ins, select **Active Directory Users and Computers**.

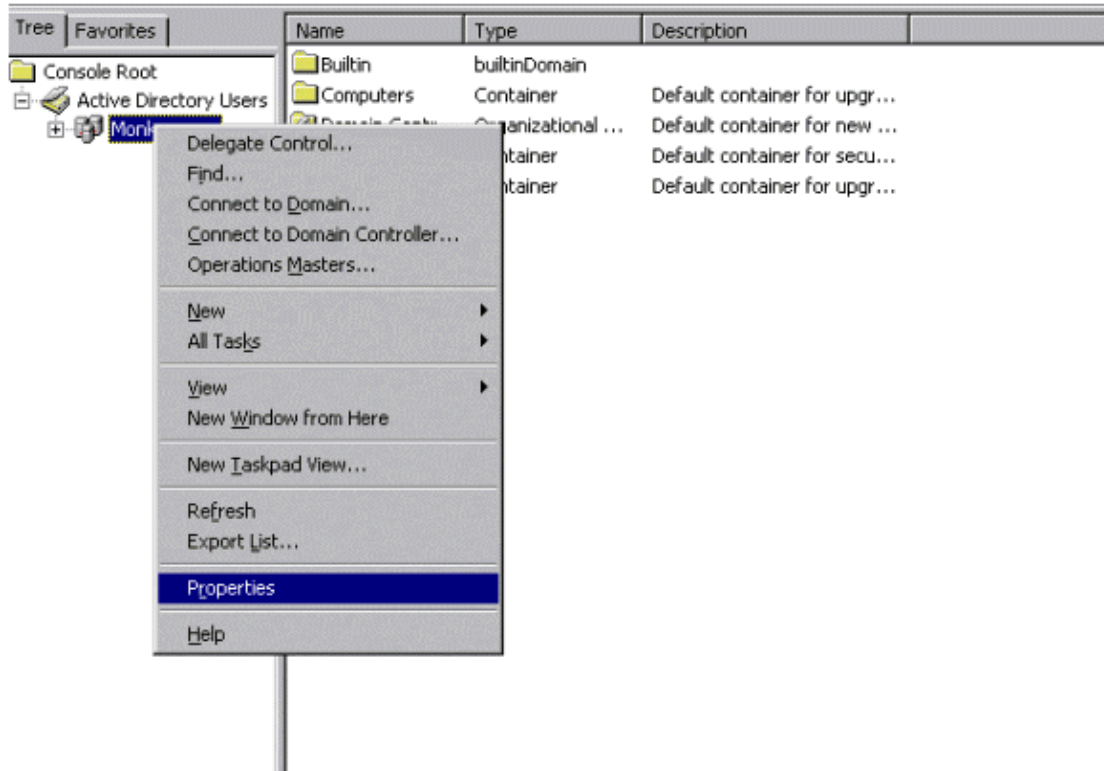
6. Click the **Add** button at the bottom of the window, then click **Close**.

The Add/Remove Snap-in window reappears with the Active Directory Users and Computers displayed in the main panel.

7. Click **OK**.

The Active Directory Users and Computers window appears.

8. Navigate to your domain and right-click on your domain. From the menu, select **Properties**, as shown in this window:

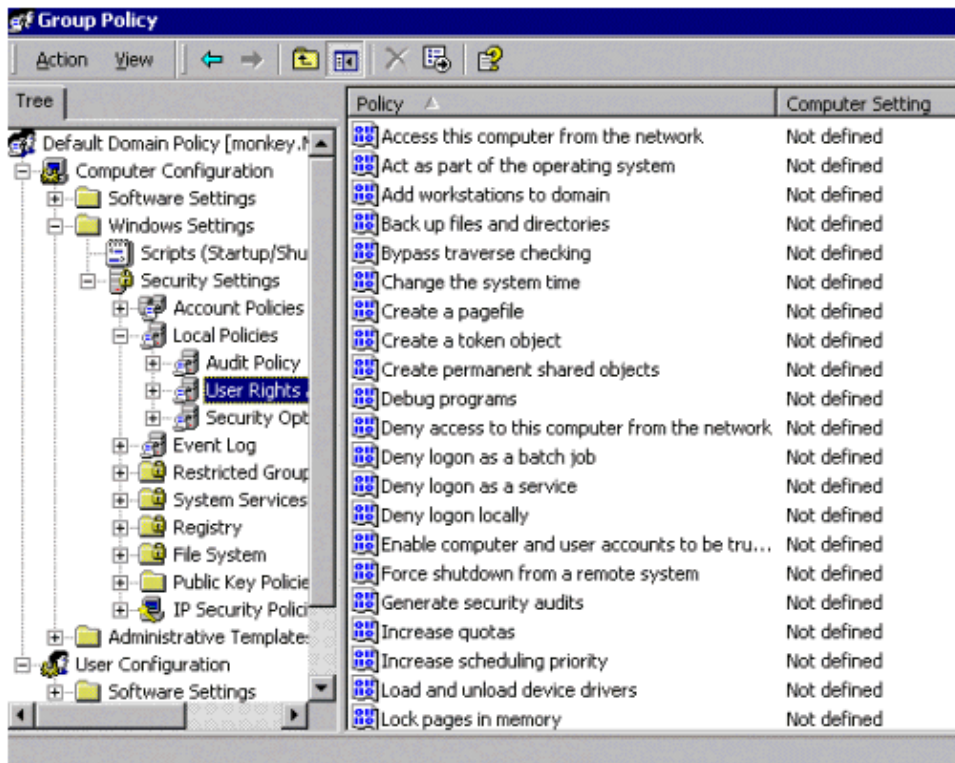


The Properties window appears.

9. From the Properties window, select the **Group Policy** tab, then click **Edit**.

The Group Policy window appears.

10. As shown in this window, navigate to the **User Rights** option. Select **Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights** to do this.



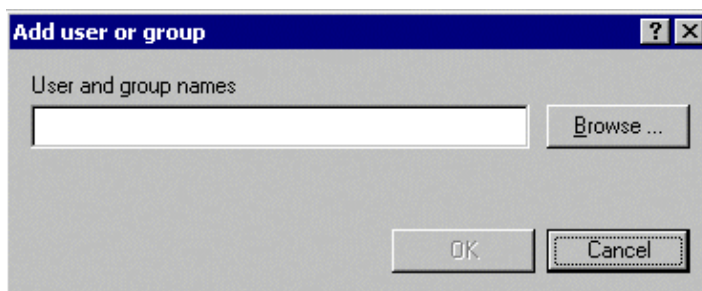
11. From the right panel, double-click the **Act as part of the operating system** option.

The Security Policy Setting window appears:



12. Check the **Define These Policy Settings** checkbox, then click **Add**. If this option is already activated, simply click the **Add** button.

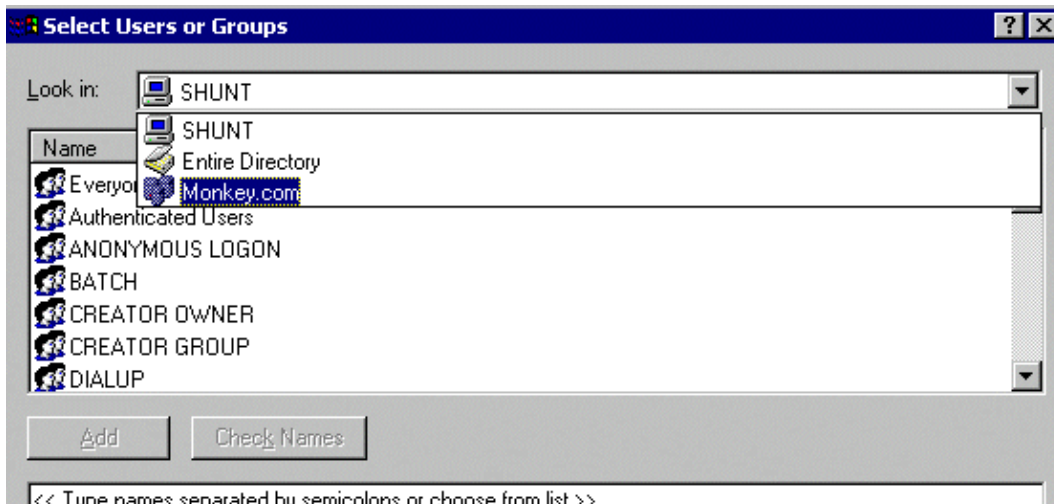
The Add User or Group window appears:



13. Click Browse to locate the domain.

The Select Users or Groups window appears.

14. From the Look In field, select the account with which you are installing Unity.



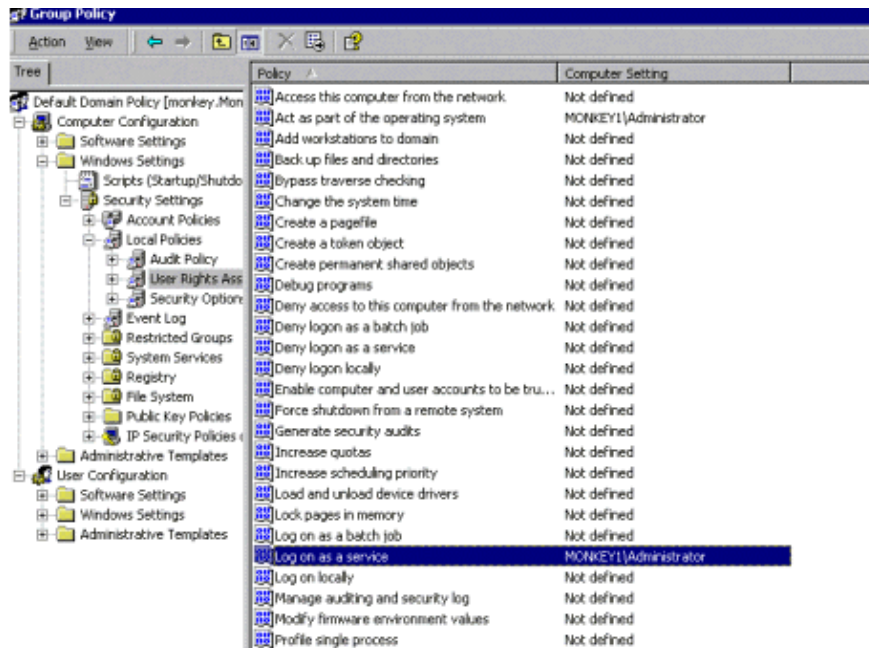
15. In the main panel, select the type of user.

Note: For the purpose of this document, the Administrator was selected because the user logged in as an administrator.

16. After you select the user type, click **Add**, then click **OK**.

The Group Policy window reappears.

17. From the right panel, double-click the **Log on as a service** option, as shown in this window:



The Security Policy Setting window appears.

18. Repeat steps 12 through 16 for this option.

19. Reboot the Cisco Unity server.

After the server reboots, you are able to configure the second part of the configuration setup.

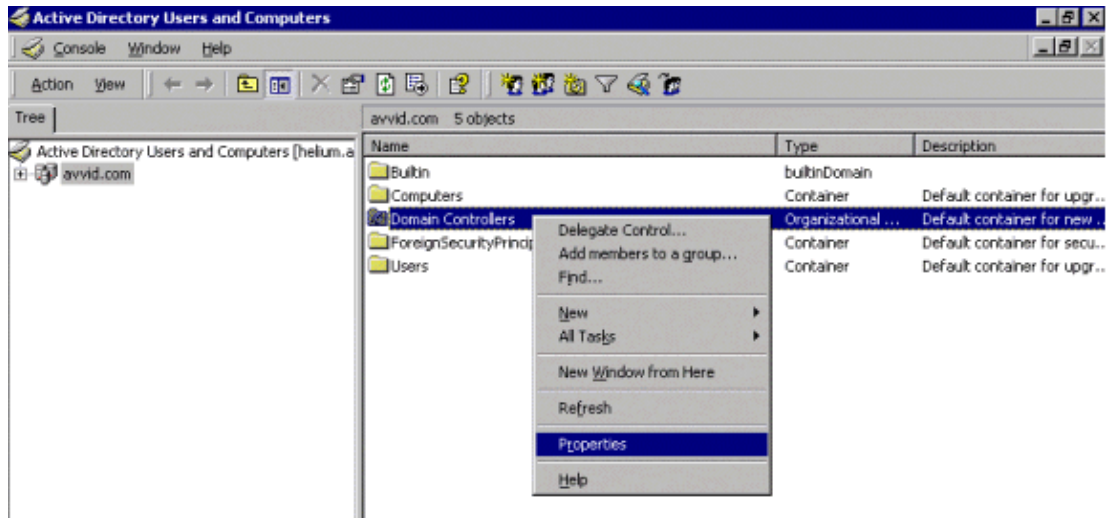
Domain Controller Step-by-step Instructions

Perform these steps:

1. Go to **Start > Programs > Administrative Tools > Active Directory Users and Computers**.

The Active Directory Users and Computers window appears.

2. Navigate to your domain. In the right panel, right-click the **Domain Controllers** folder. From the menu, select **Properties**, as shown in this window:

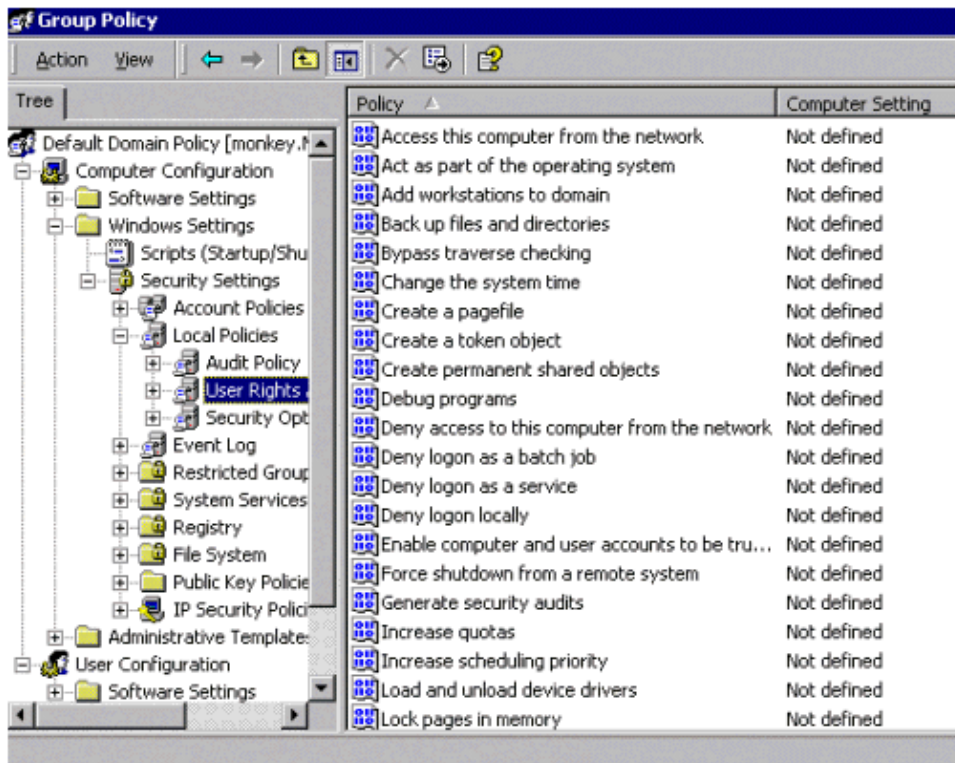


The Properties window appears.

3. From the Properties window, select the **Group Policy** tab, then click **Edit**.

The Group Policy window appears.

4. As shown in this window, navigate to the **User Rights** option. Select **Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights**.



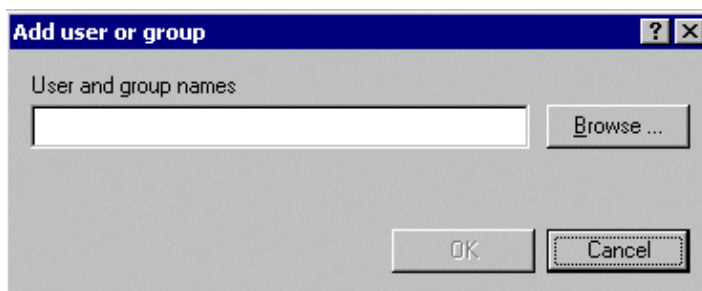
5. From the right panel, double-click the **Act as part of the operating system** option.

The Security Policy Setting window appears:



6. Check the **Define These Policy Settings** checkbox, then click **Add**. If this option is already activated, simply click the **Add** button.

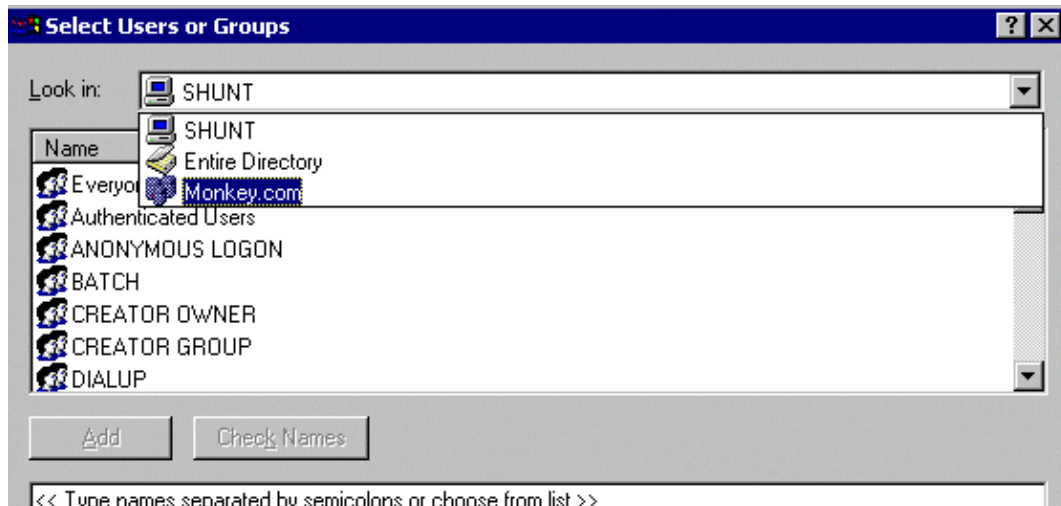
The Add User or Group window appears.



7. Click **Browse** to locate the domain.

The Select Users or Groups window appears.

- From the Look In field, select the account with which you are installing Unity.



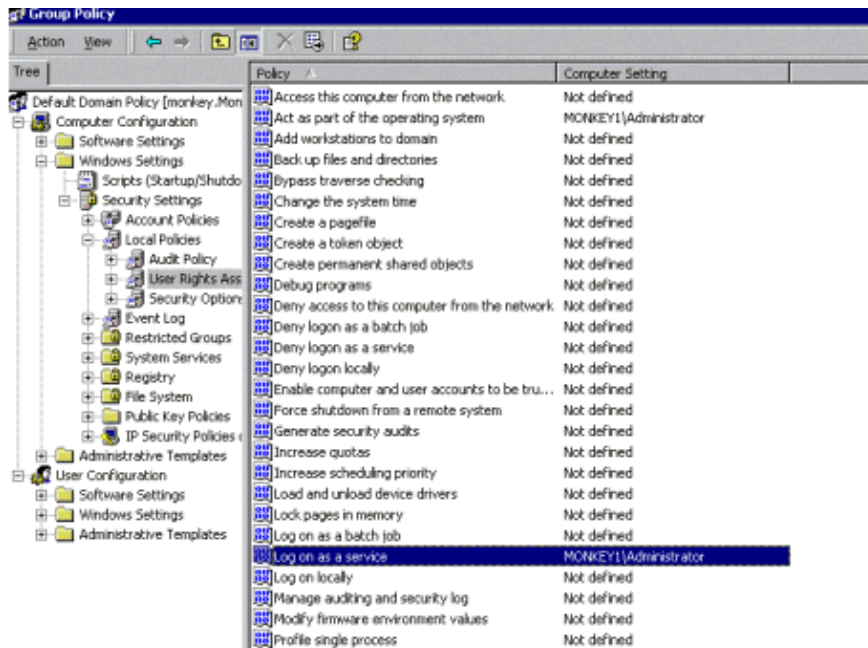
- In the main panel, select the type of user.

Note: For the purpose of this document, the Administrator was selected because the user logged in as an administrator.

- After you select the user, click **Add**, then click **OK**.

The Group Policy window appears.

- From the right panel, double-click the **Log on as a service** option, as shown in this window:



The Security Policy Setting window appears.

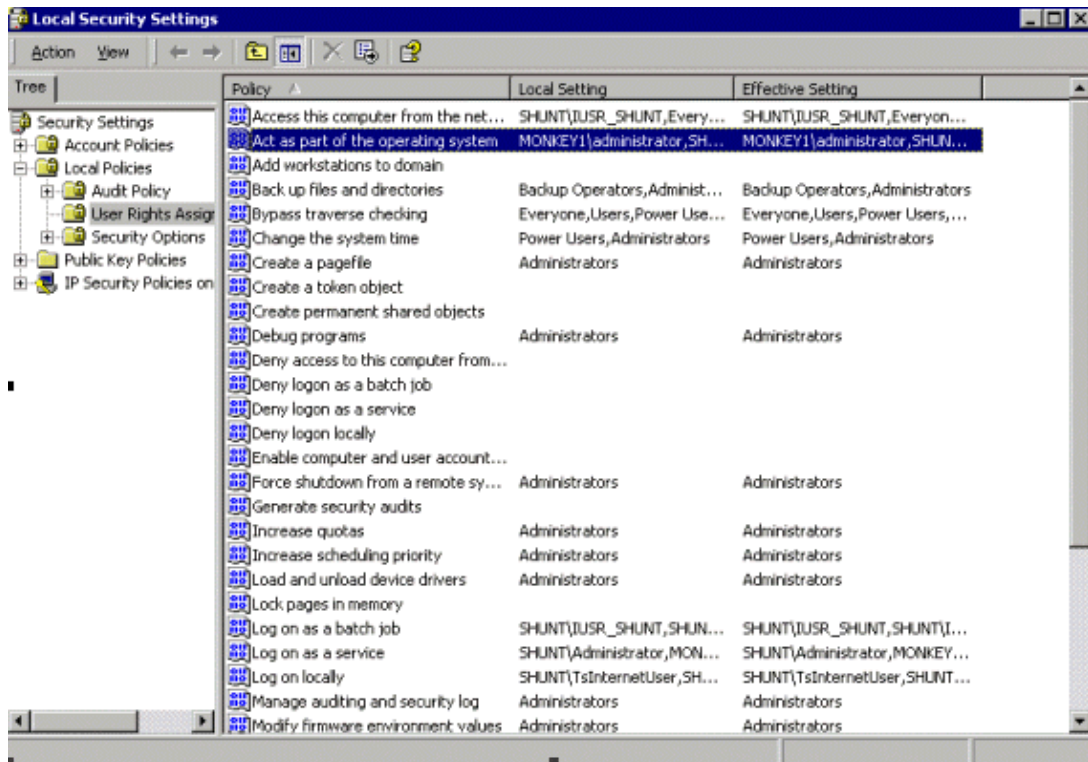
- Repeat steps 6 through 11 for this option.
- Reboot the Cisco Unity server.

After the server reboots, you are able to configure the second part of the configuration setup.

Verify the Procedure

Perform these steps in order to verify the configuration:

1. Go to **Start > Programs > Administrative Tools > Local Security Policy** and navigate to the **Local Security Settings** window, as shown.



2. In the right panel, look under the **Local Setting and Effective Setting** columns in order to verify that the accounts just configured actually exist.

Verify the existence of the accounts in both the **Act as Part of the Operating System** and **Log on as a Service** policies.

3. If the accounts do not exist, repeat the step-by-step instructions described in the configuration procedures.

Related Information

- [Cisco Unity Document page](#)
- [Voice Technology Support](#)
- [Voice and Unified Communications Product Support](#)
- [Recommended Reading: Troubleshooting Cisco IP Telephony](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)