

Domino Database Permissions for Cisco Unity

Document ID: 44702

Introduction

Before You Begin

Conventions

Prerequisites

Components Used

Domino Database Permissions for Cisco Unity

Names.nsf

Admin4.nsf

Mail Databases

Related Information

Introduction

Cisco Unity depends on the Domino subsystem for directory information, messaging, and notifications. This document discusses the various privileges the Unity server account needs to perform its job.

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

There are no specific prerequisites for this document.

Components Used

The information in this document is based on the software and hardware versions below.

- Cisco Unity 4.x and Domino

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Domino Database Permissions for Cisco Unity

Names.nsf

By default, this is the main directory database for a Domino domain. Cisco Unity needs sufficient permissions in the Access Control List (ACL) of this database to read, edit, delete, and create documents (or notes) in this database. By default, this level of permissions corresponds to editor, with the delete flag enabled (by default, the delete flag is unchecked for editor level). It is prudent to ensure the ACL permissions for the Cisco Unity server account are adequate before commencing with a Unity installation. Where a secondary address book is also used, the same privileges are required for those databases.

Admin4.nsf

This database is used by the Administrative Process task running on each Domino server. Upon importing a person into Cisco Unity, Unity submits a request to this database to Domino Unified Communication Services (DUCS)—enable the person and his or her mail file. It is the responsibility of DUCS to properly modify a user's mail file for Unified Messaging functionality.

Domino security policy requires Cisco Unity to digitally sign its requests. Signing documents involves modifying them. As such, the Unity server account will need privileges to create and modify documents in the Administrative Process database. This corresponds to editor level permissions in an ACL.

DUCS—enable requests are carried out in the database on the server containing a user's mail file. The Cisco Unity server account in Domino requires editor level permissions in the Admin4.nsf database on each server containing a Unity subscriber's mail file.

Mail Databases

Each Cisco Unity server has Manager level access to the mail files of its subscribers. Cisco Unity is added to the ACL of a mail file as part of the DUCS—enable process after import into Unity. The process is controlled by the DUCS software and not Cisco Unity. Unity creates, modifies, and deletes notes in this database. It also modifies the read/unread list, which requires Manager level access. It is imperative to ensure there does not exist any explicit deny lists or security settings which hinder Cisco Unity's ability to access a mail file after a DUCS—enable request has been executed.

Note: Immediately after importing a user into Cisco Unity, the Unity Domino Monitor attempts to access the user's mail file. However, this access is generally denied because the DUCS—enable request has not yet been executed and the Cisco Unity server account has not been added to the ACL of the mail file. This is expected behavior. Once the DUCS—enable request is executed, the Unity Domino Monitor will have access to the mail file.

Related Information

- [Setting Up the Message Store and Message Store Client](#)
- [Voice Technology Support](#)
- [Voice and Unified Communications Product Support](#)
- [Technical Support – Cisco Systems](#)

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

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Feb 02, 2006

Document ID: 44702
