

No Password is Assigned to the SQL System Administrator Account. Isn't this a Security Problem?

Document ID: 20416

Introduction

Prerequisites

Requirements

Components Used

Conventions

What Happens if You Configure Standard or Mixed Security?

Why ICM Uses Integrated Security

Related Information

Introduction

After you install Cisco Intelligent Contact Management (ICM), no password is assigned to the Microsoft SQL Server System Administrator (sa) account. This is not a security problem, because SQL is configured to use integrated security. Integrated security uses Microsoft Windows NT authentication mechanisms to validate SQL Server logins. Only trusted (multi-protocol or named pipes) connections are allowed.

Note: This document only applies to ICM version 4.5. From ICM version 4.5.1 onwards, ICM automatically creates a password for sa account.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco ICM
- Microsoft SQL Server
- Microsoft Windows NT

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ICM version 4.5.x
- Microsoft SQL Server version 6.5 and 7.0

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.

What Happens if You Configure Standard or Mixed Security?

SQL Server has three available security modes:

- **Integrated security** This mode uses Microsoft Windows NT authentication mechanisms to validate SQL Server logins, and is the only SQL Server security mode supported by ICM that runs Microsoft SQL version 6.5.
- **Standard security** This mode uses the SQL Server login validation process for all connections.
- **Mixed security** This mode allows either integrated or standard security methods to validate SQL Server login requests.

If you configure either standard or mixed security, ICM Services go into **stopshut** mode.

For example, here is an error message that appears when you configure mixed security, and then try to start ICM services:

```
09:55:11 la-lgr Fail: The logon security mode is not correct. It should be set to 'integrated'. It is currently set to 'mixed'.
```

Why ICM Uses Integrated Security

When Microsoft SQL Server is configured for integrated security, it takes advantage of the security capabilities of Microsoft Windows NT. During initial setup, you map Windows NT user accounts to SQL login IDs. This allows users to connect and login to SQL Server without a separate login or password. The credentials supplied by the user at the time of the original login to Windows NT are sufficient to allow (or, if appropriate, deny) access to SQL Server. With integrated security, users maintain one login ID and password for both Windows NT and SQL Server.

Related Information

- **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.](#)

Updated: Apr 12, 2005

Document ID: 20416
