

IIS Security and Cisco CallManager Version 2.4

Document ID: 8921

Introduction

Prerequisites

Requirements

Components Used

Conventions

Change IIS 4.0 Security through the Microsoft Management Console

Change the NTFS Permissions through Windows NT Explorer

Related Information

Introduction

This document contains the steps necessary in order to secure the Cisco CallManager version 2.4 web interface using the Internet Information Server (IIS) 4.0 and Windows NT file system (NTFS) security. This involves changing the security through the the Microsoft Management Console (MMC) for IIS and changing the NTFS permissions on the affected directories and files.

You can access Cisco CallManager using either Internet Explorer or Netscape Navigator web browsers. As a result, the instructions in this document address users with either Internet Explorer or Netscape Navigator web browsers. In order to achieve the highest level of security, Cisco recommends everyone use only Internet Explorer, and that the MMC be configured for the Windows NT Challenge Response security option. Be advised that Netscape does not work with this configuration. If Netscape Navigator is to be used, you must configure MMC for Basic Authentication using the instructions provided.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

- Cisco CallManager version 2.4 web interface
- IIS 4.0
- NTFS security
- Either Internet Explorer or Netscape Navigator web browsers

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.

Change IIS 4.0 Security through the Microsoft Management Console

Use these steps in order to change the security settings on the Cisco CallManager server PC. If you have multiple Cisco CallManager servers, repeat these steps on each PC.

1. Click **Start > Program Files > Windows NT Option Pack > Microsoft Internet Information Server > Internet Service Manager**.

Result: MMC opens.

2. Expand the **Internet Information Server** folder, and then the computer icon beneath it, and then the **Default Web Site**.

Result: The files and folders for the IIS and Cisco CallManager PCs are displayed.

3. Right-click on **Cisco** and select **Properties**.

Result: The Cisco Properties dialog box is displayed.

4. Click the **Directory Security** tab.

Result: The options for directory security are displayed.

5. In the Anonymous Access and Authentication Control area, click **Edit**.

Result: The Authentication Methods dialog box is displayed.

6. Click in order to select the **Basic Authentication** checkbox.

Result: A warning message is displayed. Basic Authentication transmits the password in clear text.

This can be a security problem. Netscape does not support NT Challenge/Response, so Basic Authentication is the normal security level chosen when Netscape web browsers will possibly be used. If security is an issue, and Internet Explorer 4.x or greater is being used, then Windows NT Challenge/Response can be used on the Cisco Web Site and the Users folder (this transmits encrypted passwords). If someone is logged onto the domain, it recognizes their account and grants them access according to the NTFS permissions.

7. Click **Yes** on the message box.

Result: The message box clears and the options for directory security are redisplayed.

8. Uncheck the **Allow Anonymous Access** checkbox.
9. Click **OK** in the Authentication Methods dialog box, and then click **OK** in the Cisco Properties window.
10. In the Microsoft Management Console, click the **plus sign** next to Cisco in order to expand the Cisco Web Site.

Result: The files and folders under the Cisco Web Site are displayed.

11. Right-click on the **Users** folder and select **Properties**.

Result: The Users Properties window is displayed.

12. Click the **Directory Security** tab.

Result: The options for directory security are displayed.

13. In the Anonymous Access and Authentication Control area, click **Edit**.

Result: The Authentication Methods dialog box is displayed.

14. Click in order to select the **Allow Anonymous Access** checkbox.

15. Uncheck the **Allow Anonymous Access** checkbox.
16. Click **OK** in the Authentication Methods dialog box, and then click **OK** in the User Properties window.
17. In the Microsoft Management Console window, right-click on the **Default Web Site** and select **Stop**.

Result: The Default Web Site is stopped and shows (stopped) next to the Default Web Site in the Microsoft Management Console window.

18. In the Microsoft Management Console window, right-click on the **Default Web Site** and select **Start**.

Result: The security changes take effect, and the Default Web Site is running.

Change the NTFS Permissions through Windows NT Explorer

Use these steps in order to change the NTFS permissions on the Cisco CallManager server PC. If you have multiple Cisco CallManager servers, repeat these steps on each PC.

1. Open Microsoft Windows NT Explorer.
2. Go to the **c:\inetpub\wwwroot\Cisco** folder. Right-click on the **Cisco** folder and select **Properties**.

Result: The Cisco Properties dialog box is displayed.

3. Click the **Security** tab.

Result: The options for security are displayed.

4. In the Permissions area, click **Permissions**.

Result: The Directory Permissions dialog box is displayed.

5. In the list of Names, click on **Everyone** and click **Remove**.

Result: Everyone is removed from the list of Names.

6. In the list of Names, verify that Administrators have Full Control.

Note: In order to change the type of access allowed, select **Administrators** and **Full Control** in the Type of Access box.

7. Click **OK** in the Directory Permissions dialog box, and then click **OK** in the Cisco Properties window.
8. In the Windows Explorer under the Cisco folder, locate the file called **global.asa**.
9. Right-click on **global.asa** and select **Properties**.

Result: The global.asa Properties dialog box is displayed.

10. Click the **Security** tab.

Result: The options for security are displayed.

11. In the Permissions area, click **Permissions**.

Result: The File Permissions dialog box is displayed.

12. Click the **Add?** button.

Result: The Add Users and Groups dialog box is displayed.

13. In the list of Names, select **Everyone**, and then select **Read** as the Type of Access.
14. Click **Add**, and then click **OK**.

- Result: Everyone displays in the list of Names on the File Permissions dialog box.
15. Click **OK** in the File Permissions dialog box, and then click **OK** in the global.asa Properties window.

Result: The NTFS permissions have been changed.

Related Information

- **Voice Technology Support**
 - **Voice and IP 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.](#)

Updated: Sep 26, 2006

Document ID: 8921
