

# Reset Your Voicemail PIN on Cisco Unity Connection

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

#### [Requirements](#)

#### [Components Used](#)

### [Configure](#)

#### [Configurations](#)

### [Verify](#)

### [Troubleshoot](#)

---

## Introduction

This document describes how you can set or change your Voicemail PIN on Cisco Unity Connection.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Unity Connection (CUXN)
- Cisco Unified Communications Manager (CUCM)
- Cisco Clients (Jabber, Webex, IP Phones)

### Components Used

This document is not restricted to specific software and hardware versions.

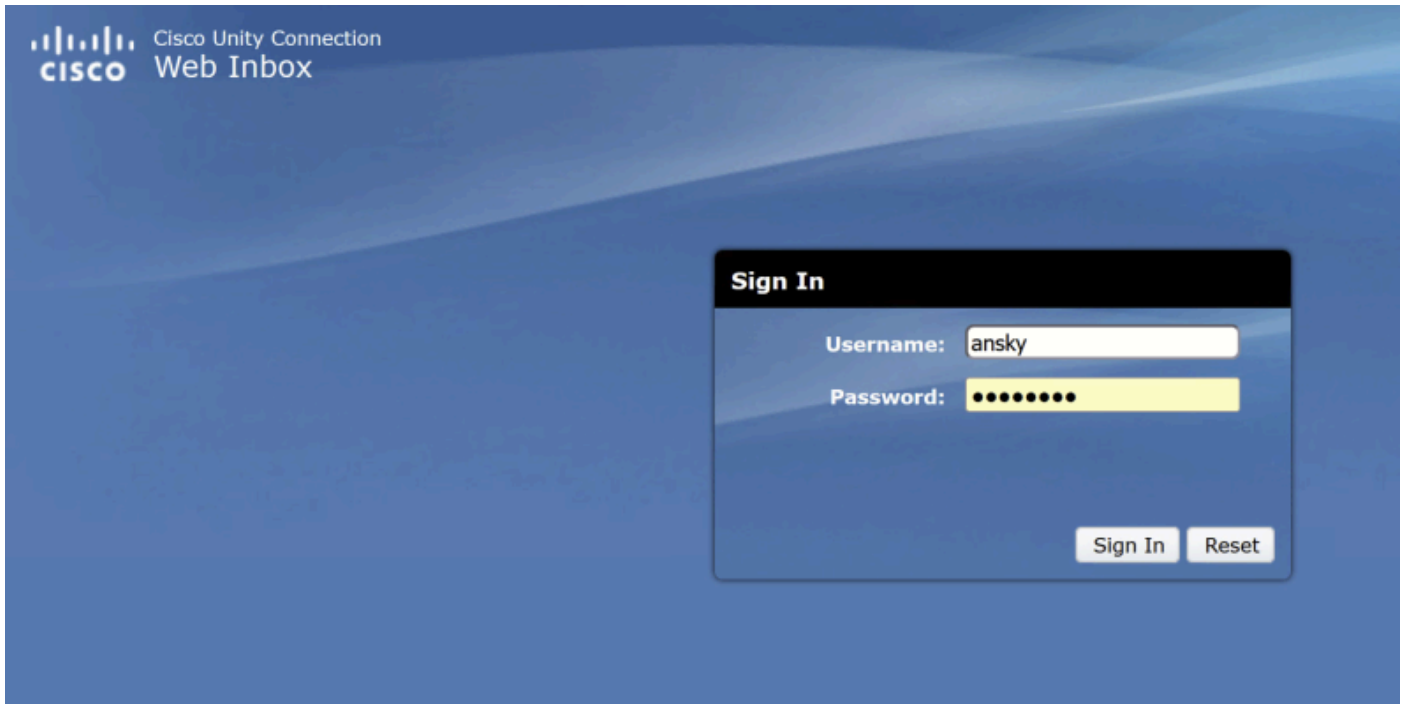
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Configure

### Configurations

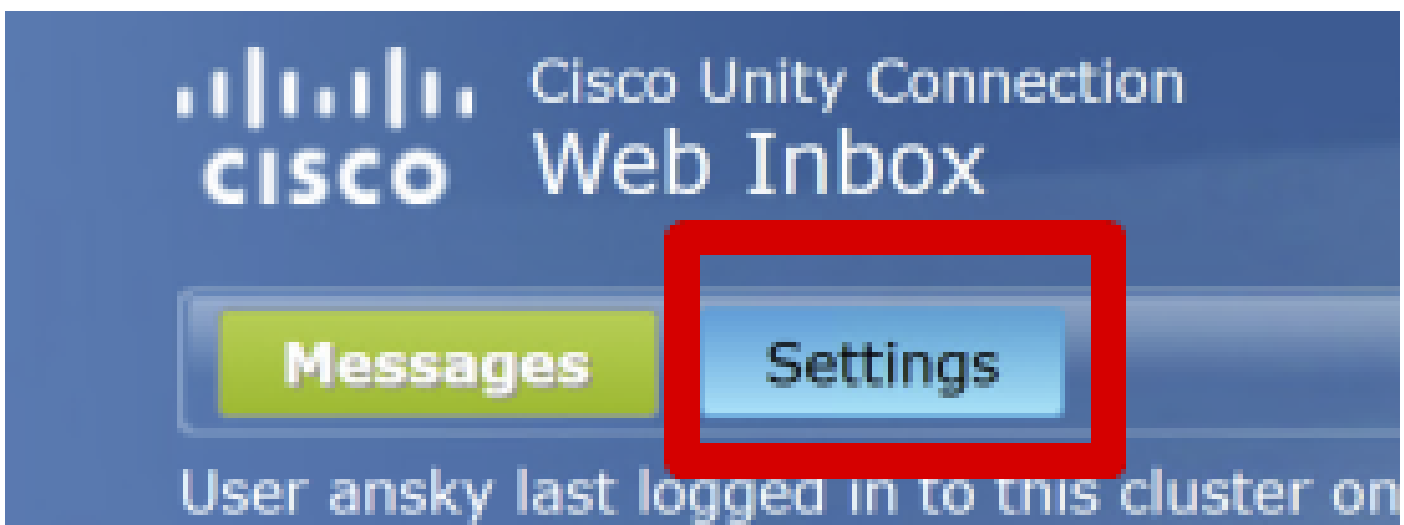
**Step 1.** Log in to the **http://<Cisco Unity Connection server>/inbox** URL from your browser while you are on your corporate network.

**Step 2.** Provide your **Username** and **Password** that you use to log in to your Cisco Jabber or Phone Services for Webex Unified Communications Manager (UCM).



*Cisco Unity Web Inbox Log in Screen*

**Step 3.** Navigate to the **Settings** tab.


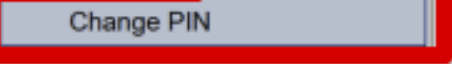


*Cisco Unity Web Inbox Settings Tab*

**Step 4.** In the new page that has been opened, select there **Passwords > Change PIN** .

Messaging Assistant >> Preferences >> Personal Options

Preferences ▾ Passwords ▾ Greetings ▾ Notification Devices ▾ Contacts ▾ Private Lists ▾ Help ▾

 Save 


**Name**

First Name Anakin

Alternate Spelling of First Name

*Cisco PCA Messaging Assistant PIN Change*


**Step 5.** Create a New PIN and Save it.

 Save

Last Changed: Thursday, December 12, 2024 10:51:22 AM GMT-06:00

New PIN:

Confirm New PIN:



*Save the New PIN on the Cisco PCA*


## Verify

There is currently no verification procedure available for this configuration.

## Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

After you save the new PIN, it is possible to see an error like the one showed in the image: "Error saving password - Trivial passwords or PINs are not allowed: Password cannot contain digits that are dialed in a straight line on a keypad."

 Error saving password - Trivial passwords or PINs are not allowed: Password cannot contain digits that are dialed in a straight line on a keypad.

*Error saving password - Trivial passwords or PINs are not allowed: Password cannot contain digits that are dialed in a straight line on a keypad*

The system provides trivial credential checks to disallow credentials that are easily hacked. You enable trivial credential checks by checking the Check for Trivial Passwords check box in the Credential Policy Configuration window.

Passwords can contain any alphanumeric ASCII character and all ASCII special characters. A non-trivial password meets this criteria:

- Must contain three of the four allowable characteristics: uppercase character, lowercase character, number, symbol
- Must not use a character or number more than three times consecutively
- Must not repeat or include the alias, username, or extension
- Cannot consist of consecutive characters or numbers (for example, passwords such as 654321 or ABCDEFG)

PINs can contain digits (0-9) only. A non-trivial PIN meets the following criteria:

- Must not use the same number more than two times consecutively
- Must not repeat or include the user extension or mailbox or the reverse of the user extension or mailbox
- Must contain three different numbers; for example, a PIN such as 121212 is trivial
- Must not match the numeric representation (that is, dial by name) for the first or last name of the user
- Must not contain groups of repeated digits, such as 408408 or 113377, or patterns that are dialed in a straight line on a keypad, such as 2580, 159, or 753

For further information on how to configure the Credentials and PIN policies, visit the [Passwords, PINs, and Authentication Rule Management](#) chapter from the Cisco Unity Connection Security guide.