Come abilitare il PIN comune per CUCM e UCXN.

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Premesse Panoramica delle funzionalità Configurazione Risoluzione dei problemi Numero 1. Numero 2. Informazioni correlate

Introduzione

Questo documento descrive la procedura per configurare il pin comune impostato per Cisco Unified Communications Manager (CUCM) e Cisco Unity Connection (UCXN) nella versione 11.5.

Prerequisiti

Requisiti

Cisco consiglia di sapere come creare gli utenti e associare i dispositivi agli utenti.

Prima di iniziare a configurare il pin comune è necessario integrare CUCM in UCXN.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware

- Cisco CallManager 11.5
- Cisco Unity 11.5

Nota: Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Quando si utilizza lo stesso PIN, l'utente deve accedere ad applicazioni UC quali la conferenza Meet Me, la mobilità di estensione e la segreteria telefonica, in modo da non dover gestire più credenziali PIN. L'utente desidera poter impostare/modificare un PIN (comune) sul portale di autogestione.

L'amministratore deve poter specificare quando deve essere utilizzato un PIN comune tra CUCM/Unity, per poter scegliere quando i PIN sono diversi o sincronizzati. L'amministratore desidera poter abilitare il PIN comune per tutti gli utenti assegnati all'unità specifica.

In CUCM versione 11.5 è presente una nuova casella di controllo **Abilita sincronizzazione PIN utente finale** nella pagina Server applicazioni quando si seleziona Tipo server applicazioni come Cisco Unity Connection.

Panoramica delle funzionalità

- Provisioning per abilitare la sincronizzazione dei pin dell'utente finale tra CUCM e UCXN tramite la pagina Application Server dall'interfaccia utente di amministrazione CUCM
- Se la sincronizzazione dei pin è abilitata e quando un utente aggiorna il pin da CUCM, BAT (Buk Administration Tool), AXL (Administrative Extensible Markup Language), UDS (User Data Service) o Portale Self Care, il pin deve essere sincronizzato con UCXN
- Il PIN deve essere sincronizzato tra CUCM e UCXN e viceversa quando la sincronizzazione del PIN è abilitata in entrambe le applicazioni
- Per impostazione predefinita, la sincronizzazione dei pin deve essere disabilitata quando si tenta di creare un nuovo record Unity Connection o quando si esegue un aggiornamento e si tenta di caricare qualsiasi record Unity Connection corrente.

Configurazione

Passaggio 1.

Creare un utente finale in CUCM e associarlo a un dispositivo

Passaggio 2.

Importa l'utente in Unity

Passaggio 3.

Passare ad Amministrazione sistema operativo in CUCM

Passaggio 4.

Scarica il certificato Tomcat

Passaggio 5.

Carica come fiducia tomcat in Unity

Passaggio 6.

Ora Scarica il certificato Tomcat da Unity e carica questo come tomcat trust in CUCM

Passaggio 7.

Crea un utente applicazione in CUCM con le credenziali Unity

Passaggio 8.

Assegna a questo utente il ruolo di AXL

Groups	Admin-3rd Party API	~				
	Application Client Users				Add to Access Control Group	
	Standard Audit Users			Ì	Remove from Access Control Gro	oup
	Standard CCM Admin Users	~	Vie	ew Details		
oles	Standard AXL API Access		^			
	Standard Admin Rep Tool Admin					
	Standard Audit Log Administration					
	Standard CCM Admin Users					
	Standard CCM End Users		\mathbf{v}	View Details		

Passaggio 9.

Assegna il ruolo AXL anche all'utente dell'app CUCM

Passaggio 10.

Passare a Cisco Unity Connection e selezionare la casella di controllo Abilita sincronizzazione PIN utente finale

Cisco Unity Conn For Cisco Unified Commu	ection Administration nications Solutions				Navigation Cisco Unity Con appadmin Search Docum	nnection Administration 🧹 😡
Cisco Unity Connection Video Services Accounts Status	Edit AXL Servers			Search Phone Syste	ms Phone System Basics (i Related Links Check T	PhoneSystem) > Edit AXL Serve
Dial Plan	Phone System Edit Refresh Help					
Partitions	Finite System Lot Keresh help					
Search Spaces	Save					
System Settings						
Cluster	AXL Servers					
Authentication Rules	Delete Selected Add New					
B Roles						
Restriction Tables	Order	IP	Address		Port	
Licenses		0.106.123.111			8443	Test
Schedules						
-Holiday Schedules	Delete Selected Add New					
-Global Nicknames						
Subject Line Formats	AXL Server Settings					
Attachment Descriptions	Lisername	hisco				
Enterprise Parameters		pisco				
Pluging	Password	•••••				
-Fax Server	Cisco Unified Communications Manager Ve	ersion 5.0 or Greater (SSL) 🗸				
E-LDAP	Enable End User PIN Synchronization for Primary AXL Server					
SAML Single Sign on	Ignore Certificate Errors					
Cross-Origin Resource Sharing (C						
SMTP Configuration	Save					
Advanced						
Telephony Integrations						
Phone System						
Port Group						
- Port						
Trunk						
E Security						
Tools						
Task Management						
Bulk Administration Tool						

Passaggio 11.

Da CUCM passare a Sistema>Server applicazioni>Aggiungi il nuovo server applicazioni come Cisco Unity Connection (se non è già stato aggiunto)

Passaggio 12.

Selezionare la casella di controllo Abilita sincronizzazione PIN utente finale

Save 🗙 Delete 🗋	Copy 📫 Add New								
Status Status: Ready									
Application Server Information									
Application Server Type Cisco Unity Connection									
Name*	cuc								
IP Address*	10.106.107.145								
Available Application Users	c CCMSysUser WDSysUser CCMQRTSysUser IPMASysUser	~							
Selected Application Users*	appadmin	^							
Enable End User Pin Synchronization									
Save Delete Copy Add New									

Passaggio 13.

Fare clic su Salva

Viene ricevuto il messaggio Sincronizzazione PIN completata.

Risoluzione dei problemi

Numero 1.

Messaggio di errore "La sincronizzazione del PIN non è abilitata perché il certificato non è stato verificato."

Risoluzione dei problemi relativi alle fasi

- Verificare che i certificati siano caricati correttamente.
- Verificare che Unity Connection sia raggiungibile e che l'accesso sia riuscito.

Numero 2.

Messaggio di errore "La sincronizzazione del pin non è abilitata a causa del codice di risposta HttpsURLConnection: 401: Non autorizzato"

Procedura di risoluzione dei problemi

- Assicurarsi di aver selezionato Abilita sincronizzazione PIN utente finale in
- Verificare di aver assegnato il ruolo AXL agli utenti dell'app.

Informazioni correlate

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cuc sag/b_cucsag_appendix_01111.html#id_16699