

Comunicazione pre-release UCCX 11.6

Sommario

[Introduzione](#)

[Premesse](#)

[Preparazione dell'aggiornamento a UCCX 11.6](#)

[Aggiornamento di SocialMiner e Microsoft Exchange](#)

[Supporto TLS 1.2 per UCCX](#)

[Impatto su RTMT e Script Editor](#)

[Supporto per ESXi 6.5](#)

[Riduzione dei tempi di aggiornamento](#)

[ISO singolo per aggiornamenti e nuove installazioni](#)

[Aggiornamenti del desktop e del browser](#)

[Realtime Reporting Tool](#)

[Modalità di compatibilità per i browser](#)

[Single Sign-On \(SSO\)](#)

[Supporto per nuovi provider di identità](#)

[Miglioramenti Finesse Failover](#)

[Considerazioni importanti](#)

[Miglioramenti dei servizi](#)

[Dashboard e avvisi del servizio di contesto](#)

[Informati prima dell'aggiornamento](#)

[Coerenza delle password e impatto su LiveData](#)

[Utenti report: impossibile accedere ai report CUIC dopo l'aggiornamento a UCCX 11.6](#)

[Aumento del limite delle dimensioni degli allegati per la posta elettronica e le considerazioni su Exchange](#)

[Calcola le dimensioni massime dei messaggi](#)

[Considerazioni importanti sull'aggiornamento](#)

[Ottenere la documentazione e inviare una richiesta di assistenza](#)

Introduzione

Questo documento descrive la comunicazione pre-release UCCX 11.6.

Nota: Unified Contact Center Express (UCCX) versione 11.6 è una versione molto importante, con importanti aggiornamenti alle funzioni critiche e alla disponibilità che aiuteranno partner e clienti. Questa comunicazione preliminare fornisce una panoramica degli aggiornamenti critici e informazioni importanti che aiutano a pianificare un aggiornamento rapido e senza problemi a UCCX 11.6.

Premesse

UCCX 11.6 dispone di una serie di funzionalità volte a migliorare la serie di funzionalità del

prodotto e la produttività di agenti, supervisor e amministratori. Aggiornamenti importanti sono stati apportati tramite e-mail, funzionalità di chat, mentre gli aggiornamenti al report di Cisco Unified Intelligence Center (CUIC) e gli aggiornamenti di Finesse Desktop migliorano notevolmente l'esperienza degli utenti del contact center. Durante l'esecuzione degli aggiornamenti al sistema sono stati aggiunti importanti aggiornamenti dei servizi, ad esempio il Dashboard dei servizi di contesto, per offrire vantaggi quali una riduzione del tempo richiesto per gli aggiornamenti

Un riepilogo delle nuove funzioni (per un elenco dettagliato, fare riferimento alle note sulla versione):

Cisco Finesse	UCCX Email	UCCX Chat	CUIC reporting
<ul style="list-style-type: none"> • Trasferimento diretto • Stati dell'agente in base alla riga secondaria • Visualizza etichette codice motivo per impostazione predefinita • Enhanced Finesse Failover • Rapporti Cronologia chiamate e Stato agente recenti • Statistiche di coda per FIPPA • Possibilità di effettuare chiamate dallo stato READY • Possibilità di monitorare le chiamate in uscita sulla linea ACD • Report cronologici supervisore • Codici motivo generati dal sistema come etichette per gli agenti e possibilità di modificare le etichette dei codici motivo generati dal sistema 	<ul style="list-style-type: none"> • E-mail cc/bcc/forward • Rispondi e rispondi a tutti • Firma di posta elettronica • Supporto GMAIL • Motivi di conclusione • Report di riepilogo agente multicanale 	<ul style="list-style-type: none"> • Chat di gruppo • Motivi di riepilogo • Programmazione chat per avere ore di apertura e chiusura • Indicatore digitazione • Report di riepilogo agente multicanale 	<ul style="list-style-type: none"> • Nuovi dashb • Nuovi grafici aggiornati del visuali • Report motivi riepilo per ch e-mail • Report riepilo agente multicanale
Miglioramenti agli script	Miglioramenti campagna in uscita	SSO	Other (A
<ul style="list-style-type: none"> • Supporto intestazione e proxy per chiamata Make REST • Ottieni il passaggio Statistica report per consentire il conteggio degli agenti in base al codice motivo non pronto • Nuovo passaggio Crea documento JSON • Nuovo passaggio dati documento JSON • Script IVR basati su servizi di contesto aggiunti come modelli • Supporto TLS 1.2 	<ul style="list-style-type: none"> • Possibilità di salvare l'ordine esplicito dei campi nell'elenco contatti importato. • Importazione automatica degli elenchi di contatti tramite SFTP o HTTP Server 	<ul style="list-style-type: none"> • Autenticazione integrata di Windows • Qualificazione di 4 nuovi IDP e supporto generico SAML 2.0 	<ul style="list-style-type: none"> • Supporto ESXi 6 • Aggiornamenti TLS • Tempi di aggiornamento più rapidi • Supporto per Hyper

Preparazione dell'aggiornamento a UCCX 11.6

UCCX 11.6 supporta aggiornamenti diretti da questi percorsi:

10,x	11.0	11.5
10.5(1)SU1	11.0(1)	11.5(1)
10.6(1)	11.0(1)SU1	11.5(1)SU1
10.6(1)SU1		
10.6(1)SU2		

Qualsiasi corso tecnico speciale (ES) applicato alle versioni precedenti non influisce sul percorso di aggiornamento. L'aggiornamento può essere eseguito da qualsiasi versione precedente, indipendentemente da quale ES sia installato sul sistema. Se è presente una versione software dopo la data di pubblicazione del presente documento, controllare la matrice di compatibilità dei software UCCX per verificare la disponibilità di un percorso di aggiornamento.

Aggiornamento di SocialMiner e Microsoft Exchange

UCCX interagisce con SocialMiner per tutte le funzionalità di e-mail e chat. È necessario pianificare l'aggiornamento alla versione 11.6 per garantire che i server UCCX e SocialMiner vengano aggiornati alla versione 11.6 nella stessa finestra di manutenzione. In UCCX 11.6, le funzionalità di posta elettronica e chat sono state aggiornate. L'utilizzo di queste funzionalità di UCCX 11.6, con SocialMiner ancora sulla versione 11.5, ha risultati imprevisti e vengono visualizzati errori/avvisi.

La sequenza consigliata per l'aggiornamento consiste nell'aggiornare il server SocialMiner e i server UCCX nella stessa finestra di manutenzione.

La soluzione UCCX 11.6 supporta **Microsoft Exchange Server 2013 e 2016 - Enterprise e Standard Edition** per la funzionalità UCCX Email. Se si utilizza **Microsoft Exchange Server 2013**, assicurarsi di installare l'aggiornamento cumulativo 15 per Exchange Server 2013 (KB3197044) in modo che TLS 1.2 sia supportato da Exchange. Senza questa patch, la comunicazione tra SocialMiner e **Microsoft Exchange Server 2013** non riesce e il routing della posta elettronica non riesce. Se è già stato installato un server **Microsoft Exchange Server 2013** con UCCX, assicurarsi di installare questa patch prima che entri in produzione con UCCX 11.6.

Questa operazione non è necessaria per **Microsoft Exchange Server 2016**.

Nota: Se non si desidera utilizzare TLS 1.2 per le connessioni a Exchange, la versione minima TLS del server può essere impostata su 1.0 sul server SocialMiner (vedere i dettagli nella sezione TLS più avanti). In caso di mancata corrispondenza TLS tra Exchange e SocialMiner, tutti i feed e-mail avranno esito negativo.

Supporto TLS 1.2 per UCCX

In UCCX 11.6, il valore predefinito è TLS 1.2 per le connessioni quando UCCX opera come client o come server nella connessione. I clienti che eseguono l'aggiornamento a UCCX 11.6 e utilizzano applicazioni di terze parti che interagiscono con UCCX e utilizzano TLS devono essere consapevoli di questo cambiamento.

UCCX 11.6 consente inoltre di aggiornare la versione TLS minima per le connessioni client e server:

- set tls client min-version <1.1 o 1.0>
- set tls server min-version <1.1 o 1.0>

Esempio: `set tls server min-version 1.2`

Se si tratta di un sistema ad alta disponibilità, il comando deve essere eseguito su entrambi i nodi. Una volta eseguito il comando, il sistema deve essere riavviato utilizzando il comando **utils system restart**.

È possibile verificare la versione TLS minima supportata anche eseguendo i comandi seguenti:

- **show tls client min-version**
- **show tls server min-version**

Nota: Se la versione minima è impostata su 1.0, la connessione supporterà 1.0, 1.1 e 1.2.

Impatto su RTMT e Script Editor

In base agli standard di sicurezza TLS 1.2, e questo è lo standard, tutti i plug-in UCCX come RTMT e Script Editor vengono reinstallati in modo che possano continuare a funzionare con UCCX 11.6. Inviare l'aggiornamento a UCCX:

1. Scaricare e reinstallare RTMT su tutti i computer che in precedenza disponevano di RTMT. Le versioni precedenti di RTMT non sono in grado di stabilire una connessione con UCCX.
2. Scaricare e reinstallare UCCX Script Editor su tutti i computer in cui in precedenza era installato UCCX Script Editor.

Supporto per ESXi 6.5

Per iniziare da UCCX 11.6, è supportato ESXi 6.5. A causa di problemi di prestazioni con VMFS 6 e di indagini in corso da parte di VMWare, ESXi 6.5 è supportato solo con VMFS 5.

	Supporto ESXi 6.5	Versione VMFS con ESXi 6.5	Commenti
BE6K	Sì	VMFS 5	La dipendenza da altre applicazioni impedisce l'utilizzo di VMFS 6
non-BE6k	Sì	VMFS 5 e VMFS 6	L'aggiornamento di ESXi e VMFS potrebbe richiedere migrazione delle VM

Assicurarsi di utilizzare l'ultimo modello OVA pubblicato per la versione 11.6.

Nota: Il supporto per VMFS 6 può essere aggiornato in futuro per le versioni precedenti. Fare riferimento al [wiki sulla virtualizzazione UCCX](#) per l'ultimo aggiornamento.

Riduzione dei tempi di aggiornamento

In UCCX 11.6 sono stati eseguiti aggiornamenti per ridurre il tempo totale richiesto per un esercizio di aggiornamento completo. Nell'ambito del processo di commutazione, diversi script vengono eseguiti in sequenza per eseguire la migrazione dei dati di singole applicazioni, ad esempio Finesse, CUIC e dati cronologici. In UCCX 11.6, il progetto viene aggiornato in modo da far eseguire gli script in parallelo, riducendo in modo significativo il tempo necessario per la versione dello switch.

Sebbene non sia possibile visualizzare il tempo effettivo per la versione dello switch a causa delle dimensioni del database del cliente, i test interni hanno mostrato una riduzione del 30% del tempo necessario per il processo di creazione della versione dello switch.

ISO singolo per aggiornamenti e nuove installazioni

In UCCX 11.6, è disponibile solo un file ISO pubblicato su Cisco.com e può essere utilizzato per un aggiornamento o una nuova installazione. L'ISO segue la convenzione di denominazione regolare di `UCSInstall_UCCX_11.6.XXXXX-XX.sgn.iso`

Questo ISO è fornito con entrambe le opzioni di avvio, quindi funge anche da immagine di avvio.

Aggiornamenti del desktop e del browser

Realtime Reporting Tool

Real Time Reporting Tool non è più interamente basato su browser, ma utilizza l'applet Java che richiede il download sul PC per l'accesso. Con gli aggiornamenti della protezione introdotti nella maggior parte dei browser per quanto riguarda la protezione Java, è necessario introdurre lo strumento UCCX Real Time Reporting (RTR) come un'applet Java scaricata durante la prima installazione.

Funzionamento aggiornato nella versione 11.6:

1. RTR è ora disponibile per essere scaricato come plugin, passare alla pagina **Strumenti > Plugin**. Continua a esistere nella pagina **Strumenti > Report in tempo reale**.
2. Quando si accede a RTR per la prima volta da un determinato PC dopo l'aggiornamento a UCCX 11.6, un'applet Java viene scaricata dal server UCCX. L'utente deve disporre dei diritti per consentire il download e aprire lo stesso.

Nota: Questa operazione deve essere eseguita in tutti i PC che desiderano accedere a RTR dopo l'aggiornamento. Una volta scaricata l'applet RTR, ogni utente che ha accesso al PC può aprire lo stesso.

La versione Java consigliata per l'utilizzo di RTR è **Java 8**. Se l'utente dispone di Java 7, deve abilitare TLS 1.2 nel Pannello di controllo Java.

Modalità di compatibilità per i browser

Se si utilizza Internet Explorer, Finesse Desktop non supporta la modalità di compatibilità. Le modifiche vengono apportate per visualizzare un avviso a un agente se è attivata la modalità di compatibilità. L'unico scenario in cui è richiesta la modalità di compatibilità è per gli accessi di vecchie interfacce utente per CUIC che contengono funzioni quali Cassetto protezione, Scheduler e così via.

Single Sign-On (SSO)

UCCX ora supporta l'autenticazione integrata di Windows. Per ulteriori informazioni, consultare le note sulla versione di UCCX e i documenti correlati.

Supporto per nuovi provider di identità

In UCCX 11.6, diversi nuovi provider di identità (IDP) sono qualificati e aggiunti per il supporto:

- Microsoft AD FS (Active Directory Federation Services): 2.0, 2.1 e 3.0
- PingFederate: 8.2.2.0
- ApriAM: 10.0.1
- Shibboleth 3.3.0
- F5:13

UCCX 11.6 funziona anche con qualsiasi IDP che funziona con SAML v2.0. Purché l'IDP si confermi allo standard SAML v2.0 e sia in grado di soddisfare la configurazione UCCX (IdS), l'IDP può essere utilizzato per l'SSO UCCX anche se non fa parte dell'elenco di cui sopra.

Miglioramenti Finesse Failover

A partire da UCCX 11.6, il comportamento di failover è migliorato per garantire la produttività degli agenti durante un failover Finesse senza eseguire un failover completo del sistema. È importante capire le stesse cose in modo che gli agenti siano a conoscenza dei cambiamenti nel comportamento.

Panoramica del cambiamento di comportamento.

Scenario	Comportamento di UCCX HA	Finesse Service su Node1	Finesse Service su Node2	Comportamento del client Finesse
Errore del motore CCX sul nodo 1	CCX Engine su SideB diventa master	Finesse esce dal servizio e torna a IN_SERVICE non appena si connette al nuovo motore principale.	Finesse esce dal servizio e torna a IN_SERVICE non appena si connette al nuovo motore principale.	L'agente vede la barra di disconnessione rossa e si riconnette automaticamente al lato Finesse che viene prima in IN_SERVICE. Può essere Nodo1 o Nodo2. Gli agenti connessi al nodo 1 continuano ad essere connessi.
Errore del motore CCX sul nodo 2	Il motore CCX di SideA continua a essere il dispositivo master	Finesse continua a essere IN_SERVICE	Finesse esce dal servizio e torna a IN_SERVICE non appena si connette al motore principale.	Gli agenti connessi al nodo 2 vengono temporaneamente disconnessi e si connettono al servizio Finesse sul nodo IN_SERVICE. Tutti gli agenti collegati a Node1 vengono temporaneamente disconnessi e si connettono a Finesse su Node2. Gli agenti connessi al
Finesse Service OS su Node1	La masterizzazione del motore non è interessata	FUORI SERVIZIO	Finesse sul nodo 2 continua a essere IN_SERVICE	

Finesse Service OS sul nodo 2	La masterizzazione del motore non è interessata	Finesse su Node1 continuerà a essere IN_SERVICE	FUORI SERVIZIO	nodo 2 non saranno interessati. Tutti gli agenti collegati al nodo 2 vengono temporaneamente disconnessi e si connettono a Finesse sul nodo 2. Gli agenti connessi al nodo 1 non saranno interessati.
Errore del servizio di notifica CCX sul nodo 1	La masterizzazione del motore non è interessata	FUORI SERVIZIO	Finesse sul nodo 2 continuerà a essere IN_SERVICE	Tutti gli agenti collegati a Node1 vengono temporaneamente disconnessi e si connettono a Finesse su Node2. Gli agenti connessi al nodo 2 non sono interessati.
Errore del servizio di notifica CCX sul nodo 2	La masterizzazione del motore non è interessata	Finesse su Node1 continua a essere IN_SERVICE	FUORI SERVIZIO	Tutti gli agenti collegati al nodo 2 vengono temporaneamente disconnessi e si connettono a Finesse sul nodo 2. L'operazione non ha alcun effetto sugli agenti connessi al nodo 1.
Modalità Isola	Entrambi i nodi HA diventano master	Finesse su Node1 continua ad essere IN_SERVICE e verrà connesso al motore su Node1.	Finesse esce dal servizio e tornerà a IN_SERVICE non appena si connette al motore sul nodo 2 che è anche il master.	Gli agenti connessi al nodo 1 continuano ad essere connessi. Gli agenti connessi al nodo 2 vengono temporaneamente disconnessi e si connettono al servizio Finesse sul secondo nodo.

Considerazioni importanti

1. UCCX non supporta il bilanciamento del carico dell'accesso dell'agente. Tutti gli agenti devono accedere solo al nodo principale. Il miglioramento del comportamento è solo per il supporto del failover.
2. Non è supportato avere lo stesso accesso agente a entrambi i nodi contemporaneamente. Ciò può causare incoerenze nell'esperienza dell'agente.

- In caso di failover multipli che portano agli agenti connessi a entrambi i nodi, tutti gli agenti devono essere spostati al più presto nel nodo master. Non è necessario che venga eseguito immediatamente, ma l'amministratore può eseguire una pianificazione in base alle finestre di manutenzione disponibili.

Miglioramenti dei servizi

Dashboard e avvisi del servizio di contesto

In UCCX 11.6 è disponibile un dashboard per verificare lo stato di tutti i componenti registrati nel servizio contesto. È possibile accedere al dashboard nella pagina **UCCX Serviceability**, passando alla pagina **Strumenti > Stato servizio contesto**.

Component : Host Name	State	Status	Mode	Last Fetched at	Action
FMC : uccx1-71.cumulus-motorcycles.com	Registered	● Online	NA	Jul 5, 2017 8:55:18 AM	-
Finesse : uccx1-71.cumulus-motorcycles.com	Registered	● Online	Lab	Jul 5, 2017 8:55:27 AM	-
Finesse : uccx2-72.cumulus-motorcycles.com	Registered	● Online	Lab	Jul 5, 2017 8:55:27 AM	-
SocialMiner : sm-186.cumulus-motorcycles.com	Registered	● Online	Lab	Jul 5, 2017 8:55:26 AM	-
UCCX : uccx1-71.cumulus-motorcycles.com	Registered	● Online	Lab	Jul 5, 2017 8:55:26 AM	-
UCCX : uccx2-72.cumulus-motorcycles.com	Registered	● Online	Lab	Jul 5, 2017 8:55:26 AM	-

Ecco alcuni stati da interpretare:

Registrato Stato connettività Stato visualizzato

Sì	200	● ONLINE
Sì	NON 200	● ONLINE
Sì	N/D	● NON IN LINEA
NO	200	● NON IN LINEA
NO	NON 200	● NON IN LINEA
N/D	N/D	● ARRESTATO
N/D	N/D	● SCONOSCIUTO*

*Quando il dashboard CS non è in grado di recuperare lo stato a causa di errori o timeout.

Queste informazioni possono essere esportate anche in formato JSON/testo.

Oltre al dashboard, viene aggiunto anche un avviso RTMT:

ProblemaEsecuzionePassiServizioContesto

Questo viene attivato quando:

- Passaggi del servizio di contesto nel timeout dello script a causa di problemi di connettività con il cloud del servizio di contesto.
- Passaggi del servizio di contesto non riusciti a causa di un errore nel cloud del servizio di contesto.

Informati prima dell'aggiornamento

Coerenza delle password e impatto su LiveData

A partire dalla versione UCCX 11.6, sia LiveData che Historical Reports utilizzano la password dell'utente di reporting per impostare l'origine dati. Se le password non corrispondono tra i nodi, la creazione di report ha effetto.

Prima di eseguire l'aggiornamento, verificare che la password sia coerente tra entrambi i nodi. È possibile effettuare le seguenti verifiche:

1. Selezionare **Strumenti > Gestione password**.
2. Fare clic su **Verifica coerenza**.
3. Se non ci sono errori, sei bravo. In caso di mancata corrispondenza di coerenza, in particolare con l'utente per rapporto, aggiornare la password su entrambi i nodi.

Utenti report: impossibile accedere ai report CUIC dopo l'aggiornamento a UCCX 11.6

Cisco Unified Intelligent Center (CUIC) consente di accedere ai report in base alle autorizzazioni assegnate all'utente che accede. In base al livello di autorizzazione, all'utente viene concesso l'accesso ai report dell'agente o ai report del supervisore oppure al report completo impostato per l'amministratore dei report.

Queste autorizzazioni vengono sincronizzate da Unified Contact Center Express (UCCX) in base al ruolo assegnato all'utente su UCCX. L'utente può diventare un amministratore CUIC eseguendo il comando **utilizza cuic user make-admin CCX**

Durante il processo di aggiornamento, le autorizzazioni tra UCCX e le applicazioni CUIC vengono risincronizzate e di conseguenza i diritti di amministratore CUIC elevati concessi all'utente vengono sovrascritti. L'utente, pertanto, vede solo i report consentiti dal suo ruolo originale.

Per consentire l'accesso ai rapporti dell'utente prima dell'aggiornamento:

1. Eseguire **utils cuic user make-admin CCX\ su entrambi i nodi UCCX.**
2. Riavviare CUIC Reporting Service su entrambi i nodi UCCX.

Aumento del limite delle dimensioni degli allegati per la posta elettronica e le considerazioni su Exchange

In UCCX 11.6, i limiti relativi alle dimensioni degli allegati vengono aggiornati in base ai seguenti parametri:

- Numero massimo di allegati da parte di un agente: 10
- Dimensioni massime degli allegati totali di un agente: 20 MB
- Dimensioni massime di un singolo allegato da parte di un agente: 10 MB

Mentre la soluzione UCCX consente di aumentare le dimensioni degli allegati, il **limite delle dimensioni dei messaggi** viene aggiornato in Exchange (server di posta) in modo che gli allegati non vengano bloccati. Il limite può essere applicato in base a criteri IT a livello aziendale. Se il

server Exchange blocca il messaggio, l'agente rileva l'errore: "Impossibile rispondere all'e-mail del cliente. Fare clic su Invia per riprovare o riaccodare. Se il problema persiste, contattare l'amministratore del sistema."

Calcola le dimensioni massime dei messaggi

Dimensione del messaggio = Le dimensioni dell'e-mail includono gli allegati + codifica Base64

Codifica Base64 = circa il 33% delle dimensioni del messaggio

La formula suggerita è **Dimensione messaggio = 1.5*Dimensione dell'e-mail inclusi allegati**

Esempio: Se le dimensioni del messaggio sono di 9 MB (inclusi gli allegati), le dimensioni da impostare come limite devono essere $(9*1,5) = 14$ MB.

Dato che UCCX 11.6 consente dimensioni degli allegati fino a 20 MB, il limite per le dimensioni dei messaggi da impostare è **$1,5*20$ MB=30 MB** se si deve sfruttare questo limite più elevato sul lato della soluzione UCCX.

È possibile impostare il limite sul server Exchange eseguendo il comando:

**Set-TransportConfig -ExternalDsnMaxMessageAttachSize 30 MB -
InternalDsnMaxMessageAttachSize 30 MB -MaxReceiveSize 30 MB -MaxSendSize 30 MB**

Considerazioni importanti sull'aggiornamento

- Cancella la cache di tutti i computer agente dopo l'aggiornamento. In caso contrario, è possibile visualizzare i problemi relativi alle modifiche dello stato e ai dati in tempo reale sul desktop.
- Il layout personalizzato di Finesse Desktop non viene migrato automaticamente. Assicurarsi di inserire questa informazione e di configurare correttamente il layout dopo l'aggiornamento.
- Aggiornare le impostazioni della macchina virtuale in modo che corrispondano al modello OVA più recente per UCCX 11.6. Se si sta eseguendo una nuova installazione, utilizzare il modello OVA.
- Se si esegue l'aggiornamento durante le ore di produzione, eseguire l'aggiornamento sul nodo non principale per evitare potenziali interruzioni.
- In UCCX 11.6, la piattaforma Tomcat può essere riavviata durante l'aggiornamento. Ciò non ha alcun impatto sugli utenti, ma può generare un avviso RTMT. Ciò può essere ignorato.
- Dopo l'aggiornamento, reinstallare tutte le istanze di RTMT e Script Editor.
- Assicurarsi che dopo l'aggiornamento tutti i supervisori e gli amministratori che utilizzano Real Time Reporting Tool abbiano installato il plug-in.
- Se si dispone di integrazioni TLS, rivedere il supporto TLS e verificare di aver configurato le

versioni corrette.

- Esaminare i requisiti del browser e apportare le modifiche necessarie.
- Familiarizza con i nuovi miglioramenti di Finesse Failover e discuti con gli agenti su questo comportamento aggiornato.

Ottenere la documentazione e inviare una richiesta di assistenza

Per informazioni su come ottenere la documentazione, usare Cisco Bug Search Tool (BST), inviare una richiesta di assistenza e raccogliere ulteriori informazioni, vedere Novità della documentazione dei prodotti Cisco all'indirizzo:

<http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>.

Iscrivetevi a What's New in Cisco Product Documentation, che elenca tutta la documentazione tecnica Cisco nuova e aggiornata, come feed RSS e consegnate i contenuti direttamente al vostro desktop utilizzando un'applicazione per la lettura. I feed RSS sono un servizio gratuito.

LE SPECIFICHE E LE INFORMAZIONI RELATIVE AI PRODOTTI IN QUESTO MANUALE SONO SOGGETTE A MODIFICHE SENZA PREAVVISO. TUTTE LE AFFERMAZIONI, LE INFORMAZIONI E LE RACCOMANDAZIONI CONTENUTE NEL PRESENTE MANUALE SONO RITENUTE ACCURATE MA VENGONO PRESENTATE SENZA ALCUNA GARANZIA, ESPLICITA O IMPLICITA. GLI UTENTI DEVONO ASSUMERSI LA PIENA RESPONSABILITÀ DELL'APPLICAZIONE DI QUALSIASI PRODOTTO.

LA LICENZA SOFTWARE E LA GARANZIA LIMITATA PER IL PRODOTTO FORNITO SONO INDICATE NEL PACCHETTO INFORMATIVO FORNITO CON IL PRODOTTO E SONO QUI INCORPORATE CON QUESTO RIFERIMENTO. SE NON È POSSIBILE INDIVIDUARE LA LICENZA DEL SOFTWARE O LA GARANZIA LIMITATA, CONTATTARE IL RAPPRESENTANTE CISCO PER RICHIEDERNE UNA COPIA.

L'implementazione Cisco della compressione dell'intestazione TCP è un adattamento di un programma sviluppato dalla University of California, Berkeley (UCB) come parte della versione di dominio pubblico del sistema operativo UNIX di UCB. Tutti i diritti sono riservati. Copyright © 1981, Regents of the University of California.

INDIPENDENTEMENTE DA QUALSIASI ALTRA GARANZIA, TUTTI I FILE DI DOCUMENTAZIONE E IL SOFTWARE DI QUESTI FORNITORI VENGONO FORNITI "COSÌ COME SONO" CON TUTTI I DIFETTI. CISCO E I SUDDETTI FORNITORI NON RICONOSCONO ALCUNA GARANZIA, ESPRESSA O IMPLICITA, INCLUSE, SENZA LIMITAZIONI, QUELLE DI COMMERCIALIZZABILITÀ, IDONEITÀ PER UNO SCOPO SPECIFICO E NON VIOLAZIONE DI DIRITTI O DERIVANTI DA TRATTATIVE, USI O PRATICHE COMMERCIALI.

IN NESSUN CASO CISCO O I SUOI FORNITORI SARANNO RITENUTI RESPONSABILI PER DANNI INDIRETTI, SPECIALI, CONSEGUENZIALI O ACCIDENTALI, INCLUSI, SENZA ALCUNA LIMITAZIONE, PERDITA DI PROFITTI O PERDITA O DANNO AI DATI DERIVANTE DALL'UTILIZZO O DALL'IMPOSSIBILITÀ DI UTILIZZARE IL PRESENTE MANUALE, ANCHE SE CISCO O I SUOI FORNITORI SONO STATI AVVERTITI DELLA POSSIBILITÀ DI TALI DANNI.

Gli indirizzi IP (Internet Protocol) e i numeri di telefono utilizzati in questo documento non devono essere considerati indirizzi e numeri di telefono effettivi. Tutti gli esempi, l'output del comando

display, i diagrammi della topologia di rete e altre figure incluse nel documento sono mostrati solo a scopo illustrativo. L'utilizzo di indirizzi IP o numeri di telefono effettivi in contenuti illustrativi è involontario e casuale.

Tutte le copie stampate e le copie software duplicate sono considerate copie non controllate e per l'ultima versione è necessario fare riferimento alla versione online originale.

Cisco ha più di 200 uffici in tutto il mondo. Gli indirizzi, i numeri di telefono e di fax sono elencati nel sito Web Cisco all'indirizzo www.cisco.com/go/offices.

Cisco e il logo Cisco sono marchi o marchi registrati di Cisco e/o dei relativi affiliati negli Stati Uniti e in altri paesi. Per visualizzare un elenco di marchi Cisco, vai al seguente URL: www.cisco.com/go/trademarks. I marchi commerciali di terze parti citati sono proprietà dei rispettivi titolari. L'uso del termine "partner" non implica una relazione di partnership tra Cisco e altre aziende. (1110R)

©2016 Cisco Systems, Inc. Tutti i diritti riservati.