Användarhandbok för IM and Presence Service on Cisco Unified Communications Manager, Release 9.0(1)

Först publicerad: May 25, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

SPECIFIKATIONERNA OCH INFORMATIONEN SOM GÄLLER PRODUKTERNA I DEN HÄR BRUKSANVISNINGEN KAN ÄNDRAS UTAN FÖRVARNING. ALLA UTTALANDEN, ALL INFORMATION OCH ALLA REKOMMENDATIONER I DEN HÄR BRUKSANVISNINGEN ANSES VARA KORREKTA MEN PRESENTERAS UTAN GARANTI AV NÅGOT SLAG, VARE SIG UTTRYCKT ELLER UNDERFÖRSTÅDD. ANVÄNDARE MÅSTE TA FULLT ANSVAR FÖR SIN ANVÄNDNING AV ALLA PRODUKTER.

PROGRAMVARULICENSEN OCH DEN BEGRÄNSADE GARANTIN FÖR DEN MEDFÖLJANDE PRODUKTEN FINNS I DET INFORMATIONSPAKET SOM LEVERERADES TILLSAMMANS MED PRODUKTEN OCH INKLUDERAS HÄRI SOM REFERENS. KONTAKTA DIN CISCO-REPRESENTANT FÖR ATT FÅ ETT EXEMPLAR OM DU INTE HITTAR PROGRAMVARULICENSEN ELLER DEN BEGRÄNSADE GARANTIN.

Ciscos implementering av komprimering av TCP-huvud är en anpassning av ett program som har utvecklats av University of California, Berkeley (UCB), USAS, som en del av UCB:s offentliga domänversion av operativsystemet UNIX. Med ensamrätt. Copyright © 1981, Regents of the University of California.

OAKTAT ALLA ANDRA GARANTIER HÄRI, TILLHANDAHÅLLS ALLA DOKUMENTFILER OCH PROGRAMVARA FRÅN DESSA LEVERANTÖRER "I BEFINTLIGT SKICK" MED ALLA FEL. CISCO OCH OVANNÄMNDA LEVERANTÖRER FRÅNSÄGER SIG ALLA GARANTIER, UTTRYCKLIGA ELLER UNDERFÖRSTÅDDA, INKLUSIVE, UTAN BEGRÄNSNING, GARANTIER GÄLLANDE SÄLJBARHET, LÄMPLIGHET FÖR ETT VISST ÄNDAMÅL OCH ICKE-INTRÅNG, ELLER EVENTUELLA GARANTIER SOM UPPSTÅR FRÅN HANTERING, ANVÄNDNING ELLER HANDELSPRAXIS.

CISCO ELLER DESS LEVERANTÖRER SKALL UNDER INGA OMSTÄNDIGHETER VARA ANSVARIGA FÖR INDIREKTA ELLER SPECIELLA SKADOR ELLER FÖLJDSKADOR ELLER TILLFÄLLIGA SKADOR, INKLUSIVE, UTAN BEGRÄNSNING, VINSTFÖRLUSTER ELLER FÖRLUST AV ELLER SKADA I DATA SOM UPPSTÅR FRÅN ANVÄNDNINGEN ELLER OFÖRMÅGAN ATT ANVÄNDA DENNA BRUKSANVISNING, ÄVEN OM CISCO ELLER DESS UNDERLEVERANTÖRER HAR BLIVIT UNDERRÄTTADE OM ATT DET FINNS RISK FÖR SÅDANA SKADOR.

Cisco och Ciscos logotyp är varumärken som ägs av Cisco Systems, Inc. och/eller dess dotterbolag i USA och andra länder. En lista över Cisco:s varumärken finns på den här webbadressen: http://www.cisco.com/go/trademarks. Tredje parts varumärken tillhör sina respektive ägare. Att ordet partner används innebär inte att det föreligger ett partnersamarbete mellan Cisco och ett annat företag. (1110R)

Inga IP-adresser som används i detta dokument är avsedda att vara verkliga adresser. Alla exempel, kommandoutdata som visas och bilder som ingår i dokumentet är endast avsedda för illustration. All användning av verkliga IP-adresser i illustrationssammanhang är oavsiktlig och slumpmässig.

SPECIFIKATIONERNA OCH INFORMATIONEN SOM GÄLLER PRODUKTERNA I DEN HÄR BRUKSANVISNINGEN KAN ÄNDRAS UTAN FÖRVARNING. ALLA UTTALANDEN, ALL INFORMATION OCH ALLA REKOMMENDATIONER I DEN HÄR BRUKSANVISNINGEN ANSES VARA KORREKTA MEN PRESENTERAS UTAN GARANTI AV NÅGOT SLAG, VARE SIG UTTRYCKT ELLER UNDERFÖRSTÅDD. ANVÄNDARE MÅSTE TA FULLT ANSVAR FÖR SIN ANVÄNDNING AV ALLA PRODUKTER.

PROGRAMVARULICENSEN OCH DEN BEGRÄNSADE GARANTIN FÖR DEN MEDFÖLJANDE PRODUKTEN FINNS I DET INFORMATIONSPAKET SOM LEVERERADES TILLSAMMANS MED PRODUKTEN OCH INKLUDERAS HÄRI SOM REFERENS. KONTAKTA DIN CISCO-REPRESENTANT FÖR ATT FÅ ETT EXEMPLAR OM DU INTE HITTAR PROGRAMVARULICENSEN ELLER DEN BEGRÄNSADE GARANTIN.

Ciscos implementering av komprimering av TCP-huvud är en anpassning av ett program som har utvecklats av University of California, Berkeley (UCB), USAS, som en del av UCB:s offentliga domänversion av operativsystemet UNIX. Med ensamrätt. Copyright © 1981, Regents of the University of California.

OAKTAT ALLA ANDRA GARANTIER HÄRI, TILLHANDAHÅLLS ALLA DOKUMENTFILER OCH PROGRAMVARA FRÅN DESSA LEVERANTÖRER "I BEFINTLIGT SKICK" MED ALLA FEL. CISCO OCH OVANNÄMNDA LEVERANTÖRER FRÅNSÄGER SIG ALLA GARANTIER, UTTRYCKLIGA ELLER UNDERFÖRSTÅDDA, INKLUSIVE, UTAN BEGRÄNSNING, GARANTIER GÄLLANDE SÄLJBARHET, LÄMPLIGHET FÖR ETT VISST ÄNDAMÅL OCH ICKE-INTRÅNG, ELLER EVENTUELLA GARANTIER SOM UPPSTÅR FRÅN HANTERING, ANVÄNDNING ELLER HANDELSPRAXIS.

CISCO ELLER DESS LEVERANTÖRER SKALL UNDER INGA OMSTÄNDIGHETER VARA ANSVARIGA FÖR INDIREKTA ELLER SPECIELLA SKADOR ELLER FÖLJDSKADOR ELLER TILLFÄLLIGA SKADOR, INKLUSIVE, UTAN BEGRÄNSNING, VINSTFÖRLUSTER ELLER FÖRLUST AV ELLER SKADA I DATA SOM UPPSTÅR FRÅN ANVÄNDNINGEN ELLER OFÖRMÅGAN ATT ANVÄNDA DENNA BRUKSANVISNING, ÄVEN OM CISCO ELLER DESS UNDERLEVERANTÖRER HAR BLIVIT UNDERRÄTTADE OM ATT DET FINNS RISK FÖR SÅDANA SKADOR.

Cisco och Ciscos logotyp är varumärken som ägs av Cisco Systems, Inc. och/eller dess dotterbolag i USA och andra länder. En lista över Cisco:s varumärken finns på den här webbadressen: http://www.cisco.com/go/trademarks. Tredje parts varumärken tillhör sina respektive ägare. Att ordet partner används innebär inte att det föreligger ett partnersamarbete mellan Cisco och ett annat företag. (1110R)

Inga IP-adresser som används i detta dokument är avsedda att vara verkliga adresser. Alla exempel, kommandoutdata som visas och bilder som ingår i dokumentet är endast avsedda för illustration. All användning av verkliga IP-adresser i illustrationssammanhang är oavsiktlig och slumpmässig.

INNEHÅLL

KAPITEL 1

Komma igång med Cisco Unified CM IM and Presense-gränssnittet Användaralternativ

Webbläsare som stöds

Cisco Unified CM IM and Presence-gränssnittet Användaralternativ stöder följande webbläsare:

- Microsoft Internet Explorer 6
- Microsoft Internet Explorer 7
- Microsoft Internet Explorer 8
- Firefox 3.x

Obs! Cisco Unified Presence stöder för närvarande inte Safari eller Google Chrome.

Relaterade ämnen

Logga in i Cisco Unified CM IM and Presence-användaralternativ, på sidan 1

Logga in i Cisco Unified CM IM and Presence-användaralternativ

Innan du börjar

Du använder Cisco Unified CM IM and Presence-gränssnittet Användaralternativ för att anpassa inställningar, skapa personliga svarsmeddelanden och ordna kontakter.

- För att kunna logga in i Cisco Unified CM IM and Presence-gränssnittet Användaralternativ måste administratören ha tilldelat användaren till gruppen för standard-CCM-slutanvändare.
- Be systemadministratören om följande information:
  - En URL-adress för Cisco Unified CM IM and Presence-användaralternativ.
  - Ditt användarnamn och lösenord för Cisco Unified CM IM and Presence-användaralternativ.
- Se till att du använder en webbläsare som stöds.

Procedur

Steg 1 Öppna en webbläsare som stöds på datorn.

Steg 2 Ange URL-adressen för Cisco Unified CM IM and Presence-användaralternativ enligt följande exempel: http://<*IM and Presence-server*>/cupuser.

Steg 3 Ange ditt användarnamn för Cisco Unified CM IM and Presence-användaralternativ.

Steg 4 Ange det lösenord för Cisco Unified CM IM and Presence-användaralternativ som du har fått från systemadministratören.

Steg 5 Välj **Logga in.**
Om du vill logga ut från gränssnittet Användaralternativ väljer du **Logga ut** i det övre högra hörnet i fönstret Användaralternativ. Av säkerhetsskäl loggas du automatiskt ut från Användaralternativ efter trettio minuters inaktivitet.

Relaterade ämnen

Webbläsare som stöds, på sidan 1

KAPITEL 2

Ställa in sekretesspolicyer

Ange standardsekretesspolicy

Med sekretesspolicyer kan du fastställa vilka användare som kan se din tillgänglighetsstatus och skicka snabbmeddelanden till dig. Den här versionen av IM and Presence stöder regeln för kontaktlistor, som gör att vem som helst i din kontaktlista (som övervakas av dig) kan se din tillgänglighetsstatus som standard *förutsatt* att du inte uttryckligen nekar personen tillåtelse att se din status.

Därför kan du använda sekretesspolicyer för att tillåta och blockera användare och domäner. Nedanstående alternativ gör det möjligt att konfigurera sekretesspolicyer som en standardinställning på organisationsnivå eller specifikt för enskilda användare.

- Tillåt – Användare/domäner kan se din tillgänglighetsstatus och skicka snabbmeddelanden till dig som standard, förutsatt att du inte uttryckligen lägger till användaren/domänen till listan över blockerade kontakter. Du kan bara ange sekretesspolicyn Tillåt för interna användare och domäner. Alternativet är *inte* tillgängligt för externa (federerade) användare/domäner.
- Blockera – Användare/domäner som du blockerar kan inte se din tillgänglighet och kan inte skicka snabbmeddelanden till dig. Användare som du blockerar ser alltid din status som Ej tillgänglig. Du kan ange sekretesspolicyn Blockera för interna och externa (federerade) användare och domäner.
- Fråga mig – Sekretesspolicyn Fråga mig uppmanar användare (via en förfrågan) att uttryckligen blockera eller tillåta utbyte av tillgänglighetsstatus och snabbmeddelanden från specifika användare/domäner. Klientprogrammet uppmanar användaren att godkänna eller avvisa prenumerationen. Sekretesspolicyn Fråga mig kan bara anges för externa (federerade) användare och domäner, och bara om den externa kontakten eller domänen *inte* med på användarens lista över tillåtna eller blockerade kontakter.

Procedur

Steg 1 Välj **Användaralternativ > Sekretesspolicyer**.

Steg 2 Välj ett av dessa alternativ:

Om du vill...	Gör så här
Tillåta att alla interna användare kan se din tillgänglighet och skicka snabbmeddelanden till dig (förutom de interna användare/domäner som du uttryckligen lägger in i undantagslistan för blockerade kontakter). **Obs!** Mer information finns i inställningen för undantag till policyn i avsnittet Felsökningstips i det här ämnet. Den här policyn tillåter inte att externa användare ser din tillgänglighet.	**1** Välj **Tillåt** i listrutan Interna användare (i ditt företag/din organisation) . **2** (Valfritt) Lägg till interna användare till din undantagslista för blockerade kontakter enligt den metod som beskrivs i denna modul. Se Hur du går vidare.
Blockera alla interna användare från att se din tillgänglighet och skicka snabbmeddelanden till dig (förutom de interna användare som du uttryckligen lägger in i undantagslistan för tillåtna kontakter). **Obs!** Den här policyn blockerar inte externa användare från att se din tillgänglighet.	**1** Välj **Blockera** i listrutan Interna användare (i ditt företag/din organisation) . **2** (Valfritt) Lägg till interna användare till din undantagslista för tillåtna kontakter enligt den metod som beskrivs i denna modul. Se Hur du går vidare.
Blockera alla externa användare från att se din tillgänglighet och skicka snabbmeddelanden till dig (förutom de externa användare som du uttryckligen lägger in i undantagslistan för tillåtna kontakter). **Obs!** Den här policyn blockerar inte interna användare från att se din tillgänglighet.	**1** Välj **Blockera** i listrutan Externa användare (alla övriga). **2** (Valfritt) Lägg till externa användare till din undantagslista för tillåtna kontakter enligt den metod som beskrivs i denna modul. Se Hur du går vidare.
Uppmana alla användare (med en Fråga mig-förfrågan) att ange en egen Tillåt-/Blockera-policy för externa användare (förutom de externa användare som du uttryckligen lägger in i undantagslistan för tillåtna/blockerade kontakter). **Obs!** Den här policyn blockerar inte interna användare från att se din tillgänglighet.	**1** Välj **Fråga mig** i listrutan Externa användare (alla övriga). **2** (Valfritt) Lägg till externa användare till din undagslista för tillåtna/blockerade kontakter enligt den metod som beskrivs i denna modul. Se Hur du går vidare.

Steg 3 Välj **Spara standardinställningar**.

Felsökningstips

IM and Presence-servern godkänner automatiskt att en användare som finns med på en annan användares kontaktlista visar den senares tillgänglighetsstatus. Observera följande undantag till policyinställningen *Tillåt alla interna användare*: Om du stänger *av* automatiskt godkännande på IM and Presence-servern och standardinställningen för både den globala och lokala domänen har ställts in på Tillåt, uppmanas användaren att antingen godkänna eller avvisa prenumerationsförfrågan. Så ser Fråga mig-scenariot ut för den lokala

domänen. Mer information om inställningen av automatiskt godkännande på IM and Presence finns i *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager* (på Cisco.com).

Vad du gör sedan

- Om du vill åsidosätta standardsekretesspolicyn Tillåt/Blockera som har ställts in för interna/externa användare på organisationsnivå kan du läsa mer i avsnitten som följer. Där beskrivs hur du konfigurerar undantagslistor för användare.

Lägga till interna användare till dina undantagslistor för tillåtna eller blockerade kontakter

Den här proceduren gör att du kan hantera undantagen till den allmänna sekretesspolicyn med hjälp av listor över tillåtna och blockerade kontakter. Beroende på vilken standardsekretesspolicy du har angett på organisationsnivå är antingen listan över tillåtna eller listan över blockerade kontakter tillgänglig för redigering. På så sätt kan du åsidosätta standardpolicyreglerna för att lägga till specifika personer inom organisationen till din lista över tillåtna eller blockerade kontakter.

- När du anger policyn Tillåt för specifika användare kan de se din tillgänglighet och skicka snabbmeddelanden till dig, även om de blockeras av den allmänna policyn.
- Om du anger policyn Blockera för specifika användare förhindras de att visa din status och att skicka snabbmeddelanden till dig när de använder Cisco-klienter (Cisco Jabber version 8) – trots att den allmänna policyn tillåter det. Användare i kontaktlistan är alltid tillåtna såvida de inte uttryckligen har blockerats i undantagslistan. Observera att vissa XMPP-klienter från tredje part ändå kan skicka och ta emot snabbmeddelanden, oavsett vilken policy du anger.

Innan du börjar

Ange din standardsekretesspolicy.

Procedur

Steg 1 Välj **Användaralternativ > Sekretesspolicyer**.

Steg 2 Välj **Lägg till användare** i ramen för användarinställningar i fönstret Sekretesspolicy.

Steg 3 Utför någon av dessa åtgärder:

- Välj **Tillåt** för att tillåta användaren att se din tillgänglighet.
- Välj **Blockera** för att blockera användaren från att se din tillgänglighet.

Steg 4 Ange ett giltigt användar-ID för den interna användaren. Detta användar-ID måste finnas i ditt interna nätverk och ha formatet <*användarid@domän*>.

Steg 5 Välj **Lokal domän**.

Steg 6 Välj **Lägg till** för att lägga till den interna användaren till den lokala domänen.

Felsökningstips

- Federerade användare kan lägga till en lokal användare med hjälp av ett e-post-ID eller ett standard-JID. Valet beror på om administratören har aktiverat eller inaktiverat e-post-ID:t för domänen.
- När du har **lagt till** en användare till din lista över tillåtna/blockerade kontakter visas informationen i tabellen i det här fönstret. Om du vill ta bort en användare från någon av listorna Tillåt/Blockera, markerar du kryssrutan för användaren och väljer sedan **Ta bort markerade**.

Lägga till externa användare till dina undantagslistor för tillåtna eller blockerade kontakter

Den här proceduren gör att du kan hantera undantagen till den allmänna sekretesspolicyn med hjälp av listor över tillåtna och blockerade kontakter. Beroende på vilken standardsekretesspolicy du har angett på organisationsnivå är antingen listan över tillåtna eller listan över blockerade kontakter tillgänglig för redigering. På så sätt kan du åsidosätta standardpolicyreglerna för att lägga till specifika personer utanför organisationen till din lista över tillåtna eller blockerade kontakter.

- När du anger policyn Tillåt för specifika användare kan de se din tillgänglighet och skicka snabbmeddelanden till dig, även om de blockeras av den allmänna policyn.
- Om du anger policyn Blockera för specifika användare förhindras dessa användare att se din tillgänglighet och att skicka snabbmeddelanden till dig, trots att den allmänna policyn tillåter det (genom ett positivt svar på en Fråga mig-förfrågan).

Innan du börjar

Ange din standardsekretesspolicy.

Procedur

Steg 1 Välj **Användaralternativ > Sekretesspolicyer**.

Steg 2 Välj **Lägg till användare** i ramen för användarinställningar i fönstret Sekretesspolicy.

Steg 3 Utför någon av dessa åtgärder:

- Välj **Tillåt** för att tillåta användaren att se din tillgänglighet.
- Välj **Blockera** för att blockera användaren från att se din tillgänglighet.

Steg 4 Ange ett giltigt användar-ID för den interna användaren. Detta användar-ID måste finnas i ditt interna nätverk och ha formatet <*användarid@domän*>.

Steg 5 Markera någon av följande domäner som användaren tillhör:

- **Federerad domän**.
- **Anpassad domän** – en anpassad domän är en extern domän som inte finns med på listan över federerade domäner.

Steg 6 Utför någon av dessa åtgärder:

Om du har valt...	Gör du så här:
Federerad domän	Markera domänen som du ska ansluta dig till i listrutan.
Anpassad domän	Ange användarens domän. **Obs!** Ett exempel på en anpassad domän är "mittföretag.com".

Steg 7 Välj **Lägg till**.

Felsökningstips

När du har **lagt till** en användare till din lista över tillåtna/blockerade kontakter visas informationen i tabellen i det här fönstret. Om du vill ta bort en användare från någon av listorna Tillåt/Blockera, markerar du kryssrutan för användaren och väljer sedan **Ta bort markerade**.

Lägga till externa domäner till dina undantagslistor för tillåtna eller blockerade kontakter

Innan du börjar

Du kan tillåta eller blockera en hel extern domän. Om du blockerar en extern domän blockeras alla förfrågningar från att se din tillgänglighet från användare på den domänen, om du inte har lagt till de externa användarna till din lista över tillåtna kontakter.

Procedur

Steg 1 Välj **Användaralternativ > Sekretesspolicyer**.

Steg 2 Välj **Lägg till domän** i ramen för användarinställningar i fönstret Sekretesspolicy.

Steg 3 Utför någon av dessa åtgärder:

- Välj **Tillåt** för att tillåta användaren att se din tillgänglighet.
- Välj **Blockera** för att blockera användaren från att se din tillgänglighet.

Steg 4 Välj att tillåta eller blockera någon av dessa domäner:

- **Federerad domän**
- **Anpassad domän** – en anpassad domän är en extern domän som inte finns med på listan över federerade domäner.

Steg 5 Utför någon av dessa åtgärder:

Om du har valt...	Gör du så här:
Federerad domän	Markera domänen som du ska ansluta dig till i listrutan.

Om du har valt...	Gör du så här:
Anpassad domän	Ange användarens domän. **Obs!** Ett exempel på en anpassad domän är "mittföretag.com".

Steg 6 Välj **Lägg till**.

Felsökningstips

När du har **lagt till** en domän till din lista över tillåtna/blockerade kontakter visas informationen i tabellen i det här fönstret. Om du vill ta bort en domän från någon av listorna Tillåt/Blockera, markerar du kryssrutan för domänen och väljer sedan **Ta bort markerade**.

KAPITEL 3

Ordna kontaktlistan

Lägga till kontakter till kontaktlistan

Innan du börjar

- Systemadministratören ställer in hur många kontakter som kan finnas i listan. Maxantalet är 100. Kontakta systemadministratören om du vill veta begränsningen för din telefon.
- Du kan lägga till en extern kontakt genom att antingen välja en extern domän eller konfigurera en egen domän för användare som finns utanför din organisation.
- Interna och externa användare i kontaktlistan utgör undantag från policyerna för interna och externa kontakter. Användare i kontaktlistan är alltid tillåtna såvida de inte uttryckligen har blockerats i undantagslistan.
- I din applikation för snabbmeddelanden kan du lägga till kontakter vars tillgänglighetsstatus inte är synlig för dig, till exempel till personer som du bara vill ringa till från listan i applikationen. Denna typ av kontakter visas inte i kontaktlistan i gränssnittet **Användaralternativ**.
- Om du gör ändringar i kontaktlistan (lägger till/tar bort/ändrar) syns ändringarna automatiskt på Cisco-klienter (för alla inloggade användare).

Procedur

Steg 1 Välj **Användaralternativ > Kontakter**.

Steg 2 Välj **Lägg till ny**.

Steg 3 Välj ett av dessa alternativ:

Om kontakten som du vill lägga till är...	Gör du så här:
Intern – en användare som hör till din lokala domän (oftast ditt företag eller din organisation)	**1** Lägg till användar-ID för den federerade kontakt som du vill lägga till i fältet Kontakt. **2** Välj **Välj från domänlistan** **3** Välj en intern (lokal) domän från menyn Domän. **4** Du kan också ange ett alternativt namn för användaren om du vill att ett smeknamn ska visas på användarens dator. **Obs!** Du kan inte lägga till användare/domäner som redan har blockerats av administratören. Organisationens sekretesspolicy måste vara inställd så att den interna domänen eller specifika användare från denna domän kan se din tillgänglighetsstatus och skicka snabbmeddelanden till dig.
Extern – en användare som inte hör till din lokala domän (oftast ditt företag eller din organisation)	Utför en av följande åtgärder: **1** Lägg till användar-ID för den federerade kontakt som du vill lägga till i fältet Kontakt. **2** Välj **Välj från domänlistan.** • Välj en extern domän från menyn Domän. **3** Välj **Ange anpassad domän.** • Ange den anpassade domänen för de kontakter som finns utanför din organisation. **Obs!** Du kan inte lägga till användare/domäner som redan har blockerats av administratören. Organisationens sekretesspolicy måste vara inställd så att du tillfrågas (i ett popup-fönster) om du vill tillåta att den externa domänen eller specifika användare från denna domän kan se din tillgänglighetsstatus och skicka snabbmeddelanden till dig.

Steg 4 (Valfritt) Ange ett alternativt namn (smeknamn) för kontakten.

Steg 5 Välj **Spara**.

Felsökningstips

Du kan endast ha ett alternativt namn (smeknamn) per kontakt. Om du frivilligt anger ett alternativt namn för en kontakt, visas det på Cisco-klienter men inte nödvändigtvis på XMPP-klienter från tredje part. Om du

uppdaterar namnet på en kontakt uppdateras detta namnbyte i kontaktlistan på Cisco Jabber och i alla dina kontaktgrupper.

Ta bort kontakter från kontaktlistan

Procedur

Steg 1 Välj **Användaralternativ** > **Kontakter**.

Steg 2 Välj Sök.

Steg 3 Utför någon av dessa åtgärder:

Om du vill...	Gör du så här:
Ta bort alla kontakter	Välj **Markera alla.**
Ta bort markerade kontakter	Markera kryssrutan bredvid namnet på den kontakt som du vill ta bort.

Steg 4 Välj **Ta bort markerade**.

Steg 5 Välj **OK**.

Felsökningstips

Det kan dröja en stund innan en kontakt tas bort, eftersom åtgärden kräver bearbetning av databasen. Ett meddelande med följande text visas i gränssnittet: "En tidigare uppdatering av kontaktlistan har inte börjat gälla än. Den ligger i kö och bearbetas snart." Om du uppdaterar sidan visas den uppdaterade kontaktlistan.

Visa kontaktlistan

Procedur

Steg 1 Välj **Användaralternativ > Kontakter**.

Steg 2 Välj **Sök**.

Konfigurera uppdateringstimer för kontaktlistan

Du kan ändra hur ofta du vill att kontaktlistan ska uppdateras på din telefon.

Procedur

Steg 1 Välj **Användaralternativ > Inställningar**.

Steg 2 Ange ett värde (i sekunder) mellan 7 och 3 600 i fältet **Telefonskärmens uppdateringsintervall**. Standardvärdet är 30 sekunder.

Steg 3 Välj **Spara**.

KAPITEL 4

Felsökning av Cisco Unified CM IM and Presence-gränssnittet Användaralternativ

Jag kan inte logga in på gränssnittet Användaralternativ

Problem Jag kommer åt rätt webbsida för **Användaralternativ**, men kan inte logga in med mitt användarnamn och lösenord.

Lösning Kontakta systemadministratören för att kontrollera att du använder rätt länk till webbsidorna för **Användaralternativ** och att du anger korrekt användarnamn och lösenord. Kontrollera också att du är registrerad som en licensierad användare och att du har behörighet till webbsidorna för **Användaralternativ**.

Jag loggades ut automatiskt från gränssnittet Användaralternativ

Problem Jag måste ange mitt användarnamn och lösenord för Användaralternativ igen för att få åtkomst till gränssnittet Användaralternativ.

Lösning För ökad säkerhet loggas du automatiskt ut från webbsidorna Användaralternativ efter trettio minuters inaktivitet.

Jag loggades ut automatiskt från gränssnittet Användaralternativ

KAPITEL 5

Få åtkomst till alternativen för tillgänglighet

Få åtkomst till ikonerna i fönstret

Cisco Unified CM IM and Presence-användaralternativ erbjuder funktioner som gör att du kan få åtkomst till ikoner i fönstret utan att behöva använda musen. Du kan utföra denna åtgärd från vilken plats som helst i fönstret, så du behöver inte bläddra eller förflytta dig genom olika fält.

Många fönster i IM and Presence har ikoner som visas längst upp i fönstret, till exempel en ikon med en skiva för Spara eller en ikon med ett plustecken (+) för Lägg till.

Procedur

Steg 1 Tryck på Alt, tryck på 1 och tryck sedan på Tab.

Steg 2 Markören markerar den första ikonen från vänster. Tryck på Tab igen för att flytta till nästa ikon.

Steg 3 Tryck på Retur för att utföra ikonens funktion.

Få åtkomst till knapparna i fönstret

Cisco Unified CM IM and Presence-användaralternativ erbjuder funktioner som gör att du kan få åtkomst till ikoner i fönstret utan att behöva använda musen. Du kan utföra denna åtgärd från vilken plats som helst i fönstret, så du behöver inte bläddra eller förflytta dig genom olika fält.

Många av fönstren i IM and Presence har knappar som visas längst ned i fönstret, till exempel en knapp för Spara eller en knapp för Lägg till.

Procedur

Steg 1 Tryck på Alt, tryck på 2 och tryck sedan på Tab.

Steg 2 Markören markerar den första knappen från vänster. Tryck på Tab igen för att flytta till nästa knapp.

Steg 3 Tryck på Retur för att utföra knappens funktion.