FirstClass NewsLetter NUMERO 1/2005

Benvenuto

Le news

Applicazioni e approfondimenti

Le migliori "buone pratiche" e alcuni aggiornamenti tecnici su FirstClass

Le domande più frequenti

In questa rubrica i quesiti degli utenti FirstClass

Nel prossimo numero

Alcune anticipazioni

Contattaci

Benvenuto

Abbiamo il piacere di annunciarvi che nasce oggi la newsletter italiana di FirstClass, uno spazio d'informazione dove non solo si potranno trovare le novità che riguardano il mondo di FirstClass, ma anche suggerimenti utili per utilizzare al meglio questo ambiente.

La newsletter verrà inviata periodicamente dalla nostra redazione e si potrà trovare anche all'interno del nostro sito http://www.neol.it.

L'obiettivo è di segnalare nuove possibilità d'utilizzo del software e supportare gli amministratori FirstClass con informazioni e dettagli utili alla gestione del server, il tutto affiancato a case study e novità che il mondo FirstClass mette a disposizione dell'utente finale.

Potrete anche voi inviarci suggerimenti, domande, commenti e segnalazioni sulle vostre esperienze all'indirizzo email redazione@neol.it, all'attenzione dei responsabili della redazione Daniele Lincetto e Serena Schiaffini.

Sperando che questo nuovo strumento di comunicazione, pensato apposta per diffondere la conoscenza dell'ambiente FirstClass, possa esservi utile, auguriamo a tutti una buona lettura ed un arrivederci alla prossima!

NEOL SRL

Le news

Una nuova politica di distribuzione per il mercato italiano

Nel corso del 2004 la distribuzione di FirstClass sul mercato italiano è mutata. Invece di basarsi sulla presenza di un proprio responsabile commerciale, OpenText ha ritenuto opportuno indirizzarsi verso la collaborazione con una struttura mirata ad una politica di marketing e coordinamento a livello nazionale.

La scelta del partner si è quindi indirizzata verso la nostra società, NEOL srl, da diversi anni impegnata nel campo della diffusione del software FirstClass. Costituita nell'aprile del 2004, NEOL srl prosegue, infatti, l'attività della precedente società Gaia srl, già utilizzatrice e promotrice del software FirstClass.

FirstClass, conosciuto e largamente utilizzato sia a livello internazionale che nazionale da Scuole ed Università, si è dimostrato anche un ottimo prodotto per l'implementazione di intranet di comunicazione e collaborazione a livello aziendale. Oggi, le nuove funzionalità legate all'amministrazione ed alla sicurezza lo rendono ancor più competitivo.

FirstClass, per scalabilità, limitati costi di esercizio e flessibilità, oltre che per le numerose funzionalità immediatamente disponibili nella versione base, può essere apprezzato come una effettiva alternativa a prodotti di collaborazione e comunicazione ben più blasonati, quali Lotus Domino o Microsoft Exchange.

Per ora, sul mercato italiano, verrà commercializzato l'ambiente collaborativo (Core Server e Application Server) ed i servizi internet (l'interfacciamento con tutti i protocolli internet), mentre il più sofisticato ambiente di unified messaging che gestisce le interfacce vocali (Voices Services) verrà riservato ad utenti con particolari esigenze e richieste.

Tra gli obiettivi di NEOL srl come distributore vi è quindi quello di far conoscere FirstClass valorizzandolo e ponendo particolare attenzione a quelle caratteristiche che lo contraddistinguono dalla concorrenza.

FirstClass certificato da H3G per il servizio mobile UMTS

Il 2004 ha segnato l'avvio in grande stile dei servizi basati sulla terza generazione di cellulari, il cosidetto UMTS. Rispetto allo standard per la trasmissione dati della precedente generazione, il GPRS, la caratteristica di questa nuova modalità di comunicazione è quella di riuscire a garantire una buona qualità ed una elevata velocità nella trasmissione dati.

La velocità di cui si può disporre nell'accedere ad internet tramite UMTS si avvicina a quella di una connessione ADSL. In situazione ottimale, una connessione ad internet tramite UMTS può raggiungere fino a 380 kbps. Questa carateristica ha permesso di realizzare servizi innovativi, a livello di massa, quali la videocomunicazione o l'accesso ad internet in mobilità.

Curiosi di testare il funzionamento di FirstClass con accesso internet/UMTS, nell'estate scorsa i nostri responsabili hanno contattato il principale fornitore di servizi UMTS in Italia, la società H3G "3", per verificare nella pratica l'adattabilità e l'efficienza di FirstClass in un ambiente nuovo, quale quello dato dalle connessioni internet tramite UMTS.

Queste, se da un lato sono caratterizzate da una buona velocità, dall'altro sono soggette ad una forte variabilità di banda, anche nell'arco di pochi secondi o minuti, richiedendo pertanto da parte del software applicativo una particolare flessibilità e capacità di adattamento.

I test sono stati effettuati con l'accesso ad internet in tre modalità:
a) usando il telefonino UMTS come modem, da un PC o Mac con client FirstClass
b) utilizzando la data card 3, da PC, tramite client FirstClass
c) accedendo a FirstClass attraverso l'interfaccia mobile con i palmari Motorola A925 e A1000, e il browser interno

La sperimentazione ha avuto un successo significativo, permettendo, soprattutto tramite UMTS e client FirstClass, di ricreare un ambiente di lavoro completamente simile a quello di una connessione fissa via ADSL.

L'adattabilità del client FirstClass ha permesso di utilizzare la connessione per ore intere di lavoro senza avvertire praticamente alcun svantaggio per l'operatività spicciola nell'uso di FirstClass e dei suoi diversi servizi, tipo chat, calendari, accesso a documenti condivisi etc. Molto efficiente anche l'accesso tramite la modalità browser con i palmari di nuova generazione Motorola. Particolarmente efficace la connessione di accesso ad internet tramite datacard dal client FirstClass. L'ottimizzazione del client nella trasmissione dati ha permesso di mantenere aperte sessioni di lavoro per ore intere sul server FirstClass, riducendo al minimo il traffico.

L'esperienza si è conclusa con una forte soddisfazione da parte di H3G che ha ritenuto di consigliare FirstClass quale applicativo a forte valore aggiunto per gli utenti business dei propri servizi UMTS.

Chi volesse verificare l'interfaccia mobile di FirstClass può collegarsi con il browser alla pagina http://mobile.neol.it/login ed accedere con nome utente

"demo" e password "palm", mentre, per collegarsi con lo stesso utente in modalità client, va indicato alla voce server il nome "fc.neol.it."

Il nostro staff è disponibile ad offrire maggiori informazioni per chi volesse attivare l'interfaccia mobile su server FirstClass ed utilizzare la nuova tecnologia di connessione UMTS abbinata a FirstClass.

La Rete Civica Milanese conferma la scelta di FirstClass

Con l'occasione dataci dall'uscita di questa prima newsletter siamo lieti di annunciare che La Rete Civica di Milano, ancora una volta, conferma la scelta di FirstClass quale software di riferimento per la gestione della community dei cittadini milanesi... e non solo!

RCM è una tra le più grosse realtà di collaborazione on line, per numero di utenti, attivate in Italia. E' un ambiente dove trovare informazioni, notizie, discussioni e servizi per i cittadini, le associazioni, gli enti ecc... ma sopratutto è una comunità virtuale dove gli aderenti possono partecipare in prima persona grazie alle funzionalità per l'interazione di FirstClass, utilizzato fin dall'inizio come piattaforma tecnologica.

Le esigenze sono molteplici: combinare aree pubbliche e riservate, istituzionali e aperte agli interventi di ciascuno, necessità di comunicare tramite messaggi di posta, chat, di consentire agli utenti di conoscersi tra loro per una più immedita possibilità di collaborazione oltre alla gestione di un elevato numero di servizi, in continua crescita, spesso correlati tra loro. Per rispondere a tutto questo, RCM ben si sposa con le caratteristiche di flessibilità di FirstClass. La semplicità di gestione del software inoltre è determinante per dare la possibilità ai gestori dei forum e delle aree tematiche di svolgere il loro lavoro anche in mancanza di particolari conoscenze informatiche.

Uno dei prossimi numeri della nostra newsletter verrà arricchito con il *case study* della Rete Civica di Milano, ma chi volesse da subito maggiori informazioni in merito alla comunità può collegarsi al sito http://www.retecivica.milano.it.

Tra le novità di RCM è prevista a breve la pubblicazione, a cura di NEOL, di un'area dedicata a FirstClass "FirstClass Suite" con informazioni, aggiornamenti ed un forum di discussione sull'ambiente.

Da OpenText due nuovi strumenti per FirstClass: Log Analyzer e Rapid Web Designer

L'offerta degli strumenti per migliorare l'uso di FirstClass si arricchisce di due nuove ed importanti applicazioni realizzate per essere integrate all'ambiente FirstClass Server e per semplificare la vita degli amministratori di sistema:

- Log Analyzer
- Rapid Web Designer (RWD)

FirstClass Log Analyzer è un interessante ed utile strumento a disposizione degli amministratori che consente di svolgere, in modo efficiente e rapido, analisi complesse e dettagliate dei dati di utilizzo del sistema. Log Analyzer, al primo impatto risulta essere estremamente flessibile e dettagliato nelle possibilità di ricerca, oltre a fornire dei report avanzati. Le funzionalità e modalità di utilizzo dell'applicazione verranno descritte nel prossimo numero di questa newsletter.

L'ultima novità dal mondo FirstClass è invece l'annuncio di un nuovo applicativo: il Rapid Web Designer. E' un prodotto che integrato al server permette la realizzazione di pagine web professionali e sofisticate in maniera semplice ed immediata, in linea con la filosofia di FirstClass. Una descrizione dettagliata e maggiori informazioni in merito alla disponibilità di questo prodotto verranno inserite nei prossimi numeri di questa pubblicazione.

Per chi fosse interessato, da subito, ad approfondire le possibilità di utilizzo di Rapid Web Designer segnaliamo l'invito di OpenText ad un seminario on line (**Interactive Webinar)** che si svolgerà il 22 marzo. Per l'iscrizione è necessario inviare un messaggio all'indirizzo **webinar_registrations@firstclass-intl.com** con l'indicazione del vostro nome, struttura di appartenenza, indirizzo e numero di telefono. Maggiori informazioni sulle modalità di svolgimento, sul programma e gli orari potranno essere richieste alla nostra redazione.

FirstClass e l'insegnamento delle lingue al Centro Linguistico di Ateneo di Padova

Francesca Helm e Charlotte Whigham – Centro Linguistico di Ateneo, Università di Padova

FirstClass è stato introdotto nel Centro Linguistico di Ateneo dell'Università di Padova nel 1998, e da allora il CLA ha fatto un uso crescente di questo software per computer conferencing (v. per es. Ackerley 2002, Dalziel e Helm 2000, Dalzie 2002, Mazzurelle e Ferrazza 2002, Whigham e Carraro 2002, Whigham 2002). Attualmente ci sono circa 3000 utenti contemporanei fra docenti, studenti e personale tecnico-amministrativo. *FirstClass* viene adoperato sia per comunicazioni e scambi di informazioni fra il personale, sia per la didattica delle lingue: *FirstClass* viene utilizzato nell'insegnamento di sette lingue, francese, inglese, italiano, neerlandese, portoghese, spagnolo e tedesco, per circa trenta corsi.

Per una struttura come il Centro Linguistico di Padova con 4 poli nella città di Padova e collaboratori che insegnano in tutte le facoltà uno strumento efficace di comunicazione è essenziale.

Coordinazione progetti

FirstClass viene adoperato come strumento organizzativo e di discussione sulla didattica, come nel caso del progetto del Portfolio Europeo delle Lingue *http://culture2.coe.int/portfolio/inc.asp?L=E&M=$t/208-1-0-/main_pages/welcome.html*, svolto a Padova, nell'ambito della sperimentazione CercleS/AICLU e presentato al Convegno AICLU a Trieste, nel giugno del 2003 e nel Convegno CercleS a Bratislava nel settembre del 2004. Per gli scopi di questo progetto è importante fornire agli studenti informazioni e dare a loro la possibilità di chiedere chiarimenti qualora necessario. Per gli insegnanti invece l'uso di *FirstClass* permette uno scambio di idee e suggerimenti su come integrare il *Portfolio* nei corsi di lingua, e può dare luogo ad un dibattito.

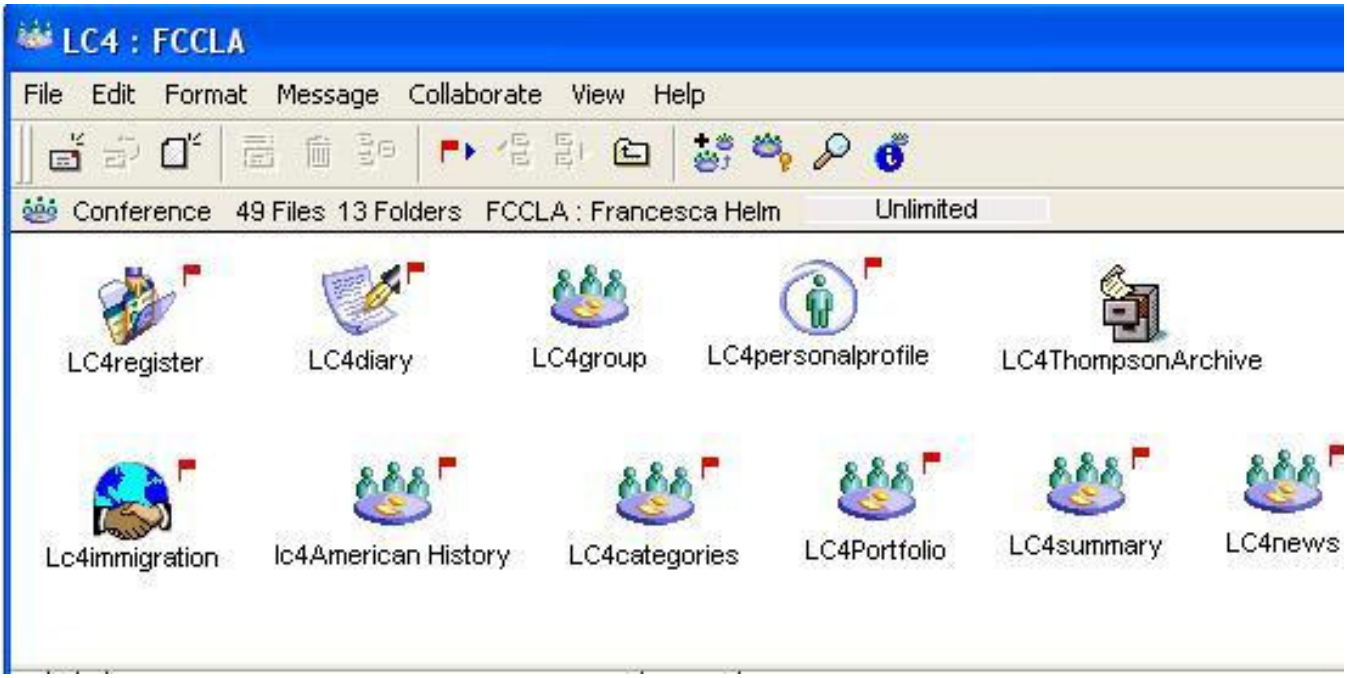
Formazione insegnanti e una comunità di pratica

La formazione degli insegnanti è anche molto importante per il Centro Linguistico, ma a volte difficile da organizzare per orari e impegni diversi dei collaboratori. I vantaggi della formazione online sono ben noti, come la indipendenza dallo spazio e dal tempo che facilitano la partecipazione di un numero maggiore di persone, come nel seminario online sulla verifica tenuto in giugno 2003. Con l'aiuto di *FirstClass* si è istaurata una comunità di pratica al CLA, in continua evoluzione.

FirstClass e la didattica delle lingue

FirstClass risponde alle esigenze di studenti con abilità linguistiche, esigenze e obiettivi diversi e questo strumento facilita lo sviluppo di attività quali la discussione, il dibattito, la *chat*, la correzione in autonomia e quella tra pari, la verifica in itinere, gli scambi interculturali. *FirstClass* favorisce la collaborazione fra studenti, facilita la cooperazione positiva e, fornendo un pubblico, porta all'autonomia e allo sviluppo del senso critico. Inoltre, l'uso di *FirstClass* semplifica l'organizzazione dei corsi e la gestione degli studenti, permettendo la divulgazione di informazioni su vari aspetti del corso.

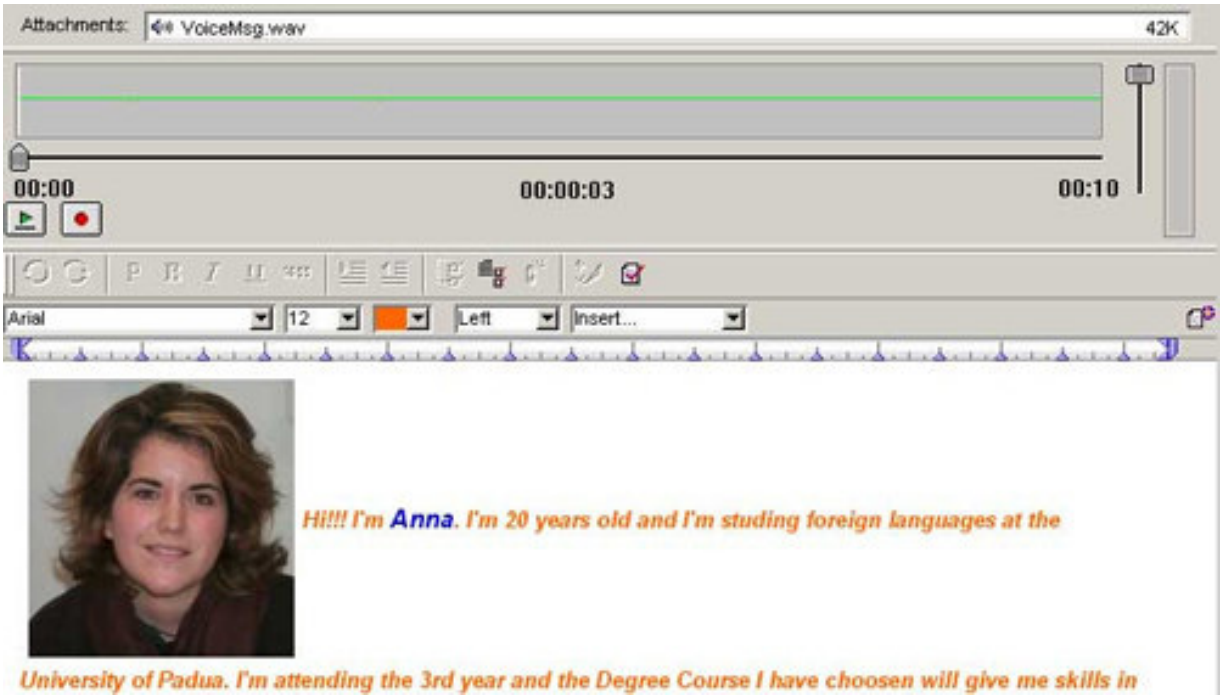
Nei corsi di lingua vengono sfruttati i diversi tipi di scrittura che *FirstClass* permette: la scrittura collaborativa dove ogni componente di un gruppo contribuisce all'elaborazione di un testo compiuto; la scrittura riflessiva, una forma più personale e privata di cui è esempio il diario; la scrittura controllata dove lo studente scrive un compito di esame per il quale c'è un limite di tempo; la scrittura di un testo con più elaborazioni: quest'ultima può essere il risultato di una ricerca e il prodotto che viene arricchito di elementi multimediali, come immagini, audio e *link* ipertestuali.

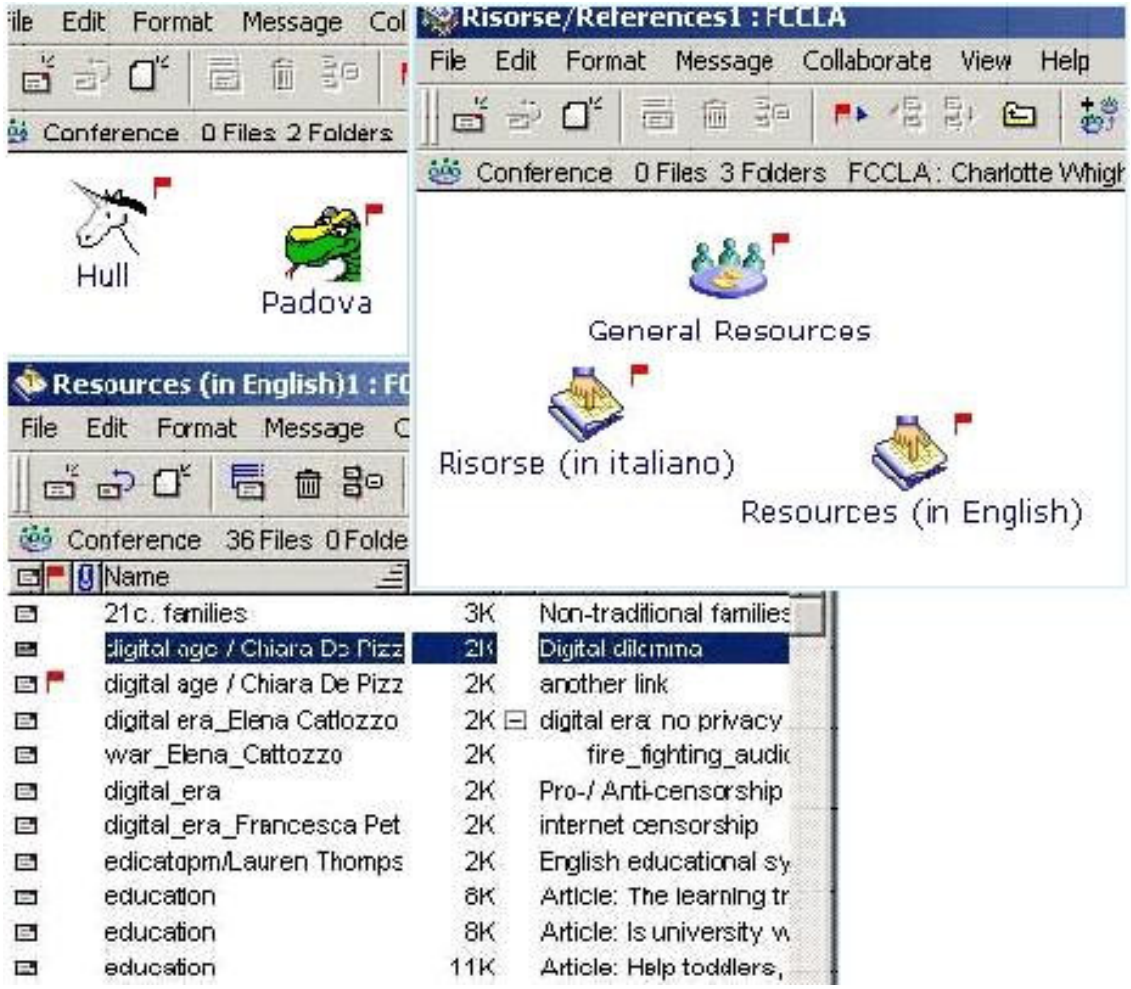


Oltre alla comunicazione asincrona, ci sono molti modi in cui la *chat* sincrona può essere utilizzata per la didattica delle lingue, come *brainstorming*, traduzione, scrittura collaborativa, descrizione immagini e per comunicare con studenti in altre università. L'immediatezza della modalità sincrona di comunicazione è motivante per gli studenti e può complementare in diversi modi le attività asincrone.
Gli studenti possono anche comunicare oralmente semplicemente registrando messaggi vocali e insere ndoli nei messaggi che spediscono.

Progetto di scambio tra l'Ateneo di Padova e l'Università di Hull.

Uno dei vantaggi più grandi che offre la comunicazione mediata dal computer per studenti di una lingua straniera è la possibilità di comunicare con studenti che vivono in altri paesi, come ad esempio nel progetto di scambio tra l'Università di Padova e l'Università di Hull in Inghilterra. Gli studenti italiani e inglesi vengono divisi in gruppi e, alternando la lingua, ricercano informazioni e si scambiano messaggi su un dato argomento; vengono utilizzati anche messaggi vocali. Questo lavoro porta all'elaborazione di testi scritti che, dopo essere stati sottoposti alla correzione tra pari, vengono rivisti dall'insegnante. Il lavoro viene quindi coronato da videoconferenze che riscuotono grande successo. Infatti, grazie al lavoro svolto in *FirstClass*, gli studenti si sentono pronti ad intervenire oralmente a proposito degli argomenti trattati. Quindi, *FirstClass*, noto come strumento di scrittura, può essere utilizzato per aiutare gli studenti a sviluppare le loro abilità orali.


Attachments:
VoiceMsg.wav
42K
00:00
00:00:03
00:10
Arial
12
Left
Insert...
Hi!!! I'm Anna. I'm 20 years old and I'm studing foreign languages at the
University of Padua. I'm attending the 3rd year and the Degree Course I have choosen will give me skills in


File Edit Format Message Col
Conference 0 Files 2 Folders
Hull
Padova
Risorse/References1 : FCCLA
File Edit Format Message Collaborate View Help
Conference 0 Files 3 Folders FCCLA : Charlotte Whigh
General Resources
Risorse (in italiano)
Resources (in English)
Resources (in English)1 : FC
File Edit Format Message C
Conference 36 Files 0 Folde
Name
21c. families 3K Non-tradiltional families
digital age / Chiara De Pizz 2K Digital dilemma
digital age / Chiara De Pizz 2K another link
digital era_Elena Cattozzo 2K digital era: no privacy
war_Elena_Cattozzo 2K fire_fighting_audi
digital_era 2K Pro-/ Anti-censorship
digital_era_Francesca Pet 2K internet censorship
edicatopm/Lauren Thomps 2K English educational sy
education 8K Article: The learning tr
education 8K Article: Is university w
education 11K Article: Help toddlers,

Bibliografia

Ackerley, K. (2002) "A FirstClass Debate – Using computer Conferencing to Promote Oral Communication". *Innovazioni Nell'Apprendimento Linguistico Con Il Supporto Del C.L.A. a cura di C. Taylor Torsello e R. Guerini* . *Il C.L.A. Per Le Lingue Straniere: Esperienze e Prospettive 1,* Padova, CLEUP, 59-68.
Council of Europe portfolio site: *http://culture2.coe.int/portfolio/inc.asp?L=E&M=$t/208-1-0-1/main_pages/welcome.html* (visitato 16.07.03).
Dalziel, F. e Helm, F. (2000) "Computer conferencing software e il riassunto: Le competenze dello studente come risorsa per l'insegnamento della composizione scritta" in R. Favretti *(*a cura di) *Linguistica e Informatica: Corpora, Multimedialità e percorsi di apprendimento* , Roma, Bulzoni, 409-426.
Dalziel, F. (2002) "Teacher Feedback in Online Language Education", in C. Taylor Torsello, M. Catricalà e J. Morley (a cura di), *2001 – Anno europeo delle lingue: proposte della nuova università italiana*. Siena, Terre de Sienne, 131-138.
Mazzurelle, S. e Ferrazza, E. (2002) "L'apprentissage du francais écrit avec les conférences de *FirstClass",* in C. Taylor Torsello e R. Guerini (a cura di), *Innovazioni Nell'Apprendimento Linguistico Con Il Supporto Del C.L.A.* (Il C.L.A. per le Lingue Straniere: Esperienze e Prospettive n°1), Padova, CLEUP, 119-136.
Whigham, C. (2002) "The benefits of computer conferencing software in peer revision" in C. Taylor Torsello, M. Catricalà e J. Morley (Eds.), *2001 – Anno europeo delle lingue: proposte della nuova università italiana,* Siena, Terre de Sienne editrice, 139-150.
Whigham, C. e Carraro, K. (2002) "Il valore della cooperazione e dell'interdipendenza nella didattica delle lingue", in C. Taylor Torsello e R. Guerini (Eds.), *Innovazioni Nell'Apprendimento Linguistico Con Il Supporto Del C.L.A.* (Il C.L.A. per le Lingue Straniere: Esperienze e Prospettive n°1), Padova, CLEUP, 151-164.

Per maggiori informazioni è possibile contattare:
Francesca Helm e Charlotte Whigham – Centro Linguistico di Ateneo, Università di Padova
http://claweb.cla.unipd.it/cla/

Gli strumenti per la sicurezza in FirstClass 8 - prima parte

Terry Whyte, responsabile dello sviluppo dei Servizi Internet e dei Servizi Voce, FirstClass Division - OpenText Corporation

Riprodotto per gentile concessione dal numero speciale dedicato alla sicurezza della "FirstClass Newsletter", agosto 2004, Copyright 2004 Open Text Corp.

I Servizi Internet (Internet Services) nella loro versione 8.0 rendono ancora più semplice proteggere il sistema FirstClass dagli abusi e dagli attacchi sempre più frequenti in rete. Per fare questo, molti settaggi preconfigurati dei Servizi Internet sono stati modificati, così come i settaggi nel quadro UCE/Spam e nel quadro di configurazione base dei servizi internet (Basic Internet Setup). Tutti questi cambiamenti sono stati intesi a:

- rendere i Servizi Internet di FirstClass più sicuri "out of the box" (nella loro configurazione predefinita);

- rendere più semplice bloccare lo spam che infastidisce gli utenti

- rendere più semplice bloccare gli attacchi al sistema prima che questi esauriscano le risorse di sistema.

Questo documento discute i vari modi con cui si può rendere sicuro un sistema FirstClass usando queste nuove e migliorate caratteristiche dei Servizi Internet. Nonostante sia possibile leggere a piacimento ognuno dei seguenti documenti, raccomandiamo di leggerli nell'ordine:

- nuovi ed accresciuti meccanismi di sicurezza
- prevenire accessi/connessioni non volute
- rispondere alle aggressioni (blackholing)
- prevenire scambi di mail non autorizzati
- ridurre lo spam
- regole di posta SMTP

Gli ultimi due punti saranno trattati nel prossimo numero della newsletter.

Nuovi ed accresciuti meccanismi di sicurezza dei Servizi Internet 8.0

Nuovi meccanismi di sicurezza

Questo è un sommario dei nuovi meccanismi di sicurezza che è possibile utilizzare (per facilitare quanti finora hanno letto la documentazione FirstClass in inglese, manteniamo in parte anche la dicitura inglese originale dei vari argomenti).

Liste di blocco temporanee dei numeri IP (Temporary IP blocking lists)

I Servizi Internet, ora, gestiscono liste di indirizzi IP per il blocco temporaneo. Nella versione precedente, gli indirizzi IP indesiderati dovevano essere aggiunti manualmente alla cartella filtri. Nei Servizi Internet 8.0 è possibile far aggiungere gli indirizzi IP ad una lista temporanea, mantenuta nella memoria dei Servizi Internet, con una permanenza in questa lista limitata da una scadenza definibile nel tempo.

E' possibile accedere a questo nuovo servizio attraverso un'azione nel documento rules.Mailrules (le regole di posta) o dal quadro Status, nel Monitor dei Servizi Internet. E' possibile controllare la lista dei blocchi temporanei ed aggiungere e cancellare le entrate dinamicamente nel riquadro Sicurezza.

Supporto del Blackhole (BucoNero)

Mettere un indirizzo IP nel BucoNero è funzionalmente simile a metterlo nella lista degli IP soggetti a blocco temporaneo, solo che nei Buchi Neri è mantenuto separatamente. Un Buco Nero catturerà ogni connessione da un indirizzo IP ostile e lo sposterà su un singolo task a bassa priorità dei Servizi Internet. Questo task dismetterà ogni dato ricevuto producendo allo stesso tempo uno stream molto lento e temporizzato di caratteri per mantenere attiva la connessione.

Il concetto è in questo caso quello di rispondere agli attacchi degli spammer, catturando le loro risorse e rallentando la loro abilità di colpire il nostro sistema (e quello di altri). Alcuni servizi RBL (server che gestiscono le black list) richiedono di abilitare questa funzione per poter usare i loro servizi. Questa opzione è sotto controllo dell'amministratore, ed è possibile accedervi dal quadro connessioni (Connections-Basic Internet Setup).

Memorizzare gli attacchi RBL

Un comune assalto ai Servizi Internet avviene sotto forma di un singolo SMTP server che spedisce dozzine (o centinaia) di messaggi spam in rapida successione al server. Anche usando un servizio RBL che attiva un blocco su uno specifico server, lo stesso server può riconnettersi e il sistema dovrà spendere le proprie risorse per ripetere la stessa richiesta di verifica al server RBL.

I Servizi Internet ora ricordano i risultati delle interrogazioni ai server RBL usando il valore della scadenza "time to live" fornito dal server RBL (con una funzione simile a quello dei record DNS memorizzati dagli Servizi Internet più vecchi) per impedire ai server che svolgono un'attività di spamming dal riconnettersi immediatamente al tuo sistema. Questo elimina lo spreco di risorse per eseguire nuovamente le interrogazioni verso i server RBL.

Rivelazione degli attacchi alle password sul servizio SMTP AUTH

Usando la nuova funzionalità delle liste di blocco temporaneo degli IP, i Servizi Internet proteggono automaticamente il sistema dall'indirizzo IP che sembra condurre un attacco tentando di indovinare la password di un particolare utente. Benchè i Servizi Internet abbiano già una protezione contro l'individuazione delle password (il sistema SMTP AUTH), è stata aggiunta una speciale variante per gestire gli attacchi automatici.

Usando un sistema basato sul numero di attacchi (strike), i Servizi Internet bloccano temporaneamente un indirizzo IP, al momento in cui questo effetui ripetuti tentativi di loggarsi usando SMTP AUTH con un incorretto User ID o password. Gli attacchi vengono conteggiati rispetto ad un un particolare indirizzo IP così che, anche se nel corso dell'attacco, gli User ID e le password vengono continuamente cambiate, gli Internet Sevices possono bloccarli.

Rivelazione degli abusi (System Abuse)

Adesso, i Servizi Internet possono segnalare attività sospette svolte sul sistema. Tale attività è tracciata attraverso i diversi protocolli e, basandosi su quanto definito nel setup, usa i led presenti nel quadro del monitor dei Servizi Internet per avvisare. L'attività sospetta include il monitoraggio dei seguenti fenomeni:

- numero di connessioni usate da un singolo IP

- le velocità di trasferimento dati

- frequenza delle connessione

- tentativi di login falliti

- tentativi di loggarsi all'account dell'amministratore.

Scansione dei virus negli allegati SMTP

Usando il Symantec AV Scan Engine, i Servizi Internet ora supportano lo scan di virus negli allegati in entrata ed in uscita. E' possibile collegare diversi motori antivirus ad una singola macchina Servizi Internet per smaltire in modo adeguato carichi di lavoro pesanti in un ambiente con un alto numero di messaggi scambiati.

Se si trova un virus in un allegato in entrata, questo è riposizionato da un allegato contenente un testo di allarme. Se si trova un virus in un allegato in uscita, Servizi Internet spedisce un NDN con un testo di allarme al ricevente. Si può configurare il testo di allarme sul tab Antivirus del form Advanced Mail.

I Servizi Internet possono girare come un daemon (OS X) o servizio (Windows)

Adesso, i Servizi Internet possono girare come un daemon di Mac OS X o come

un servizio di Windows. I Servizi Internet ripartono automaticamente al riavvio della macchina. Questa opzione permette di lasciare incustodita la macchina server, senza nessun utente loggato, prevenendo attacchi da persone fisiche quando non è possibile fisicamente mettere in sicurezza il computer.

Meccanismi di sicurezza accresciuti

Questo è un sommario dei miglioramenti nei meccanismi di sicurezza che possono essere utilizzati.

Regole di posta (Mail rules)

Il documento rules.MailRules contiene vari miglioramenti:

- nuove azioni per posizionare gli indirizzi IP nella lista di blocco temporaneo o nell'area di quarantena (blackhole);

- nuove condizioni di regole per implementare liste multiple di blocco dell'oggetto delle mail, consentendo differenti punteggi spam a seconda del tipo di parole usate;

- possibilità di fare la scansione di messaggi per parole bloccate prima della consegna al destinatario;

- un nuovo ed avanzato analizzatore di espressioni regolari (parser di regular expression) per codificare condizioni di regole molto avanzate;

- nuove funzioni e variabili che danno all'autore delle regole più informazioni circa la gestione del messaggio e i dialoghi svolti dal servizio SMTP

- possbilità di leggere dati dai quadri di setup dei Servizi Internet.

Tutto questo permette di configurare alcune delle regole incorporate nel quadro Basic Internet Setup, invece di dover armeggiare con i più complicati file rules.MailRules.
Per esempio è possibile definire:

- i livelli del punteggio alto, medio e basso dello spam

- il limite dell'invio multiplo via SMTP (SMTP crosspost)

- l'invio di messaggi NDN nel caso di punteggio spam al di sopra di Extreme

- l'invio di messaggi NDN nel caso di soggetti bloccati.

Lista dei task dei Servizi Internet

Adesso, la lista dei task mostra gli indirizzi IP, il tempo di connessione e l'ammontare dei dati trasferiti a fianco di ogni task in entrata. Questo permette di correlare più facilmente l'attività inusuale nel sistema con gli indirizzi IP che causano problemi.

IP / liste dei filtri di dominio

Adesso, è possibile bloccare una serie di indirizzi IP nei documenti filtri (per esempio, 127.0.0.1-127.0.0.92) ed usare wildcard ed espressioni regolari.

Il Monitor dei Servizi Internet

Adesso, è possibile eseguire mansioni di mantenimento di routine e monitorare lo stato dei Servizi Internet in remoto dall' Internet Services Monitor. Tra queste funzioni vi sono le seguenti:

- pieno controllo remoto dei comandi da menù dei Servizi Internet, utili per operazioni in cui non vi è la console locale dei servizi internet,

- nuovi indicatori di stato, che includono Task load e Abuse display, che permettono di monitorare costantemente l'attività sul sistema.

Privacy HTTP server

Questa funzione è stata disabilitata per default, in quanto più organizzazioni di sicurezza Internet hanno espresso preoccupazione che l'utility HTTP TRACE possa porre a rischio di privacy.

Prevenzione di accessi e connessioni indesiderate

A causa di atteggiamenti da parte degli spammer sempre più aggressivi, del diffondersi di meccanismi automatizzati di pirateria, di virus auto-diffondenti e dei vecchi metodi degli hackers, la quantità di traffico molesto è cresciuta a dismisura. In FirstClass 8.0 abbiamo aggiunto numerose funzioni e strumenti per aiutare a scoprire e bloccare tali abusi. I Servizi Internet hanno metodi di sicurezza multipli di arresto reciproco, che permettono di scegliere la maniera più adeguata per proteggere il sistema FirstClass.

Questi nuovi strumenti sono sicuramente potenti, tuttavia occorre considerare che alcuni potrebbero non essere appropriati per il singolo sistema e quindi il loro utilizzo deve essere valutato con attenzione.

Sommario su come disabilitare le caratteristiche

Questo è un sommario delle nuove funzionalità e su come disabilitarle.

Tabella 1

Funzionalità	Introdotta/Migliorata	Come disabilitare
Filtro degli indirizzi IP	7.1/ aggiunti gli intervalli	Non introdurre nuove linee
Monitoraggio degli abusi	8.0	Mettere come Disabilitata la voce Basic Internet Setup -> UCE/SPAM -> Abuso -> Abuso livello di attenzione
Blacklisting	8.0	Mettere come Disabilitata la voce Basic Internet Setup -> UCE/SPAM -> Abuso -> Abuso livello blocco automatico
Striking out connections	8.0	Mettere la voce Basic Internet Setup -> UCE/SPAM -> Junk -> Abuso -> Numero attacchi permessi a 32767 e tempo di blocco a 0.
Blackholing	8.0	Mettere a zero la voce Basic Internet Setup -> Connessioni -> Numero massimo di connessioni bloccate a Nessuno

Quando si considera un problema con una connessione IP, occorre prendere in considerazione in quale stato queste connessioni potrebbero essere e quali caratteristiche incidono su questi stati. Questo è un breve sommario dei tipi di connessioni e come è possibile controllarle-verificarle.

Tabella 2

Stato	**Caratteristiche**	**Controllato da**
Affidabile	Può connettersi sempre	File dei Filtri IP, voci con il '+'
Bloccato	Non può mai connettersi	Voci del file dei filtri IP, Connessioni -> Rifiuta le connessioni basate sui filtri
Sospetto	Appare in Internet Monitor-> Sicurezza, si connette normalmente	UCE /Spam-> Sospetto di abuso -> Livello di pericolosità dell'abuso
Messo nella lista attacchi	Appare nel Monitor Internet -> Controllo-> Blacklist numeri IP -> Presente nei Log specifici, si connette normalmente	UCE/SPam-> Junk (spazzatura)-> Numero di attacchi (strike) permessi, azione di una regola di posta relativa alle blacklist o errati login al servizio SMTP AUTH
Messo nella lista nera	Appare in Internet Monitor-> Controllo->Blackl ist numeri IP -> Presente nei Log specifici, non può connettersi	UCE/Spam-> Abuso-> Livello di autobloccaggio, azione di una regola di posta relativa alle blacklist
Quarantena	Appare in Internet Monitor-> Controllo-> Connessioni congelate (Blackholed) -> Presente nei Log specifici, connessione molto lenta	Connessioni-> Numero massimo di connessioni da congelare, Connessioni-> connessioni congelate dai setting
Normale	Si collega normalmente	Configurazione IS

Adesso è possibile anche monitorare l'efficacia della politica di blocco degli IP. Nel quadro Sicurezza del Monitor dei Servizi Internet c'è una sezione denominata "Tentativi di connessione". Questo quadro dà le statistiche di quante connessioni sono accettate o rifiutate dal sistema, sia in modo incrementale che in assoluto.

Tentativi di connessione

Filtrare gli indirizzi IP

Uno degli strumenti più vecchi e preferiti (ma ancora potente) per controllare gli accessi indesiderati al sistema, è il filtraggio dei numeri IP. E' possibile bloccare gli indirizzi IP individualmente, o usando wildcards o serie di numeri IP nei documenti di filtro posizionati in Servizi Internet/Cartella Filters, sul Desktop dell'amministratore, e poi abilitare l'opzione sul quadro Connessioni del Basic Internet Setup.

Quadro Connessioni

Questa opzione blocca gli indirizzi IP dalla connessione ai Servizi Internet su ogni protocollo, se gli indirizzi sono elencati all'interno di uno dei documenti Filter. Ogni connessione dagli indirizzi elencati è rifiutata immediatamente, usando la minima potenza possibile di processo e risorse di sistema. Questo rende l'uso del blocco degli IP uno strumento utile per sbarazzarsi delle macchine "fabbrica-guai" su Internet, sia che stiano tentando di attaccare il tuo sistema, sia che stiano negando i propri servizi ai tuoi utenti. Se è disponibile un firewall hardware, è opportuno usarlo per proteggere la macchina dove risiedono i Servizi Internet, visto che così si evitano sforzi eccessivi ad una risorsa dedicata. Tuttavia, per bloccare rapidamente un indirizzo problematico o per un sito che non vuol tenere i Servizi Internet all'interno di un firewall, questa è una buona opzione.

Per configurare il tuo sistema affinchè blocchi gli accessi indesiderati:

1 Seleziona "Rifiuta le connessioni basandoti sui filtri".

2 Apri la cartella Filters che si trova nella cartella Servizi Internet nel Desktop dell'amministratore.

3 Crea un documento FirstClass nella cartella Filters elencando gli indirizzi che vuoi bloccare.

Raccomandiamo di dare un nome significativo al documento (un nome del tipo IP Bloccati) ed elencare solo gli indirizzi IP che si desiderano bloccare. Altri documenti Filter possono contenere blocchi IP, ma mantenendoli separati è più facile gestirli.

4 Aprire il Monitor dei Servizi Internet, che si trova nella cartella Servizi Internet sul Desktop dell'amministratore.

5 Fare click su Ricarica Configurazione (Reload Config).

Se è necessario bloccare un nuovo indirizzo IP in futuro, tutto quello che occorre fare è aprire questo documento ed aggiungere il nuovo indrizzo o maschera IP. Bisogna ricordarsi di cliccare Reload Config o riavvia i Servizi Internet dopo ogni aggiunta a questo documento.

Sintassi per bloccare gli indirizzi IP nel documento di filtro.
La sintassi per bloccare un numero IP assume una delle tre forme: un singolo indirizzo IP per linea, una "maschera" IP che può bloccare gruppi di indirizzi IP simili, o un range di numeri IP che specifica una gamma di IP da bloccare. Qui c'è un esempio di documento IP Bloccati:

Table 3

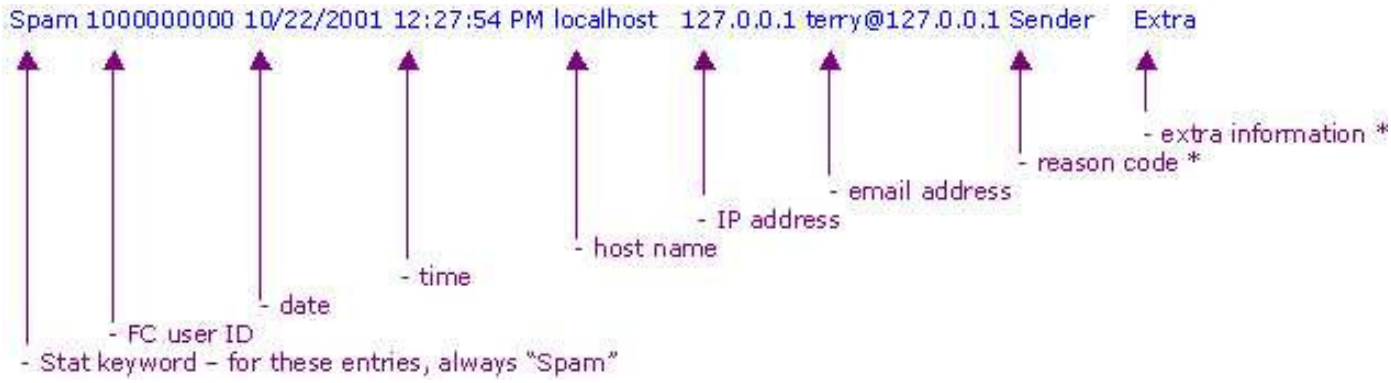
111.222.111.222	blocca l' IP 111.222.111.222
111.*.*.*	una maschera IP - questa blocca ogni indirizzo IP che comincia con 111. Nota - 111.* non è un'abbreviazione valida per 111.*.*.*
111.222.111.200.- 111.222.111.222	un intervallo - blocca indirizzi IP dal 111.222.111.200 al 111.222.111.223 incluso
111/112.222/223.1 11/115.223/255	un intervallo espresso in modo alternativo - blocca gli indirizzi IP dal 111.222.111.223 al 112.223.115.255 incluso

Chi filtrare?

Uno dei compiti a cui un amministratore si trova di fronte nell'usare liste di filtri è capire quale indirizzo IP bloccare. Anche se possiamo usare le vecchie tecniche preferite da ciascuno di noi, FirstClass 8.0 ne introduce alcune di nuove per semplificare il lavoro degli amministratori. Lo strumento classico è il file delle statistiche server di FirstClass, che è controllato usando Admin > Statistics & Billing > Statistics Control.

Sebbene le regole dei Servizi Internet nel riquadro UCE/Spam possono bloccare un messaggio prima che arrivi nella Mailbox di un utente, un'annotazione viene sempre aggiunta al file di statistiche server. Per esempio:

Riga nelle statistiche server:



* il codice (reason code) è uno tra questi: Virus, Strikeout, MailRule, Sender, RBL, ReverseDNS, Host, RelayReject***

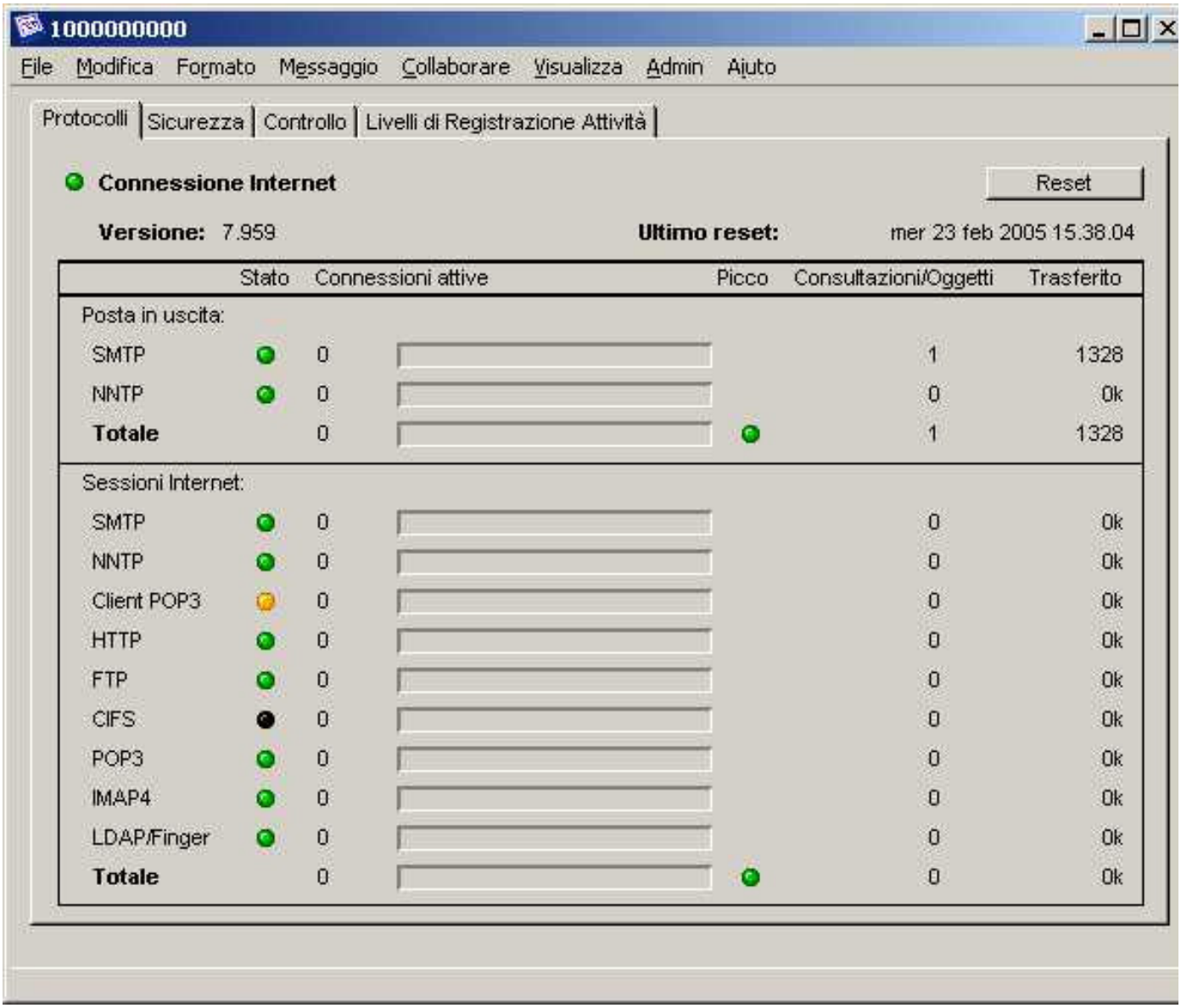
** informazioni ulteriori contengono:
• per il tipo MailRule - qualsiasi testo NDN (Non Delivery Note) inviato
• per il tipo RelayReject (relay rifiutato) - l'indirizzo a cui si fa relay (ponte)
• per il tipo Virus - il nome dell'attachment infettato e il nome del virus.

*** Il RelayReject (relay respinto) non è registrato quando è disabilitata la possibilità di qualsiasi relay.

Raccomandiamo di aprire tutte le statistiche che sono appropriate per il server amministrato e, periodicamente, dar loro un'occhiata usando un text editor, il programma spreadsheet favorito, o il nuovo programma FC Log Analyzer. Il FirstClass Log Analyzer, o ogni altro programma per l'analisi dei log dei server web, possono leggere i log web che i Servizi Internet producono. Per informazioni su come ordinare il FirstClass Log Analyzer, contatta il tuo rivenditore o distributore FirstClass.

Gli strumenti tradizionali contenuti nei Servizi Internet per monitorare il sistema sono il Monitor dei Servizi Internet e la Lista dei Task dei Servizi Internet. Entrambi sono stati rinforzati in FirstClass 8.0. Il riquadro dei Protocolli del monitor mostra l'attività globale di sistema, con una vista che può essere verificata aprendo con una console con vista sulla Task List e la nuova sezione sull'abuso del riquadro Sicurezza. Per esempio:

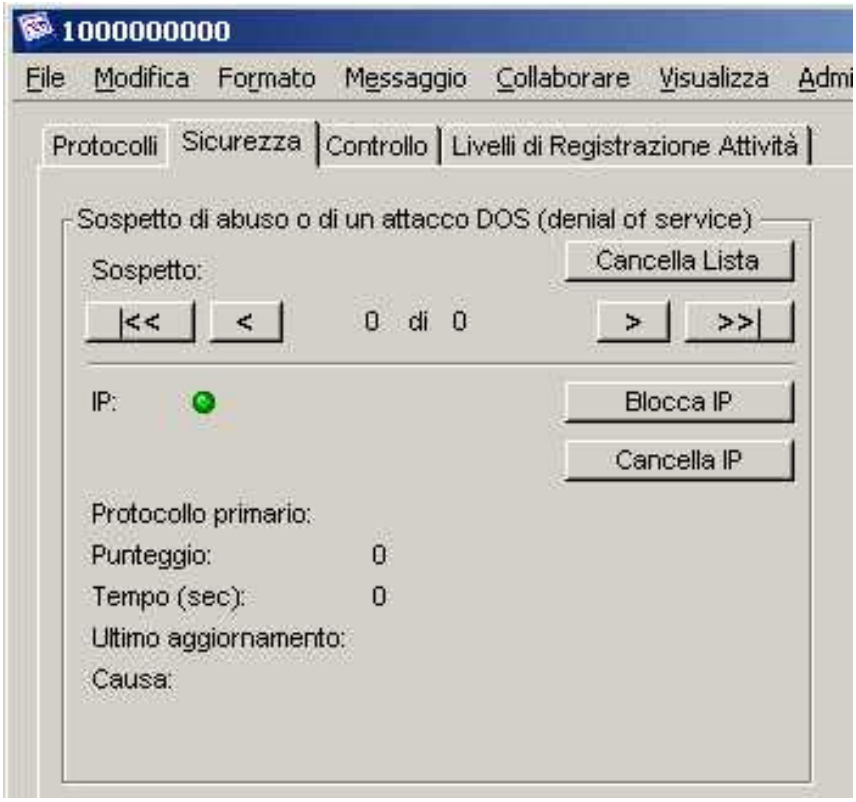
Internet Monitor - Quadro dei protocolli



Task list

```
---  Task List  ---
[   ID] Type- IP Address    :Port, Time,  Bytes Transferred, D1, D2, Comment
-------------------------------------------------------------------------
[    3] main-  0.  0.  0.  0:   0,    0, 0x0000000000000000,  0,  0,
[s   4] DNSr-  0.  0.  0.  0:   0,    0, 0x0000000000000000,  0,  0, Begin Queue
task
[s   5] SCon-192.168. 20.107:  25,    8, 0x0000000000000042,  0,  0, Waiting for
EHLO/HELO
```

Monitor Internet - Riquadro Sicurezza (Security)



Si può identificare l'indirizzo IP di potenziali guastatori, usando in maniera combinata questi tre strumenti.

Il riquadro di monitoraggio dell'abuso traccia una lista di indirizzi IP che sono coinvolti in attività sospette, come:

- mantenimento di una quota di dati di trasferimento molto bassa

- uso di un numero elevato di sessioni concorrenti

- connessioni mantenute per un periodo di tempo molto lungo

- uso ripetitivo di password incorrette

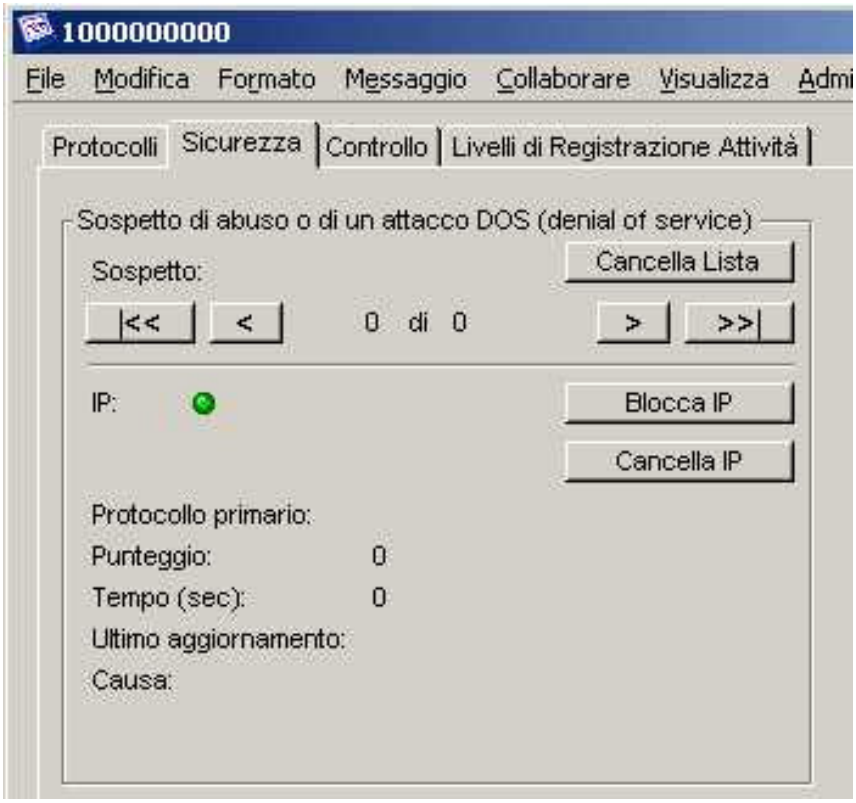
- connessioni simultanee su molti protocolli.

Il punteggio rappresenta il livello di attività sospetta e, ad ogni evenienza del fenomeno si aggiungono punti a seconda della severità dell'attività svolta. L'amministratore può gestire la lista di connessioni sospette, pulendo singoli IP che sono ritenuti innocenti o pulendo l'intera lista per cercare nuove attività sospette.

Blocco temporaneo (Temporary blocking - blacklisting)

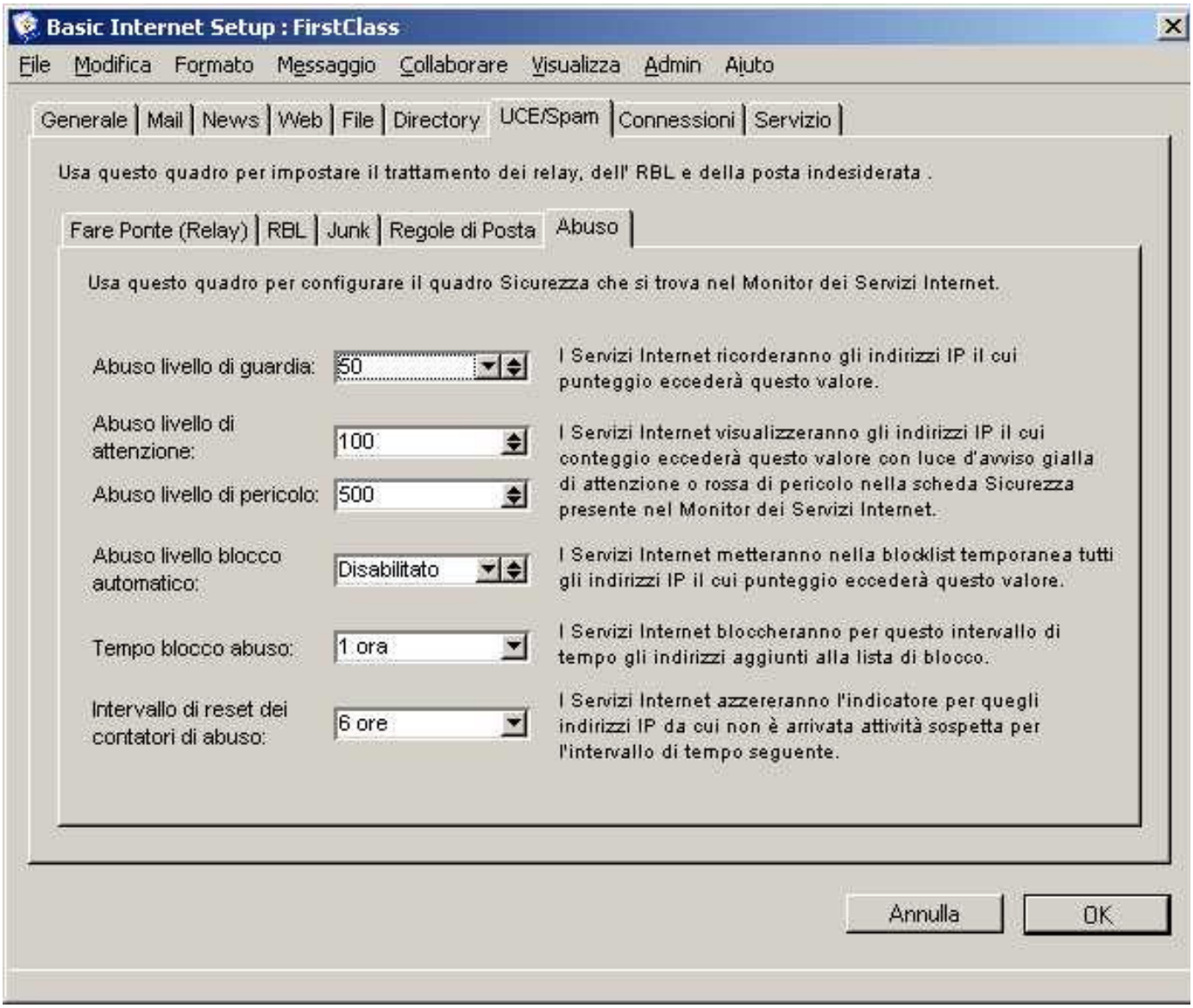
L'altro bottone importante del riquadro di monitoraggio dell'abuso è il bottone Blocca IP nel riquadro Sicurezza del Monitor dei Servizi Internet. Questo bottone permette all'amministratore di posizionare istantaneamente l'indirizzo IP sospetto nella black list temporanea degli IP.

Monitor Internet - Riquadro Sicurezza



A differenza dei documenti di filtro nella cartella Filter, questa blacklist di numeri IP è tenuta solo nella memoria dei Servizi Internet, dove gli elementi in memoria scadono e sono rimossi dalla lista. I comportamenti della abuse list e dell'IP blacklist sono controllati dal riquadro Abuso del modulo UCE/Spam nel modulo Basic Internet Setup.

Riquadro Abuso



I primi tre campi indicano i livelli di abuso, definendo le soglie secondo cui le connessioni IP appariranno nelle liste di abuso e per quando le luci di allarme verranno accese. Il campo successivo controlla la funzione di blocco automatico (autoblocking), funzione che ti permette di bloccare automaticamente IP sospetti il cui punteggio eccede la soglia limite. Raccomandiamo di mantenere il livello di blocco automatico disabilitato fino a che non si sia presa confidenza con quanto appare tra gli indirizzi IP nella lista di abusi del riquadro Sicurezza degli Servizi Internet Monitor.

Il prossimo campo, "Tempo blocco abuso" (Abuse block time), indica quanto a lungo i Servizi Internet bloccheranno un indirizzo IP, tramite il blocco automatico o manuale una volta premuto il bottone "Blocca IP" nel riquadro Sicurezza del Monitor dei Servizi Internet. Se pensi che il blocco accidentale potrebbe essere un problema per il tuo sito, abbassando questo valore verrà ridotto il tempo di blocco delle connessioni e degli abusi sospetti.

Il campo finale, "Intervallo di reset dei contatori di abuso" (Abuse reset interval),

determina quanto a lungo i Servizi Internet ricorderanno un indirizzo IP sospetto. Accorciando questo valore si rende più difficile per i Servizi Internet correlare l'attività sospetta svolta in differenti momenti del giorno.

I Servizi Internet della versione 8.0, inoltre, forniscono all'amministratore degli strumenti per gestire il temporary IP blacklist. Sul riquadro Controllo tab del Monitor dei Servizi Internet, c'è una sezione denominata "Blacklist numeri IP" contenente i bottoni Log e Svuota (Flush)

Bottoni

Gli indirizzi IP possono entrare a far parte delle blacklist solo attraverso una di queste quattro azioni:

- cliccando il bottone Block IP sul riquadro Sicurezza del Monitor dei Servizi Internet

- se hai l'autoblock configurato su riquadro Abuso/UCE/Spam nell' Internet Setup, e l'indirizzo IP in questione eccede il punteggio di soglia

- l'indirizzo IP è aggiunto alla lista usando una regola mail (vedi la sezione regole mail SMTP)

- l'indirizzo IP viene individualmente "staccato".

Quando clicchi sul bottone Log, ottieni una lista di indirizzi IP elencati nella blacklist, ragioni e tempo rimanente di sblocco da parte della console. Allo stesso tempo, i dettagli delle strike list sono anch'essi fotografati. Se sospetti che gli indirizzi IP vengano bloccati in maniera non corretta, seleziona il bottone Svuota per rimuovere tutti gli elementi dalla blacklist. Tale azione rimuoverà anche tutti gli elementi dalla strike list.

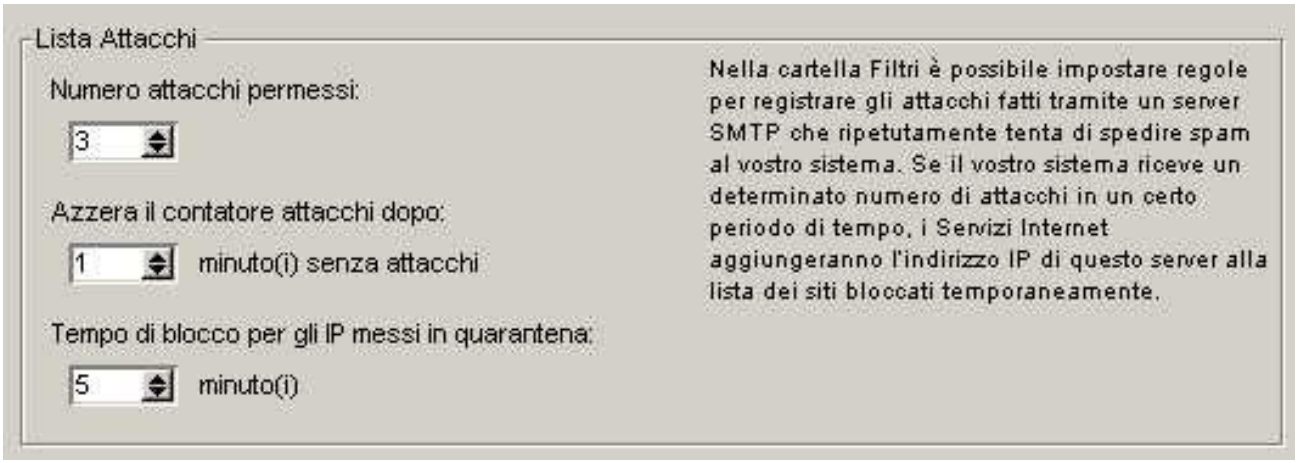
Striking out

La abuse list controlla l'attività sospetta basandosi su un punteggio, calcolato in base alla natura ed alla durata dell'attività sospetta. Questo approccio lavora bene per l'attività automatica da parte del server, ma può essere complesso quando si usano le regole mail. E' stato introdotto, quindi, il concetto di striking out (rendere inoffensivo o mettere in sicurezza) un indirizzo IP, dandogli uno specifico numero di possibilità per dimostrare di essere inoffensivo per poi bloccarlo nel caso di comportamento scorretto. Ci sono due azioni che possono far scattare uno strike (attacco) contro un indirizzo IP: l'azione STRIKE in una regola di posta (da verificare le regole MAIL SMTP), o un tentativo di accedere al servizio SMTP in modo autenticato (SMTP AUTH) con user ID e password non

validi.

Si può configurare la Strike List operando sul riguadro Junk della UCE/Spam nel quadro Basic Internet Setup. In questo posto viene indicato il numero di attacchi (strike) permessi, il tempo di azzeramento della strike list e il tempo di mantenimento in quarantena. Come menzionato sopra, anche i bottoni "IP blacklist" del riquadro "Controllo" gestiscono le strike list.

Strike list



Rispondere agli attacchi (mettere nel buco nero - blackholing)

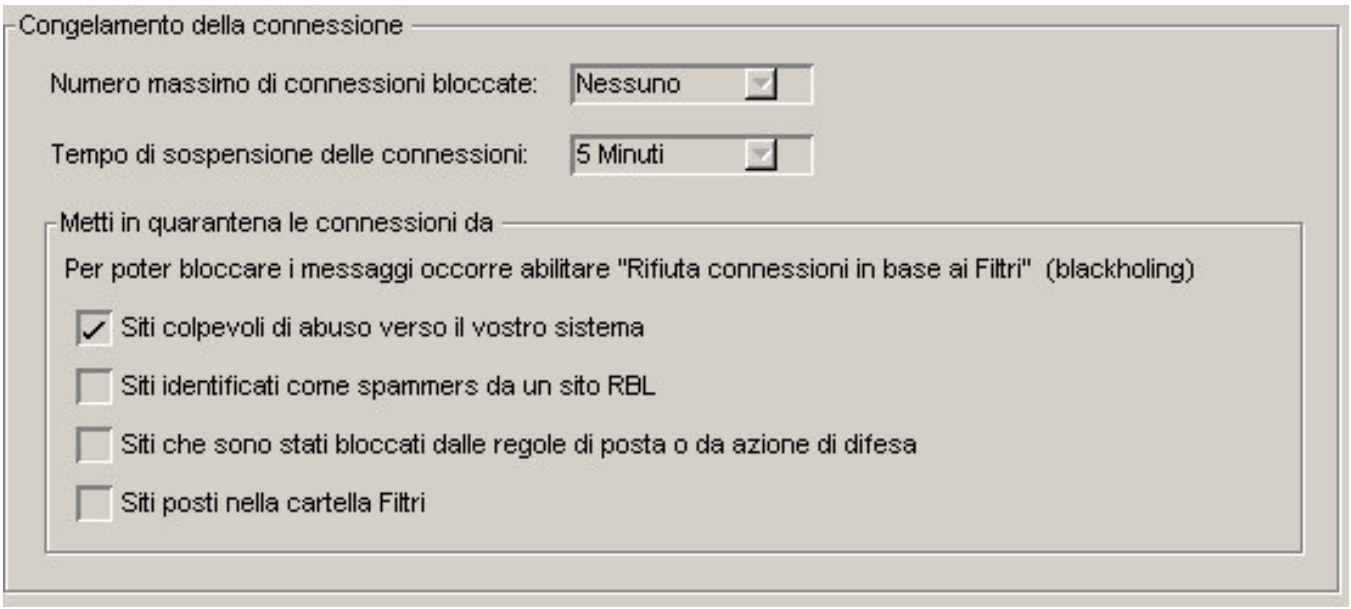
Se le contromisure descritte precedentemente risultano troppo passive per i vostri gusti, è possibile attivare una nuova funzionalità definita come blackholing (il termine vuol dire letteralmente "mettere in un buco nero" e cioè mettere in quarantena). Il principio che sta dietro a questa funzione è che la maggior parte dei programmi di disturbo automatizzati che colpiscono i nostri sistemi (spammers, strumenti di pirateria, virus spreaders, e così via) sono davvero abbastanza stupidi e possono non riconoscere che potrebbero stare sprecando il loro tempo attaccando il nostro sistema.

L'uso della funzione di blackholing permette di identificare una cattiva connessione e di affidare il dialogo con questa connessione ad un singolo task a bassa priorità, tale purtuttavia da svolgere abbastanza attività TCP per mantenere attiva la connessione. Questo costa poco al sistema in termini di potenza di calcolo, ma tiene impegnato lo spammer (o qualsiasi cosa vi muova un attacco) ed evita che questo spammer si muova sulla prossima macchina. Se tutta Internet agisse in questo modo, lo spam calerebbe ed i virus si diffonderebbero meno rapidamente. Alcuni provider RBL insistono perchè venga utilizzato qualche forma di blackholing se si vogliono usare i loro servizi.

D'altro canto, il blackholing è un atto aggressivo e molto fastidioso per il server che tenta di connettersi. Se quella persona è un vostro cliente, potrebbe non esserne troppo colpito; ma se è un hacker, potrebbe raddoppiare il suo sforzo per danneggiare il vostro sistema. Il blackholing dovrebbe essere usato quindi con molta attenzione.

Configurazione del blackhole

Le caratteristiche delle funzioni di blackhole sono configurabili sul riquadro Connessioni, nel Basic Internet Setup. Questo riquadro permette di scegliere il numero di connessioni da mantenere, per quanto a lungo mantenerle e per quale genere di abusi attivare il blackholing. Per disabilitare questa funzione sistema il "Numero massimo di connessioni bloccate" (Maximum number of connections to tie up) a "Nessuno".



I Servizi Internet hanno anche degli strumenti per gestire le liste di connessioni messe in quarantena (blackholed connections). Nel riquadro Controllo del Monitor dei Servizi Internet c'è una sezione denominata Connessioni congelate (Blackholed connections) contenente i bottoni Log e Svuota (Flush) e una barra grafica che mostra il numero di connessioni mantenute in quarantena (blackholed). Gli indirizzi IP vengono inseriti nella lista di quarantena solo se rispondono ad uno dei criteri indicati nella sezione Connessioni (Basic Internet Setup).

Connessioni congelate (blackholed)

Cliccando sul bottone Log, è possibile avere una lista degli indirizzi IP messi in quarantena, con l'indicazione del tempo trascorso da quando vi sono stati messi, e il tempo che deve trascorrere perchè vengano "rimessi in libertà" da parte del sistema. Se vi è il sospetto che gli indirizzi IP siano stati messi in quarantena in modo incorretto, si può cliccare il bottone Svuota (Flush) per rimuovere tutti gli elementi dalla lista delle connessioni congelate.

Prevenire il passaggio (relay) di mail non autorizzato

Il servizio di relay (far ponte) della posta SMTP interviene quando i Servizi Internet ricevono una mail via SMTP che non è destinata ad un utente del vostro sistema FirstClass. In questo caso, i Servizi Internet accettano il messaggio e lo passano poi, via SMTP, ad un altro server SMTP da qualche parte in Internet.

Se vi sono problemi con la trasmissione SMTP sul tuo sistema, è possibile disabilitare completamente questa funzione dal riquadro "Fare Ponte" (Relay), posizionato nel quadro UCE/Spam del Basic Internet Setup. Adesso, questo riquadro contiene un solo checkbox "Disabilita tutti i relay, inclusi i relay SMTP AUTH e gli IP abilitati" (Disable all relaying, including SMTP AUTH and trusted IPs), che è di fatto il grande interruttore per disabilitare tutte le trasmissioni SMTP che passano facendo relay attraverso i Servizi Internet.

Su come gestire la questione del permettere o meno l'attività di relay via SMTP vi sono tipicamente tre scenari di fondo:

- il vostro sito non ha bisogno di permettere di fare relay;

- il vostro sito ha bisogno di permettere il relay per gli utenti POP3 o IMAP4

- il vostro sito ha bisogno di agire come Internet contact point per un gruppo di server SMTP.

Il vostro sito non ha bisogno di permettere di fare relay

Se il tuo sito non deve permettere di fare relay per la posta SMTP, dovresti selezionare l'opzione "Disabilita tutti i relay, inclusi i relay SMTP AUTH e gli IP abilitati" (Disable all relaying, including SMTP AUTH and trusted IPs), nel riquadro Fare Ponte (Relay) del quadro UCE/Spam del Basic Internet Setup.

Riquadro Fare Ponte (Relay)

Dopo aver selezionato questa opzione, apri il Monitor dei Servizi Internet/Controllo e clicca sul bottone Ricarica Configurazione o riavvia i Servizi Internet.

Questo setup è facile da amministrare ed estremamente sicuro, visto che il tuo sistema non permette assolutamente scambi SMTP. Se è possibile, è consigliato utilizzare questa configurazione.

Il vostro sito ha bisogno di fare relay per utenti POP3 o IMAP4
Se c'è bisogno di supportare utenti POP3 e IMAP4 che spediscono mail all'esterno della vostra organizzazione, allora raccomandiamo di usare la funzione di SMTP AUHT, un'estensione del protocollo SMTP. Questa estensione sta a significare che se un server vuole fare relay per delle mail fuori dal vostro server SMTP, deve prima qualificarsi fornendo delle credenziali (user ID ed autenticazione password) così che possa essere verificato che non è uno spammer. A meno che non si abbia esplicitamente disabilitato ogni relay, i Servizi Internet permetteranno il relay sul server SMTP a coloro che avranno fornito queste credenziali. Nelle vecchie versioni dei Servizi Internet bisognava configurare quali funzioni dovessero avere gli utenti per poter usare questa funzione. In FirstClass 8.0, abbiamo sostituito questa opzione con la nuova funzionalità a livello di server "Abilita il relay di posta" che può essere definita per singolo gruppo utente.

Abilita il relay di posta

Questa caratteristica ha effetto appena il form è chiuso sul server. Ti raccomandiamo di creare un gruppo di privilegi utente esplicitamente per i tuoi utenti POP3 e IMAP4.

Il tuo sito ha bisogno di agire come Internet contact point per un gruppo di server SMTP

Se questa è la situazione si potrebbe non poter utilizzare l' SMTP AUTH a causa del software del server SMTP usato dai server di connessione. Per questa ragione (e per garantire il supporto dei software legacy, cioè vecchi ma ancora usati), è possibile configurare i Servizi Internet perchè utilizzino elenchi di indirizzi IP fidati contenuti nei documenti di filtro della cartella Filters. Se un indirizzo è in un documento filtro di IP fidato, i Servizi Internet permetteranno il relay della posta SMTP.

Questo setup è abbastanza sicuro (il mascheramento del numero di IP è abbastanza difficile) ma potrebbe richiedere una notevole impegno se ci fossero un numero abbastanza largo di numeri e di indirizzi fidati da mantenere. Sii prudente quando crei il tuo documento filtro, attenzione agli errori, l'inserimento di un indirizzo IP o di maschera IP sbagliato può far sì che il vostro sistema sia usato come testa di ponte per trasmettere spam.

Per configurare un indirizzo IP fidato a cui viene permesso di fare relay:

1 Apri la cartella Filtri nella cartella Servizi Internet sul Desktop dell'amministratore.

2 Crea un documento FirstClass nella tua cartella Filtri elencando gli indirizzi IP fidati (usando il formato presentato negli esempi)

Per semplicità, ti raccomandiamo di nominare il tuo documento filtro con un nome del tipo IPs Fidati. Altri Indirizzi IP fidati possono essere registrati in altri documenti, tenendoli in documenti separati è più facile mantenerli.

3 Chiudi il documento.

4 Apri il Monitor dei Servizi Internet e clicca sul bottone Ricarica Configurazione o riavvia i Servizi Internet dopo ogni cambiamento.

Come deve essere scritto un documento Filtri

Le voci relativi agli IP "fidati" possono essere scritte in una delle seguenti tre forme. Occorre premettere ad ogni linea che contiene degli IP affidabili in ingresso un segno più (+).

- un singolo indirizzo IP (preceduto da un '+') per linea
- una maschera IP (preceduta da un '+') che può rendere fidati gruppi di indirizzi IP simili
- un intervallo di di numeri IP (preceduto da un '+'), con il quale si indicherà che gli IP compresi tra un valore x ed un valore y sono fidati.

Ecco un esempio:
Questo è un documento di IP Fidati contenente gli indirizzi IP per i quali permettiamo il relay:

Tabella 4

+111.222.111.222	l'indirizzo IP 111.222.111.222 viene dichiarato affidabile
+111.*.*.*	una maschera - così viene dichiarato affidabile ogni indirizzo IP che inizia con 111.
+111.222.111.200.-111.222.111.222	un intervallo - tutti gli indirizzi IP dal 111.222.111.200 al 111.222.111.223 incluso sono dichiarati affidabili
+111/112.222/223.111/115.223/255	un intervallo espresso in modo alternativo - sono dichiarati affidabili gli indirizzi IP dal 111.222.111.223 al 112.223.115.255 incluso
+111.222.112.223/255	un altro intervallo espresso in modo diverso - sono dichiarati affidabili gli indirizzi IP dal 111.222.112.223 al 111.222.112.255 incluso

Gli indirizzi IP fidati non tengono conto degli indirizzi IP bloccati. Se si desidera bloccare un gruppo di indirizzi IP ma accettare il relay da un singolo IP all'interno del gruppo, si potrebbe inserire questa sintassi nel documento filtro:

Questa definizione blocca un gruppo di numeri IP, pur dichiarando affidabile uno di essi:

Tabella 5

111.*.*.*	una maschera IP - questa riga blocca ogni indirizzo IP che comincia col 111. ...
+111.222.111.222	... ecceto che per questo! Questa linea dice che questo indirizzo IP (111.222.111.222) è affidabile anche se i vicini sono dei cattivi ragazzi

Cosa succede se vengo inlcuso in una blacklist come un server aperto al relay?

C'è un certo numero di organizzazioni (inclusi i fornitori del servizio di RBL) che identificano in modo aggressivo i siti che permettono il relay aggiungendoli alle loro blacklist. Se il vostro sito viene incluso in una blacklist, ecco cosa è possibile fare:

• controllare il settaggio del tuo relay

Probabilmente sei stato segnalato perchè dal tuo sito proviene dello spam. Previeni la cosa con i metodi indicati in "Previeni il relay delle mail non autorizzate" e cerca di isolare il problema. Se non riesci a localizzare il problema, rivolgiti all'organizzazione che ha identificato il tuo relay e chiedi il loro aiuto.

• chiedere all'organizzazione che ha identificato il relay di testare nuovamente il tuo sito dopo aver localizzato e risolto il problema di relay.

Ci sono alcune organizzazioni (per esempio, 0RBS) che usano test di relay automatici non corretti che identificano ogni server di posta come fosse il programma unix "SendMail" e partono dal presupposto che ogni server si comporti nella stessa maniera di SendMail. Se avete il relay bloccato e tuttavia non riuscite a passare i loro test, sono possibili ancora alcune opzioni:

• riconfigurare Servizi Internet affinchè funzionino in maniera più simile a SendMail

Il problema principale con questo tipo di test è che i Servizi Internet assorbono alcuni tentativi di fare relay come se intendessero effettivamente consegnare il messaggio, pur spedendo successivamente una NDN (Non Delivery Note). Dal momento che i test non attendono l'invio successivo della NDN pensano che il tentativo di fare relay abbia funzionato. Scegliendo la voce "Solo Alias" nell'indirizzamento della mail in entrata, nel riquadro Advanced Directory collocato nella cartella degli Servizi Internet del Desktop dell'amministratore, i Servizi Internet vengono forzati a rifiutare questi sforzi

Ricorda: l'uso di questa tattica ti costringerà a definire un alias (o attivare il setup automatico degli alias) per tutti i tuoi utenti mail su internet.

• E' possibile informare l'organizzazione che vi ha messo nella blacklist che il vostro server non permette il relay, chiedendo loro di provare direttamente ad effettuare il relay verso qualche destinazione esterna attraverso il vostro server. Le organizzazioni migliori rispondono ragionevolmente a questa richiesta.

• Provate a convincere i siti con cui scambiate le vostre email a non usare dei servizi di black list non adeguati e datati.

WebKit per creare pagine web professionali con FirstClass

Mario Quagliana, Servizi LAN sas, Milano

WebKit è un'applicazione sviluppata per l'ambiente FirsClass con lo scopo di semplificare e guidare lo sviluppo di siti internet per la pubblicazione di contenuti, uno strumento per creare pagine web professionali.

WebKit è rivolto agli Amministratori di server FirstClass versione 7.1 o superiore, che intendono dare ai propri utenti la possibilità di creare con il clent FirstClass pagine web altamente personalizzabili e con un'aspetto professionale, gradevole e senza la necessità di conoscere il codice HTML.

WebKit è un prodotto per server FirstClass sia su piattaforma Windows che Mac.

La pagina web sritta con WebKit è divisa in tre principali sezioni

1 - Intestazione
2 - corpo del documento
3 - pie pagina

Qui di seguito l'elenco delle principali funzioni.

INTESTAZIONE

1 Può essere inserita un'immagine (ad esempio il logo del sito) affiancata da una descrizione
2 la data odierna
3 una linea di separazione
4 un testo con entrata progressiva per attirare l'attenzione su uno specifico argomento
5 una barra degli strumenti
6 una barra di navigazione
7 una barra con bottoni
8 una barra con menu a cascata
9 un file esterno con codice HTML personalizzato

CORPO DEL DOCUMENTO

1 Può essere inserita una colonna di navigazione a sinistra o a destra e/o un file esterno con codice HTML personalizzato
2 una colonna con menu a cascata
3 opposta alla colonna di navigazione può essere inserita una colonna di descrizione e-o un file esterno con codice HTML personalizzato
4 al centro rimane il corpo del documento e se il documento contiene file-s allegati questi vengono elencati in fondo alla pagina.

PIE' PAGINA

1 Può essere inserita la data dell'ultima modica
2 un contatore di visite (solo per server su piattaforma win)
3 una pagina esterna con codice HTML personalizzato

Per ogni elemento inserito è possibile assegnare uno stile di testo, definendo valori personalizzati per il colore, il tipo di carattere, la dimensione.
In alternativa si possono sceglire dei valori predefiniti presi dalla configurazione del server dalla scheda "Global Site Preference" oppure ".sitepref" per ambienti multi-dominio.

Queste sono solo le principali caratteristiche, ma altre funzioni si possono attivare e disattivare, definendo per ognuna molti parametri personalizzabili oppure assegnare i valori predefiniti.

Con webKit vengono forniti anche dei templates personalizzati per il renderig web di calendari.

Alcuni link:

Screenshoots
http://webkit.sisint.net/webKitExsamples/WebKitGlobalELScreen
http://webkit.sisint.net/webKitExsamples/WebKitNAVScreen
http://webkit.sisint.net/webkitExsamples/WebKitDescriptionsScreen

Qualche esempio
http://webkit.sisint.net/webKitExsamples/calendarInBody
http://webkit.sisint.net/webKitExsamples/calendario2
http://webkit.sisint.net/esempiMara

Alcune pagine realizzate con WebKit
http://www.zassrl.com/azienda
http://www.zassrl.it/azienda
http://www.consedis.it
http://www.apobrusuglio.org
http://www.sistemintegratisrl.it
http://www.mediabellusco.it/clientdownloads
http://www.sisint.net

Per maggiori informazioni visita il sito http://webkit.sisint.net o contatta la nostra redazione

Le domande più frequenti

In questa rubrica i quesiti degli utenti FirstClass

Gli Internet Services vanno in sovraccarico quando troppi utenti cercano di accedere alla stessa homepage simultaneamente. Come posso evitarlo?

Devi aumentare il numero delle sessioni Internet, ecco come fare:

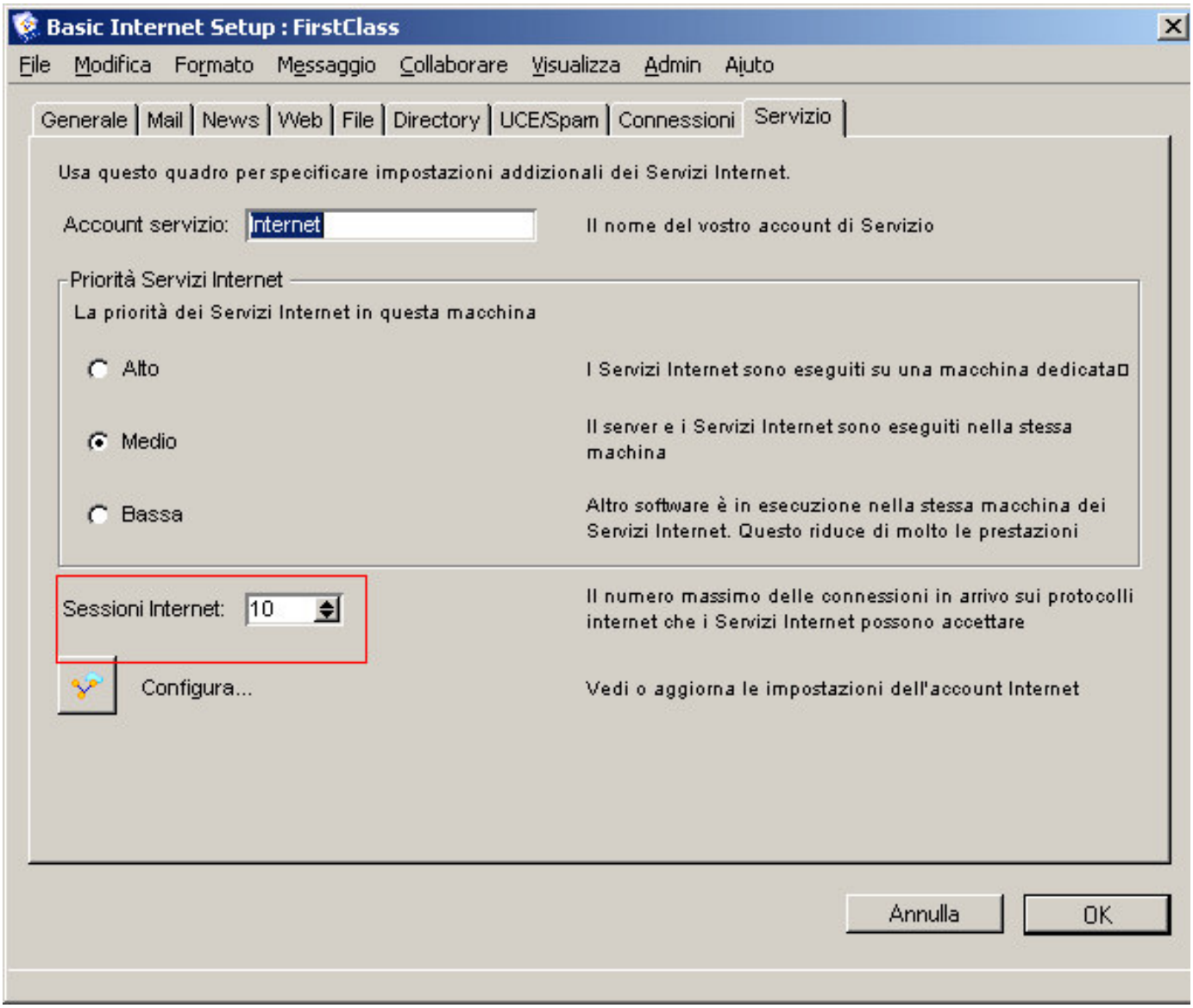
1 Apri la cartella Internet Services dal desktop dell'amministratore.

2 Apri Basic Internet Setup.

3 Clicca sulla tabella Service.

4 Aumenta il numero delle sessioni Internet che ti servono.

Sessioni Internet

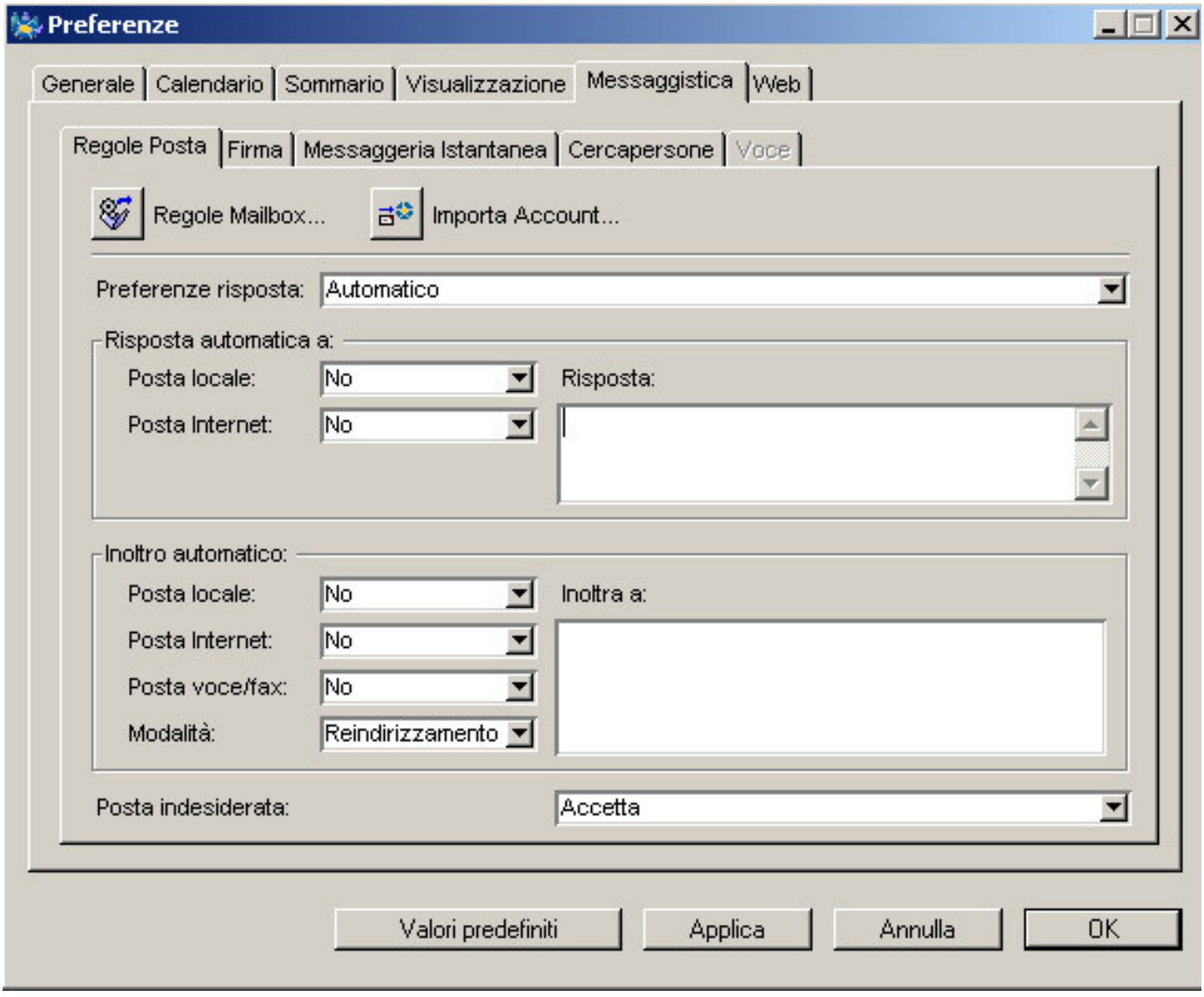


Posso inoltrare in automatico le mail in entrata dalla mia Mailbox su un altro account email esterno? Quale differenza c'è tra rispedire e inoltrare verso un indirizzo prescelto dall'utente?

Ecco i passaggi per configurare la tua Mailbox per rispedire o inoltrare le mail in entrata verso un altro account esterno di posta:

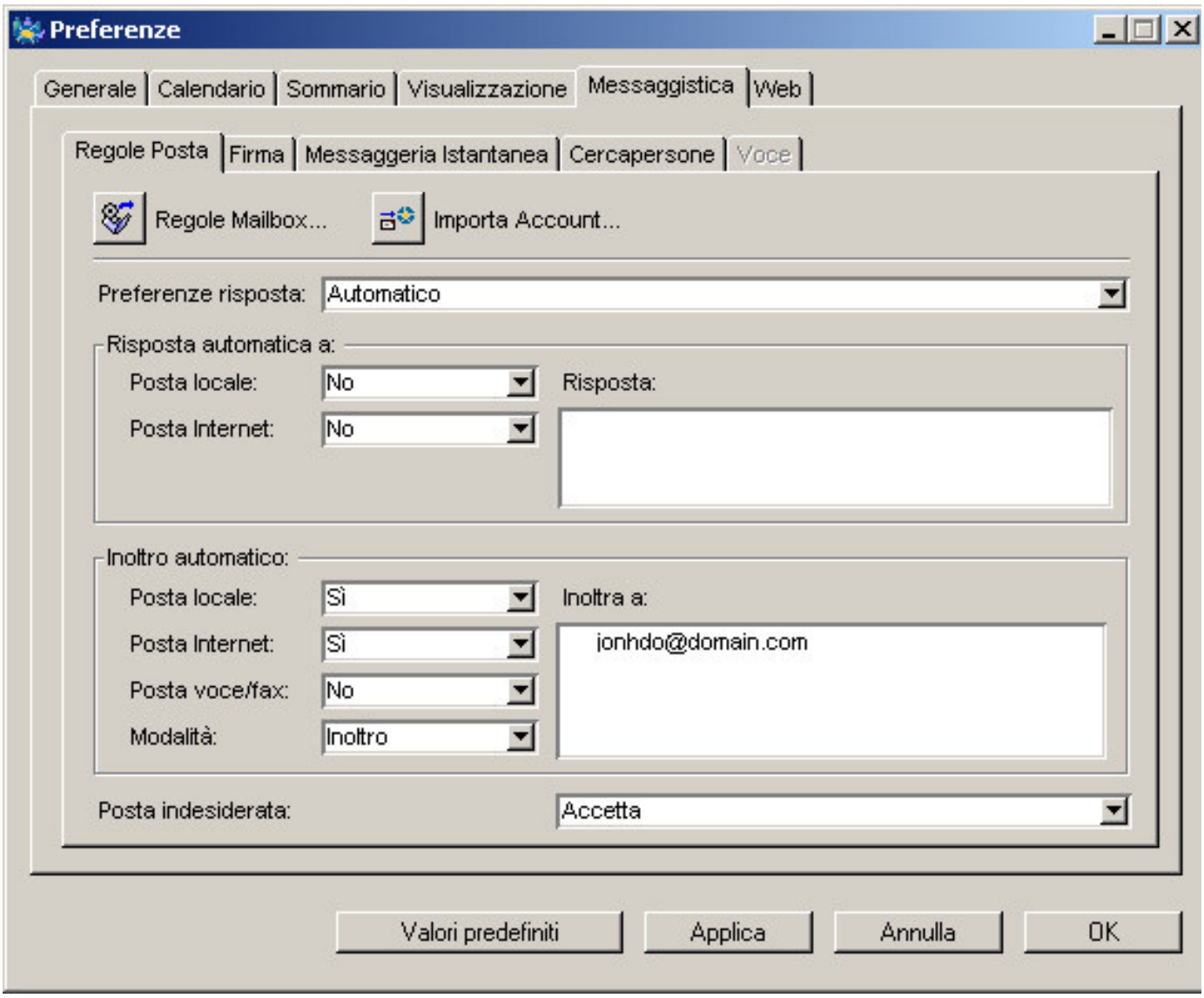
1 Dal tuo desktop, scegli Edit > Preferences > Messaging tab > Mail Rules tab. Dovresti vedere il quadro seguente:

Regole Posta



2 Sotto il forward automatico, configura la posta locale, la posta internet e i campi voce/fax per le tue preferenze.

Preferenze di forward



3 Sotto Metodi, scegli Redirect or Forward.

Forward (inoltra) significa che i messaggi ricevuti sembrano stati mandati dall'accont che ha fatto il forward. Invece Redirect (rispedire) significa che i messaggi ricevuti sembrano stati mandati dall'account iniziale, non da chi inolta. In entrambi i casi, rimane nella Mailbox di FirstClass una copia del messaggio spedito.

4 Scrivi il tuo indirizzo di posta esterna nel campo "Forward to:".

Quando guardo la mia pagina web, vedo le barre degli strumenti sulla sinistra e all'inizio della pagina. Posso toglierle?

Certo, ecco come fare.

1 Apri la tua cartella Home Page (in FirstClass 8.0 è chiamata My Web Site).

2 Scegli File > New > New Document Special > Personal Web Page. Con questo passaggio crei un nuovo file chiamato Personal Web Page.

3 Copia e incolla i contenuti della tua home page sulla nuova Personal Web Page.

4 Cancella la vecchia pagina .

5 Rinomina la Personal Web Page come Home Page.

Quando ricarichi la tua pagina web, non dovresti più vedere le barre degli strumenti di default.

Nel prossimo numero

Alcune anticipazioni dal prossimo numero

Prossimamente uscirà il secondo numero della nostra newsletter che porrà particolare attenzione alle nuove possibilità offerte agli amministratori FirstClass per la gestione del server.... ma non solo, conterrà nuove esperienze di utilizzo dell'ambiente, risposte alle vostre domande ed altro... a presto!!

Tra gli argomenti che verranno trattati:

- L'applicazione LOG ANALYZER
- Come gestire la difesa dagli attacchi sulla rete e dallo spamming in FirstClass 8
- seconda parte
- FirstClass e l'amministrazione pubblica: l'esempio della rete Onde di Desenzano sul Garda

CONTATTACI

La nostra redazione è a disposizione per fornire maggiori informazioni in merito ai contenuti della newsletter. Potete inoltre inviarci commenti, suggerimenti, domande o proposte per le prossime uscite.

Lo staff di redazione rimane in attesa delle vostre email all'indirizzo redazione@neol.it

Ricordiamo che è a vostra disposizione il sito http://www.neol.it

I nostri riferimenti telefonici e di fax sono:
tel. +00-39-049 7386590
fax +00-39-049 7397318

La redazione
Daniele Lincetto
Serena Schiaffini