CAPTIVE PORTAL AUTO DISCONNECTION

Di seguito sono descritte le impostazioni per eseguire la disconnessione automatica dal CAPTIVE PORTAL (eliminazione della regola di granting sul firewall del NAT) per le postazioni windows con accesso interattivo di tipo guest.

La procedura, eseguita in modalita' utente al logoff della sessione interattiva, invia al CAPTIVE PORTAL sottorichieste http(s) per:

- determinare i parametri di login e di autorizzazione all'accesso alla rete esterna;
- richiedere la disconnessione dalla rete pubblica/esterna.

Installando preventivamente WinExit, la piattaforma puo' essere configurara per il logoff automatico di sessione e di conseguenza per l'auto disconnect dallo stesso CAPTIVE PORTAL.

Procedure di setup-configurazione

- 1. Eseguire il login come utente amministratore
- 2. Copiare in %windir% (es: c:\Windows) i file: TinoLogout.exe e TinoLogout.ini
- 3. Installare nelle Autorita' di Certificazioni Attendibili del computer il certificato dell'INFN CA
 - eseguire il download del certificato (con I.Explorer) dal sito <u>https://security.fi.infn.it</u> cliccando sul pulsante 'Scarica Certificato' e salvando temporaneamente il file .cer sul desktop

Istruzioni

- Per l'installazione nel browser:
 - o premete il bottone "Scarica Certificato"
 - o salvate il certificato su disco usando il nome proposto per il download
 - o cliccate due volte sul file salvato e in base al sistema operativo impiegato apparirà una finestra di dialogo per l'installazione

In Internet Explorer/Windows seguite le istruzioni del gestore dei certificati scegliendo, quando proposto, l'opzione 'Seleziona automaticamente l'archivio'.

In Safari/Mac OS usando il gestore dei certificati "Keychain Access" aggiungete il certificato nel keychain "X509 Anchors"

• In alternativa il certificato è disponibile anche in formato PEM.

Scarica Certificato

- o aprire la console di management di windows tramite start/run: mmc.exe + INVIO
- eseguire il comando File/Aggiungi Rimuovi snap in
- o premere il pulsante 'Aggiungi' nella relativa finestra di dialogo
- o selezionare certificati e premere 'Aggiungi' nella seconda finestra di dialogo
- o selezionare 'Account del computer'

Console1						
File Azi	one Visualizza Pre	feriti Finestra ?				
File Azi ← → Min Direct	Aggiungi/Rimuovi snap-in Autonomo Estensinni Utilizzare questa nella console. Snap-in aggiunti Snap-in autonomi disponibili: Snap-in aggiunti Autonomi disponibili: Snap-in Analisi e configurazione della pr Avvisi e registri di prestazioni Cartella Cartella Cartella Controllo ActiveX		Snap-in certificati Lo snap-in gestirà sempre certificati per: Account dell'utente Account del servizio Account del computer			
	Descrizione	Descrizione La Gestione certificati consente di si certificati ad uso personale, oppure j	< Indietro Avanti > Annulla			
	Aggiungi	UK	Aggiungi Chiudi ///////////////////////////////////			

- cliccare su 'Avanti' e, lasciando selezionato il computer locale, cliccare su 'Fine' confermare cliccando rispettivamente su 'Chiudi' e quindi su 'OK' tramite tasto destro del mouse scegliere 'Importa' cliccando sui certificati delle autorita' attendibili selezionare il file del certificato preventivamente scaricato e cliccare su 'Avanti'

🚡 Console2					
File Azione Visualizza Preferiti Finestra ?					
🚡 Directory principale\Certificati (computer locale)\Autorità di certificazione fonti attendibili\Certificati					
Directory principale	Rilasciato a 🛛 🗠	Emesso da	Data scadenza 🤅		
🖻 💮 Certificati (computer locale)	GTE CyberTrust Root	GTE CyberTrust Root	24/02/2006 F		
		http://www.valicert.com/	26/06/2019 F		
Autorità di certificazione fonti a	attendib 🔛 http://www.valicert.com/	http://www.valicert.com/	26/06/2019 F		
	Importazione guidata certificati		X 9 F		
Accentabilità per l'organizzazion	File da importare		9 F		
🗄 📄 Autori attendibili	Specificare il file da importare.	E da Importare Spacificare il filo da importano			
庄 🔁 Certificati non attendibili	Specificare inflie da importare.	specificare il file da importare.			
🔁 📴 Autorità di certificazione princi			1		
Persone attendibili	Persone attendibili				
	C:\Documents and Settings\ro				
	C. (Docaments and Decangs)				
	Nota: è possibile memorizzare più certificati in un singolo file nei seguenti formati:				
	Scambio di informazioni personali - PKCS #12 (*.PFX, .P12)				
	Standard di sintassi dei mess	Standard di sintassi dei messaggi crittografati - Certificati PKCS #7 (.P7B) 0			
	Archivio certificati cerializzati Microsoft (* SST)				
		9			
			0 F		
			9 1		
		< Indietro Avanti >	Annulla 9 F		
	CERISTA SECURE Server CA	SIA SECURE SERVER CA	09/07/2019 F		
	📟 Swisskey Root CA	Swisskey Root CA	01/01/2016 F		
	Symantec Root CA	Symantec Root CA	01/05/2011		

- cliccare di nuovo su 'Avanti' e poi su 'Fine' verificare che il certificato sia stato importato e che nelle sue proprieta' siano abilitati tutti gli scopi

🚡 Console2					
File Azione Visualizza Preferiti Finestra ?					
Directory principale Directory principale Directory principale Oretificati (computer locale) Oretificati (computer locale) Oretificati (computer locale) Oretificati Oret	r locale) Autorità Rilasciato a A FINMT Clase 2 C GlobalSign Root GTE CyberTrust GTE CyberTrust GTE CyberTrust GTE CyberTrust Http://www.vali Http://www.vali Http://www.vali Http://www.vali Http://www.vali Http://www.vali Http://www.vali Http://www.vali Http://www.vali Http://www.vali NFN CA NFN CA NFN CA NetCock Express NetLock Express NetLock Kozjeg; NetLock Kozjeg; NetLock Kozjeg; NetLock Uzleti (No LIABILITY A PTT Post Root C Saunalahden Se Saunalahden Se Secure Server C SecureNet CA C SecureNet CA R SecureNet CA S SecureNet CA S SecureSign Roo	di certificazione fonti attendibili Certificati Proprietà - INFN CA Generale Certificati incrociati Nome: Descrizione: Scopi certificato Abilita tutti gli scopi per il certificato Abilita tutti gli scopi per il certificato Abilita solo i seguenti scopi Nota. È possibile modificare solo gli scopi certificato o percorso certificazione. Autenticazione server Autenticazione client Firma codice Posta elettronica protetta Timbro ora Elenco firme attendibili Microsoft Timestamp Microsoft	Sourcestriit dal		
	🔤 Securesign Rooti	LAZ SECURESIGN ROOCLAZ	15/09/2020 P0		

- 4. Impostazioni per l'esecuzione automatica al logoff della sessione interattiva
 - da start/run digitare gpedit.msc + INVIO 0
 - 0
 - 0
 - doppio click su Configurazione utente/Impostazioni di windows/script accesso-fine sessione/uscita nella finestra di definizione del criterio cliccare su 'Aggiungi' digitare il nome dello script: TinoLogout.exe (il path non e' necesserio se lo script e' installato in 0 %systemroot%)
 - confermare cliccando 2 volte su OK e chiudere la console dei criteri 0

🚡 Criterio gruppo						
File Azione Visualizza ?			Proprietà	- Uscita		<u>? ×</u>
			Script			
Criteri Computer locale	Script (Accesso/Fine sessione)					
Impostazioni del software Impostazioni di Windows	Uscita	Nome		Uscita script per Computer	r locale	
Modelli amministrativi	Visualizza <u>Proprietà</u>	Uscita Modifica	script		<u>?×</u>	
Impostazioni del software	Descrizione: Contiene di script di disconnessione	Nome so	ript:			Su
Script (Accesso/Fine se:	dell'utente.	TinoLog	out.exe		Sfoglia	Giù
 Impostazioni protezione Manutenzione di Interni 		Paramet	i script:			
						Aggiungi
				ок	Annulla	Modifica
						Rimuovi
			Per visu pulsante	ualizzare i file di script archiviati e sequente.	nell'oggetto Criteri gi	ruppo, premere il
			Vis	sualizza file		
				OK	. Annulla	Applica

File di configurazione

Nella stesso folder dell'applicazione deve risiedere il file TinoLogout.ini. Il file definisce i seguenti 4 parametri:

- LogoutURL: url relativa alla sottorichiesta http(s) per la disconnessione del client dal NAT
- StatusURL: ulr relativa alla sottorichiesta http(s) per determinare lo stato corrente di connessione
- UserFieldMask: segnaposto per individuare la username di connessione nella pagina html di risposta alla richiesta di stato: deve assumere la forma <TAG>x</TAG> assumendo che vi sia al piu' una sola occorrenza di <TAG> nella pagina
- StatusToDo: se impostato a yes l'applicazione esegue il controllo dello stato di connessione eseguendo la sottorichiesta alla url definita da StatusURL.

I paramentri sono dichiarati, ciascuno in una riga dedicata, nella forma nomeparametro = valore Per i commenti occorre anteporre il carattere ';'

Logging

TinoLogout genera eventi di sistema nel Registro Applicazione su tre livelli di severita' (informazione, avviso, errore). A ciascun evento e' associato uno specifico ID determinato come segue:

ID = 1000: l'esecuzione e' interrotta a causa di un errore di inizializzazione ovvero di I/O del file di configurazione
 ID<>1000: sono utilizzati 4 bit per la determinazione del codice di evento secondo la seguente tabella

Bit	Valori	Peso	Descrizione evento	Note		
0	0	0	Il client e' riuscito ad inviare la richiesta https per	Non viene eseguito riscontro sull'esito della		
			la disconnessione del client	richiesta di disaconnessione		
	1	1	Il client non e' riuscito a contattare il CAPTIVE	_		
			PORTAL per inviare la richiesta di disconnessione			
1	0	0	Le impostazioni di configurazione non richiedono	l successivi hit sono posti a zero		
			di tracciare i parametri di connessione			
	1	2	Prima della disconnessione viene verificato lo	L'esito della richiesta e' fornito dai successivi		
			stato e i parametri di connessione	bit		
2		0	Il client e' riuscito ad inviare la richiesta per	Ottiene la pagina che contiene		
	0			eventualmente la username dell'utente		
				autorizzato all'accesso oltre il NAT		
				L'esito della richiesta e' determinato dal bit		
				SUCCESSIVO		
	1	4	Il client non e' riuscito a contattare il CAPTIVE	Il bit successivo e' zero		
			PORTAL per ottenere lo stato di connessione			
3	0	0	E' stato individuata con successo la username	-		
			autorizzata sul NA I			
	1	8		Nessun utente era connesso al momento		
			Non e' stato possibile determinare la username autorizzata dal NAT	dell'esecuzione dello script		
				ovvero		
		· ·		si e' verificato un errore/inconsistenza nel		
				flusso di risposta secondo I meta forniti nel		
				file di configurazione		

Sono tracciati I seguenti parametri di connessione:

- nome netbios delle piattaforma machine name
- indirizzi IP assegnati a tutte le interfacce con stack TCP/IP abilitato
- username@domain dell'utente che esegue la sessione di login interattivo
- username dell'utente connesso/autorizzato ad uscire sulla rete pubblica tramite CAPTIVE PORTAL

Nunzio AMANZI – LNF INFN Computing Service Luglio 2007