# Controllo degli accessi

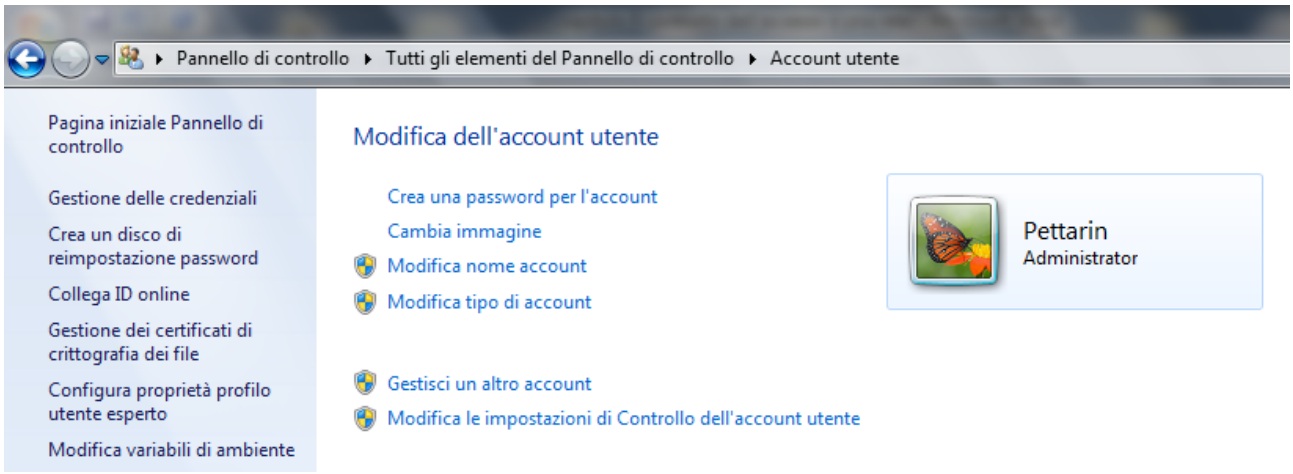
## Regolare gli accessi alla rete

Nella gestione di una rete è fondamentale che l'amministratore regoli e controlli gli accessi alle informazioni e alle risorse della stessa da parte degli utenti: per due motivi:

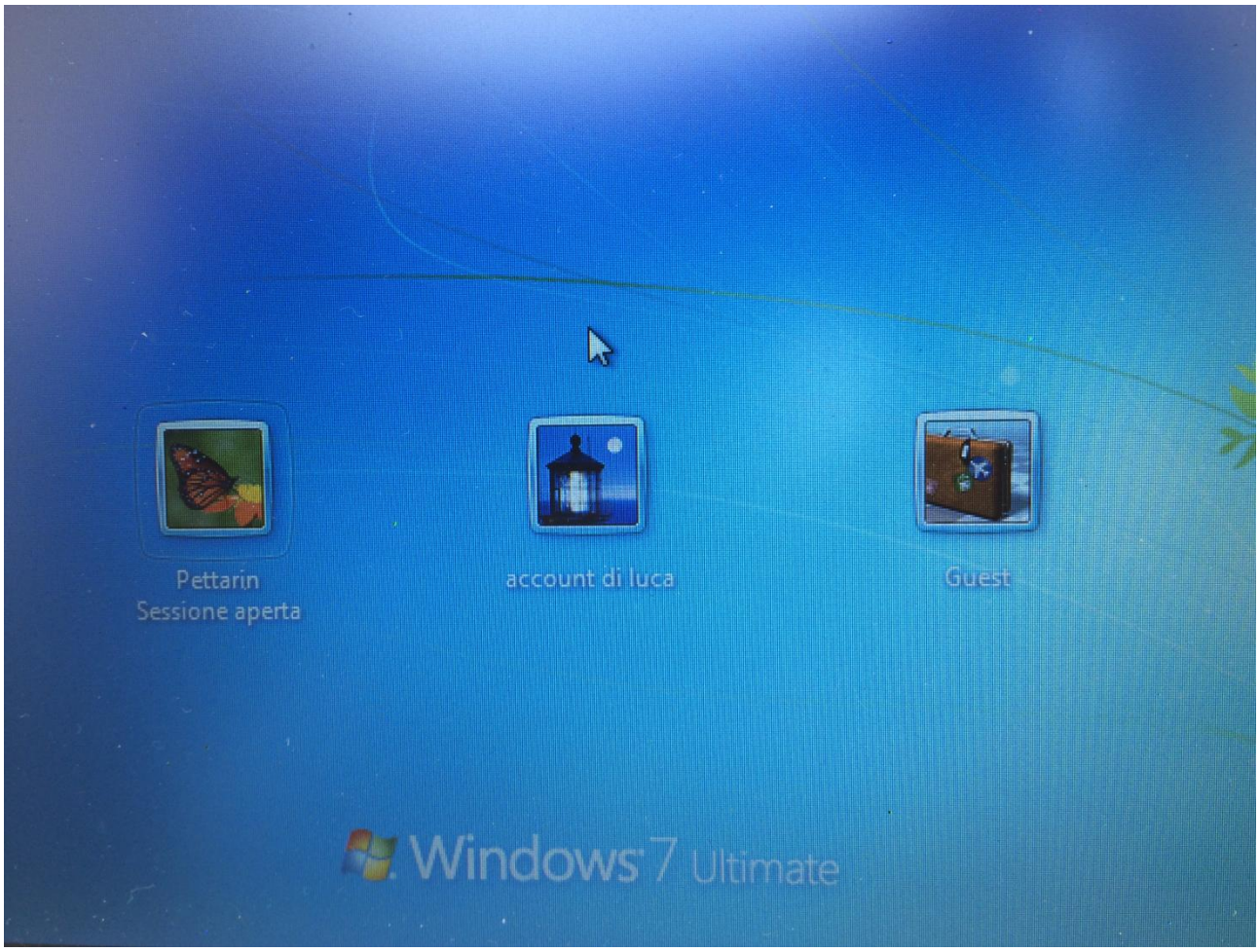
1. controllare che l'accesso avvenga solo da parte di utenti autorizzati;
2. regolare l'utilizzo delle risorse e delle informazioni presenti nella rete a seconda dell'utente.

### Account di rete

Abbiamo accennato come l'amministrazione di rete implichi responsabilità maggiori rispetto alla semplice installazione e risoluzione dei problemi hardware. In particolare, una volta che l'hardware è installato e configurato, l'amministratore deve verificare che gli utenti possano accedere alle risorse che sono autorizzati a utilizzare.
È quindi necessario che ciascun utente di una rete sia in possesso di un **account di rete**: sono delle credenziali personali (nome utente e password) che permettono all'utente di accedere alla rete e utilizzare le risorse che l'amministratore ritiene opportuno concedergli.
L'accesso a un account è un processo chiamato *login* (o *logon*): è una procedura di riconoscimento, detta autenticazione, dove sono richieste le credenziali d'accesso, il nome utente (*username*) e la *password* (parola d'ordine).
Lo username dovrebbe consentire un riconoscimento del tipo di utente: amministratore, ospite (guest), segreteria, ecc. Lo username, può essere noto a tutti ed è sempre noto all'amministratore del sistema. La password, invece, è un'informazione rigorosamente attribuita al possesso dell'utente, che ne è unico responsabile.
I sistemi Windows sono multiutente: consentono di creare e gestire diversi account Windows sulla stessa macchina, ognuno di essi accederà al sistema a mezzo delle credenziali.
Per creare, modificare o cancellare un account utente in Windows, nel **Pannello di Controllo** si seleziona **Account Utente**.




Attraverso un Wizard si può procedere alla creazione e gestione di ogni account presente nella macchina.
L'account di livello più elevato è **Administrator**: con questo account si può eseguire qualsiasi operazione sul computer o sulla rete: cambiare e modificare password, installare e disinstallare programmi, aprire e modificare qualsiasi file o cartella, cancellare o creare altri account. In Windows deve essere presente almeno un'utente con permessi d'amministratore.
Quello a livello più basso è **Guest**: per questo account non è prevista la password e consente l'accesso solo temporaneo ad ospiti.



L'accesso alla rete dipende dalla sua architettura. Ci possono essere reti di tipo **paritetico** dove non ci sono server sulla rete. Ogni computer funge contemporaneamente da client e da server e tutti i computer svolgono funzioni simili. L'autenticazione degli utenti avviene a livello locale: è il caso di piccoli uffici dove ogni pc è autosufficiente, dotato di propria stampante e di ogni altro dispositivo necessario. L'addetto al computer è sia amministratore che utente.
Nelle reti **client/server** il *server*, cioè il computer che offre le proprie potenzialità a tutti gli altri computer (*client*) connessi alla rete, gestisce l'autenticazione degli utenti su tutti i client e centralizza i permessi di accesso alle risorse di tutta la rete.

## Politiche per la scelta e la gestione delle password

Scegliere una password adeguata alla sicurezza informatica richiesta è importantissimo. Una password "robusta" è il migliore strumento per proteggere le informazioni personali. Per quanto ci possa sembrare sicura e impenetrabile, ci sono diversi sistemi a disposizione per forzare una password:

1. **un attacco "a forza bruta" (brute-force)**: mediante software che tentano di risalire a una password provando tutte le combinazioni possibili oppure con un attacco "a dizionario", utilizzando un elenco di termini usuali;
2. **tecniche di phishing o di "ingegneria del sociale"**; questi sistemi utilizzano soprattutto messaggi di posta elettronica fasulli o messaggi istantanei, ma anche contatti telefonici, che ingannano l'utente portandolo a rivelare i propri dati personali;
3. **installare programmi in grado di trafugare informazioni**: per prevenire questo tipo di attacchi può servire un buon antivirus e un firewall.

Come abbiamo già detto, per avere delle minime caratteristiche di sicurezza, una password:

1. deve essere piuttosto lunga e dovrebbe contenere non meno di 8 o 10 caratteri. La lunghezza ideale è dai 14 caratteri in su;
2. deve contenere una serie di numeri, lettere (maiuscole e minuscole), e magari caratteri diversi tipo # @. Un eventuale attacco brute-force dovrebbe provare un grande numero di combinazioni;
3. non utilizzare la data di nascita, la targa dell'auto, il numero del cellulare o qualunque altro dato personale facilmente individuabile;
4. non inserire una serie di numeri o caratteri ripetuti o composte da lettere (e numeri) che nella tastiera sono vicine;
5. non utilizzare la stessa password per più account;
6. modificare periodicamente la password: comunque la complessità della password garantisce la sicurezza nel tempo. Una password con 14 o più caratteri può essere utilizzata per molti anni.

## Tecniche di sicurezza biometriche

In alcuni casi, al posto delle password, per accedere al computer in modo sicuro vengono utilizzati dei sistemi che si basano su **tecniche biometriche**: sono delle tecniche che permettono di identificare una persona sulla base di una o più caratteristiche fisiche.
Le tecniche biometriche più comuni sono:

1. **riconoscimento vocale**: il riconoscimento della voce è una delle tecniche biometriche più utilizzate. Si rileva il timbro, la tonalità e la velocità con cui si parla;

2. **lettore impronte digitali**: un lettore di impronte digitali riesce a diversificare le diverse impronti umane che sono tutte una diversa dall'altra. Questa tecnologia è già presente in diversi computer portatili, cellulari, ecc.;


3. **scansione dell'iride dell'occhio**: questi sistemi di controllo funzionano tramite la lettura ed il riconoscimento dell'iride umana. Una speciale telecamera, in un paio di secondi, fa la scansione dell'iride. Dopo aver fotografato l'occhio, il sistema elabora le possibili variazioni dovute alla luce e salva l'immagine digitale in un apposito database. In seguito l'utente dovrà soltanto guardare nella stessa telecamera e il controllo dell'iride avverrà in meno di un secondo. I costi di questa tecnologia sono ancora abbastanza elevati.