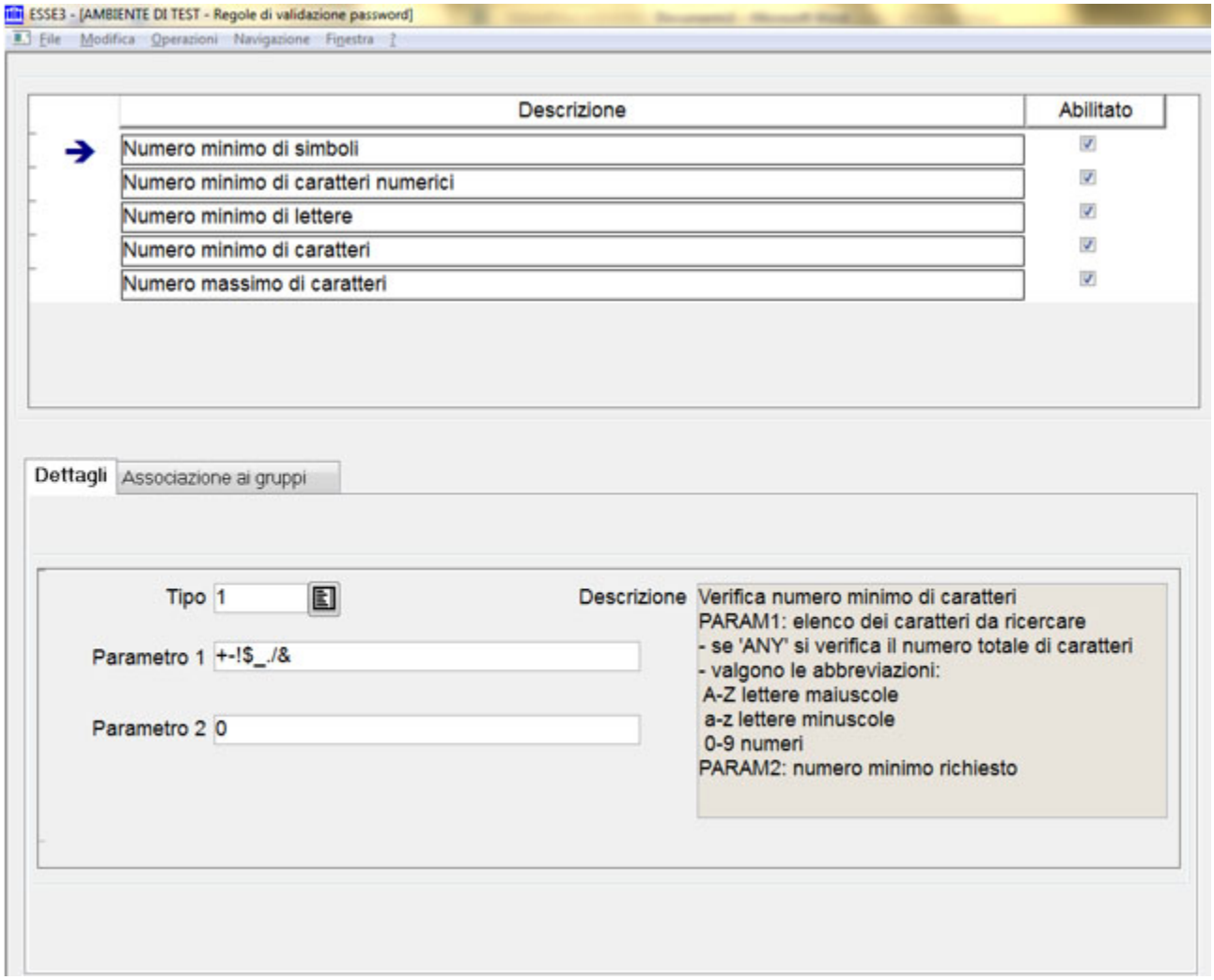
Regole di validazione password

Tramite la maschera è possibile definire tutte le regole di validazione delle password.

Nella sezione in alto si definisce la testata della regola con la possibilità di abilitarla o meno in qualsiasi momento. Si consiglia di definire una descrizione della regola che possa descriverne al meglio la logica, la stessa descrizione apparirà nel processo web di scelta della password.

Per ogni regola creata occorre definire la logica della regola utilizzando la sezione *Dettagli*.



Di seguito le tipologie di regole possibili

TIPO 1: Verifica numero minimo di caratteri (MIN)

La regola analizza il numero dei caratteri specificati:

- Parametro1 - valori possibili:
  - 'ANY' verifica il numero totale di caratteri
  - A-Z verifica il numero di lettere maiuscole
  - a-z verifica il numero di lettere minuscole
  - A-Za-z verifica il numero di lettere (senza distinzione maiuscole e minuscole)
  - 0-9 verifica il numero di caratteri numerici
- Parametro 2: indica il numero minimo richiesto dei valori definiti in Parametro1

***Nota**: se non si vuole porre un limite al numero di caratteri ed è indifferente che questi vengano utilizzati o meno, basta valorizzare Parametro2=0 (che significa numero minimo di caratteri 0 - non c'è un minimo)*

TIPO 2: Verifica numero massimo di caratteri (MAX)

La regola analizza il numero dei caratteri specificati:

- Parametro1 - valori possibili:
  - 'ANY' verifica il numero totale di caratteri
  - A-Z verifica il numero di lettere maiuscole
  - a-z verifica il numero di lettere minuscole
  - A-Za-z verifica il numero di lettere (senza distinzione maiuscole e minuscole)
  - 0-9 verifica il numero di caratteri numerici
- Parametro 2: indica il numero minimo richiesto dei valori definiti in Parametro1

***Nota**: se si voglio escludere dei caratteri, basta valorizzare Parametro2 =0 (che significa numero massimi di caratteri: 0)*

TIPO 3: Verifica non congruenza con nome utente (USER_ID)

La regola analizza il numero dei caratteri specificati:

- Parametro1 - lunghezza minima della sottostringa del nome utente che NON deve essere presente nella password
- Parametro2: specificare '1' se la verifica deve essere case insensitive

TIPO 4: Verifica non congruenza con nome persona (NOME)

La regola analizza il numero dei caratteri specificati:

- Parametro1 - lunghezza minima della sottostringa del nome persona che NON deve essere presente nella password

TIPO 5: Verifica non congruenza con cognome persona (COGNOME)

La regola analizza il numero dei caratteri specificati:

- Parametro1 - lunghezza minima della sottostringa del cognome persona che NON deve essere presente nella password

TIPO 6: Verifica non esistenza di caratteri uguali consecutivi

La regola analizza il numero dei caratteri specificati:

- Parametro1: indica il numero (minimo) di caratteri uguali consecutivi da verificare.

Es. Se parametro1= 2, le password come *a**TT**ore, Test**22, 00**_testpwd* non saranno accettate (a prescindere se i caratteri uguali consecutivi sono all'inizio, nel mezzo o alla fine).
Es. Se parametro1= 3, la password ***AAA**cercasi* non sarà accettata

Regole per password generate automaticamente dal sistema

Quando la password viene generata "random" dal sistema (es. alla prima creazione se non la sceglie l'utente e se i parametri PWD_RIGEN e RECUPERA_PWD_RIGEN sono abilitati), Esse3 basa le sue logiche per creare la password con i seguenti parametri di configurazione (PAR_CONF). pertanto è bene che le regole validazione descritte in precedenza e le logiche definite nei parametri rispondano alla stessa logica:

PWD_MIN_LENGTH : Indica la lunghezza minima che deve avere la password. (Qualora sia uguale a 0 significa che può anche essere nulla)

PWD_MAX_LENGTH: Indica la lunghezza massima che deve avere la password. (Qualora sia uguale a 0 significa che non vi è limite superiore)

PWD_GEN_SPECIAL_CHARS: Caratteri speciali utilizzati in fase di generazione automatica delle password. (VAL_ALFA = stringa con tutti i caratteri speciali (non alfanumerici) utilizzati)

PWD_CHAR_REQ: Formato per generazione casuale password (Il formato del parametro e' **C**x**N**y**S**z, le password generate casualmente avranno x lettere (caratteri alfabetici), y numeri e z simboli speciali; se la lunghezza totale risulta inferiore a 8 caratteri verranno aggiunte lettere per raggiungere tale quota

PWD_AUTO_FORMAT: Indica la gestione Upper, Lower o Mixed Case della password generata in automatico da Esse3. (Se impostato a U, le password generate in automatico alla creazione dell`utente saranno sempre con lettere maiuscole, se impostato a L saranno sempre in minuscolo, se impostate a M, potranno essere indistintamente maiuscole o minuscole.)

NOTA IMPORTANTE: *si consiglia vivamente di configurare le regole affinché non sia mai possibile utilizzare il carattere | (pipe) nelle password, potrebbe generare dei problemi in alcuni processi.*