

B Handbuch

Dieses Handbuch beschreibt die Benutzung und einige Anwendungsfälle des Policy-Editors.

B.1 Start des Programms - Datei-Auswahl

Voraussetzung für den Start des Policy-Editors ist Java in der Version 1.6. Um den Policy-Editor zu starten, genügt ein Doppelklick auf die ausführbare Jar-Datei „Po-Ed.jar“. Auch ein Start über die Konsole ist möglich, mit dem Befehl „java -jar Po-Ed.jar“. Zum Programmstart bietet sich dem Nutzer das Bild wie in Abbildung B.1 dargestellt:

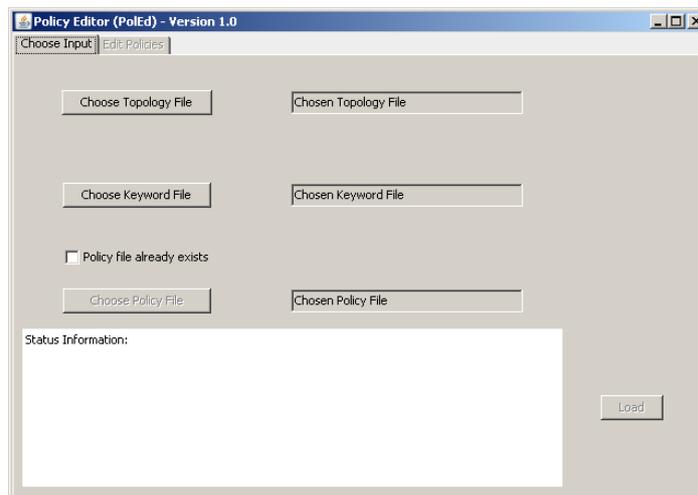


Abbildung B.1: Ansicht nach dem Öffnen des Policy-Editors

Zu beachten sind die deaktivierten Elemente „Load“-Knopf, sowie „Editor“-Reiter (siehe Abbildung B.2). Diese werden erst aktiviert, nachdem eine OWL-Netztopologie und eine Keyword-Datei (Reizwortkatalog) ausgewählt wurden.

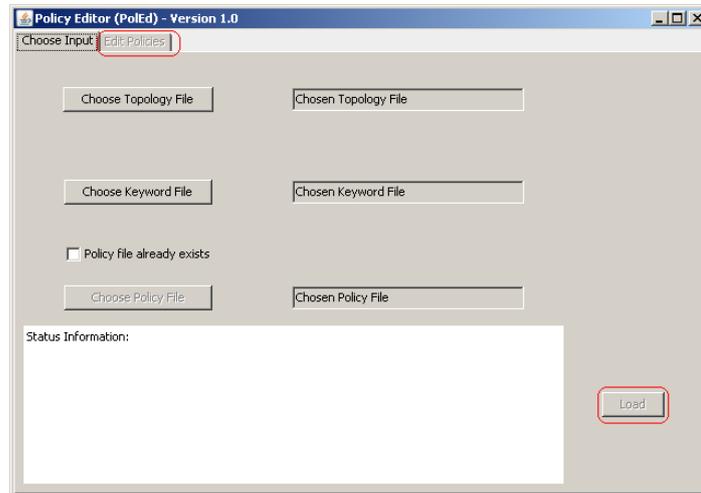


Abbildung B.2: Deaktivierte Elemente

Wählen Sie zunächst eine Topologie-Datei.

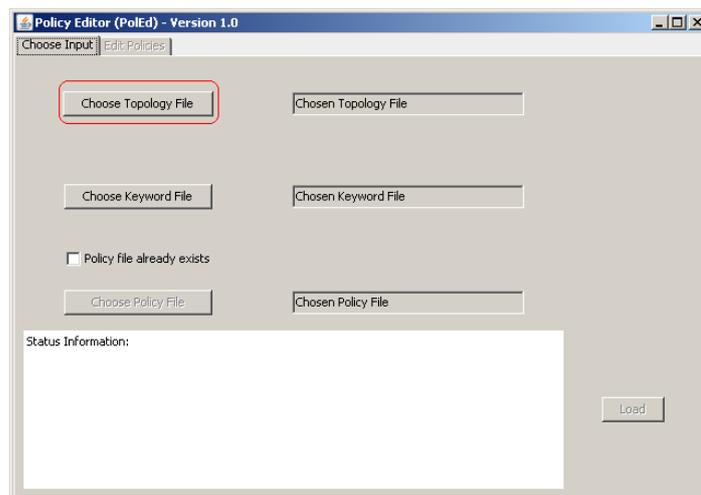


Abbildung B.3: Auswahl der Topologie

Nach Druck auf den „Choose Topology File“-Button öffnet sich ein Fenster zur Dateiauswahl. Beachten Sie, dass nur Dateien der Endung „owl“ zulässig sind.

B.1 Start des Programms - Datei-Auswahl

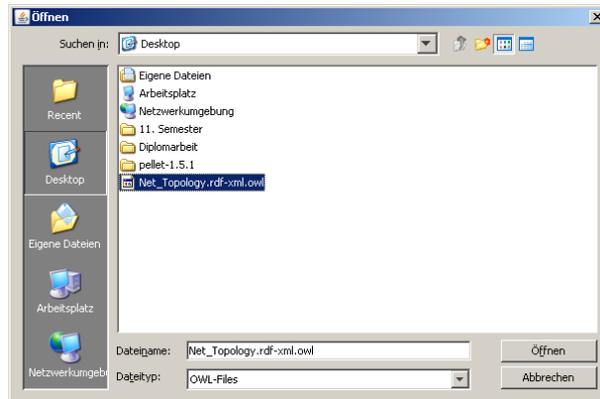


Abbildung B.4: Datei-Auswahl-Fenster

Nach Auswahl der Datei wird dies im Hauptfenster bestätigt, wie Abbildung B.5 zeigt.

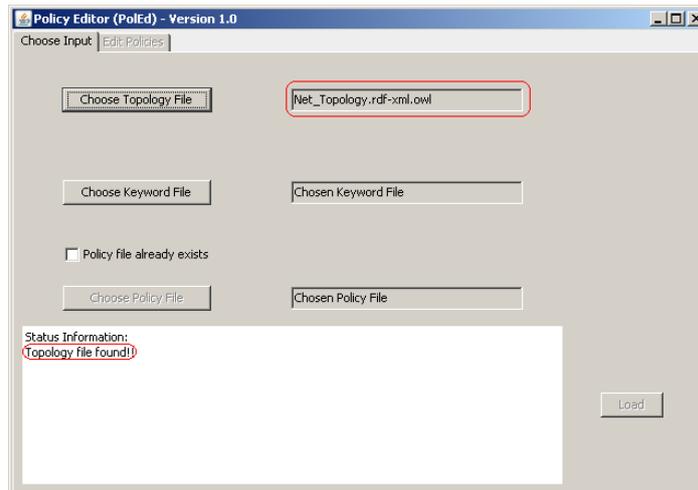


Abbildung B.5: Topologie ausgewählt

Die Auswahl des Reizwortkataloges erfolgt analog, wobei hier keine Einschränkung bezüglich der Dateierdung vorliegt. (Abbildung B.6) Beim Anlegen bzw. Ergänzen eines Reizwortkataloges achten Sie bitte auf die interne Formatierung gemäß dem Schema:

- Pro Zeile ein Reizwort [Leerzeichen] gefolgt vom zugehörigen Netzwerkgerät,
- als Trennung zwischen Device- und Main-Area mindestens ein „-“,
- Pro Zeile ein Reizwort [Leerzeichen] gefolgt von der zugehörigen Aktion bzw. dem maschinenverständlichen Konfigurationspendant.

B Handbuch

Ein Beispiel-Reizwortkatalog gestaltet sich wie folgt:

```
1 Webcam Router
2 Voip Gateway
3 Address Client
4 -Main-Keyword-Area-
5 clock time
6 time time
7 ip IP
8 address IP
9 users usercount
10 shutdown shutdown
11 priority priority
12 open port
13 close port
```

Ist ein Reizwortkatalog gewählt, wird dies vom Programm bestätigt. Ab jetzt lässt sich auch der „Load“-Button betätigen.

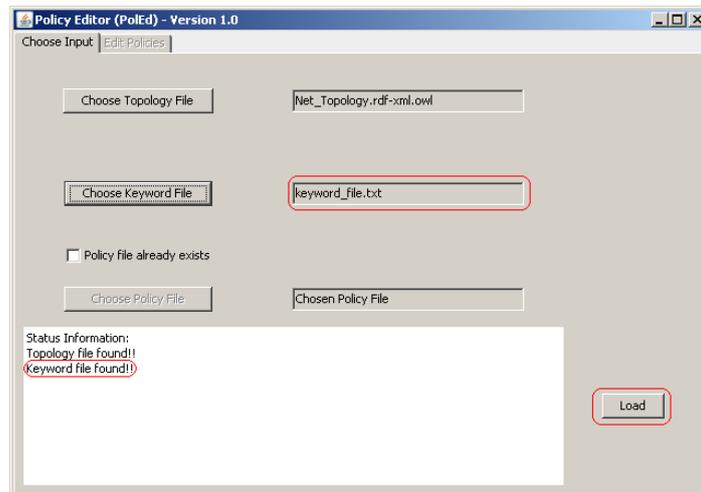


Abbildung B.6: Reizwort-Katalog ausgewählt

Zusätzlich besteht die Möglichkeit, bereits gespeicherte Policies aus vorherigen Sitzungen zu importieren. Die Dateiauswahl erfolgt analog der in Abbildung B.4 gezeigten Vorgehensweise.

Werden Policies abgespeichert erfolgt dies nach dem Schema:

- Zunächst die gesamte Policy,
- gefolgt von einem „|“-Trennsymbol,
- danach die Elemente Event, Condition und Action, jeweils durch „|“ getrennt,
- zuletzt das identifizierte Netzwerkgerät für die Policy.

Eine Policy-Datei könnte wie folgt aussehen:

B.1 Start des Programms - Datei-Auswahl

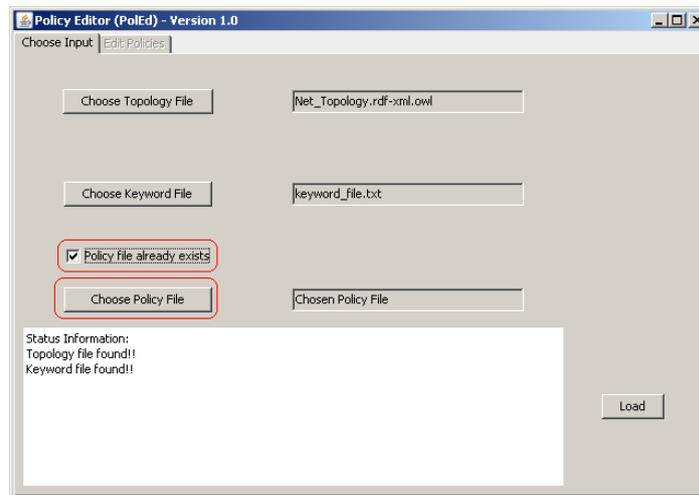


Abbildung B.7: Optional: Auswahl bereits bestehender Policies

```
1 Webcam connects, we have More than '50' users online $AND$ priority =  
  'high', shutdown system || a Webcam connects|| we have More  
  than '50' users online $AND$ priority = 'high' || shutdown system  
  || Router  
2 Voip is started, the time = '18:30', open port '60' || a Voip is  
  started || the time = '18:30' || open port '60' || Gateway  
3 Voip is started, the time = '18:30', open port '9000' || a Voip is  
  started || the time = '18:30' || open port '9000' || Client  
4 Webcam policy, if More than '20' users are online, we want a system  
  shutdown || a Webcam policy|| if More than '20' users are online  
  || we want a system shutdown|| Router
```

Hier ist bereits die Eingabeformatierung von Policies mit einigen Besonderheiten zu erkennen, die später in Anhang B.2 noch erläutert werden.

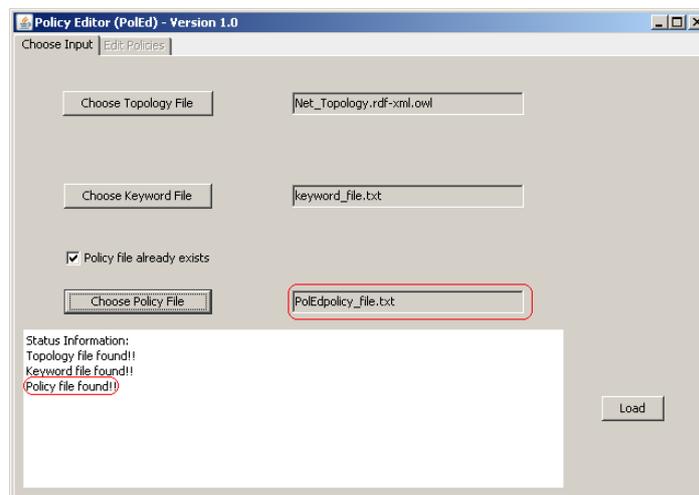


Abbildung B.8: Vorhandene Policies gewählt

B Handbuch

Sind alle Datei-Auswahlen getroffen, betätigen Sie bitte den „Load“-Knopf. Die gefundenen Dateien werden eingelesen und der Policy-Editor wird aktiviert. Eine weitere Dateiauswahl ist jetzt nicht mehr möglich! Sollten sie eine falsche Datei gewählt haben und dies feststellen, nachdem der „Load“-Knopf betätigt wurde, müssen Sie das Programm neu starten.

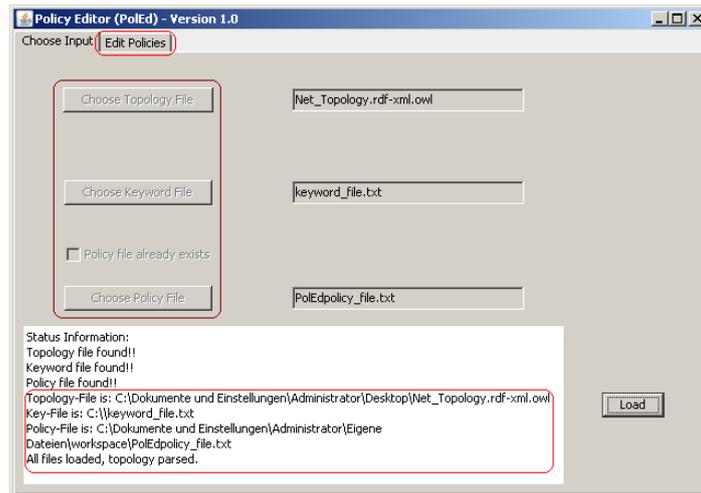


Abbildung B.9: Alle Dateien ausgewählt, Editor freigeschaltet

Fahren Sie nun mit dem Policy-Editor fort.

B.2 Der Policy-Editor

Nach der Dateiauswahl erfolgt die eigentliche Arbeit mit Policies. Hat der Benutzer keine Policies aus einer Datei importiert, bietet sich das Bild B.10. Wurden Policies eingelesen, sieht der Editor wie in Abbildung B.11 aus. Die importierten Policies wurden dann in die Tabelle übernommen. Sie haben dann bereits die Möglichkeit, vorhandene Policies zu bearbeiten bzw. zu löschen. Im oberen Bereich ist das Formularfeld markiert, hier werden neue Policies eingegeben, bzw. bereits vorhandene editiert. Im unteren Bereich befindet sich eine Status-Anzeige, die den Benutzer mit Informationen über den aktuellen Stand bzw. eventuelle Fehlermeldungen versorgt. Der große weiße Bereich beinhaltet, entweder direkt zu Anfang (wie in Abbildung B.11) oder nach Speicherung der ersten Policy, eine Tabelle der bereits formulierten Policies.

B.2 Der Policy-Editor

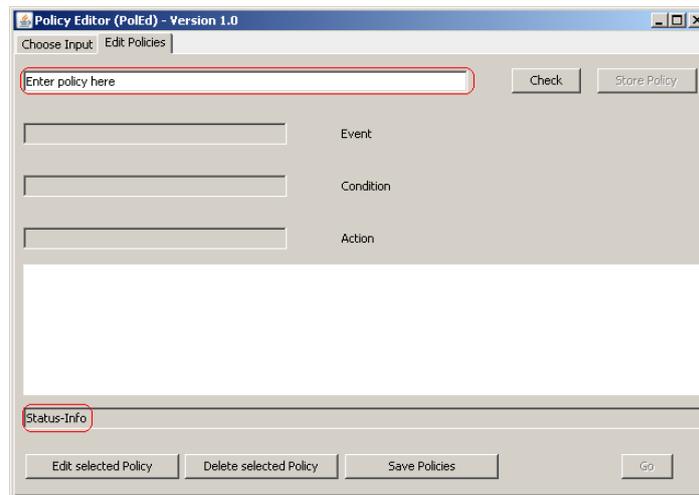


Abbildung B.10: Editor, Ansicht ohne geladene Policies

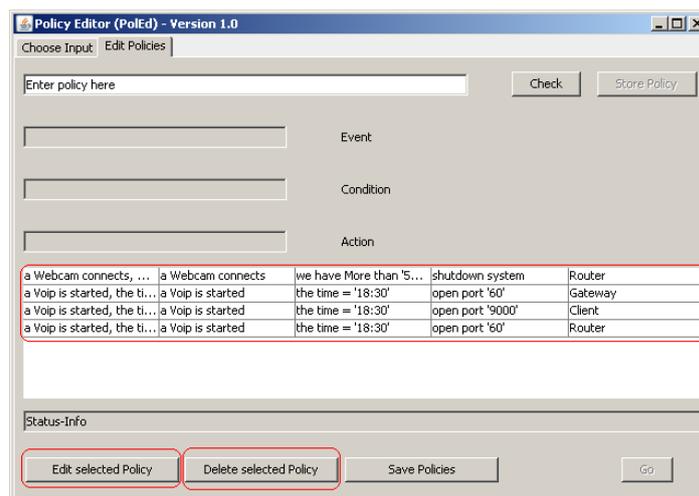


Abbildung B.11: Ansicht bei eingelesenen Policies

Eine neue Policy können Sie anlegen, indem Sie diese in das obere Formularfeld eintragen. Beachten Sie dabei bitte folgende Vorgaben:

- Der Editor „spricht“ nur Englisch!
- Da Policies aus drei Elementen (Event, Condition, Action) bestehen, werden diese durch ein Komma getrennt: „a Webcam connects (*Event*), More than '50' users online (*Condition*), shutdown the system *Action*.“
- In der Action bzw. der Condition können Parameter bzw. Bedingungen enthalten sein. Parameter werden in einfache Hochkommata gestellt. Operatoren - auch zur Verknüpfung zweier Bedingungen - werden entweder in Großbuchstaben oder als mathematische Operatoren eingegeben. Dabei sind folgende Operatoren zulässig:

B Handbuch

- AND für und
- OR für oder
- NOT für nicht
- != für ungleich
- >= für grösser-gleich
- <= für kleiner-gleich
- More für größer
- Less für kleiner
- = für gleich

Haben Sie eine Policy entsprechend der o.g. Formatierung eingegeben, betätigen Sie den „Check“-Knopf. Die Policy wird eingelesen und in ihre Bestandteile zerlegt (Abbildung B.13). Wollen Sie die Policy nachträglich ändern, tun Sie dies in der noch im Formularfeld stehenden Policy und drücken Sie abermals „Check“.

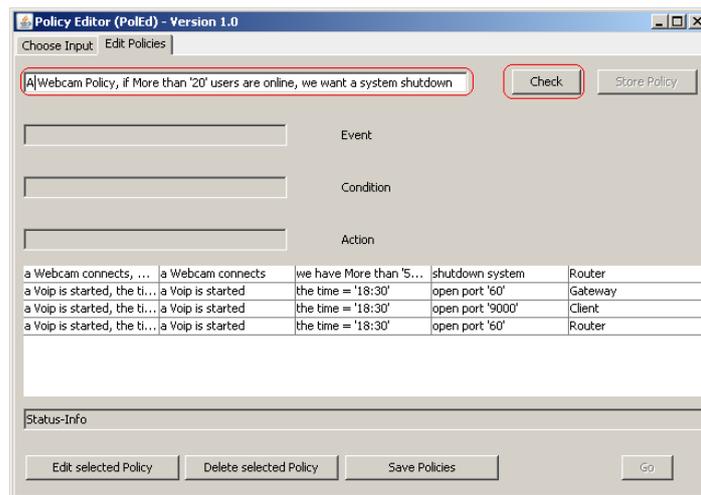


Abbildung B.12: Eingegebene Policy

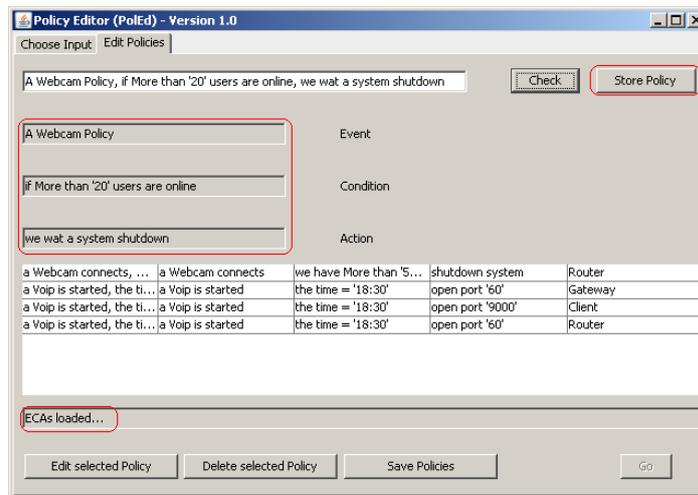


Abbildung B.13: Editor: nach Drücken des Check-Buttons

Sind Sie mit der Aufteilung der Policy einverstanden, betätigen Sie den „Store“-Knopf. Das Programm übernimmt die Policy in die Tabelle und bestätigt - im Falle eines Fundes innerhalb des Reizwortkataloges - bereits die Zuordnung zu einem Netzwerkgerät.(Abbildung B.14)

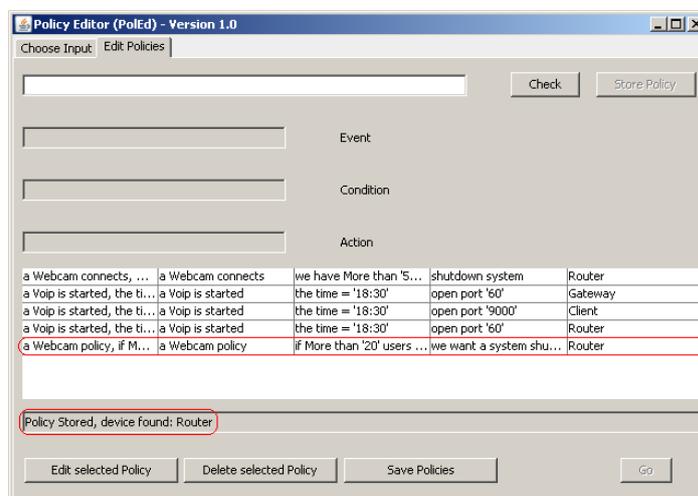


Abbildung B.14: Editor: Policy in die Tabelle übernommen

Zum Löschen einer Policy genügt eine Auswahl der entsprechenden Policy aus der Tabelle und ein Druck auf „Delete selected Policy“. Die gewählte Policy wird aus der Tabelle entfernt und die Aktion bestätigt.

Soll eine bereits eingegebene Policy nachträglich verändert werden, wählen Sie die Policy aus der Tabelle aus und betätigen „Edit selected Policy“. Die gewählte Policy wird in das Formularfeld geladen und die Elemente in den entsprechenden Feldern dargestellt. Haben Sie die Policy nach Ihren Wünschen verändert, drücken Sie „Check“ und - nach erfolgreicher Übernahme der Daten in die ECA-Felder sowie Bestätigung

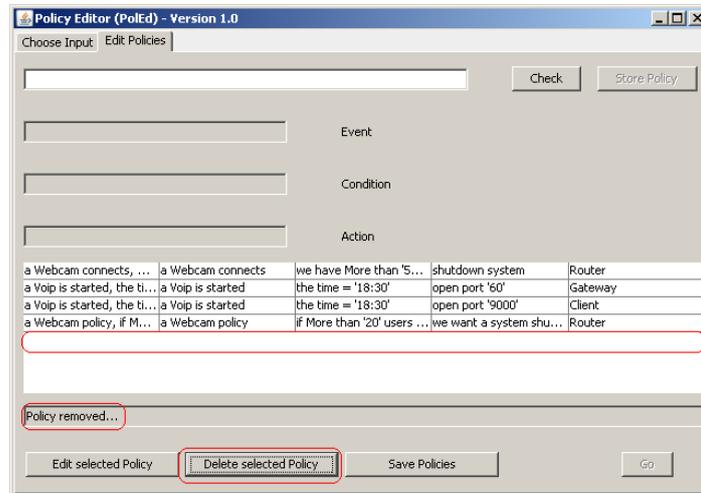


Abbildung B.15: Editor: Löschen einer Policy

des gefundenen Gerätes - auf „Store Policy“. Eine Meldung im Info-Panel bestätigt die veränderten Daten (Abbildung B.17).

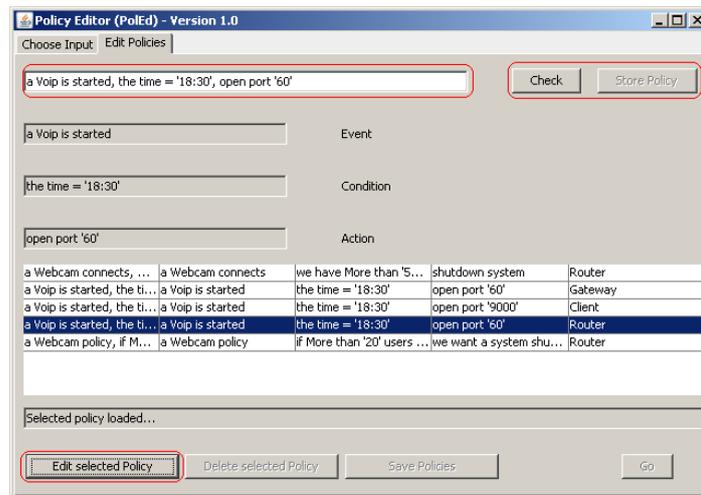


Abbildung B.16: Editor: Bearbeiten einer bereits eingegebenen Policy

Haben Sie die Eingabe sämtlicher Policies beendet und wollen zur Transformation in Ponder-Policies übergehen, bzw. möchten die bereits eingegebenen Daten für eine spätere Session speichern, drücken Sie auf „Save Policies“. Der Speicherort der Policies wird im Info-Panel dargestellt (Standard: Benutzer-Home-Verzeichnis mit dem Dateinamen „policy_file.txt“). Sobald dies geschehen ist, wird der „Go“-Knopf aktiviert (Abbildung B.18) und der zweite Refinement-Schritt kann gestartet werden (Abbildung B.19).

B.2 Der Policy-Editor

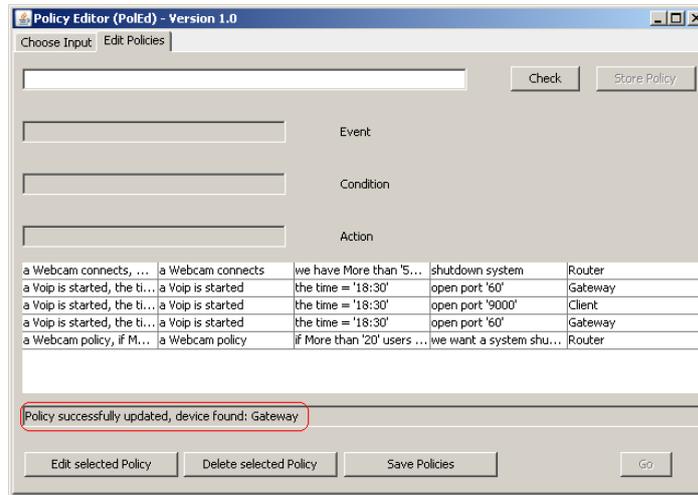


Abbildung B.17: Editor: Fertig bearbeitete Policy

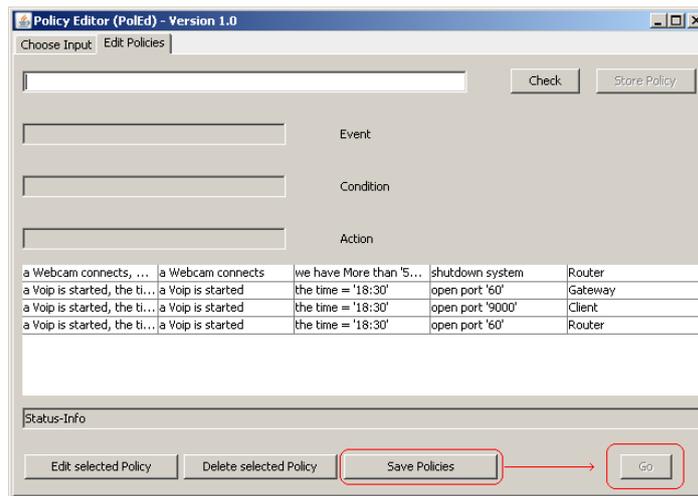


Abbildung B.18: Editor: Go-Button inaktiv

Nach Betätigung des „Go“-Buttons werden die in der Tabelle befindlichen Policies in Ponder2-Policies überführt. Eventuelle Fehler dabei finden sich als Kommentar, bzw. als Variablenname „null“ in der Ponder-Datei wieder. Ist der Vorgang abgeschlossen, wird dies mit dem Speicherort (Standard ist das Benutzer-Home-Verzeichnis mit dem Dateinamen „ponder_policies.txt“) bestätigt und der Vorgang ist abgeschlossen.

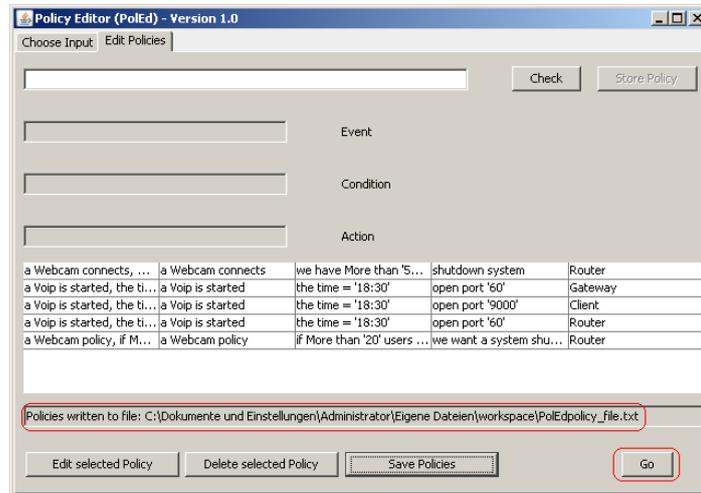


Abbildung B.19: Editor: Go-Button aktiviert

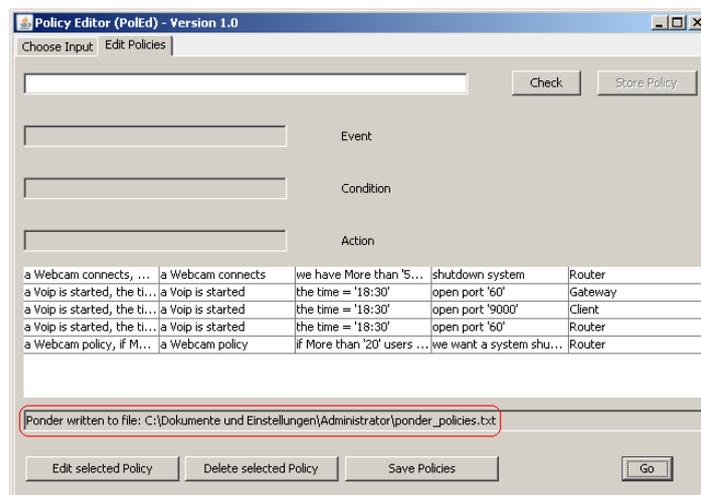


Abbildung B.20: Editor: Ponder-Transformation abgeschlossen.

Sie können das Programm nun schließen und die Ponder-Policies weiter verarbeiten bzw. in einem Editor Ihrer Wahl betrachten.