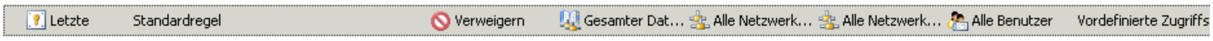
Forefront TMG – Modifying TMG System Policy rules with TMG Export / Import functionality

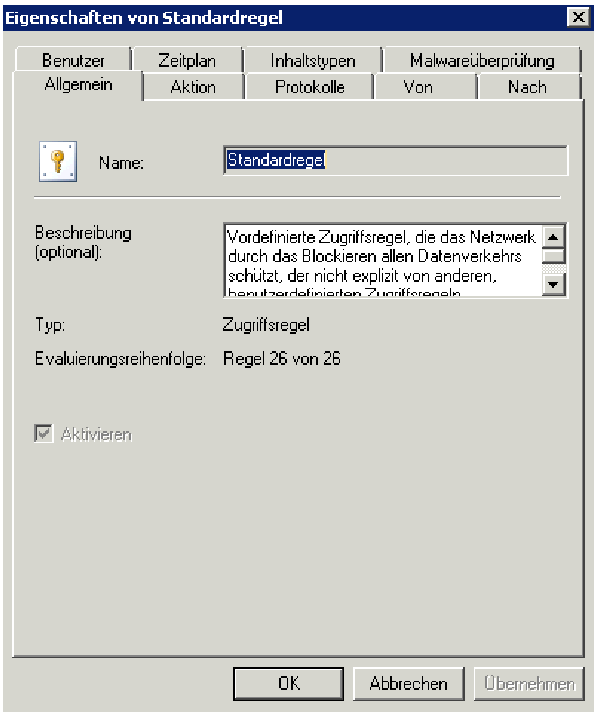
Some Forefront TMG Firewall policy rules cannot be modified (for example it is not possible to disable the Default Firewall policy rule and is not possible to disable logging for the Default Firewall policy rule.

Example Standardregel (Default rule)



Letzte Standardregel Verweigern Gesamter Dat… Alle Netzwerk… Alle Netzwerk… Alle Benutzer Vordefinierte Zugriffs

Properties of the Default rule. You cannot disable this rule.



Eigenschaften von Standardregel

Name: Standardregel

Beschreibung (optional): Vordefinierte Zugriffsregel, die das Netzwerk durch das Blockieren allen Datenverkehrs schützt, der nicht explizit von anderen, benutzerdefinierten Zugriffsregeln

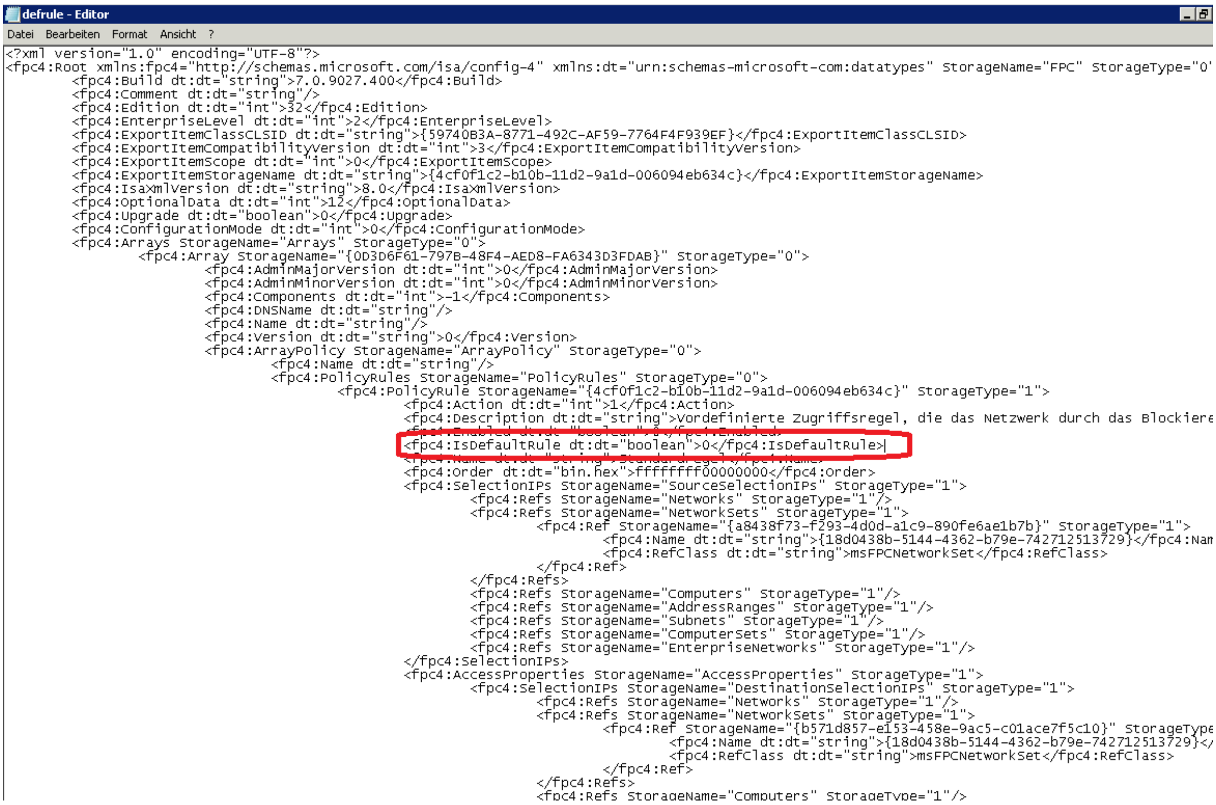
Typ: Zugriffsregel

Evaluierungsreihenfolge: Regel 26 von 26

☑ Aktivieren

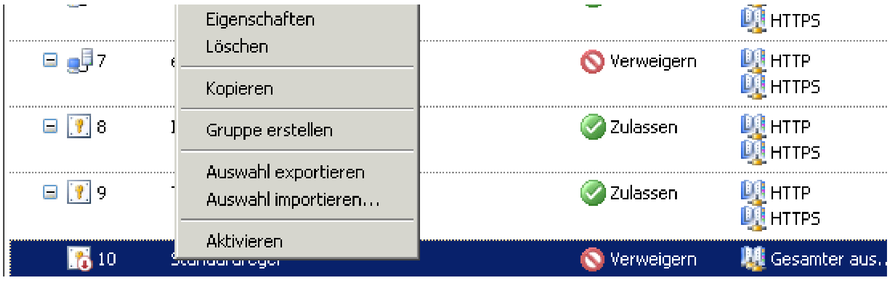
Please note: Use this information at your own risk, no warranty and always create a backup of your TMG configuration before you modify something ☺

To deactivate or activate the system policy rule, export the default rule with the TMG MMC into a XML file and edit the XML file with a text or XML editor and change the “IsDefaultRule” entry to 0 from 1 and save the XML file. More information about Backup/restore – Import/export capabilities of Forefront TMG: http://www.isaserver.org/tutorials/Microsoft-Forefront-TMG-Backup-Restore-Capabilities.html



```
<?xml version="1.0" encoding="UTF-8"?>
<fpc4:Root xmlns:fpc4="http://schemas.microsoft.com/isa/config-4" xmlns:dt="urn:schemas-microsoft-com:datatypes" StorageName="FPC" StorageType="0'
        <fpc4:Build dt:dt="string">7.0.9027.400</fpc4:Build>
        <fpc4:Comment dt:dt="string"/>
        <fpc4:Edition dt:dt="int">32</fpc4:Edition>
        <fpc4:EnterpriseLevel dt:dt="int">2</fpc4:EnterpriseLevel>
        <fpc4:ExportItemClassCLSID dt:dt="string">{59740B3A-8771-492C-AF59-7764F4F939EF}</fpc4:ExportItemClassCLSID>
        <fpc4:ExportItemCompatibilityVersion dt:dt="int">3</fpc4:ExportItemCompatibilityVersion>
        <fpc4:ExportItemScope dt:dt="int">0</fpc4:ExportItemScope>
        <fpc4:ExportItemStorageName dt:dt="string">{4cf0f1c2-b10b-11d2-9a1d-006094eb634c}</fpc4:ExportItemStorageName>
        <fpc4:IsaXmlVersion dt:dt="string">8.0</fpc4:IsaXmlVersion>
        <fpc4:OptionalData dt:dt="int">12</fpc4:OptionalData>
        <fpc4:Upgrade dt:dt="boolean">0</fpc4:Upgrade>
        <fpc4:ConfigurationMode dt:dt="int">0</fpc4:ConfigurationMode>
        <fpc4:Arrays StorageName="Arrays" StorageType="0">
                <fpc4:Array StorageName="{0D3D6F61-797B-48F4-AED8-FA6343D3FDAB}" StorageType="0">
                        <fpc4:AdminMajorVersion dt:dt="int">0</fpc4:AdminMajorVersion>
                        <fpc4:AdminMinorVersion dt:dt="int">0</fpc4:AdminMinorVersion>
                        <fpc4:Components dt:dt="int">-1</fpc4:Components>
                        <fpc4:DNSName dt:dt="string"/>
                        <fpc4:Name dt:dt="string"/>
                        <fpc4:Version dt:dt="string">0</fpc4:Version>
                        <fpc4:ArrayPolicy StorageName="ArrayPolicy" StorageType="0">
                                <fpc4:Name dt:dt="string"/>
                                <fpc4:PolicyRules StorageName="PolicyRules" StorageType="0">
                                        <fpc4:PolicyRule StorageName="{4cf0f1c2-b10b-11d2-9a1d-006094eb634c}" StorageType="1">
                                                <fpc4:Action dt:dt="int">1</fpc4:Action>
                                                <fpc4:Description dt:dt="string">Vordefinierte Zugriffsregel, die das Netzwerk durch das Blockiere
                                                <fpc4:Enabled dt:dt="boolean">0</fpc4:Enabled>
                                                <fpc4:IsDefaultRule dt:dt="boolean">0</fpc4:IsDefaultRule>
                                                <fpc4:Name dt:dt="string">Standardregel</fpc4:Name>
                                                <fpc4:Order dt:dt="bin.hex">ffffffff00000000</fpc4:Order>
                                                <fpc4:SelectionIPs StorageName="SourceSelectionIPs" StorageType="1">
                                                        <fpc4:Refs StorageName="Networks" StorageType="1"/>
                                                        <fpc4:Refs StorageName="NetworkSets" StorageType="1">
                                                                <fpc4:Ref StorageName="{a8438f73-f293-4d0d-a1c9-890fe6ae1b7b}" StorageType="1">
                                                                        <fpc4:Name dt:dt="string">{18d0438b-5144-4362-b79e-742712513729}</fpc4:Nam
                                                                        <fpc4:RefClass dt:dt="string">msFPCNetworkSet</fpc4:RefClass>
                                                                </fpc4:Ref>
                                                        </fpc4:Refs>
                                                        <fpc4:Refs StorageName="Computers" StorageType="1"/>
                                                        <fpc4:Refs StorageName="AddressRanges" StorageType="1"/>
                                                        <fpc4:Refs StorageName="Subnets" StorageType="1"/>
                                                        <fpc4:Refs StorageName="ComputerSets" StorageType="1"/>
                                                        <fpc4:Refs StorageName="EnterpriseNetworks" StorageType="1"/>
                                                </fpc4:SelectionIPs>
                                                <fpc4:AccessProperties StorageName="AccessProperties" StorageType="1">
                                                        <fpc4:SelectionIPs StorageName="DestinationSelectionIPs" StorageType="1">
                                                                <fpc4:Refs StorageName="Networks" StorageType="1"/>
                                                                <fpc4:Refs StorageName="NetworkSets" StorageType="1">
                                                                        <fpc4:Ref StorageName="{b571d857-e153-458e-9ac5-c01ace7f5c10}" StorageType
                                                                                <fpc4:Name dt:dt="string">{18d0438b-5144-4362-b79e-742712513729}</
                                                                                <fpc4:RefClass dt:dt="string">msFPCNetworkSet</fpc4:RefClass>
                                                                        </fpc4:Ref>
                                                                </fpc4:Refs>
                                                                <fpc4:Refs StorageName="Computers" StorageType="1"/>
```

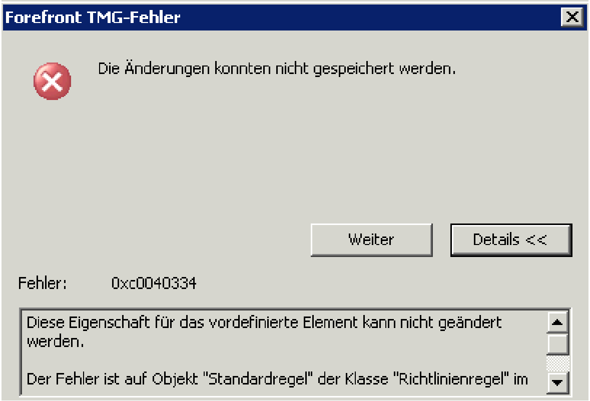
After the XML file is saved, import the XML file into your TMG configuration. From now on it is possible to activate or deactivate the default rule. You can do the same with the Forefront TMG system policy rule: http://technet.microsoft.com/de-de/library/cc441740.aspx



```
                    HTTPS
7      Verweigern   HTTP
                    HTTPS
8      Zulassen     HTTP
                    HTTPS
9      Zulassen     HTTP
                    HTTPS
10     Verweigern   Gesamter aus…
```

Disable Logging for the Standardregel (Default rule)

If you try to disable the logging for the Default Firewall policy rule, you will get the following error message:



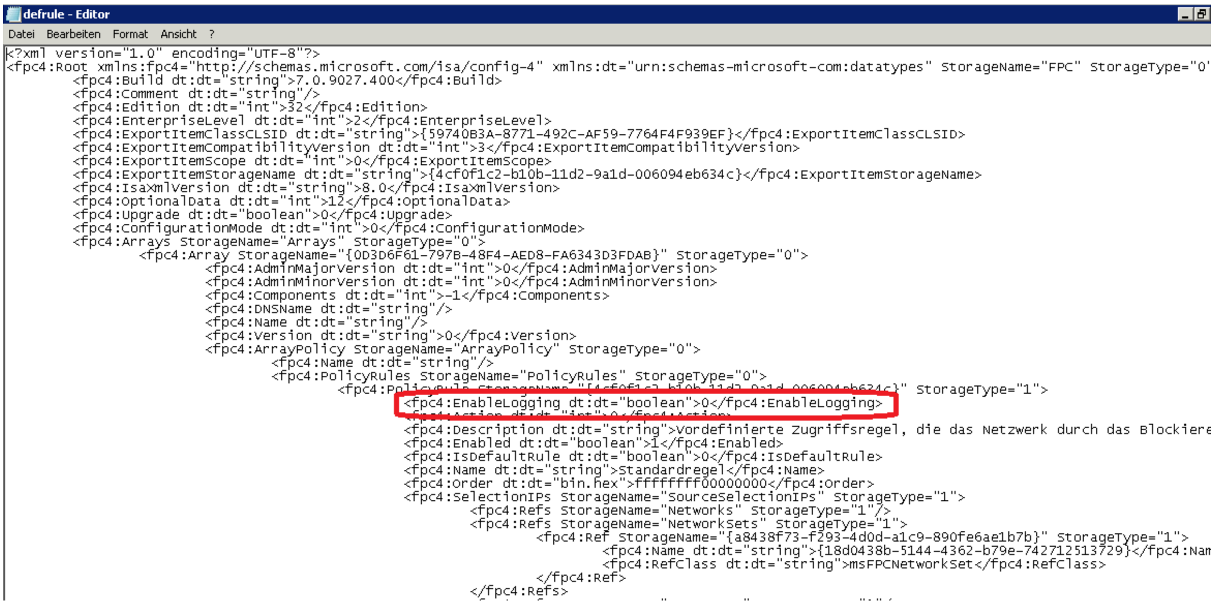
Die Änderungen konnten nicht gespeichert werden.

Fehler: 0xc0040334

Diese Eigenschaft für das vordefinierte Element kann nicht geändert werden.

Der Fehler ist auf Objekt "Standardregel" der Klasse "Richtlinienregel" im

Solution: Export a user defined Firewall policy rule to a XML file and copy the line of the following screenshot into the clipboard and insert this line in the exported XML file for the Default policy rule under the same structure as in the user defined Firewall policy rule.



```
<?xml version="1.0" encoding="UTF-8"?>
<fpc4:Root xmlns:fpc4="http://schemas.microsoft.com/isa/config-4" xmlns:dt="urn:schemas-microsoft-com:datatypes" StorageName="FPC" StorageType="0'
        <fpc4:Build dt:dt="string">7.0.9027.400</fpc4:Build>
        <fpc4:Comment dt:dt="string"/>
        <fpc4:Edition dt:dt="int">32</fpc4:Edition>
        <fpc4:EnterpriseLevel dt:dt="int">2</fpc4:EnterpriseLevel>
        <fpc4:ExportItemClassCLSID dt:dt="string">{59740B3A-8771-492C-AF59-7764F4F939EF}</fpc4:ExportItemClassCLSID>
        <fpc4:ExportItemCompatibilityVersion dt:dt="int">3</fpc4:ExportItemCompatibilityVersion>
        <fpc4:ExportItemScope dt:dt="int">0</fpc4:ExportItemScope>
        <fpc4:ExportItemStorageName dt:dt="string">{4cf0f1c2-b10b-11d2-9a1d-006094eb634c}</fpc4:ExportItemStorageName>
        <fpc4:IsaXmlVersion dt:dt="string">8.0</fpc4:IsaXmlVersion>
        <fpc4:OptionalData dt:dt="int">12</fpc4:OptionalData>
        <fpc4:Upgrade dt:dt="boolean">0</fpc4:Upgrade>
        <fpc4:ConfigurationMode dt:dt="int">0</fpc4:ConfigurationMode>
        <fpc4:Arrays StorageName="Arrays" StorageType="0">
                <fpc4:Array StorageName="{0D3D6F61-797B-48F4-AED8-FA6343D3FDAB}" StorageType="0">
                        <fpc4:AdminMajorVersion dt:dt="int">0</fpc4:AdminMajorVersion>
                        <fpc4:AdminMinorVersion dt:dt="int">0</fpc4:AdminMinorVersion>
                        <fpc4:Components dt:dt="int">-1</fpc4:Components>
                        <fpc4:DNSName dt:dt="string"/>
                        <fpc4:Name dt:dt="string"/>
                        <fpc4:Version dt:dt="string">0</fpc4:Version>
                        <fpc4:ArrayPolicy StorageName="ArrayPolicy" StorageType="0">
                                <fpc4:Name dt:dt="string"/>
                                <fpc4:PolicyRules StorageName="PolicyRules" StorageType="0">
                                        <fpc4:PolicyRule StorageName="{4cf0f1c2-b10b-11d2-9a1d-006094eb634c}" StorageType="1">
                                                <fpc4:EnableLogging dt:dt="boolean">0</fpc4:EnableLogging>
                                                <fpc4:Action dt:dt="int">0</fpc4:Action>
                                                <fpc4:Description dt:dt="string">Vordefinierte Zugriffsregel, die das Netzwerk durch das Blockiere
                                                <fpc4:Enabled dt:dt="boolean">1</fpc4:Enabled>
                                                <fpc4:IsDefaultRule dt:dt="boolean">0</fpc4:IsDefaultRule>
                                                <fpc4:Name dt:dt="string">Standardregel</fpc4:Name>
                                                <fpc4:Order dt:dt="bin.hex">ffffffff00000000</fpc4:Order>
                                                <fpc4:SelectionIPs StorageName="SourceSelectionIPs" StorageType="1">
                                                        <fpc4:Refs StorageName="Networks" StorageType="1"/>
                                                        <fpc4:Refs StorageName="NetworkSets" StorageType="1">
                                                                <fpc4:Ref StorageName="{a8438f73-f293-4d0d-a1c9-890fe6ae1b7b}" StorageType="1">
                                                                        <fpc4:Name dt:dt="string">{18d0438b-5144-4362-b79e-742712513729}</fpc4:Nam
                                                                        <fpc4:RefClass dt:dt="string">msFPCNetworkSet</fpc4:RefClass>
                                                                </fpc4:Ref>
                                                        </fpc4:Refs>
```

Import the modified XML file into the TMG MMC and save the configuration.