

paedML Die Musterlösung
Baden-Württemberg

Windows 2003 Server paedML[®] Windows 2.1 für schulische Netzwerke

ISA-Logfiles auswerten / Erweiterung / Anleitung
Stand: 20.02.2008



Impressum

Herausgeber

Landesmedienzentrum Baden-Württemberg (LMZ)
Projekt „Support-Netz“
Rosensteinstraße 24
70191 Stuttgart

Autoren

der Zentralen Expertengruppe Netze (ZEN),
Projekt „Support-Netz“, LMZ

Tamer Berber
Adrian Koch
Andreas Mayer
Martin Resch
Jürgen Schnaiter

Endredaktion

Ulrike Boscher

Weitere Informationen

www.support-netz.de
www.lmz-bw.de
www.medienoffensive.schule-bw.de

Veröffentlicht: **2008**

© Landesmedienzentrum Baden-Württemberg

Inhaltsverzeichnis

1.	ISA Logfiles auslesen	2
1.1.	Vorbemerkungen	2
1.2.	Konfiguration der Regeln	2
1.3.	Auswertung der Logfiles	5
1.4.	Vorbereitungen und Installation	6
1.5.	Verwenden des Tools	11
1.6.	Anpassung an spezielle Einstellungen	13
1.7.	Anpassungen an ISA 2000	15

1. ISA Logfiles auslesen

1.1. Vorbemerkungen

Der ISA-Server protokolliert jeden Zugriff aus dem paedML-Netz in das Internet. Die Auswertung dieser Daten ist jedoch ein sensibles Thema, da sie in das Persönlichkeitsrecht der Benutzer eingreift. Deshalb ist das System zunächst so konfiguriert, dass die Zugriffe nur anonym gespeichert werden, das heißt Sie können zwar nachverfolgen, zu welchem Zeitpunkt welche Internetadressen aufgerufen wurden, aber nicht von welchem Benutzer¹.

Bevor Sie sich also weiter mit der Auswertung dieser Daten beschäftigen, sollten Sie die datenschutzrechtlichen und pädagogischen Konsequenzen abwägen.

- Ist es überhaupt notwendig zu kontrollieren? Genügt vielleicht der Jugendschutzfilter von BelWü?
- Welchen Sinn hat die Kontrolle? Was konkret soll kontrolliert werden?
- Wer führt die Kontrolle durch? Welche Konsequenzen werden aus Verstößen gezogen?
- In Betrieben erfordert das Logging eine Betriebsvereinbarung, dazu ist der Betriebsrat zu beteiligen. Ähnliches gilt für die Schule. Sie sollten das Vorgehen also zuvor mit der Schulleitung, der GLK und ggf. auch der Schulkonferenz und dem Personalrat absprechen.
- Die Betroffenen (Schüler wie Kollegen) sind auf die Tatsache hinzuweisen. Es wird empfohlen, dass man sich die Kenntnisnahme schriftlich, ggf. durch die Eltern, bestätigen lässt, z.B. in Form einer Benutzerordnung.
- Eine Kontrolle der Internetzugriffe von Kollegen steht dem Netzwerkberater nicht zu.
- Das vorgestellte Tool erleichtert nur das gezielte Finden von Daten. Es greift nicht in den Datenschutz ein.

1.2. Konfiguration der Regeln

Der ISA Server 2006 protokolliert (wie bereits der ISA 2000) im Verzeichnis C:\Programme\Microsoft ISA Server\ISALogs die Internetzugriffe. Dort werden mit den Standardeinstellungen des ISA Servers alle Zugriffe ins Internet mit dem Benutzer *anonymous* eingetragen. Sie können in der ISA-Konsole für jede einzelne Regel bestimmen, ob überhaupt eine Protokollierung stattfinden soll und ob diese anonym oder personalisiert stattfinden soll. Diese Einstellungen können Sie jederzeit ändern.²

¹ Mit sehr großem Aufwand wäre es unter Umständen möglich, den Benutzer festzustellen, da der Clientname festgehalten wurde. Dieser Hinweis könnte wichtig sein, sollte es jemals zu strafrechtlich relevanten Ermittlungen kommen.

² Eine Beschreibung der Regeln samt der Defaulteinstellungen finden Sie unter http://lehrerfortbildung-bw.de/netz/muster/win2000/material/basis30/pdf/kap_13_Internetsteuerung2006.pdf im Abschnitt 13.2.3ff.

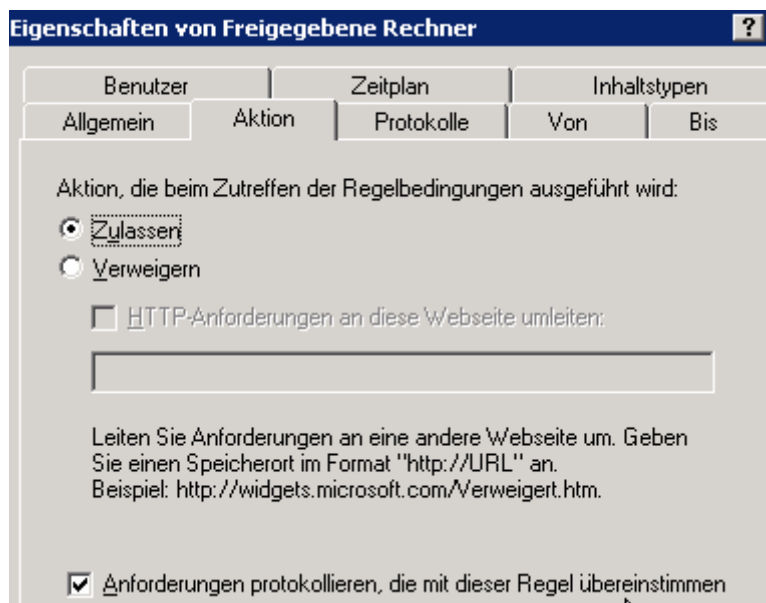
Fast alle Internetzugriffe finden über die Regel *Freigegebene Rechner* statt. Hier wird standardmäßig anonym protokolliert³.

Öffnen Sie über *Start | Programme | Microsoft ISA-Server* die *ISA-Server Verwaltungskontrolle*. Klicken Sie auf der linken Seite auf den Bereich *Firewallrichtlinie* (gegebenenfalls müssen Sie die Ansicht unter S1 erweitern).

Im mittleren Fenster gehen Sie mit Doppelklick auf die Regel *Freigegebene Rechner*.



Im Reiter *Aktion* legen Sie fest, ob überhaupt eine Protokollierung stattfinden soll oder nicht.

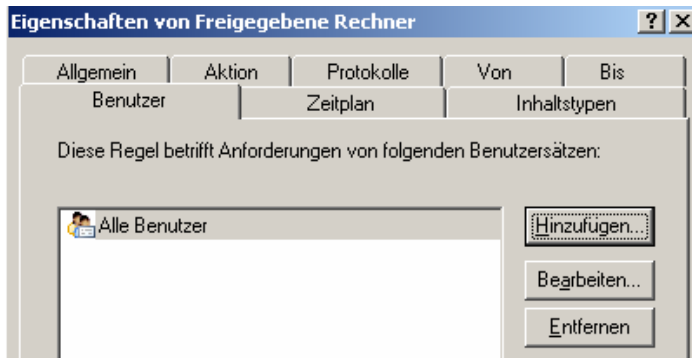


Dazu setzen Sie den Haken bei „Anforderung protokollieren“ oder entfernen ihn, wenn Sie komplett auf eine Protokollierung verzichten wollen.

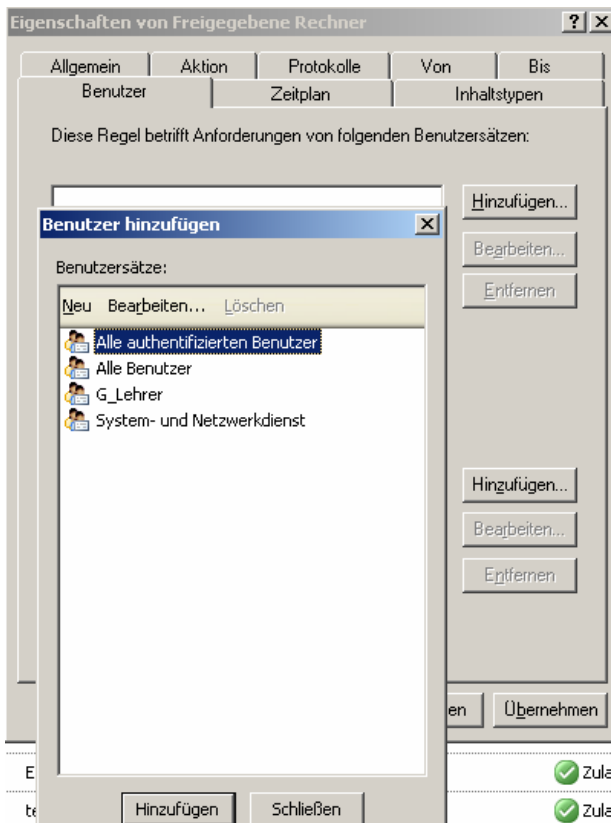
Wählen Sie die Registerkarte *Benutzer* aus. Wie unten abgebildet, ist hier als Standardwert *Alle Benutzer* eingetragen. Diese Einstellung führt dazu, dass zum einen der ISA-Server keine Authentifizierung verlangt, also jeder an einem Client angemeldete Benutzer auf das Internet zugreifen darf. Zum anderen bedeutet das aber auch, dass der ISA-Server nicht weiß, wer den Aufruf startet und daher im Protokoll nur *anonymous* ausgeben kann.

Markieren Sie *Alle Benutzer* und klicken Sie auf *Entfernen*.

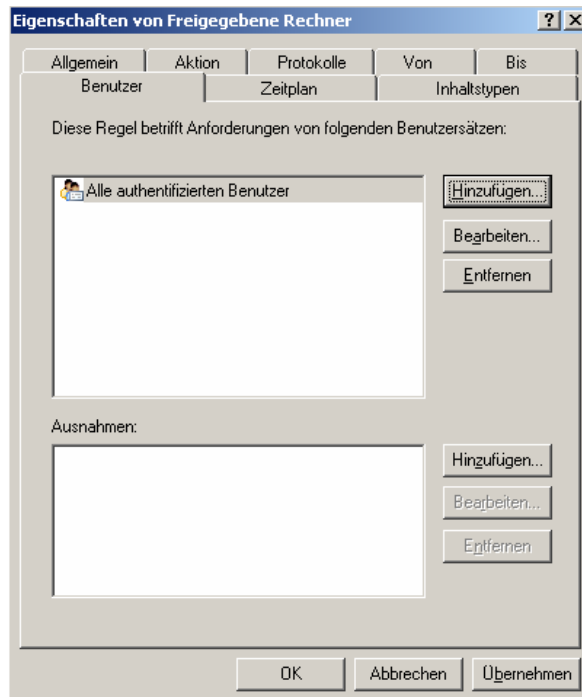
³ Das gilt für den ISA 2000 zunächst auch, jedoch muss die Authentifizierung bei der Installation der Schulkonsole aktiviert werden, um klassen- oder benutzerbezogene Sperrungen möglich zu machen. Vgl. hierzu <http://www.support-netz.de/nc/kundenportal/updates-und-patches/windows/schulkonsole-21-fuer-paedml-windows.html>, S. 25 ISA 2000 Authentifizierung



Drücken Sie auf *Hinzufügen*, markieren Sie die Gruppe *Alle authentifizierten Benutzer* und klicken Sie erneut auf *Hinzufügen*. Jetzt kann das Fenster *Benutzer hinzufügen* geschlossen werden.



Klicken Sie auf *OK*, um die Änderung zu übernehmen.



Speichern Sie die Änderung der Firewall wie gewohnt mit *Übernehmen* ab.

In der Firewallregel *Sonstige Rechner* werden alle Computer abgebildet, die zwar Verbindung zum ISA-Server haben, aber nicht in einem Raum als Client eingetragen sind. Hier ist der personalisierte Zugriff schon voreingestellt. Natürlich können Sie hier analog Veränderung vornehmen, um die Zugriffe nicht oder anonym zu protokollieren.

Wenn Sie zusätzlich auch die Zugriffe von den Servern ins Internet dokumentieren möchten, ändern Sie analog die Regel *Internet Zugriff für Server*. Sobald *Alle authentifizierten Benutzer* in der Registerkarte Benutzer eingetragen und die Regel übernommen wurde, werden im Logfile die richtigen Benutzer protokolliert.

1.3. Auswertung der Logfiles

Es werden nun zwar alle Zugriffe namentlich geloggt, allerdings ist es sehr schwierig, die Daten auszuwerten. Konkret wird ja nicht nur der Zugriff auf eine Webseite, sondern auf jedes einzelne Element einer Webseite, z.B. jedes Icon und jede Grafik festgehalten. Das führt zu enormen und völlig unübersichtlichen Datenmengen.

Mit Hilfe einer EXCEL-basierten Skriptdatei können Sie in den Textdateien suchen, die Treffen werden dann sortiert ausgegeben.

Bitte beachten Sie:

- Das Skript kann nur Daten finden, die in den Logdateien vorhanden sind. Konkret sind das aufgerufene Adressen, Namen von Dokumenten, Bilder etc., Datum, Uhrzeit, Name des Benutzers.
- Eine Suche nach Inhalten der Seiten ist nicht möglich.

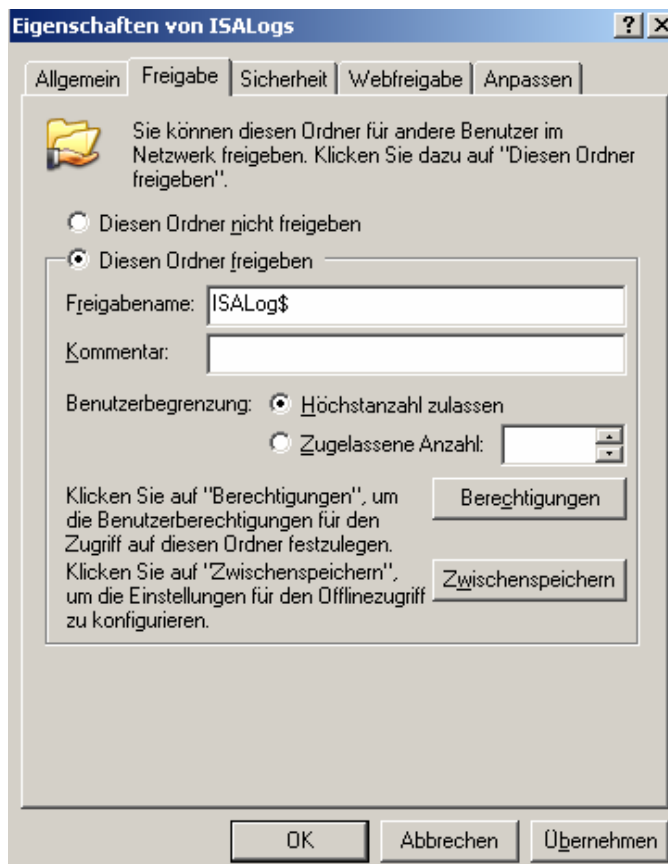
- Die Suche dauert je nach zu verarbeitenden Datenmenge mehrere Minuten.
- Das Dokument arbeitet nur mit EXCEL, Star- oder OpenOffice unterstützt die Makros nicht.
- Sie müssen die Anzahl der Treffer beschränken. 5000 Treffer sind voreingestellt.
- Das Skript arbeitet auch mit dem ISA 2000 zusammen.
- Eventuell müssen Sie Anpassungen vornehmen, um die Datenfelder korrekt zuzuordnen.

1.4. Vorbereitungen und Installation

Erstellen Sie auf dem Server eine Freigabe für den Ordner C:\Programme\Microsoft ISA Server\ISALogs
Rufen Sie dieses Verzeichnis auf und führen Sie einen rechten Mausklick aus. Wählen Sie *Freigabe und Sicherheit...*



Wählen Sie „Diesen Ordner freigeben“ aus und geben Sie unter Freigabename ISALog\$ ein.

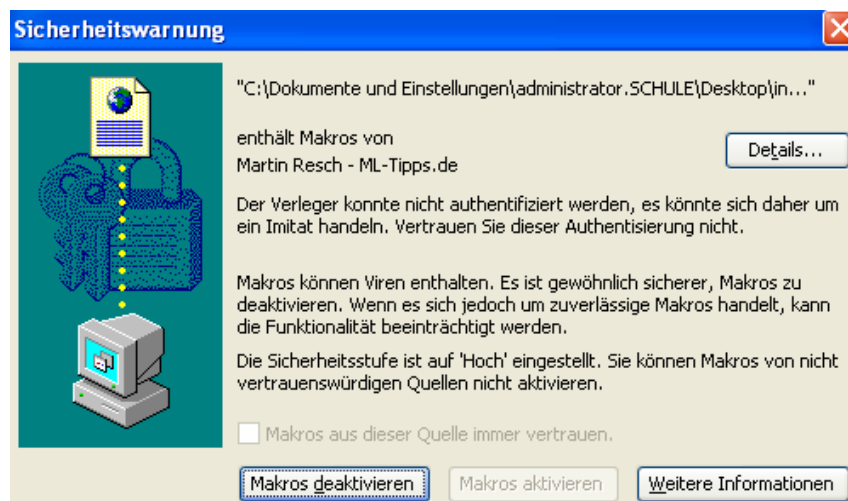


Klicken Sie auf *Übernehmen*, um die Freigabe zu übernehmen.

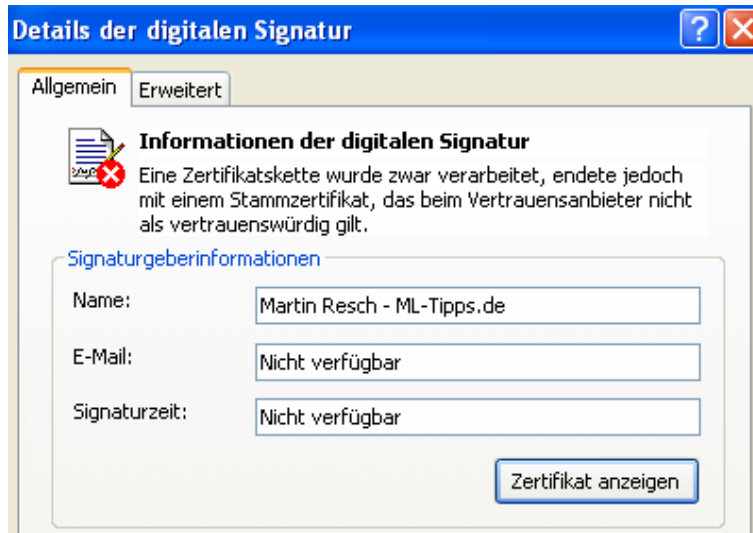
Über den Reiter *Sicherheit* könnten Sie nun noch differenziert einstellen, wer das Tool bedienen darf. Standardmäßig ist das nur der Administrator. Sie können jedoch einem weiteren Benutzer Leserechte erteilen, z.B. wenn Sie sich als Client wie empfohlen nur als Lehrer anmelden. Es wird aus Datenschutzgründen jedoch dringend davon abgeraten, pauschal allen Lehrern den Zugriff zu gestatten.

Jetzt benötigen Sie noch einen Arbeitsplatzrechner auf dem die Anwendung Excel ab der Version 2000 installiert ist. Zur Konfiguration sollten Sie sich mit einem Benutzer (Administrator oder aproflehrer) anmelden, der genügend Rechte besitzt, um auf dem Order `\\S1\ISALog$` zuzugreifen und ein Zertifikat einzutragen.

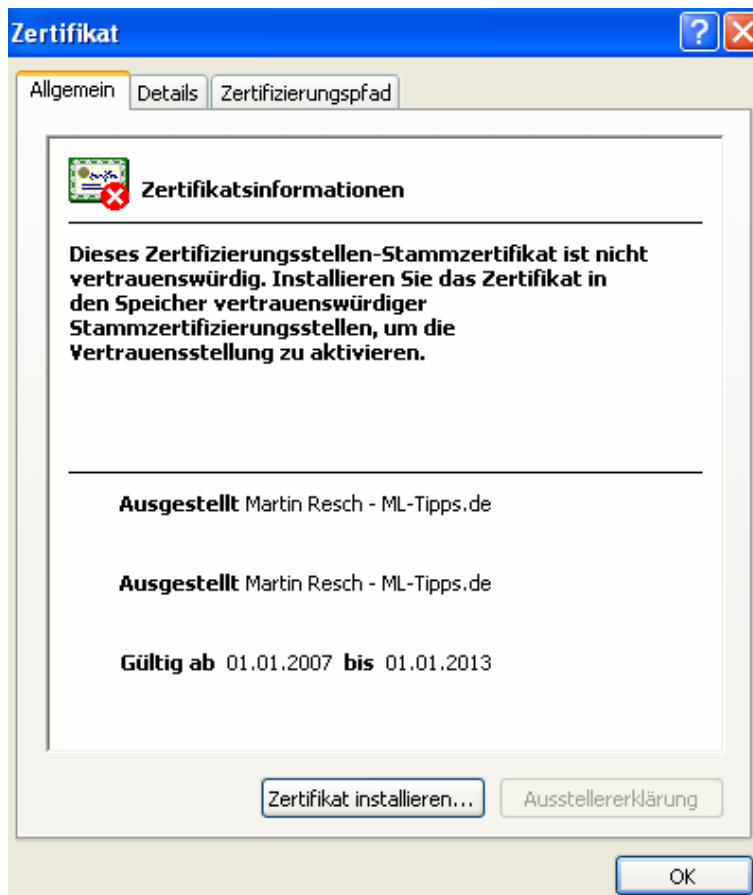
Starten Sie die Datei *internetlogs.xls*, die Sie unter <http://www.support-netz.de/nc/kundenportal/erweiterungen/windows/isa-logfiles.html> heruntergeladen haben und die jetzt auf dem lokalen Rechner, einem USB-Stick oder eine Netzwerkfreigabe vorliegt. Sie erhalten eine Sicherheitswarnung. Klicken Sie auf *Details...*



Klicken Sie auf den Button *Zertifikat anzeigen*, um weitere Informationen zu bekommen.



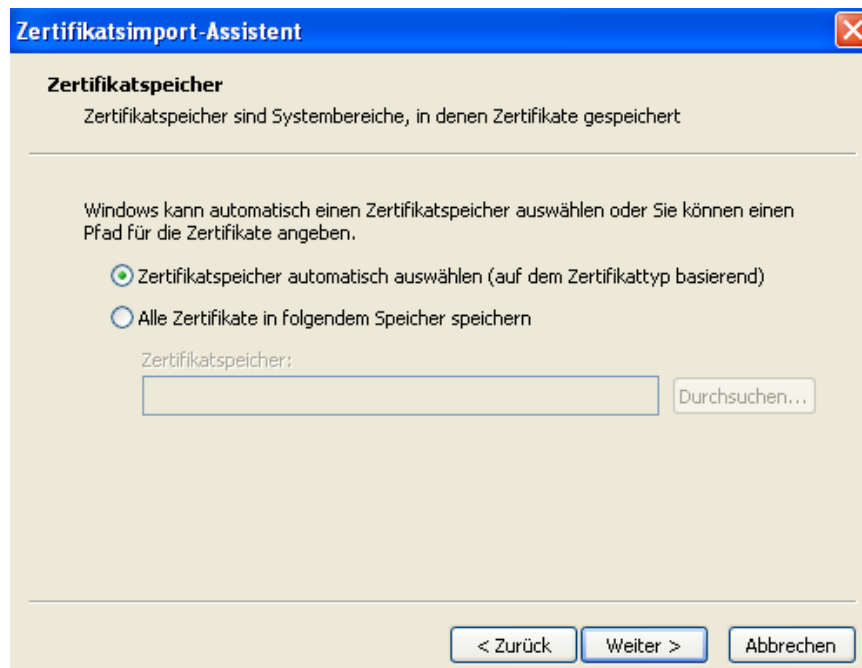
Klicken Sie auf den Button *Zertifikat installieren*, um dieses aufzunehmen.



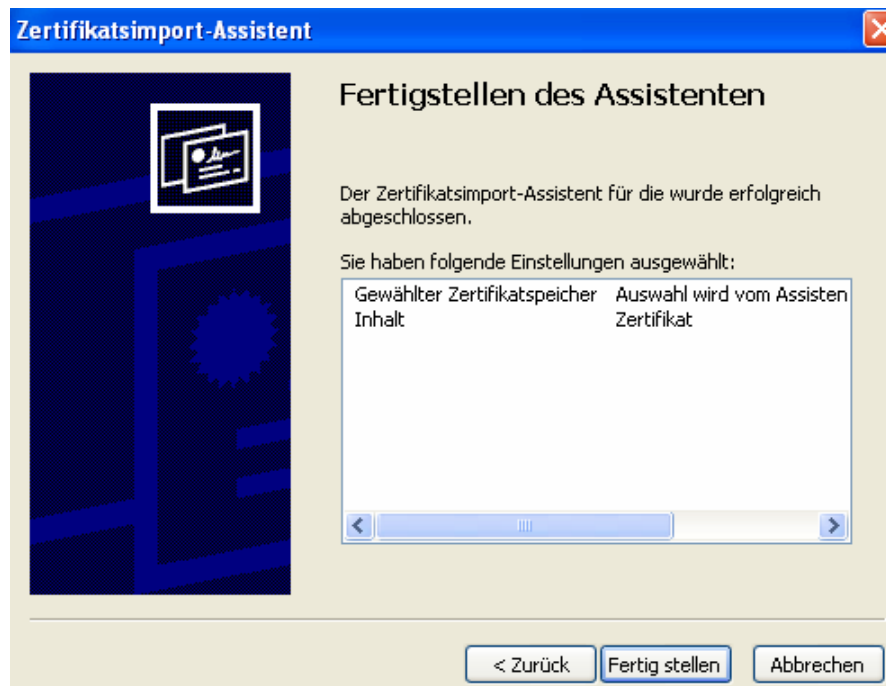
Bestätigen Sie mit *Weiter*.



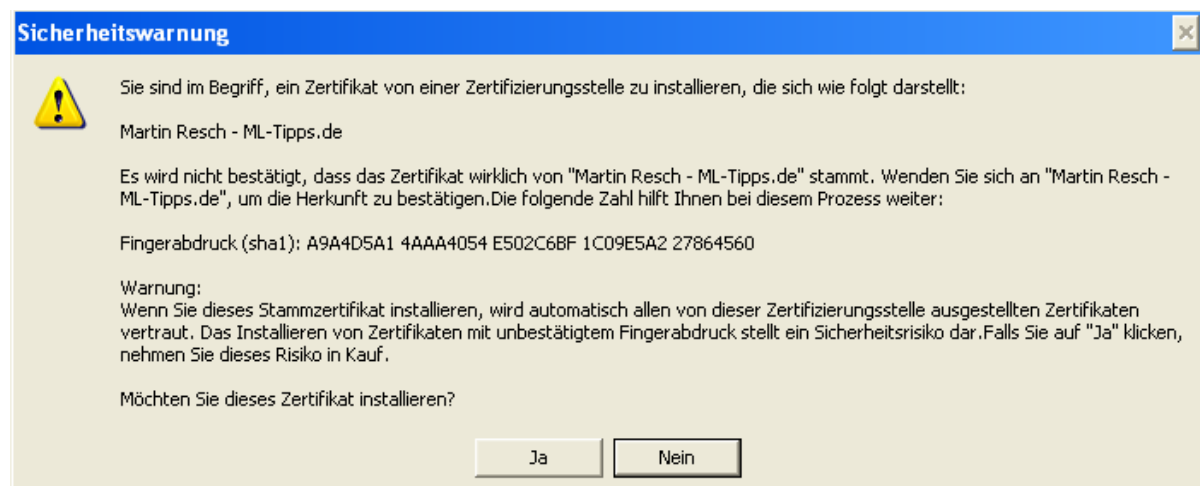
Wählen Sie „Zertifikatspeicher automatisch auswählen“ aus.



Schließen Sie den Vorgang mit *Fertig stellen* ab.



Die Sicherheitswarnung bestätigen Sie mit *Ja*.



Klicken Sie auf OK.



Bestätigen Sie die beiden Fenster *Zertifikat* und *Details der Digitalen Signatur* mit *OK*. Setzen Sie den Haken bei „Makros aus dieser Quelle immer vertrauen“ und drücken Sie auf *Makros aktivieren*.

Hinweise:

- Sollte diese Option nicht zur Verfügung stehen, starten Sie den Rechner neu und rufen Sie die Excel-Datei erneut auf.

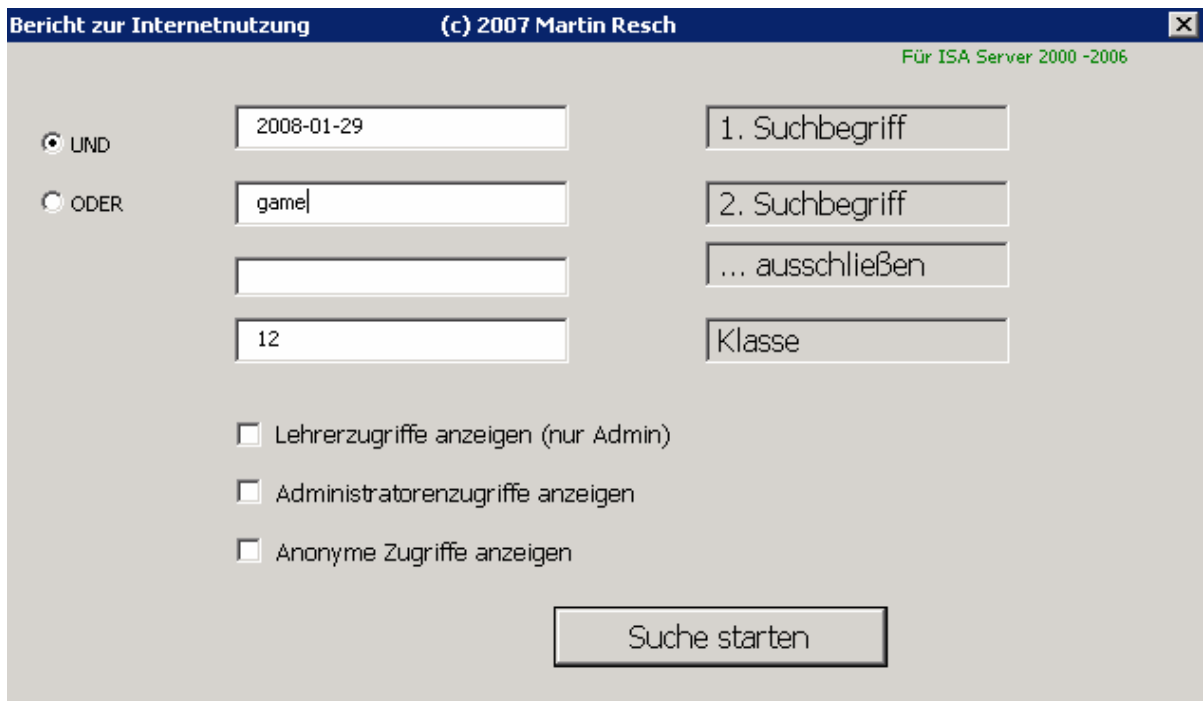
- Es gibt keine einfache Möglichkeit, das Zertifikat Lehrern zur Verfügung zu stellen. Wenn Sie die Tabelle als Lehrer verwenden wollen, stellen Sie die Makrosicherheit auf „Mittel“ und aktivieren Sie bei jedem Start die Makros.

1.5. Verwenden des Tools

Öffnen Sie die Excel-Datei, sie besteht aus drei Komponenten. Das Eingabeformular öffnet sich bereits beim Start. In dieses können Sie die Suchkriterien eintragen und logisch verknüpfen.

Beispiel: Suche nach dem Begriff „game“:

Im abgebildeten Beispiel wird überprüft, ob ein Schüler der Klasse 12 am 29.1.2008 eine Seite aufgerufen hat, die im URL den Ausdruck game enthält. Los geht's mit *Suche starten*.



Bericht zur Internetnutzung (c) 2007 Martin Resch Für ISA Server 2000 -2006

UND
 ODER

Lehrerzugriffe anzeigen (nur Admin)
 Administratorenzugriffe anzeigen
 Anonyme Zugriffe anzeigen

Die Auswertung dauert eine Weile, da alle Protokolldateien durchsucht werden müssen. Zugleich wird zu den Benutzern ermittelt, ob sie Schüler sind und welcher Klasse sie angehören. Aus der IP wird der Rechnername zugeordnet.

Auf dem Tabellenblatt *Daten* werden die Ergebnisse angezeigt. Die Einträge sind nach Benutzername, dann nach Zugriffszeitpunkt sortiert.

Auswertung vom 30.01.2008 20:35:17

Benutzer	Klasse	Datum	Uhrzeit	IP	Rechner	URL	Reg
a	12	29.01.08	11:06:58	10.1.10.103	pc03	http://img.web.de/web/img/v4/home06/icons/ico-games.gif	freig
d	12	29.01.08	11:16:40	10.1.10.107	pc07	http://img.ui-portal.de/gmx/homegmx/icons/ico-games.gif	freig
n	12	29.01.08	11:04:23	10.1.10.16	pc08a	http://img.web.de/web/img/v4/home06/icons/ico-games.gif	freig
p	12	29.01.08	9:53:04	10.1.10.106	pc06	http://img.web.de/web/img/v4/home06/icons/ico-games.gif	freig
p	12	29.01.08	11:06:40	10.1.10.111	pc11	http://img.web.de/web/img/v4/home06/icons/ico-games.gif	freig
p	12	29.01.08	11:29:21	10.1.10.111	pc11	http://games.entertainment.web.de/de/entertainment/games	freig

Der Name ist in der Abbildung absichtlich unkenntlich gemacht.

Als Suchbegriffe können Sie verwenden:

- Benutzernamen
- Datum
- URL-Bruchstücke

Die ersten beiden Begriffe lassen sich wahlweise per UND oder ODER verknüpfen, der dritte immer per UND NICHT. Die Klasse wird, falls eingegeben, ebenfalls über UND verknüpft.

Lehrerzugriffe sollten Sie, wie eingangs erläutert, in der Regel ausgeblendet lassen.

Die angezeigten URLs sind als Verknüpfungen definiert, können also direkt aufgerufen werden.

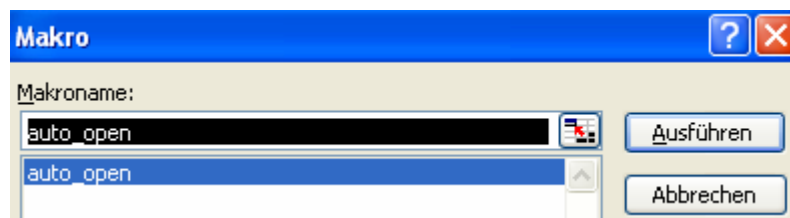
Sinnvolle Suchbegriffe:

- sex ODER porn
- Porn UND NICHT blacklist
- Klaus.Frech
- Klaus.Frech UND 2006-10-04
- 2006-10-04 zusammen mit Klasse 10b
- Google UND ?q= NICHT tbn

Weniger sinnvoll

- Google.de (zu hohe Trefferzahl)
- 11:05 (Zeit wird zwar erfasst, aber nicht unbedingt MEZ)

Wenn Sie erneut eine Abfrage starten möchten, drücken Sie [ALT + F8] und wählen Sie das Makro *auto_open* aus.



Jetzt haben Sie die Möglichkeit eine neue Abfrage zu starten.

1.6. Anpassung an spezielle Einstellungen

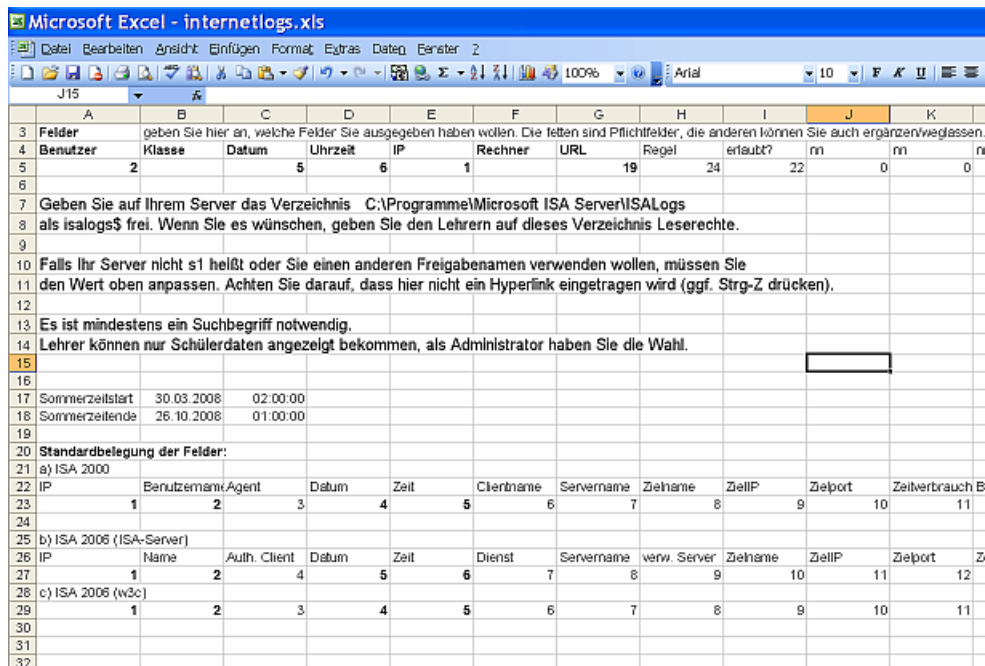
Wenn Sie das zweite Tabellenblatt *Optionen und Kurzanleitung* auswählen, haben Sie die Möglichkeit den Zugriff auf das ISA Logfile zu konfigurieren.

Quellpfad: Hier haben Sie die Möglichkeit den UNC Pfad zu den ISA Logfiles zu ändern.

Mehrserverbetrieb: S2 oder S3 z.B. \\S2\ISAlog\$

Max. Treffer: Begrenzung der Ergebnisse, um die Übersichtlichkeit zu bewahren.

Felder: Hier wird definiert in welcher Spalte der ausgewählte Wert im ISA Logfile dargestellt wird. Unter *Standardbelegung der Felder* können Sie sehen, wie die Logfiles der ISA Server Versionen aufgebaut sind⁴.

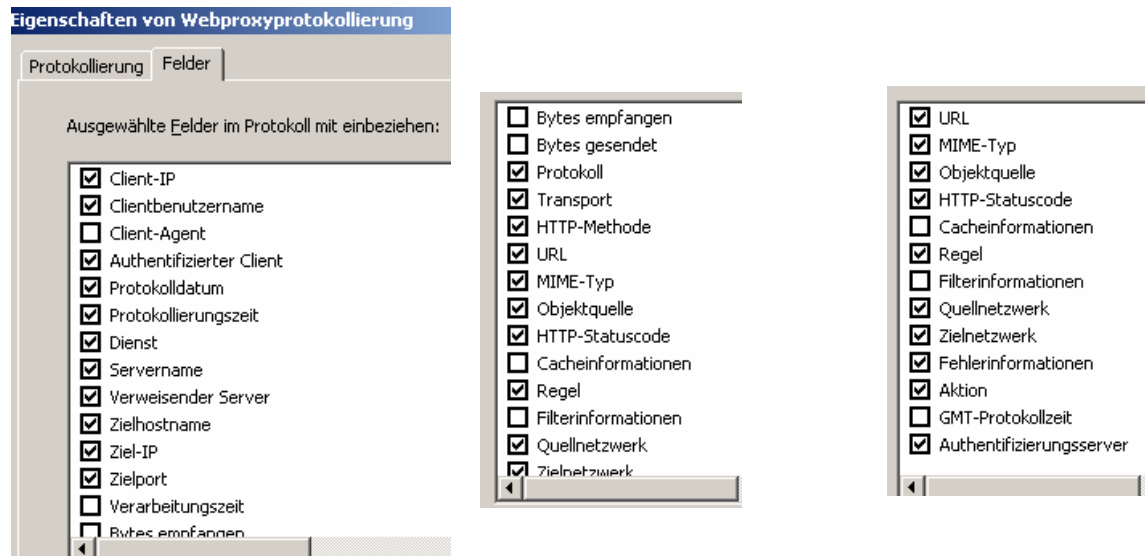


Felder	geben Sie hier an, welche Felder Sie ausgegeben haben wollen. Die fetten sind Pflichtfelder, die anderen können Sie auch ergänzen/weglassen.										
Benutzer	Klasse	Datum	Uhrzeit	IP	Rechner	URL	Regel	erlaubt?	nn	nn	nn
2		5	6	1		19	24	22	0	0	0
Geben Sie auf Ihrem Server das Verzeichnis C:\Programme\Microsoft ISA Server\ISALogs als isalogs\$ frei. Wenn Sie es wünschen, geben Sie den Lehrern auf dieses Verzeichnis Leserechte.											
Falls Ihr Server nicht s1 heißt oder Sie einen anderen Freigabennamen verwenden wollen, müssen Sie den Wert oben anpassen. Achten Sie darauf, dass hier nicht ein Hyperlink eingetragen wird (ggf. Strg-Z drücken).											
Es ist mindestens ein Suchbegriff notwendig.											
Lehrer können nur Schülerdaten angezeigt bekommen, als Administrator haben Sie die Wahl.											
Standardbelegung der Felder:											
a) ISA 2000											
IP	Benutzernam	Agent	Datum	Zeit	Clientname	Servername	Zielname	ZiellIP	Zielport	Zeitverbrauch	B
1	2	3	4	5	6	7	8	9	10	11	
b) ISA 2005 (ISA-Server)											
IP	Name	Auth. Client	Datum	Zeit	Dienst	Servername	verw. Server	Zielname	ZiellIP	Zielport	Z
1	2	4	5	6	7	8	9	10	11	12	
c) ISA 2005 (w3c)											
1	2	3	4	5	6	7	8	9	10	11	

Die zu protokollierenden Felder können Sie selbst auswählen. Beim ISA 2006 stehen Ihnen die unten aufgeführten Felder zur Verfügung (siehe Abbildung):

⁴ Leider ist das nicht eindeutig, sondern hängt vom Protokollierungstyp ab. So werden beim ISA-Serverformat auch ausgelassene Felder mitgezählt, beim w3c-Format hingegen nicht.

Voreingestellt ist ISA-Format (ISA2006) bzw. w3c-Format (ISA2000). Genaueres entnehmen Sie bitte der Hilfe zum ISA-Server.



Die zu protokollierenden Felder können Sie selbst bestimmen (aus der Onlinehilfe):

So legen Sie die zu protokollierenden Felder fest:

- Klicken Sie in der Konsolenstruktur der ISA Server-Verwaltung auf *Überwachung*.
- Klicken Sie im Detailbereich auf die Registerkarte *Protokollierung*.
- Wählen Sie auf der Registerkarte *Aufgaben* die gewünschte Aufgabe aus:
- *Firewallprotokollierung konfigurieren*. Dient zum Konfigurieren des Speicherorts der Firewallprotokollierung.
- *Webproxyprotokollierung konfigurieren*. Dient zum Konfigurieren des Speicherorts der Webproxyprotokollierung (das sind die Browserzugriffe).

Führen Sie auf der Registerkarte *Felder* einen der folgenden Schritte durch:

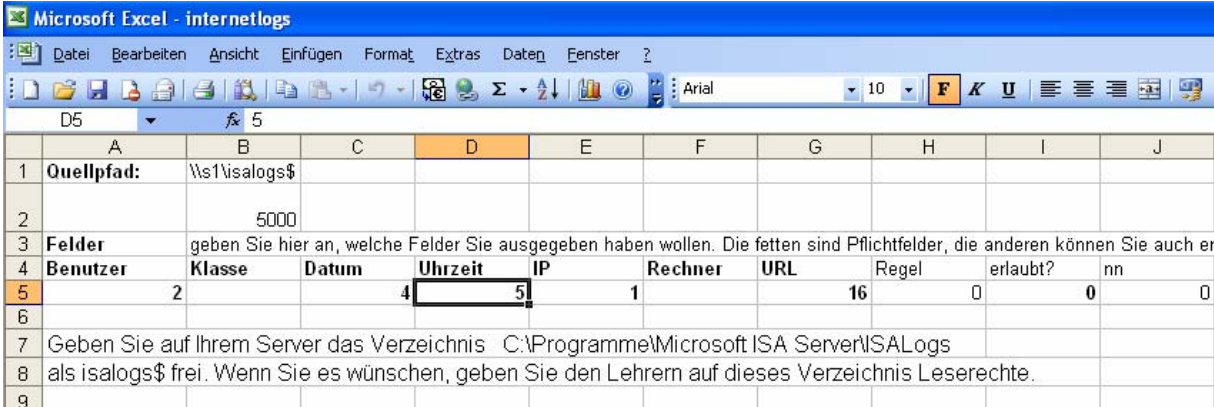
- Um bestimmte Felder auszuwählen, aktivieren Sie das entsprechende Kontrollkästchen.
- Um alle Kontrollkästchen in der Feldliste zu deaktivieren, klicken Sie auf *Auswahl aufheben*.
- Um alle Kontrollkästchen in der Feldliste zu aktivieren, klicken Sie auf *Alle auswählen*.
- Um die Standardfelder für die ISA Server-Protokollierungsdatei auszuwählen, klicken Sie auf *Wiederherstellen*.

Durch Abzählen der verwendeten Kästchen (w3c) bzw. aller Kästchen nehmen Sie dann in der Excel-Tabelle Bezug auf das entsprechende Feld.

Die Sommerzeitangabe müssen Sie in jedem Jahr anpassen. Sie dient dazu, bei der w3c-Protokollierung in die richtige Zeit umzurechnen.

1.7. Anpassungen an ISA 2000

Verwenden Sie noch einen ISA 2000 Server, so müssen Sie zwingend die Felder gemäß der Tabelle anpassen. In diesem Fall sehen die Einstellungen wie abgebildet aus:



	A	B	C	D	E	F	G	H	I	J
1	Quellpfad:	\\s1\isalogs\$								
2		5000								
3	Felder	geben Sie hier an, welche Felder Sie ausgegeben haben wollen. Die fetten sind Pflichtfelder, die anderen können Sie auch er								
4	Benutzer	Klasse	Datum	Uhrzeit	IP	Rechner	URL	Regel	erlaubt?	nn
5		2	4	5	1		16	0	0	0
6										
7	Geben Sie auf Ihrem Server das Verzeichnis C:\Programme\Microsoft ISA Server\ISALogs									
8	als isalogs\$ frei. Wenn Sie es wünschen, geben Sie den Lehrern auf dieses Verzeichnis Leserechte.									
9										

Ausführliche Informationen zur Protokollierung mit dem ISA 2000 finden Sie unter <http://www.msisafaq.de/Anleitungen/2000/Konfiguration/Protokollierung.htm>