

Future enhancements: (Anticipated in early 2012)

- Mac processes
- Linux desktop processes
- Surrey & Vancouver campuses

Note:

- Cheque printers must be PCL5 Universal, No spaces in queue names

Legend:

(Current as of November 2011)

- ADSFU Print Server = print4.its.sfu.ca
- SAD Print Server = print5.its.sfu.ca
- HCS App/Print Servers = AS-TSAPP10 and AS-TSAPP9

Contributors:

- Sean Faulkner, CaRS
- Scott Wang, CaRS
- Alan Rothenbush, CaRS
- Brian Haubrick, CaRS (Surrey)
- Michael Hayward, CaRS (Vancouver)
- Darlene Merlyn, ITI
- Steve Hillman, ITI
- Luis Fernandes, ESPM
- Tom Szeto, ESPM

SFU IT Services Printing Setup Workflow

Contents

ITDS consultations	4
Printer setup and security	5
Creating and maintaining print queues on Windows-based Print Servers.....	5
Pre-requisites	5
Creating Queues	6
Exporting Queues.....	8
Endnotes	10
Health and Counselling Secure Printing Solution	11
Unix Print Queues.....	27

Appendix A

Initial consultation

ITDS will ask questions such as the following of their clients when they request to purchase a new printer:

- Why do you need this printer?
- Does it need duplexing capability?
- Does it need to be networked?
- What is your budget?

In general, as part of the ongoing Managed Print Services (MPS) project, we are encouraging everyone to use the new Konica Minolta MFDs for all possible printing; these devices are networked and much more powerful than any desktop printer, and the cost per page is substantially lower.

Appendix B:

Printer setup and security

The first things we will do upon connecting a networked printer is:

- Set an administrator password
- Set the printer's IP
- Review the open ports:
 - Port 9100 (a.k.a. HP JetDirect, socket): Most printing services use this protocol, especially drivers from HP, so you may not be able to disable it.
 - LPD: LPD is used for printing by many Unix and Linux systems. However, many can now also use CUPS (the Common UNIX Printing System), which allows for printing via a number of protocols. If you do not need LPD, disable it.
 - IPP: If the Internet Printing Protocol is not used in your environment, then disable it.
 - **NOTE: SNMPv3 will be needed for Konica Minolta accounting**
 - Turn on and set firewall rules; this is only done mandatorily for cheque printers so as to restrict access between certain IP ranges

Appendix C:

Creating and maintaining print queues on Windows-based Print Servers

Pre-requisites

In order to create new print queues on either Print4 or Print5, delegated queue creators need to be added in the following user groups:

- For AD: CaRS Print Queue Admins (local)
- For SAD: CaRS Print Queue Admins (local)

Please contact the appropriate Domain Admins to add users to these groups.

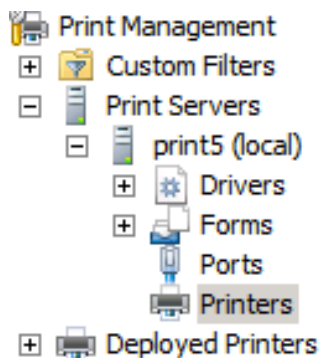
Note that the users should be vetted first.

Additionally, Health Services has its own IPSEC enabled print server. Please see Appendix D for more information

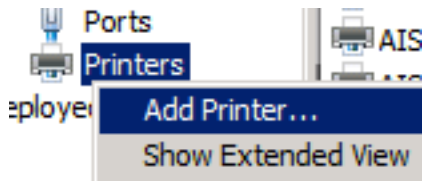
Creating Queues

Following steps are based on W2K8 server and are to be performed by a CaRS Print Queue Admins

1. Login to **Print5** (print5.its.sfu.ca) using your SAD credentials
2. Click **Start** → **Administrative Tools** → **Print Management**
3. Expand **Print Servers** on the left panel:



4. Click **Drivers** and make sure drivers exist for the printer model
5. If it does not exist, please contact ITI or CaRS T3 for installations¹. You may only proceed from this point if the requisite print drivers are already installed on the server.
6. Right-click on **Printers**
7. Click **Add Printer...**



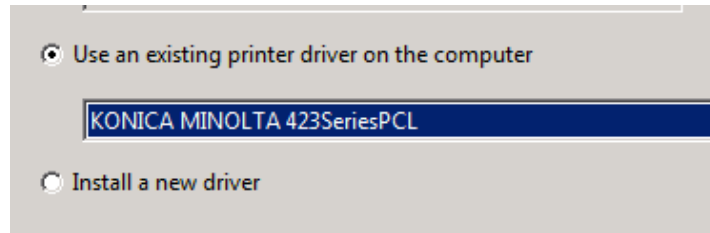
8. Follow the on screen setup wizard (assume a brand new printer):
- i. In **Printer Installation**, select "Add a TCP/IP or Web Services Printer by IP address or hostname"
 - ii. In **Printer Address**,
 - **Type of Device:** TCP/IP Device
 - **Hostname or IP address:** [Your Printer IP]
 - **Port name:** [Auto populate once you entered the IP above]
 - **Uncheck** "Auto detect the printer driver to use"

A screenshot of the 'Printer Address' setup wizard. It features three input fields: 'Type of Device' with a dropdown menu set to 'TCP/IP Device', 'Host name or IP address' with the text '142.58.1.1', and 'Port name' with the text '142.58.1.1'. Below these fields is a checkbox labeled 'Auto detect the printer driver to use.' which is currently unchecked.

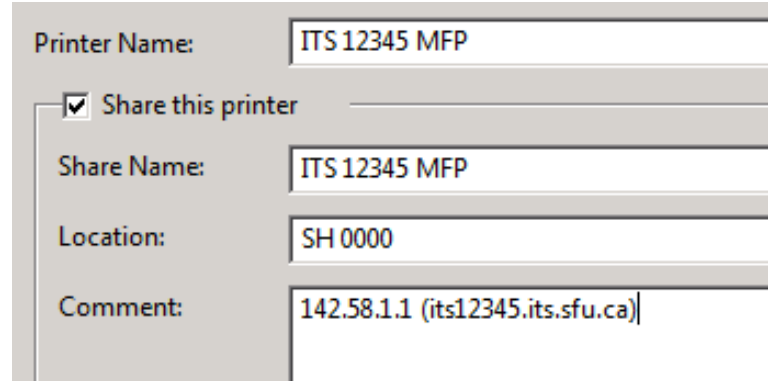
- iii. In **Additional port information required**,
 - Select **Standard** and pick **Generic Network Card**

A screenshot of the 'Device Type' selection screen. It has two radio buttons: 'Standard' (which is selected) and 'Custom'. To the right of the 'Standard' radio button is a list box containing 'Generic Network Card', which is highlighted with a blue selection bar. Below the list box is a 'Settings...' button.

- iv. In **Printer Driver**,
 - Select "Use an existing printer driver on the computer" and pick the appropriate driver



- v. In **Printer Name and Sharing Settings**,
- **Printer Name:** [Name of the print queue]²
 - **Check “Share this printer”**
 - **Share Name:** [Exactly the same as Printer Name]
 - **Location:** [Physical location of this printer]
 - **Comment:** [A few comments about this printer such as IP, hostname, permitted users, ACL, etc.]



- vi. In **Printer Found**, click **“Next”** to finish

9. When a queue is created, contact a server administrator (ITI or CaRS T3) for an export³ to Print⁴. Ideally, this should only take place once a day and preferably in the evening in order to have access to more of the server’s resources.

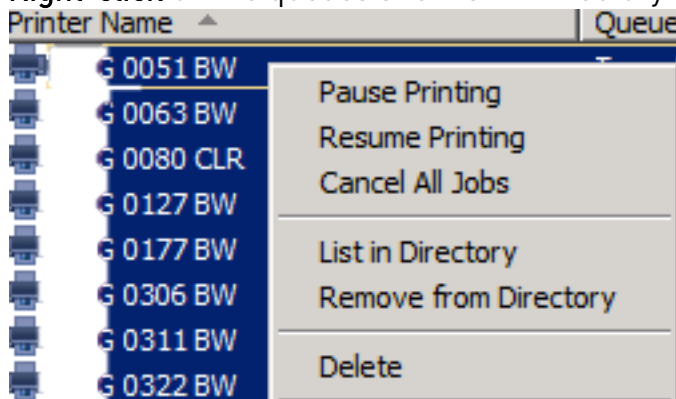
Exporting Queues

These steps should and can only be completed by a server admin (either ITI or CaRS T3).

1. Login to **Print5** (print5.its.sfu.ca)

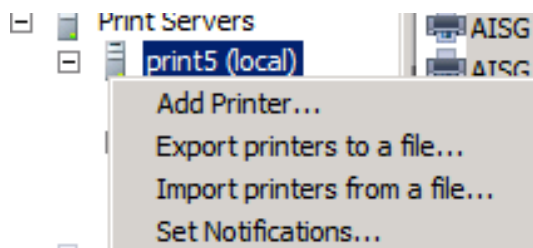
2. Click **Printers** and **select all** print queues

3. **Right-click** on the queues and **List in Directory**



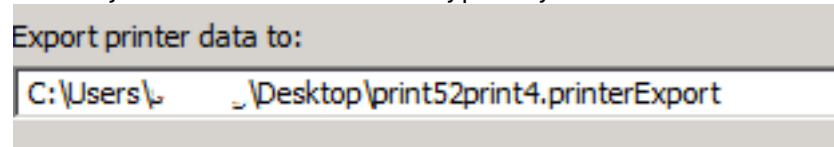
4. **Right-click** print5 (local)

5. Click “**Export printers to a file...**”



6. Follow the on-screen wizard:

- In “**Select the file location**”, export printer data to: [Anywhere on Print5 where you can write the file. I typically save it on the desktop]



7. Once the setup wizard finishes exporting queues to a file, copy the file to a shared folder on Print4. You can map a network share using your AD credentials to `\\print4.its.sfu.ca\PrintMigration`

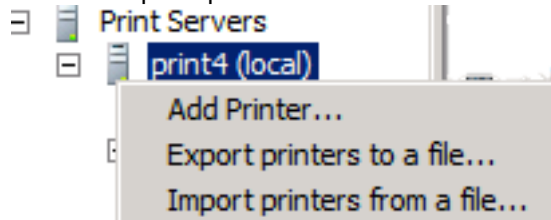
8. Login to Print4 (print4.its.sfu.ca) using your AD credentials

9. Click **Start** → **Administrative Tools** → **Print Management**

10. Expand Print Servers on the left panel

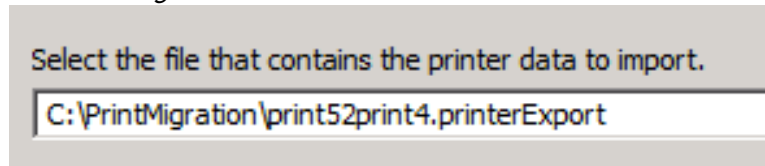
11. Right-click on **print4 (local)**

12. Click “Import printers from a file...”



13. Follow the on-screen wizard

- Select the file that you have just copied from Print5. It should be in *C:\PrintMigration*



14. Once the server has finished importing the queues, complete the tasks below:

- Delete ALL cheque print queues
- Set print queues to duplex

Endnotes

1. Members of the CaRS Print Queue Admins group do not have full access to the server, and as such new drivers will need to be installed by a server administrator first (ITI or CaRS T3). Once it is installed, it becomes available for everyone. New drivers should first be installed and tested on PrintDev (printdev.its.sfu.ca) to ensure stability.
2. Our standard print queue naming convention is in the form of: (note the spaces):

[Department/OU] [Unique Identifier] [Printer Type]

For example: ITS 12345 MFD or ITS 12345 BW or ITS 12345 CLR

However, there are exceptions:

- Cheque printers: Queue name should be all one word without any spaces
3. The main reason we create print queues on Print5 (Tier2) and then export to Print4 (Tier1) is so we can keep both servers in sync. We want to have queues available on Print4 be available on Print5 so when a user needs access to the same physical printer, most queue settings (e.g. names, drivers, etc.) will be the same. The easiest way is to have a master source and in this case we have chosen to use Print5. Since queues on Print5 need the least amount of customizations (e.g. duplex or custom paper sizes), it gives us the most flexibility to make the needed changes after exporting queues to Print4.

Appendix D

Health and Counselling Secure Printing Solution

Technology Overview:

Our objective is to secure the traffic with IPSEC between workstations and printers in areas of the university with confidential printing requirements. There are 3 steps in setting this up: client, Windows print server, and Lexmark MarkNet IPsec enabled print server. The client will negotiate with the windows server first and thus these two devices must be configured to negotiate using the same methods. The Windows print server will then negotiate with the MarkNet print server which must also be configured to negotiate using the same methods. This means the client-Windows print server configuration could be different than the Windows print server-MarkNet print server configuration.

In our scenario we chose to use Kerberos between the clients and Windows print servers and PSK between the Windows print server and MarkNet print server.

Requirements:

- Supported printer with parallel or USB ports
- Workstation running Windows XP SP2
- Lexmark MarkNet 7002e, or 7002e Print Server
- Windows 2003 based print server
- Ipseccmd.exe installed on the client

Setting up the client

Create a local or domain GPO and configure it to run the following script when the computer logs into the network:

```
ipseccmd.exe -f 0+server1FQDN 0+server2FQDN -n INPASS ESP[3DES,SHA] -a  
KERBEROS -1s 3DES-SHA-3 -w REG -p SecurePolicy -r SecureRule -x -o
```

```
ipseccmd.exe -f 0+server1FQDN 0+server2FQDN -n INPASS ESP[3DES,SHA] -a  
KERBEROS -1s 3DES-SHA-3 -w REG -p SecurePolicy -r SecureRule -x
```

The first line in this script removes the IPsecurity policy and filter list while the second creates new ones. We do this in order to ensure any changes we make to the policy immediately take effect. Here is a breakdown of the commands we use:

- **Ipseccmd.exe** – Executable
- **-f 0+server1FQDN 0+server2FQDN** – Filter list
This command creates a new filter list to include communications between “my ip address (0)” and the listed servers (0+server1FQDN 0+server2FQDN). The + indicates a mirrored rule where traffic in the opposite direction is also included.
- **-n ESP[3DES,SHA]** – Negotiation method list
Here we specify the supported integrity and encryption algorithms. We have employed 3DES for encryption and SHA1 for integrity.
- **-a KERBEROS** – Authentication methods
On the client side we are only supporting Kerberos. This integrates with AD and is the most secure yet simplistic method of authentication supported in the Windows implementation of IPsec.
- **-1s 3DES-SHA-3** – Security method list
Here we specify how we are going to secure the key exchange. We have chosen to use 3DES for encryption, SHA1 for integrity and Diffie-Hellman Group 14 (2048bit) for key establishment.

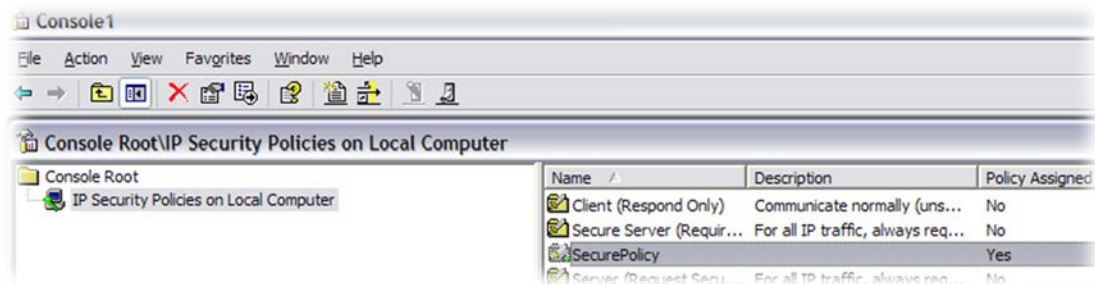
- **-w REG** – Location
REG specifies that the policy is to be installed locally.
- **-p SecurePolicy** – Policy name
This specifies a name for the policy.
- **-r SecureRule** – Rule name
This specifies a name for the filter list.
- **-x** – Assigns the policy.
- **-o** – Deletes the policy.

Verifying the policy

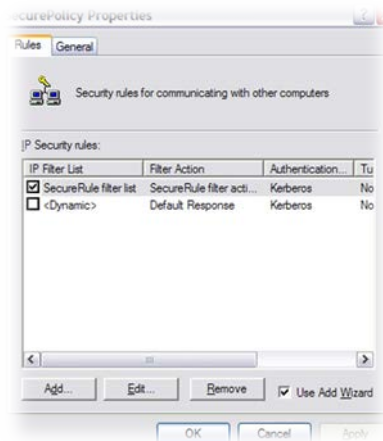
The easiest way to verify the policy is to view it through the GUI. Alternatively you may also verify the policy by executing the *ipseccmd show all* command or viewing the following registry location:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\IPSec\Policy.

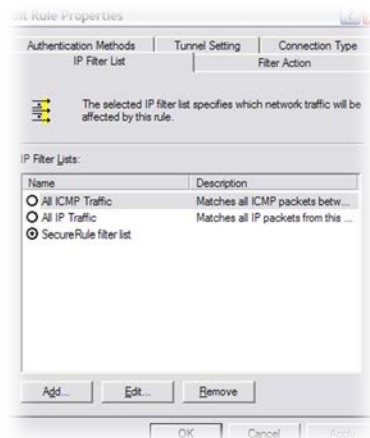
1. Launch the Microsoft Management Console (mmc) by clicking **Start, Run** then enter **MMC** and click **Ok**.
2. Press **Ctrl + M** or click **File, Add/Remove Snapin** and add the **IP Security Policies** snapin for the local machine.
3. Click the **IP Security Policies on Local Computer** node. This will display the installed policies in the right pane.
4. Ensure **SecurePolicy** is assigned.



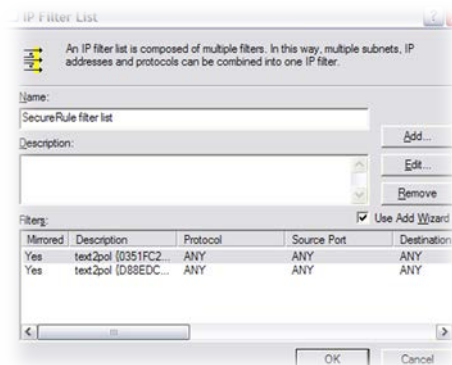
5. Double click **SecurePolicy** to open its properties. Verify that **SecureRule filter list** is the only item selected.



6. Double click **SecureRule filter list** and verify that **SecureRule filter list** is selected on the **IP Filter List** tab.



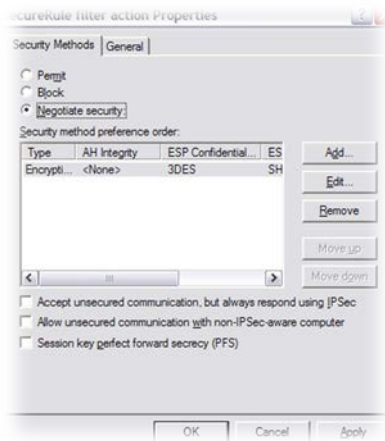
7. Double click **SecureRule filter list** and verify that the filters match your requirements. For example in our scenerio our filters look like this:



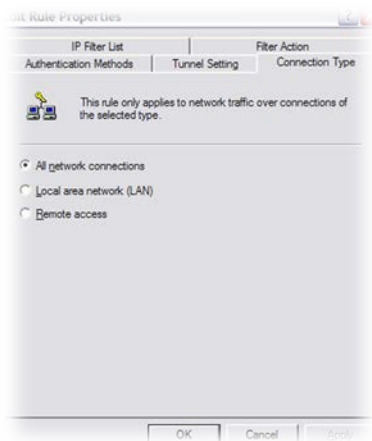
Using any protocol or port, all traffic from the client this policy is installed on to a destination of server1 or server2 and back will be included.

Click **Cancel**.

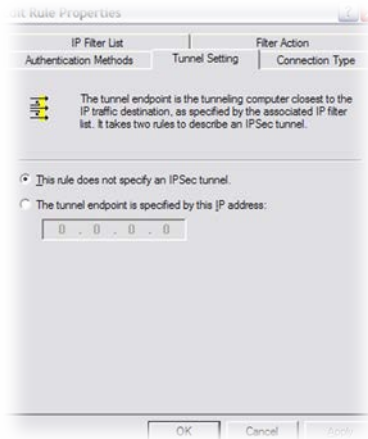
8. Select the **Filter Action** tab and verify **SecureRule** filter action is selected. Double click the filter action to view its properties. Ensure **Negotiate security** is selected and that none of the other boxes are. Ensure there is only one security method and that it says **Encryption and integrity** under **Type**. **AH Integrity** should be set to none, **ESP Confidentiality** to 3DES, **ESP Integrity** to **SHA1** and **Key Lifetimes** to 0/0 (default).



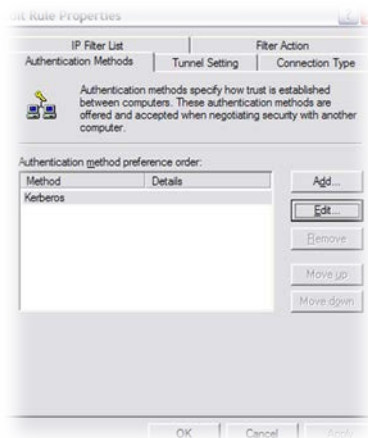
9. Click **Cancel** then select the **Connection Type** tab. Ensure **All network connections** is selected.



10. Select the **Tunnel Setting** tab and ensure **This rule does not specify an IPSec tunnel** is selected.



11. Select the **Authentication Methods** tab and verify that **Kerberos** is the only item listed.

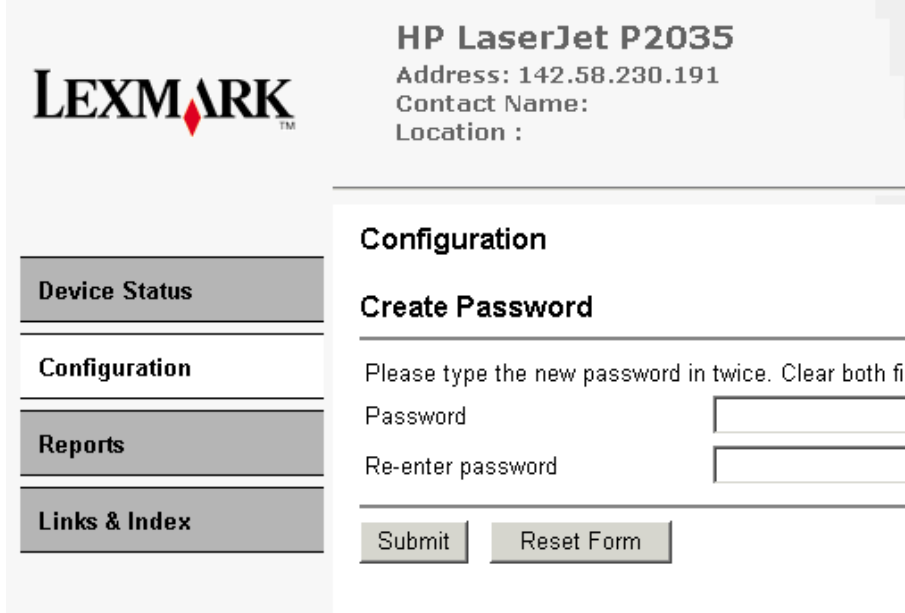


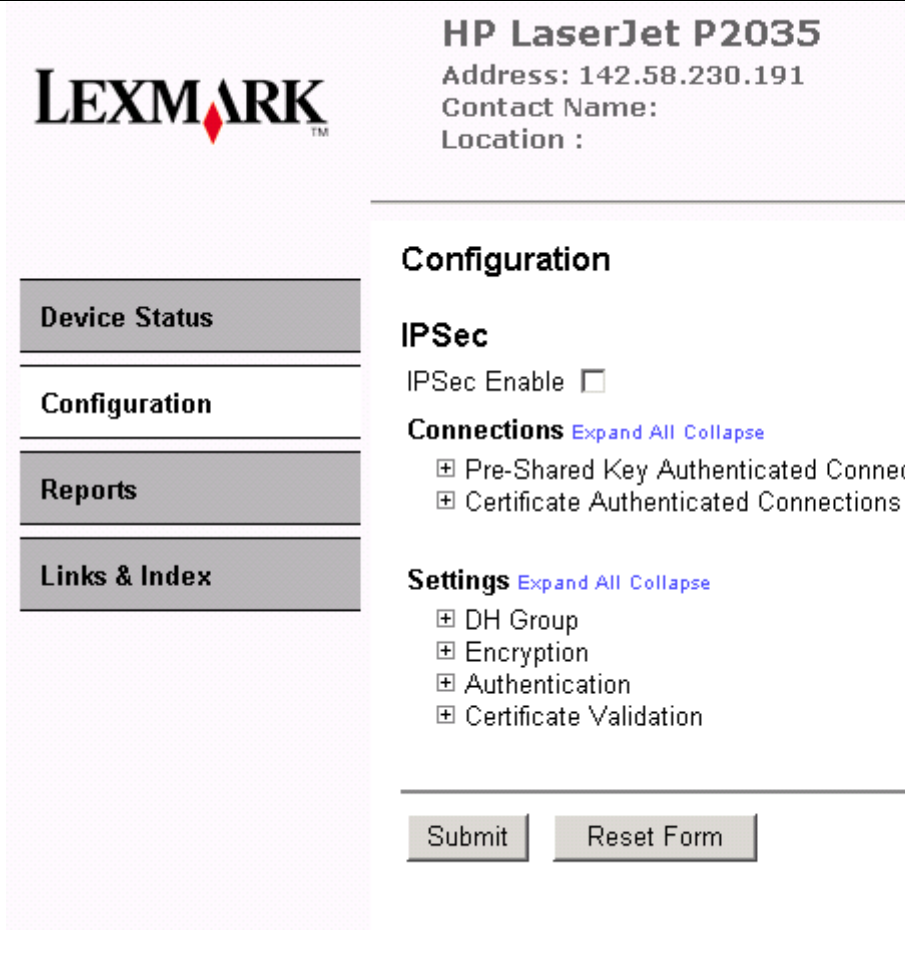
12. Click **Ok** and **Close** to exit the policy.

Setting up the MarkNet Print Server

Power up the MarkNet Print Server and specify the TCP/IP settings. Connect a printer to the device then connect it to the network. You should be able to connect to the device via the web interface (<https://ipaddress>) in order to configure it:

Make sure it is HTTPS used to communicate!

<p>Enable an administrator password. The username is admin. The password scheme is the old ITDS default scheme.</p> <p>Click Submit (and wait)</p>	 <p>The screenshot shows the Lexmark HP LaserJet P2035 web interface. On the left is a navigation menu with 'Device Status', 'Configuration', 'Reports', and 'Links & Index'. The main content area shows the device name and IP address (142.58.230.191). Under the 'Configuration' section, the 'Create Password' page is active, prompting the user to enter a new password twice. There are 'Submit' and 'Reset Form' buttons at the bottom.</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


<p>Click the Configuration link on the left side then the Security link on the right then IPSec on the right.</p>	 <p>The screenshot shows the Lexmark HP LaserJet P2035 web interface. The 'Configuration' link in the left navigation menu is highlighted. The main content area shows the 'IPSec' configuration page. The 'IPSec Enable' checkbox is unchecked. Under the 'Connections' section, 'Pre-Shared Key Authenticated Connections' and 'Certificate Authenticated Connections' are listed with expand/collapse icons. Under the 'Settings' section, 'DH Group', 'Encryption', 'Authentication', and 'Certificate Validation' are listed with expand/collapse icons. 'Submit' and 'Reset Form' buttons are at the bottom.</p>
----------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Click the **IPSec Enable** check box and enter the appropriate configuration details. At time of writing, there are two print servers, so there should be two Hosts configured.

- These are
1. AIS-TSAPP10 (142.58.102.44) the Tier1 printserver and
 2. AIS-TSAPP9 (142.58.102.43) the Tier2 print server

Notes:

1. the IP specified should be the IP of the host that will be establishing a secure channel of communication with the MarkNet device. This



HP LaserJet P2035
 Address: 142.58.230.191
 Contact Name:
 Location :

Device Status

Configuration

Reports

Links & Index

Configuration

IPSec
 IPSec Enable

Connections [Expand All](#) [Collapse](#)

Pre-Shared Key Authenticated Connect

Host 1

Address

Key

Host 2

Address

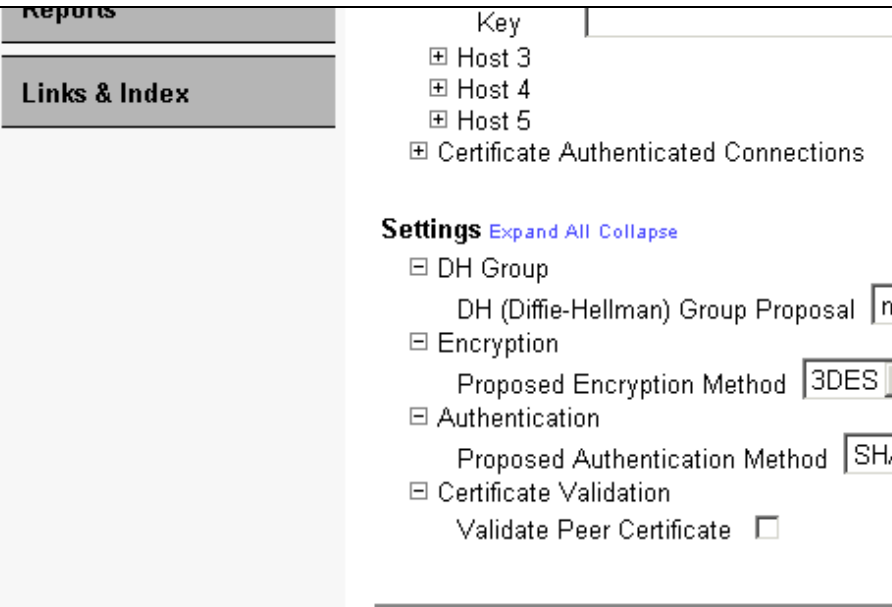
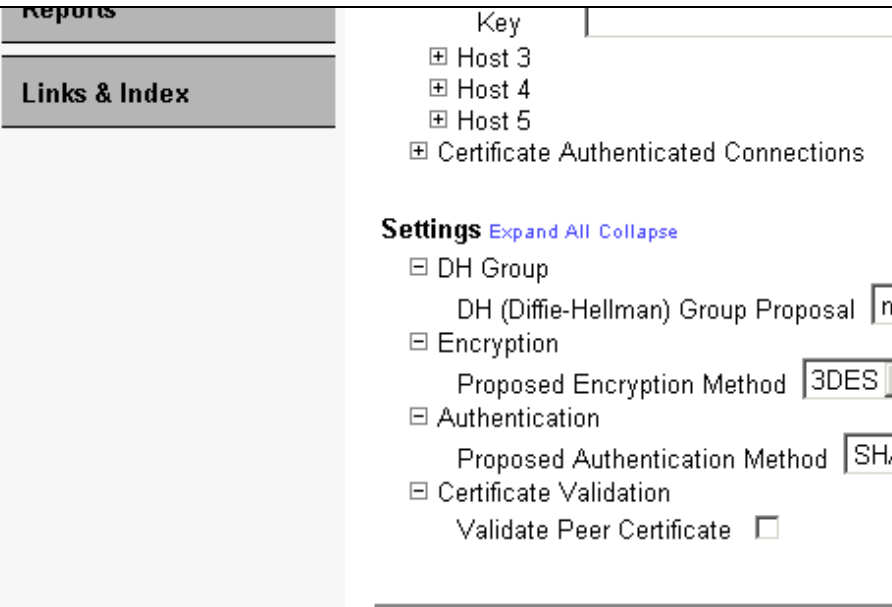
Key

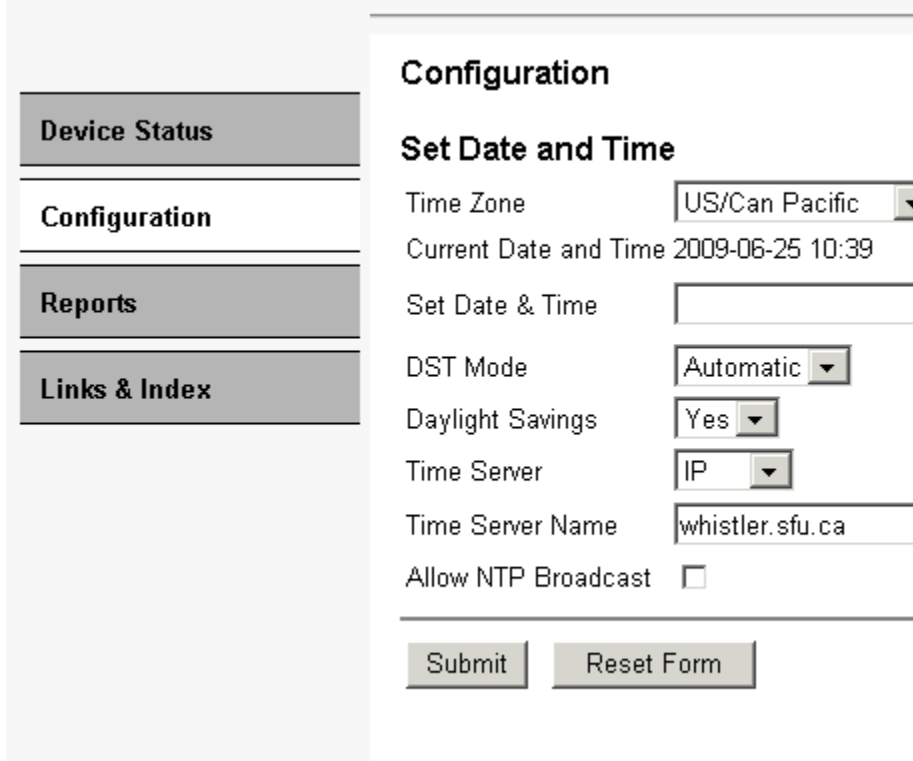
Host 3

Host 4

Host 5

Certificate Authenticated Connections

<p>will typically be the Windows Print Server not the client. A client address would only be entered for testing purposes.</p> <p>2. The key is obscured in this document, but Alan or Scott can provide it.</p>	
<p>3. The Settings should be configured as shown here.</p> <p>Once done, click Submit (and wait)</p>	

<p>Set up the Date and Time</p> <p>(Configuration - Set Date and Time)</p> <p>Set as shown here.</p> <p>Click Submit wait as usual and then go back in to determine that the unit did pick up the settings from Whistler.</p>	
<p>Close the web page. (Interesting that there is no way to Log Out.)</p>	
<p>RDP to AIS-TSAPP10.UCS.SFU.CA From a command prompt, ping the device.</p> <p>Note that the first line says Negotiating IP Security followed by replies. This is good, and is a positive indication that</p>	<pre>C:\Documents and Settings\alan>ping 142.58.235.115 Pinging 142.58.235.115 with 32 bytes of data: Negotiating IP Security. Reply from 142.58.235.115: bytes=32 time=2ms TTL=250 Reply from 142.58.235.115: bytes=32 time=1ms TTL=250 Reply from 142.58.235.115: bytes=32 time=1ms TTL=250 Ping statistics for 142.58.235.115: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 2ms, Average = 1ms</pre>

everything is working properly. Nothing but Negotiating IP Security is a sign that something is wrong. Either the server is not configured to speak IPSEC to this IP address or some settings are wrong.

If you do NOT see Negotiating IP Security but do see Replies, then the network is OK and IPSEC *might* be OK. It only negotiates the very first time it contacts the unit after a reboot. After that, there is no need to negotiate. Note that the Print Server reboots nightly, so for a brand new setup, it *should* negotiate.

Setting up the Windows Print Server

Assuming the printer has already been set up on the print server, this configuration won't be much different than the client. In our environment the configuration is different only due to the fact that we are authenticating with the client using Kerberos and the MarkNet device using a PSK.

Create a local or domain GPO and configure it to run the following script when the computer logs into the network:

```
ipseccmd.exe -f 0+MarkNet.ucsfu.ca 0+x.x.x.* -n ESP[3DES,SHA] -a KERBEROS  
PRESHARE:"***PreSharedKey***" -1s 3DES-SHA-3 -w REG -p SecurePolicy -r  
SecureRule -x -o
```

```
ipseccmd.exe -f 0+MarkNet.ucsfu.ca 0+x.x.x.* -n ESP[3DES,SHA] -a KERBEROS  
PRESHARE:"***PreSharedKey***" -1s 3DES-SHA-3 -w REG -p SecurePolicy -r  
SecureRule -x
```

The first line in this script removes the IPsecurity policy and filter list while the second creates new ones. We do this in order to ensure any changes we make to the policy immediately take effect. Here is a breakdown of the commands we use:

- **Ipseccmd.exe** – Executable
- **-f 0+MarkNet.ucsfu.ca 0+x.x.x.*** – Filter list
This command creates a new filter list to include communications between “my ip address (0)” and the listed subnet and MarkNet device. We use x.x.x.* to specify a subnet rather than a host name as we used on the client. The + indicates a mirrored rule where traffic in the opposite direction is also included.
- **-n ESP[3DES,SHA]** – Negotiation method list
Here we specify the supported integrity and encryption algorithms. We have employed 3DES for encryption and SHA1 for integrity.
- **-a KERBEROS PRESHARE:"***PreSharedKey***"** – Authentication methods
On the client side we are only supporting Kerberos. This integrates with AD and is the most secure yet simplistic method of authentication supported in the Windows implementation of IPsec.
- **-1s 3DES-SHA-3** – Security method list
Here we specify how we are going to secure the key exchange. We have

chosen to use 3DES for encryption, SHA1 for integrity and Diffie-Hellman Group 14 (2048bit) for key establishment.

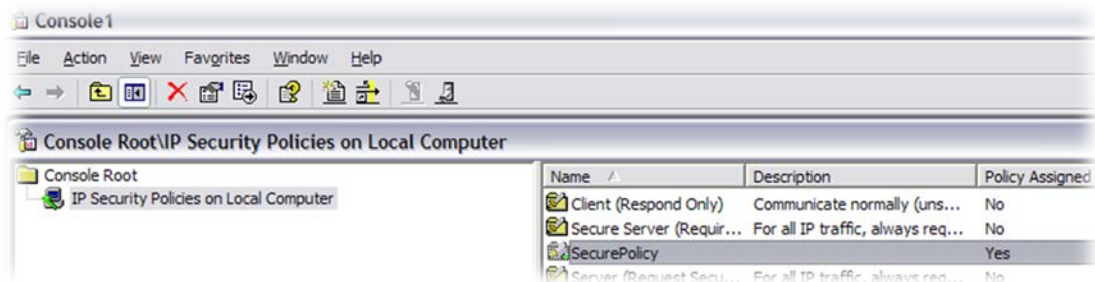
- **-w REG** – Location
REG specifies that the policy is to be installed locally.
- **-p SecurePolicy** – Policy name
This specifies a name for the policy.
- **-r SecureRule** – Rule name
This specifies a name for the filter list.
- **-x** – Assigns the policy.
- **-o** – Deletes the policy.

Verifying the policy

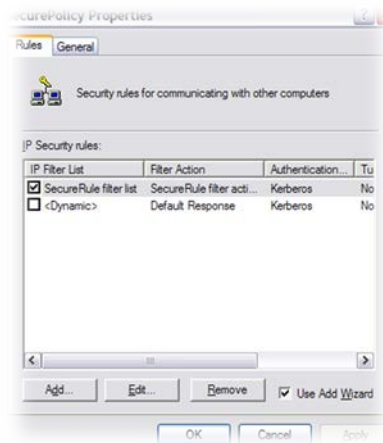
The easiest way to verify the policy is to view it through the GUI. Alternatively you may also verify the policy by executing the *ipseccmd show all* command or viewing the following registry location:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\IPSec\Policy.

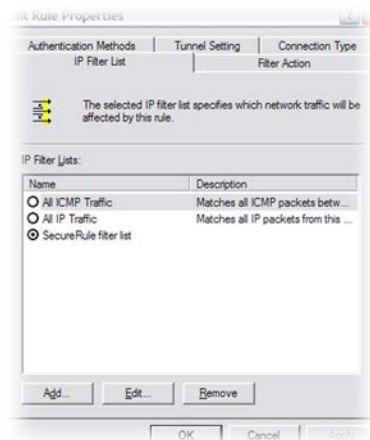
13. Launch the Microsoft Management Console (mmc) by clicking **Start, Run** then enter **MMC** and click **Ok**.
14. Press **Ctrl + M** or click **File, Add/Remove Snapin** and add the **IP Security Policies** snapin for the local machine.
15. Click the **IP Security Policies on Local Computer** node. This will display the installed policies in the right pane.
16. Ensure **SecurePolicy** is assigned.



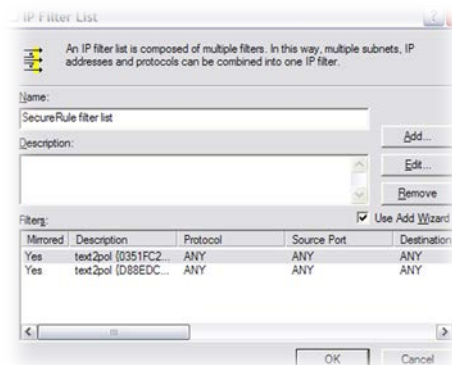
17. Double click **SecurePolicy** to open its properties. Verify that **SecureRule filter list** is the only item selected.



18. Double click **SecureRule filter list** and verify that **SecureRule filter list** is selected on the **IP Filter List** tab.



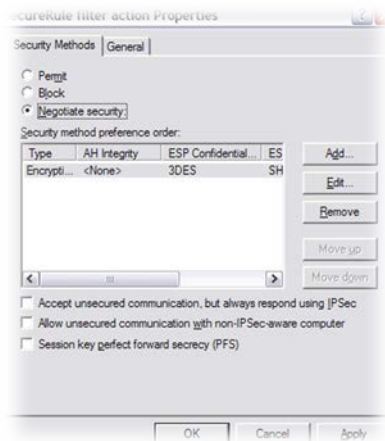
19. Double click **SecureRule filter list** and verify that the filters match your requirements. For example in our scenerio our filters look like this:



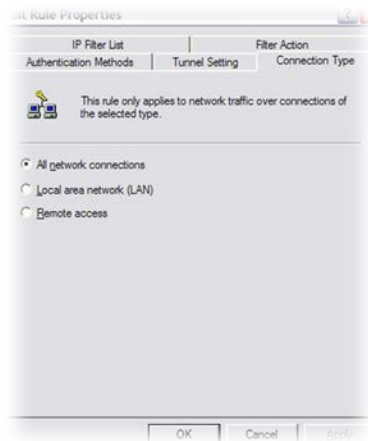
Using any protocol or port, all traffic between this server and the client subnets as well as the MarkNet print server will be included.

Click **Cancel**.

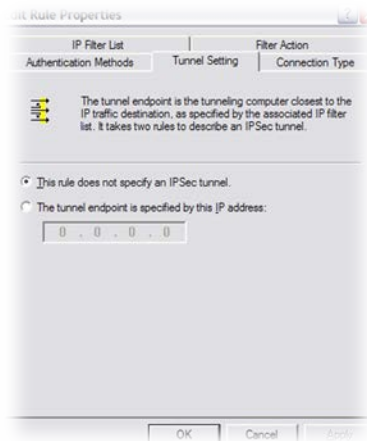
20. Select the **Filter Action** tab and verify **SecureRule** filter action is selected. Double click the filter action to view its properties. Ensure **Negotiate security** is selected and that none of the other boxes are. Ensure there is only one security method and that it says **Encryption and integrity** under **Type**. **AH Integrity** should be set to none, **ESP Confidentiality** to 3DES, **ESP Integrity** to **SHA1** and **Key Lifetimes** to 0/0 (default).



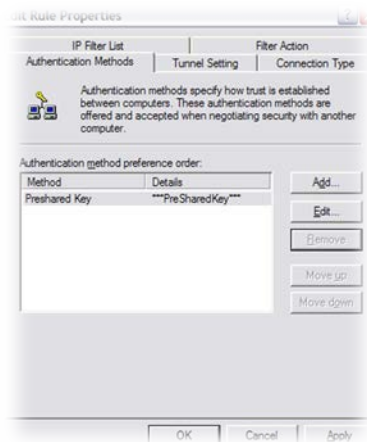
21. Click **Cancel** then select the **Connection Type** tab. Ensure **All network connections** is selected.



22. Select the **Tunnel Setting** tab and ensure “This rule does not specify an IPsec tunnel” is selected.



23. Select the **Authentication Methods** tab and verify that **Kerberos** and **Preshared Key** are listed.



Click Ok and Close to exit the policy.

Appendix E

Unix Print Queues

- Unix print queues are managed by a process called lprng (runs as /usr/localzone/sbin/lpd) on lpr.sfu.ca (hatzic.sfu.ca)
- lprng gets its config from /etc/printcap
- ITI-admins can add entries to /etc/printcap. Instructions are in the file for what to do to add a printer
- lprng supports certain types of transformations on print jobs when sending them through to the printer but we just do 'raw' pass through, so lpd process to each printer on its "raw" printer port (typically 9100)
- Messages from Unix servers are sent to lpr.sfu.ca (or lpr.nfs.sfu.ca or lpr.tier2.sfu.ca) via the LPR protocol
- Jobs are stored in /var/spool/lpd/<printername>. There are also a couple of status files in that directory that can be queried to look for problems

NOTE: Print queue names in Unix cannot have spaces because LPR is a very old text-based protocol and spaces were used to separate arguments on the line. Encapsulating the printer name in quotes remains an untested possibility.