Fortigate FSAE FSSO - Also NTLM Browser Setup Info

Current Method - Fortigate FSSO AD Collector Method WITH Agent

Quick info on Install and Functionality

- FSSO Agent is installed on a DC you select as PRIMARY. During the install a Domain Collector Agent is installed on ALL domain controllers to intercept username and IP for login events.
- **A reboot is required on all DC's** (eventually on a time of your choosing) to enable the DC agents and have the setup function
- Once the main agent is installed and all DC's have been rebooted for the agent install the DC Agents send login info to the main Fortinet FSSO Collector agent. The agent then pushes the username, associated IP and all windows groups to the Fortigate along with the group membership of the user. On the Fortigate you map a Windows group to a Fortigate group and then add the Fortigate group to a firewall rule. Users who are members of the windows group mapped to the fortigate group then are allowed access based on firewall rules linked to the configured Fortigate groups (based on the workstation IP that the login event originated from).
- When a user logs out of the machine the IP to user mapping disappears/is removed from the fortigate.
- If your MAIN Collector Domain Controller (with the agent) goes down. Firewall rules will NOT be created. When the DC with agent comes back up existing logins will not map to the fortigate. Users must log out of their PC and log back in to re-authenticate on the fortigate.
- Due to the above fact you should have a fall through rule allowing basic internet below your FSSO authentication rules in case your main collector DC goes down.
- Remember If you have a catch-all rule enabled under your FSSO rules: If a user fails authentication/does not log into AD/has no FSSO user login event then that user will fall through to the catchall rule. Therefore if you have a catch-all rule you cannot shut off a users internet completely by disabling their AD user.

Phase 1: FSSO AD Collector Setup

1. Setup an admin AD user (we call it fsso or fsae) and then LOG INTO THE DC AS THE USER.
2. Download and start the FSSO agent install with admin privileges: FSSO_Setup_5.0.0302_x64.exe
3. Follow these instructions to make your way through the setup but please also look at the following advice below while making your way through the steps: FSSO_Collector_setup.pdf
4. When it asks for the user/pass to run the service as USE THE FSAE or FSSO USER YOU ARE LOGGED IN AS and make sure to format the username properly. Dont use .\ use domain\user or user@domain.name (the actual name of your domain. Its possible you may not HAVE to even feed in the domain part depending on your forest setup. Do NOT use administrator. You shouldnt be using that account anywhere. If you are you should be changing its password regularly and you dont want to keep updating the service when you do.
5. On step 5 of the PDF for the Collector Agent IP address you would input the IP address of the domain controller you are currently installing the collector on. This will be the MAIN collector server. Leave the port at 8002.
6. For step 6 of the PDF if you are a non-REMC1 Supportnet district you likely only have one domain here to select. If you DO have multiple domains only select the domain of the current Member/district you are in. DO NOT CHECK THEM ALL. If you feel like you need to check more then one please discuss with REMC1 engineers. Feeding 1000's of unnecessary login information to your collector as well as the Fortigate is NOT NECESSARY and will likely cause performance issues and unreliability.
7. On step 7 of the PDF do put checkmarks by service accounts and users who should not make dynamic firewall rules/be monitored. MSSQL users, test users, guest users, service accounts. If this is a REMC1 staff please look at the accounts we exempted on remc1dc1 for examples. This IS an important step.
8. On step 9 make sure ALL your domain controllers are checked for install of the DC Agent. If you dont... you will miss login events and have unreliable webfilter/firewall rule assignment.
9. **You must restart each domain controller before setting up/enabling FSSO on the Fortigate vdom.** Only after reboot will the DC agents start collecting login Information.
10. On the PDF page 6 (actually labeled 126 in the bottom right corner since its a PDF excerpt) it shows opening up the FSSO collector config after setup. Make sure "Require Authentication from Fortigate" is checked and you put a complex password in the box. Keep track of this because you need to use the same password on the Fortigate later.

11. Otherwise after setting the password the rest of the config should already be set. Hit Apply then save&close.
12. If all DC's are rebooted we can continue to the Fortigate config. Continue using the same PDF instructions but move on to phase 2 below.

Phase 2: FSSO Fortigate Vdom Setup

1. Continue on with the same FSSO Collector PDF as above.
2. Ya know what. Just skip over the LDAP part. I havent needed it because I select "push group membership from the FSSO agent". Why make things complicated if we dont have to?
3. For step 3 go to Security FabricExternal Connectors and create a new "FSSO Agent on Windows AD" connector
4. Type in a good name eg: FSSO_Agent_REMC1 or FSSO_Agent_DistrictName
5. Type in the IP of the server you installed the agent on. Use the password you set when you went into the FSSO agent config on step 10 above.
6. Set "User Group Source" to collector agent (vs ldap/advanced)
7. Click "Apply and Refresh" then Save.
8. If you go back into the Connector config you should now see all your groups and the connector should show as connected.
9. Move on to "Create a user group for FSSO users" which goes over doing just that.
10. Below that are examples of using that new Fortigate group to create firewall rules.
11. The instructions for viewing logins are incorrect. In 6.4 and above you have to go to Dashboard then to the lower plus sign and "add monitor" to add a firewall user monitor to the list (if its not already there). Now you can click on that and view all firewall/FSSO users with IP. You can force de-authenticate a user that you previously locked out of AD.
12. Remember If you have a catch-all rule enabled under your FSSO rules: If a user fails authentication/does not log into AD/has no FSSO user login event then that user will fall through to the catchall rule. Therefore if you have a catch-all rule you cannot shut off a users internet completely by disabling their AD user.

LEGACY yet still relevant NTLM Method - Server Side Config Setup

Browser config for Firefox and IE is at the bottom

- For NTLM based single-sign-on you first need to download the Collector and Agent install from support.fortinet.com.
- Here is the latest FSSO AD connector install for FortiOS 6.2.X and up
    - FSSO_Setup_5.0.0302_x64.exe

---

1. Log into support.fortinet.com
2. Go to the downloads section and click on Fortigate
3. You're now in an FTP session in your browser. Browse up the folder tree to the most recent maintenance release of the overall major release that we are currently running.
4. Look for an FSAE or SSO folder in the firmware download folder. If you don't find one... they didn't release a new version for that maintenance release. Try the previous one. Rinse and repeat until you find the latest one.
5. Save it onto the Active Directory server/domain controller you want to install it on (install it on all of them in the domain as you can list multiple FSAE/SSO servers in the Fortigate to create redundancy)
6. DO NOT INSTALL IT UNDER THE ADMINISTRATOR ACCOUNT!!! If you ever change the password of administrator it will break the FSAE service.
7. The manual says to create an FSAE domain admin user and generate a password in the Password Vault.
8. Log in as that FSAE user via RDP and install the service.
9. Click next through the defaults until you get to the username/password part
10. Make sure .\fsae is the user (if that's the user you created and are logged in as) and set the password to the one set for FSAE (or the user you created)
11. On the next screen UNCHECK: "Monitor user events and send the information to Fortigate"
12. Leave checked: Serve NTLM authentication requests....
13. Leave the radio button on "Standard"
14. Click Next then Install then Finish
15. Now run the setup: Start->All Programs->Fortinet->Configure FSAE (or SSO for later versions)
16. Once the config window pops open click "Run as Administrator" in the bottom left
17. Make sure "Require Authentication from Fortigate" is checked and find the FSAE password in password vault to put in the password box. If there is no password yet and you are setting up FSAE/SSO for the first time in a domain, make one in PV.
18. Click the "Select domains to monitor" button and make sure all domains are selected. I don't think the part matters for NTLM auth though but just note that it's there and you may need to put a check next to any new domains that are added to the forest later.
19. Click apply then save&close.
20. In group policy for this domain go to the district Domain and edit the (district)Security Group policy (for REMC1 Supportnet Districts) or for non-supportnet districts Create a FortinetFSSO group policy linked to the base of your domain OU structure.
21. Go to: Policies->Windows Settings->Security Settings->Local Policies->Security Options
22. Make sure: Network security: Restrict NTLM: Incoming NTLM traffic is set to "allow all"
23. Make sure: Network security: Restrict NTLM: NTLM authentication in this domain is set to "Disable"
24. Make sure: Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers is set to "allow all"
25. If you had to change any of those settings, drop down to an administrative command prompt and do a: gpupdate /force
26. Possibly restart the FSAE service too
27. Probably have to open the firewall for the FSAE port
28. Go to the network and sharing center
29. Click the "Windows Firewall" link in the bottom left corner
30. Click Advanced Settings on the right side of the window.
31. Click "Inbound Rules"

32. Click New Rule in the left pane
33. For rule type select "Port"
34. For tcp make the port range 8000-8002 (hit next)
35. Make sure allow the connection is select and hit next
36. Make sure the rule applies to all network types (private, public, domain)
37. Name it something good like FSAE or FortigateSSO
38. Make two more rules to allow LDAP and LDAPS (Ports 389 and 636)
39. Now go to active directory users and computers.
40. Optional (and unnecessary for REMC1 agencies): Create a group of type GLOBAL in the appropriate OU called <domain>StaffInternet and <domain>StudentInternet example: LLStaffInternet. and add all staff users individually to the staff group and students individually to the student group. The LDAP connector will not follow nested groups so all users must reside in their respective groups.
41. Required (if you didnt do optional step 40) Make sure you have an existing staff and student group where all users reside individually in their respective groups. REMC1 agencies do have this. Do not add groups as shown above. You will link the fortigate to these groups in the steps below.
42. Option if you followed step 40: Add the appropriate groups or users to this/these group(s) who will be allowed internet access.

Fortigate Config

Fortigate Settings (setting up the foundation)

1. Time to configure the FortiGate. Log in and go to the appropriate Vdom.
2. Optional but HIGHTLY recommended: Under the vdom go to: config user setting and then set "**set auth-on-demand**"

3. Go to User&Device
4. Make sure "NewREMC1Sha2-CA is selected for certificate.
5. Make sure (via the cli) that set auth-ca-cert is set to "NewREMC1Sha2-CA"
6. ssh to fortigateconfig vdom edit vdomnamehereconfig user settingset auth-ca-cert "NewREMC1Sha2-CA" (Yes both certs must be set to this per Fortinet instructions in a ticket I had with them).
7. Click the User Section->User&DeviceLDAP Servers
8. Create new (button on top left)
9. Name it after your servers FQDN (eg: file1.remc1.adremc1.org)
10. Server Port 389 (for REMC1 our standard is to use 636 LDAPS so use this)
11. Common Name Identifier switch to: sAMAccountName
12. For Distinguished name just use the base of your domain. You can change it later if you really want but its not necessary. Eg: dn=remc1, dn=adremc1, dn=org
13. Bind Type: Regular
14. Username (MAKE A NEW USER IN YOUR AD INFRASTRUCTURE. REMC1 STANDARD IS DISTRICT ABBREVIATION+FSSO EG: remc1fsso. Give it domain admin (easy) or simply rights to authenticate for your whole domain OU structure (more complicated. Not gone over here).
15. DO NOT use administrator for the previous step. If you have to change it (and you should do so on a schedule) you disconnect the fortigate until you fix it there. You should never link administrator to services.
16. If you are connecting via LDAPS (RECOMMENDED and is the REMC1 standard or everything flows plain text) then click the "Secure Connection" switch.
17. Here you need to select your servers CA certificate. The Fortigate needs to trust your servers server certificate therefore it needs your CA (certificate authority) public cert uploaded and selected here to trust. REMC1 may have to do this for you. If you don't have a CA (you should...) then use unsecure ldap/normal ldap on port 389. You should add a CA.
18. Click the OK button. Now you can go back in and click the "test connectivity" button.
19. Add any more LDAP servers you might have.
20. Go to User&DeviceSingle Sign-On
21. Click Create new button on the top of the right pane (If you're adding a second collector/fsso agent then edit the already-existing Directory Server definition for that domain and add the new server to the next open FSAE Collector IP/Name field and click ok. Skip to step 18
22. Name it the FULL DNS name of the domain example: remc1.adremc1.org as the name will represent what domain the FSSO setup is pointing to.
23. Add the new server to the first open FSAE Collector IP/Name field, put in the secret you create and record in LastPass (or the password manager you use for your district).
24. Click Advanced (for Collector Agent AD access mode)
25. For the LDAP server select one of the LDAP servers you added above.
26. Click apply and refresh button
27. You should now see an OU tree on the left side and user/group/org units on the left side.
28. Click the Recursive switch on the left side pane above the Object Unit/Distinguished name browsing section.
29. On the Right side start enabling groups you want to map to Fortigate groups. Its easiest to search for the groups you want to add.
30. For each group right click and select "add selected"
31. You should see the "selected" counter (third tab over) increase for every group you add.
32. When done click on the "Selected" tab making sure all is ok.
33. Click OK
34. Now, on the left side click the User&Device section->User Groups
35. Add a new group by clicking "create new" on top of the right pane
36. Name it very descriptive like "LakeLindenStaffInternet"
37. Set the group type: Fortinet Single Signon (FSSO)
38. Under Members click the Plus sign and add the appropriate group(s) you enabled in the Single Sign-on setup. If you dont see a group you need go back to the Single-Signon setup and enable that group. Come back here and add it.
39. Once you have added all your groups you can move on to the Firewall rule setup.

Fortigate Firewall Rule

1. Start out creating a new firewall rule as you normally would selecting the appropriate source and destination Interfaces/zones and source /destination networks
2. In the source box (along with the source subnet) Click the plus again and for the next source select type user.
3. Select the appropriate group you want to allow access.
4. Continue on as you would for a normal firewall rule selecting the appropriate webfilters, app control, setup SSL/SSH options (Cert scanning vs deep scanning).
5. NOTE: As of 5.6 FSSO/NTLM auth rules will work fine with Cert Scanning OR Deep Scanning.
6. Click OK.
7. Continue to add rules for each group you created (remc1, staff etc..)
8. If you want to allow users WITHOUT and AD username access then add the SSO_Guest_Users group to the rule. I believe you only add it to one rules per source subnet since if nobody auths via AD for that rule it will automatically fall to the guest user.
9. If you dont want to allow users without an AD username access for a certain source subnet then dont ad the SSO_Guests_Users group.
10. When a user authenticates it will grab a list of group memberships for that user and select the appropriate rule.
11. Click OK the firewall rule should add
12. TEST!! =)

FSSO Gotchas!! Important! Read!

Dual group membership

- If you are a member of both Student and Teacher groups, the FortiGate will put you into the first group rule it hits (so if it hits student first you will count as a student and not a teacher). Therefore, make sure the teacher rule is first and then it will allow those staff to count as teachers first, and it will fall back to student settings for those not in the teacher group.

Traffic that matches FSSO rule AND non-FSSO rule

- If there are two rules that match traffic: One rule matches WITH FSSO and one WITHOUT the fortigate will ALWAYS CHOOSE THE RULE OF LEAST RESISTANCE (the NON-FSSO rule) so PLAN YOUR RULES CAREFULLY. Order of rules does not matter with FSSO. If a rule more easily matches below an FSSO rule then the fortigate will use it instead.

Certificate warnings

- If this is a Chrome device you have to push and trust the cert to all devices. This works OK from the root domain but subdomains still may not trust a pushed CA. The cert will push but not trust. Could be a still open/historic Google Admin bug.
- You didnt push out the CA Certificate selected under Users & DevicesAuthentication Settings to your clients. Push it via GPO and/or Kace and/or Google Console.
- Make sure "NewREMC1Sha2-CA is selected for certificate.
- Make sure (via the cli) that set auth-ca-cert is set to "NewREMC1Sha2-CA"
- ssh to fortigateconfig vdom edit vdomnamehereconfig user settingset auth-ca-cert "NewREMC1Sha2-CA" (Yes both certs must be set to this per Fortinet instructions in a ticket I had with them).

Browser config for NTLM FSSO Authentication

Make the following changes in group policy or Kace if possible. NOT individually on each machine.

For IE

Option 1 (By Hand)

1. Tools->internet options
2. Security tab
3. Click custom level
4. Scroll all the way to the bottom
5. Under User authentication->Logon select Automatic logon with current username and password

Option 2 (By GPO)

- (For REMC1 supportnet districts this entry goes in <DOMAINabbreviation>Security) GPO location 2008 Server User Configureation - Policies - Administrative Templates - Windows Components - Internet Explorer - Internet Control Panel - Security Page - Internet Zone - Logon options = Enable (Auto login with current username and password)

For Firefox

Option 1 (by hand)

1. In the address bar type: About:Config
2. Click I understand or ok in and warnings about editing the config
3. Now in the filter bar at the top type in: security.enterprise_roots.enable (if nothing comes up right-click in the window where you'd expect it to show then add new boolean value. Enter in security.enterprise_roots.enabled as the Name and set the value to true
4. If security.enterprise_roots.enabled shows up you can double click it to flip it to true.
5. Now in the filter bar at the top type in:NTLM
6. double click: network.automatic-ntlm-auth.trusted-uris
7. In the box that pops up put in the following: http://,https://
8. Click OK
9. Make sure network.automatic-ntlm-auth.allow-proxies is set to true
10. Make sure network.ntlm.send-lm-response is set to FALSE
11. Make sure network.auth.force-generic-ntml is set to FALSE

Option 2 (Use Firefox Enterprise and import the GPO)

1. A better way is to use Firefox Enterprise with the Firefox GPO and set the settings listed in Option 1 section above via the GPO.
2. Here is where you download the ADMX file along with info on its use: https://support.mozilla.org/en-US/kb/customizing-firefox-using-group-policy-windows
3. Direct link to the github page: https://github.com/mozilla/policy-templates/releases

Options also explained here with another option of packaging Firefox with an answer file.

- Configuring Firefox to use the Windows Certificate Store.pdf
- umbrella.cfg
- local-settings.js

Chrome

- uses the settings from IE. Setup and get IE working right and Chrome will work fine.

More OS X info

- http://stackoverflow.com/questions/8616818/integrated-windows-auth-ntlm-on-a-mac-using-google-chrome-or-safari
- Instructions on better integration with safari and chrome for OS X. Should be using 10.7