Cisco live!

January 29 - February 2, 2018 · Barcelona

BRKSEC-3227

Integrating and Troubleshooting Identity Features on the Firepower System

Justin Roberts

Firepower TAC – Technical Lead

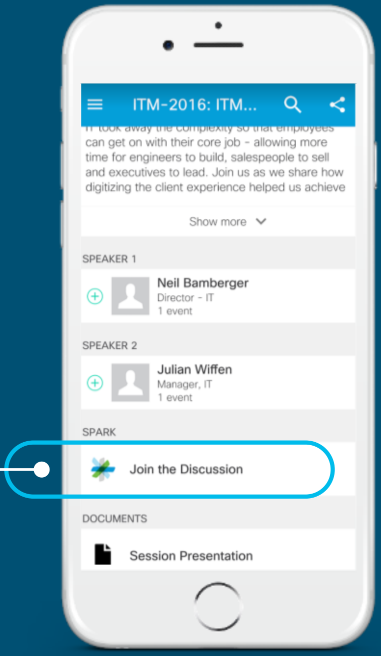
Cisco Spark

Questions?

Use Cisco Spark to communicate with the speaker after the session

How

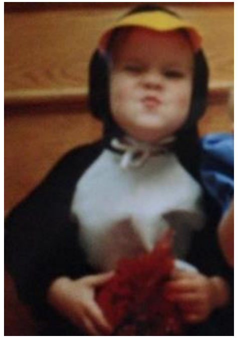
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

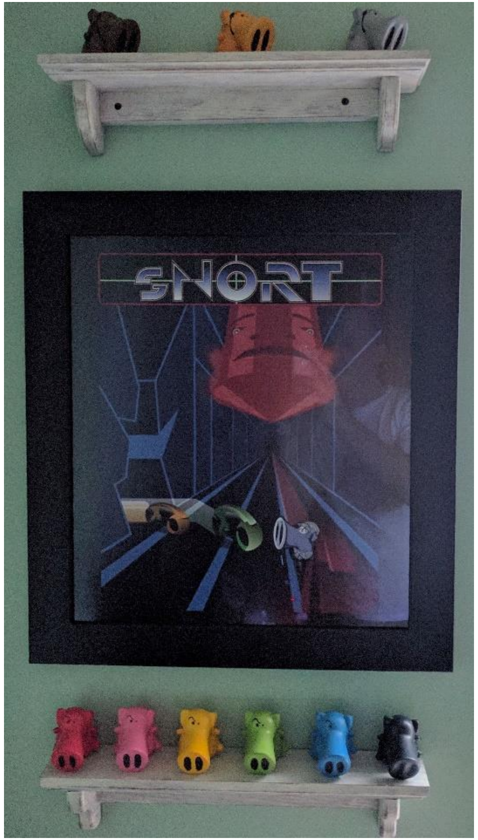


cs.co/ciscolivebot#BRKSEC-3227

A little about myself

- Born and raised in Baltimore, Maryland
  - Also where I currently live!
- Technical Lead – Fulton, Maryland
  - 4 years in TAC
- Before Cisco, Solaris Administration
  - Solaris 10/11 (Long live ZFS)
- Might have a Snorty obsession…





Agenda

- Overview of Authentication Features
- Passive Authentication Architecture Deep Dive
- Active Authentication Architecture Deep Dive
- Advanced Troubleshooting and Failure Identification
- Common Issues Discussion

Abstract

This session will provide detailed explanations and troubleshooting methodologies for the various Identity/User Awareness features available in the Firepower system:

- Identity Services Engine (ISE)
- Cisco Firepower User Agent for Active Directory
- Captive Portal
- Terminal Services Agent (TSA)

Participants will be provided with Cisco Technical Assistance Center (TAC) recommended best practices and advanced troubleshooting techniques to explain how to effectively implement and maintain Firepower Identity features.

Participants will also be provided with an Identity troubleshooting cheat-sheet with tips on how to troubleshoot each feature and enable participants to quickly isolate issues in the future.

Here are the things that will be covered

Provider technology architecture as it pertains to Firepower

- Identity Services Engine (ISE)
- Active Directory
- Terminal Services

Low level analysis of Firepower identity architecture

- Firepower Management Center
- Firepower Managed Devices

Advanced Firepower identity troubleshooting tools and techniques

Here are the things that will **not** be covered

Basic configuration information

Remote Access VPN (RA-VPN)

Advanced troubleshooting of provider side technology

- Identity Services Engine (ISE) / pxGrid
- Active Directory
- Terminal Server / Virtual Desktop Infrastructure (VDI)

Recommended Sessions

Session ID	Description
BRKSEC-3889	Advanced Security Architecture Integrations using APIs and pxGrid
BRKSEC-3229	ISE under magnifying glass. How to troubleshoot ISE
BRKSEC-2501	Deploying AnyConnect SSL *VPN* with ASA (and Firepower Threat Defence)

Cisco Firepower Sessions: Building Blocks

TUESDAY
WEDNESDAY
THURSDAY

BRKSEC-2050
Firepower NGFW Internet Edge Deployment Scenarios

BRKSEC-2051
Deploying AnyConnect SSL VPN with ASA (and Firepower Threat Defense)

BRKSEC-2058
A Deep Dive into using the Firepower Manager

BRKSEC-2064
NGFWv and ASAv in Public Cloud (AWS and Azure)

BRKSEC-2056
Threat Centric Network Security

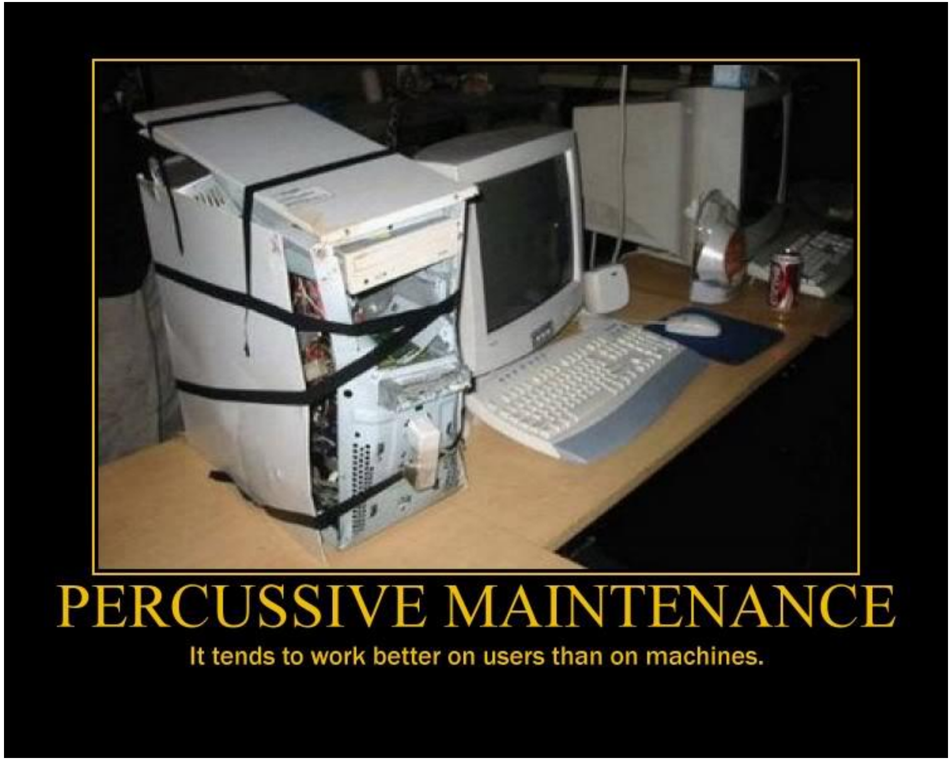
BRKSEC-3300
Advanced IPS Deployment

BRKSEC-3667
Advanced Firepower SSL policy troubleshooting

BRKSEC-3035
Firepower Platform Deep Dive

BRKSEC-3455
Dissecting Firepower NGFW “Installation & Troubleshooting

Introduction



Lets break this into two logical phases

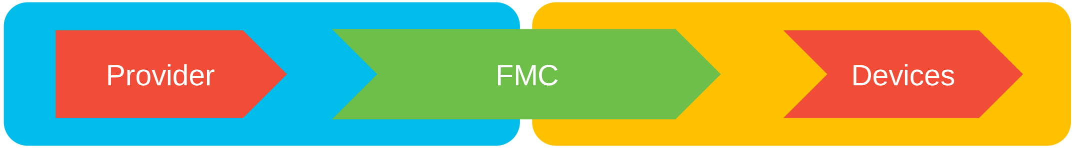
Troubleshooting Phases

Phase 1 – Provider Side

- Data capture from the authoritative identity source
- Communicating authoritative data over to Firepower

Phase 2 – Firepower Side

- Post processing of data from the authoritative source
- Propagation to sensing devices for enforcement



Overview of Authentication Features

There are two types of authentication

Passive Authentication

- Identity Services Engine (ISE)
- Terminal Services Agent (TSA)
- Cisco Firepower User Agent

Active Authentication

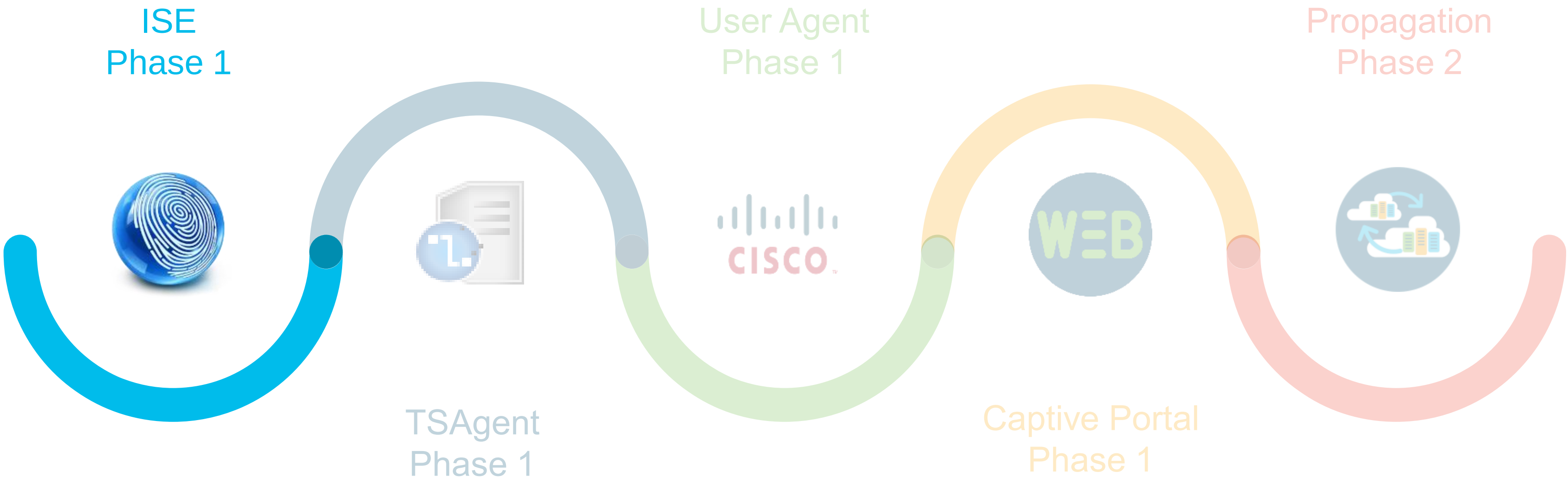
- Remote Access VPN (RA-VPN)
- Captive Portal

Before we start…

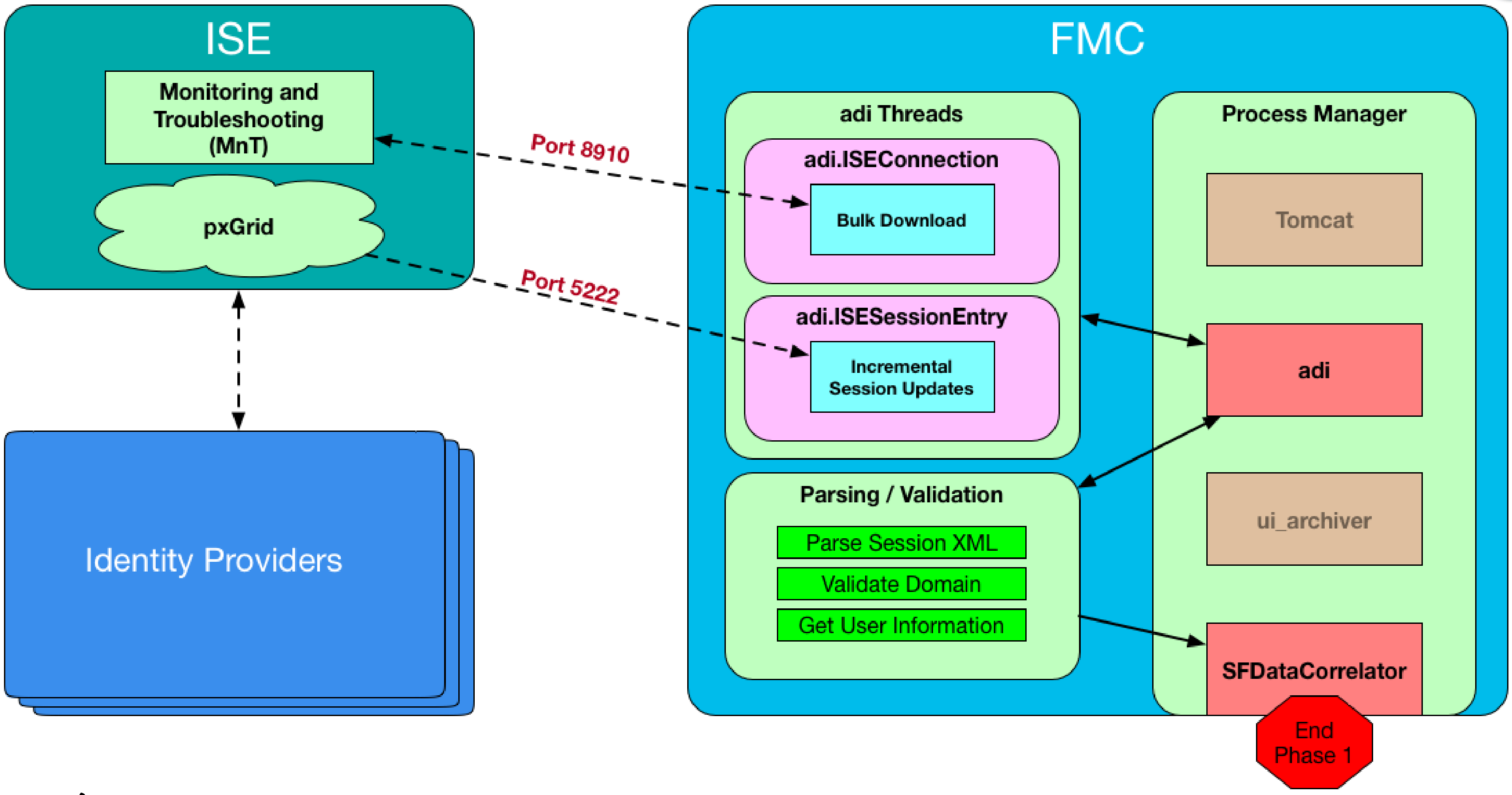
- **Process Manager (PM)**
  - Owns and controls the critical system processes for Firepower
  - Interact via the "**pmtool**" binary
    - **pmtool status** – Gives an itemized status for all processes (*Running, User-Disabled, Down, Waiting*)
    - **pmtool [*enablebyid* | *disablebyid* | *restartbyid*] <process_name>** - enable, disable, or restart specific processes (case sensitive for process_name)
- **"…"**
  - Seen frequently on Command Line slides
  - Indication that there is data in between that was omitted.
- Symbol for Reference Slides
  - Useful information in the PDF!

Passive Authentication Architecture Deep Dive

Phase Discussion

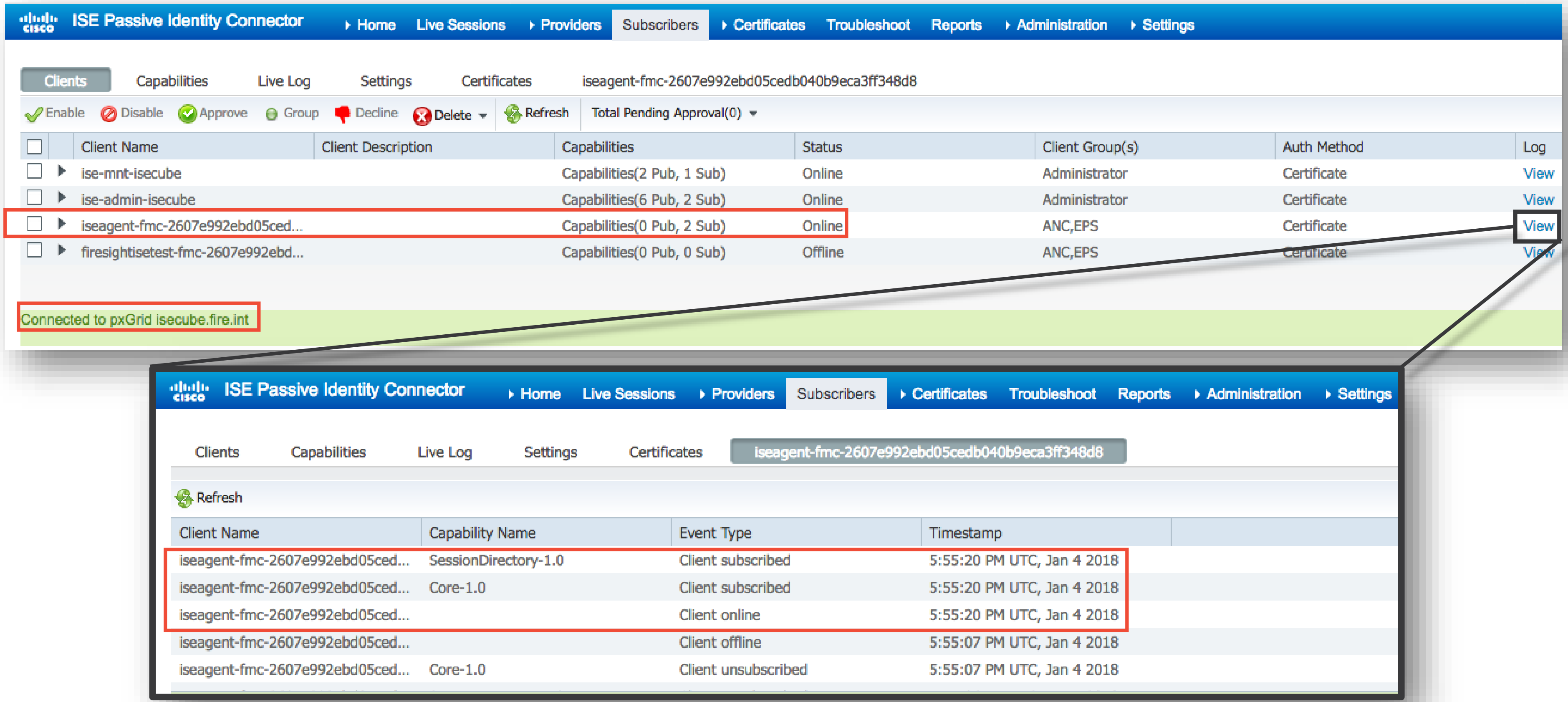


ISE Diagram



ISE
Monitoring and Troubleshooting (MnT)
pxGrid
Port 8910
Port 5222
Identity Providers
FMC
adi Threads
adi.ISEConnection
Bulk Download
adi.ISESessionEntry
Incremental Session Updates
Parsing / Validation
Parse Session XML
Validate Domain
Get User Information
Process Manager
Tomcat
adi
ui_archiver
SFDataCorrelator
End Phase 1

Starting with the basics



Once the data is sent to the FMC

Process Check!

- Critical Processes
  - **adi** - Receives and parses XML session data (bulk and incremental). Validates it and passes it off to SFDataCorrelator
  - **SFDataCorrelator** - Accepts mappings. Marks end of Phase 1

SHELL

```
root@FMC:/# pmtool status | egrep "adi \(|SFDataCorrelator \(”
SFDataCorrelator (normal) - Running 4952
adi (normal) - Running 11568
```

Running adi in debug mode

Warning While adi is in debug, you cannot make configuration changes. This is meant only to be used for testing.

1. Shut the process down from PM:
   # pmtool disablebyid adi
2. Start it manually in debug mode:
   # adi --debug (Outputs to screen only)
   # adi --debug 2>&1 | tee /var/tmp/adi.log (Outputs to screen and log)
3. Kill the process by entering "Ctrl+C" on your keyboard.
4. Start it up again from PM:
   # pmtool enablebyid adi

Bulk Session download while in debug mode

SHELL

```
root@FMC:/# pmtool disablebyid adi
root@FMC:/# adi --debug
```

Disable ADI from PM and manually start it in Debug

```
…
Jan 04 17:53:29 FMC SF-IMS[21618]: [21668] ADI:adi.ISEConnection [DEBUG] adi.cpp:512:HandleLog(): ise url for bulk download =
https://isecube.fire.int:8910/pxgrid/mnt/sd/getSessionListByTime
Jan 04 17:53:29 FMC SF-IMS[21618]: [21668] ADI:adi.ISEConnection [DEBUG] adi.cpp:512:HandleLog(): Creating bulk download request
…
Jan 04 17:53:29 FMC SF-IMS[21618]: [21668] ADI:adi.ISEConnection [DEBUG] adi.cpp:512:HandleLog(): Bulk download request: <XML Request Body>
```

Preparing the bulk download request URL and XML body

```
…
Jan 04 17:53:29 FMC SF-IMS[21618]: [21668] ADI:adi.ISEConnection [DEBUG] adi.cpp:512:HandleLog(): bulk download iter open started
…
Jan 04 17:53:31 FMC SF-IMS[21618]: [21668] ADI:adi.ISEConnection [DEBUG] adi.cpp:512:HandleLog(): bulk download invoking callback on entry# 1
```

Make the request and start iterating through results

```
…
Jan 04 17:53:31 FMC SF-IMS[21618]: [21668] ADI:adi.ISESessionEntry [DEBUG] adi.cpp:512:HandleLog(): parsing Session Entry with following text:<XML Session Data>
Jan 04 17:53:31 FMC SF-IMS[21618]: [21668] ADI:adi.ISESessionEntry [DEBUG] adi.cpp:512:HandleLog(): parsing Session Entry with following text:<XML Session Data>
```

Parse XML response twice

```
Jan 04 17:53:31 FMC SF-IMS[21618]: [21668] ADI:adi.ISESessionEntry [DEBUG] adi.cpp:512:HandleLog(): Parsing incoming DOM resulted in following ISESessionEntry:
{gid = , timestamp(raw) = 2018-01-04T13:53:17.165Z, timestamp(parsed) = 2018-01-04 13:53:17(GMT), state = Authenticated, session_id = , nas_ip = ,
mac_addr = 172.16.1.2, ip addresses = [172.16.1.2], user_name = test2, sgt = , domain = fire.int, device_name = }
```

Resulting data from parsing

```
…
Jan 04 17:53:31 FMC SF-IMS[21618]: [21668] ADI:adi.RealmContainer [DEBUG] adi.cpp:512:HandleLog(): findRealm: Found Realm for domain fire.int
Jan 04 17:53:31 FMC SF-IMS[21618]: [21668] ADI:adi.ISEConnectionSub [DEBUG] adi.cpp:512:HandleLog(): userName = 'test2' realmId = 2, ipAddress = [172.16.1.2]
Jan 04 17:53:31 FMC SF-IMS[21618]: [21668] ADI:vdi.radius [DEBUG] adi.cpp:512:HandleLog(): adding ISE session ips = [172.16.1.2]
```

Validate domain
Set userName
Set ipAddress

```
…
Jan 04 17:53:31 FMC SF-IMS[21618]: [21668] ADI:adi.LdapRealm [DEBUG] adi.cpp:512:HandleLog(): ldap: search returned (1) result pages.
Jan 04 17:53:31 FMC SF-IMS[21618]: [21668] ADI:adi.LdapRealm [DEBUG] adi.cpp:512:HandleLog(): search '(|(sAMAccountName=test2))' has the following DN:
'CN=Test2,CN=Users,DC=fire,DC=int'.
```

Get user DN

```
…
Jan 04 17:53:31 FMC SF-IMS[21618]: [21660] ADI:infra.ev-rpc [DEBUG] adi.cpp:512:HandleLog(): Server ADI, sending event for subject adi service session directory.
```

Add mapping

New session from pxGrid while in debug mode

SHELL

```
...
Jan 04 17:54:33 FMC SF-IMS[21618]: [21639] ADI:adi.ISESessionEntry [DEBUG] adi.cpp:512:HandleLog(): parsing Session Entry with following text:<XML Session Data>
Jan 04 17:54:33 FMC SF-IMS[21618]: [21639] ADI:adi.ISESessionEntry [DEBUG] adi.cpp:512:HandleLog(): parsing Session Entry with following text:<XML Session Data>
```

Parse XML response twice

```
Jan 04 17:54:33 FMC SF-IMS[21618]: [21639] ADI:adi.ISESessionEntry [DEBUG] adi.cpp:512:HandleLog(): Parsing incoming DOM resulted in following ISESessionEntry:
{gid = , timestamp(raw) = 2018-01-04T17:54:30.715Z, timestamp(parsed) = 2018-01-04 17:54:30(GMT), state = Authenticated, session_id = , nas_ip = ,
mac_addr = 172.16.1.2, ip addresses = [172.16.1.2], user_name = test1, sgt = , domain = fire.int, device_name = }
```

Resulting data from parsing

```
...
Jan 04 17:54:33 FMC SF-IMS[21618]: [21639] ADI:adi.RealmContainer [DEBUG] adi.cpp:512:HandleLog(): findRealm: Found Realm for domain fire.int
Jan 04 17:54:33 FMC SF-IMS[21618]: [21639] ADI:adi.ISEConnectionSub [DEBUG] adi.cpp:512:HandleLog(): userName = 'test1' realmId = 2, ipAddress = [172.16.1.2]
Jan 04 17:54:33 FMC SF-IMS[21618]: [21639] ADI:vdi.radius [DEBUG] adi.cpp:512:HandleLog(): adding ISE session ips = [172.16.1.2]
```

Validate domain
Set userName
Set ipAddress

```
...
Jan 04 17:54:33 FMC SF-IMS[21618]: [21639] ADI:adi.LdapRealm [DEBUG] adi.cpp:512:HandleLog(): ldap: search returned (1) result pages.
Jan 04 17:54:33 FMC SF-IMS[21618]: [21639] ADI:adi.LdapRealm [DEBUG] adi.cpp:512:HandleLog(): search '(|(sAMAccountName=test1))' has the following DN:
'CN=Test1,CN=Users,DC=fire,DC=int'.
```

Get user DN

```
...
Jan 04 17:54:33 FMC SF-IMS[21618]: [21660] ADI:infra.ev-rpc [DEBUG] adi.cpp:512:HandleLog(): Server ADI, sending event for subject adi service session directory.
```

Add mapping

```
<ctrl+c>
```

Stop the adi debug

```
root@FMC:/# pmtool enablebyid adi
```

Re-enable adi from PM

Sample of the XML session data

Raw XML from ISE

```
<ns5:sessionNotification
    xmlns:ns2='http://www.cisco.com/pxgrid'
    xmlns:ns3='http://www.cisco.com/pxgrid/net'
    xmlns:ns4='http://www.cisco.com/pxgrid/admin'
    xmlns:ns5='http://www.cisco.com/pxgrid/identity'
    xmlns:ns6='http://www.cisco.com/pxgrid/eps'
    xmlns:ns7='http://www.cisco.com/pxgrid/netcap'
    xmlns:ns8='http://www.cisco.com/pxgrid/anc'>
    <ns5:sessions>
        <ns5:session>
            <ns2:lastUpdateTime>2018-01-04T17:54:30.715Z</ns2:lastUpdateTime>
            <ns3:state>Authenticated</ns3:state>
            <ns3:RADIUSAttrs>
                <ns3:attrName>Acct-Session-Id</ns3:attrName>
            </ns3:RADIUSAttrs>
            <ns3:interface>
                <ns3:ipIntfID>
                    <ns2:ipAddress>172.16.1.2</ns2:ipAddress>
                </ns3:ipIntfID>
                <ns3:macAddress>172.16.1.2</ns3:macAddress>
                <ns3:deviceAttachPt>
                    <ns3:deviceMgmtIntfID/>
                </ns3:deviceAttachPt>
            </ns3:interface>
            <ns3:user>
                <ns2:name>test1</ns2:name>
                <ns3:ADUserDNSDomain>fire.int</ns3:ADUserDNSDomain>
                <ns3:ADUserNetBIOSName>FIRE</ns3:ADUserNetBIOSName>
                <ns3:ADUserResolvedIdentities>test1@fire.int</ns3:ADUserResolvedIdentities>
                <ns3:ADUserResolvedDNs>CN=Test1,CN=Users,DC=fire,DC=int</ns3:ADUserResolvedDNs>
            </ns3:user>
            <ns3:assessedPostureEvent/>
            <ns3:MDMEndpoint/>
            <ns3:IdentitySourcePortStart>0</ns3:IdentitySourcePortStart>
            <ns3:IdentitySourcePortEnd>0</ns3:IdentitySourcePortEnd>
            <ns3:IdentitySourceFirstPort>0</ns3:IdentitySourceFirstPort>
            <ns3:providers>WMI</ns3:providers>
        </ns5:session>
    </ns5:sessions>
</ns5:sessionNotification>
```

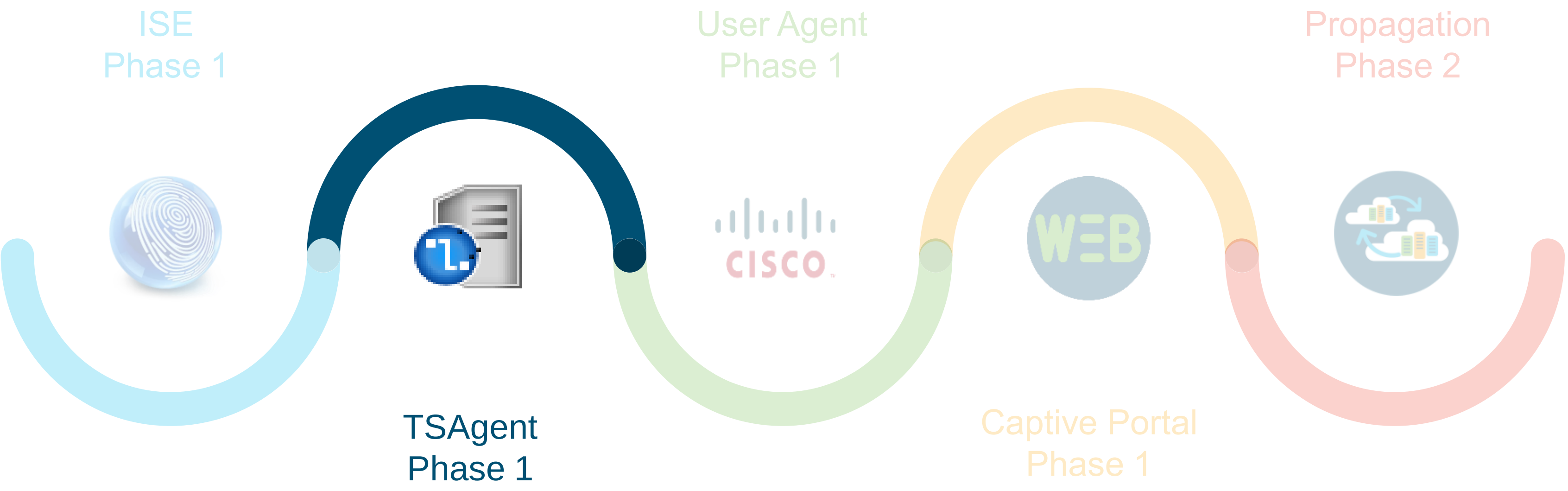
After first round of parsing

```
<session xmlns='http://www.cisco.com/pxgrid/identity'>
    <lastUpdateTime xmlns='http://www.cisco.com/pxgrid'>2018-01-04T17:54:30.715Z</lastUpdateTime>
    <state xmlns='http://www.cisco.com/pxgrid/net'>Authenticated</state>
    <RADIUSAttrs xmlns='http://www.cisco.com/pxgrid/net'>
        <attrName>Acct-Session-Id</attrName>
    </RADIUSAttrs>
    <interface xmlns='http://www.cisco.com/pxgrid/net'>
        <ipIntfID>
            <ipAddress xmlns='http://www.cisco.com/pxgrid'>172.16.1.2</ipAddress>
        </ipIntfID>
        <macAddress>172.16.1.2</macAddress>
        <deviceAttachPt>
            <deviceMgmtIntfID/>
        </deviceAttachPt>
    </interface>
    <user xmlns='http://www.cisco.com/pxgrid/net'>
        <name xmlns='http://www.cisco.com/pxgrid'>test1</name>
        <ADUserDNSDomain>fire.int</ADUserDNSDomain>
        <ADUserNetBIOSName>FIRE</ADUserNetBIOSName>
        <ADUserResolvedIdentities>test1@fire.int</ADUserResolvedIdentities>
        <ADUserResolvedDNs>CN=Test1,CN=Users,DC=fire,DC=int</ADUserResolvedDNs>
    </user>
    <assessedPostureEvent xmlns='http://www.cisco.com/pxgrid/net'/>
    <MDMEndpoint xmlns='http://www.cisco.com/pxgrid/net'/>
    <IdentitySourcePortStart xmlns='http://www.cisco.com/pxgrid/net'>0</IdentitySourcePortStart>
    <IdentitySourcePortEnd xmlns='http://www.cisco.com/pxgrid/net'>0</IdentitySourcePortEnd>
    <IdentitySourceFirstPort xmlns='http://www.cisco.com/pxgrid/net'>0</IdentitySourceFirstPort>
    <providers xmlns='http://www.cisco.com/pxgrid/net'>WMI</providers>
</session>
```

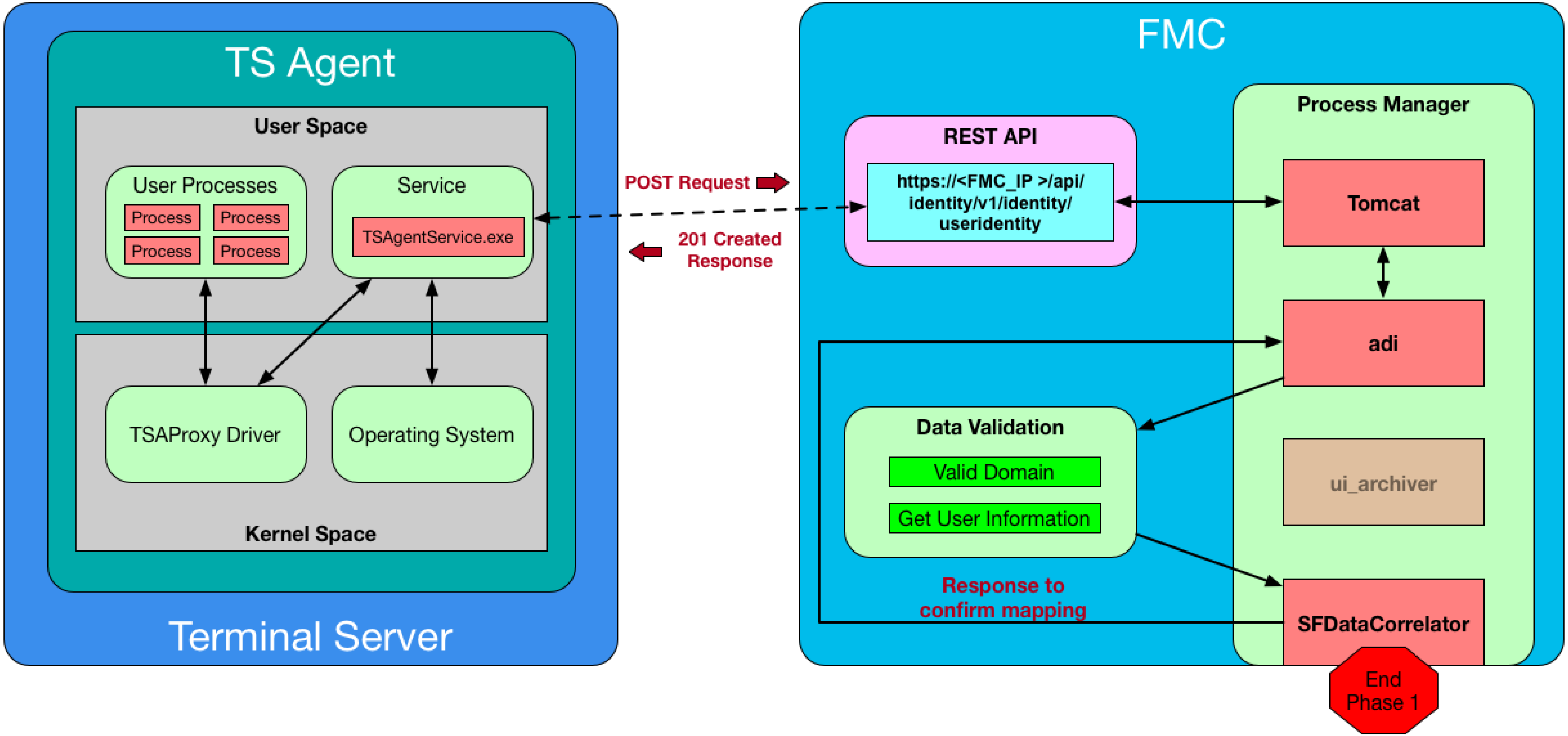
ISE Recap

- Confirm ISE is receiving data from its providers
- Validate the status of the “iseagent-fmc-<uuid>” subscriber
  - Check subscriptions / connectivity
  - Check logs for recent historical data
- Ensure the **adi** and **SFDataCorrelator** processes are up
- Put **adi** into debug mode if you suspect the problem to be on the FMC side.
- The following article is valuable for troubleshooting ISE and FMC integration:
  https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200319-Troubleshoot-ISE-and-FirePOWER-Integrati.html

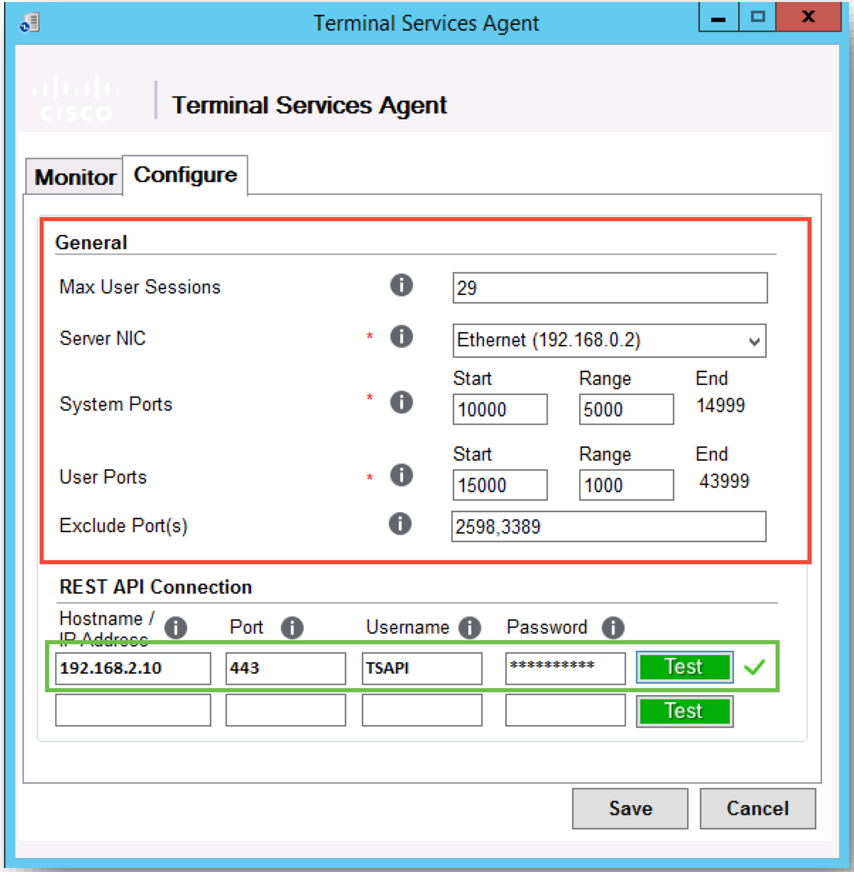
Phase Discussion



TS Agent Diagram



Starting with the basics



Check settings to ensure they are currently configured as expected

Test connections to the FMC to ensure proper connectivity and REST API user authentication

Successful test connection in FMC logs

SHELL

```
root@FMC:/# tail -f /var/opt/CSCOpx/MDC/tomcat/logs/stdout.logs
```

Start tailing Tomcat logs

```
…
[ajp-nio-127.0.0.1-9009-exec-9] INFO com.cisco.api.external.rest.common.filters.PayloadValidationFilter - No payload is available for this request
[ajp-nio-127.0.0.1-9009-exec-9] INFO com.cisco.api.external.rest.common.routing.ExtensionURLFilter - Request for extension URL passed :
/identityauth/generatetoken
[ajp-nio-127.0.0.1-9009-exec-9] INFO com.cisco.api.external.rest.common.resource.IdentityAuthenticationResource - Authentication configurable values:
[ajp-nio-127.0.0.1-9009-exec-9] INFO com.cisco.api.external.rest.common.resource.IdentityAuthenticationResource - Access Token Exp Time : 30
[ajp-nio-127.0.0.1-9009-exec-9] INFO com.cisco.api.external.rest.common.resource.IdentityAuthenticationResource - Refresh Token Exp Time : 60
[ajp-nio-127.0.0.1-9009-exec-9] INFO com.cisco.api.external.rest.common.resource.IdentityAuthenticationResource - No. of issues : 1
Nov 27, 2017 2:03:43 PM org.restlet.engine.log.LogFilter afterHandle
INFO: 2017-11-27        14:03:43        192.168.0.2     TSAPI       ::1         443         POST
          /api/fmi_platform/v1/identityauth/generatetoken       -           204         0           0           2787
          https://192.168.2.10      -         -
[ajp-nio-127.0.0.1-9009-exec-5] INFO com.cisco.api.external.rest.common.filters.PayloadValidationFilter - No payload is available for this request
[ajp-nio-127.0.0.1-9009-exec-5] INFO com.cisco.api.external.rest.common.routing.ExtensionURLFilter - Request for extension URL passed :
/identityauth/revokeaccess
[ajp-nio-127.0.0.1-9009-exec-5] INFO com.cisco.api.external.rest.common.resource.IdentityAuthenticationResource - Authentication configurable values:
[ajp-nio-127.0.0.1-9009-exec-5] INFO com.cisco.api.external.rest.common.resource.IdentityAuthenticationResource - Access Token Exp Time : 30
[ajp-nio-127.0.0.1-9009-exec-5] INFO com.cisco.api.external.rest.common.resource.IdentityAuthenticationResource - Refresh Token Exp Time : 60
[ajp-nio-127.0.0.1-9009-exec-5] INFO com.cisco.api.external.rest.common.resource.IdentityAuthenticationResource - No. of issues : 1
Nov 27, 2017 2:03:43 PM org.restlet.engine.log.LogFilter afterHandle
INFO: 2017-11-27        14:03:43        192.168.0.2     -           ::1         443         POST
          /api/fmi_platform/v1/identityauth/revokeaccess        -           204         0           0           515
          https://192.168.2.10      -         -
```

Request token

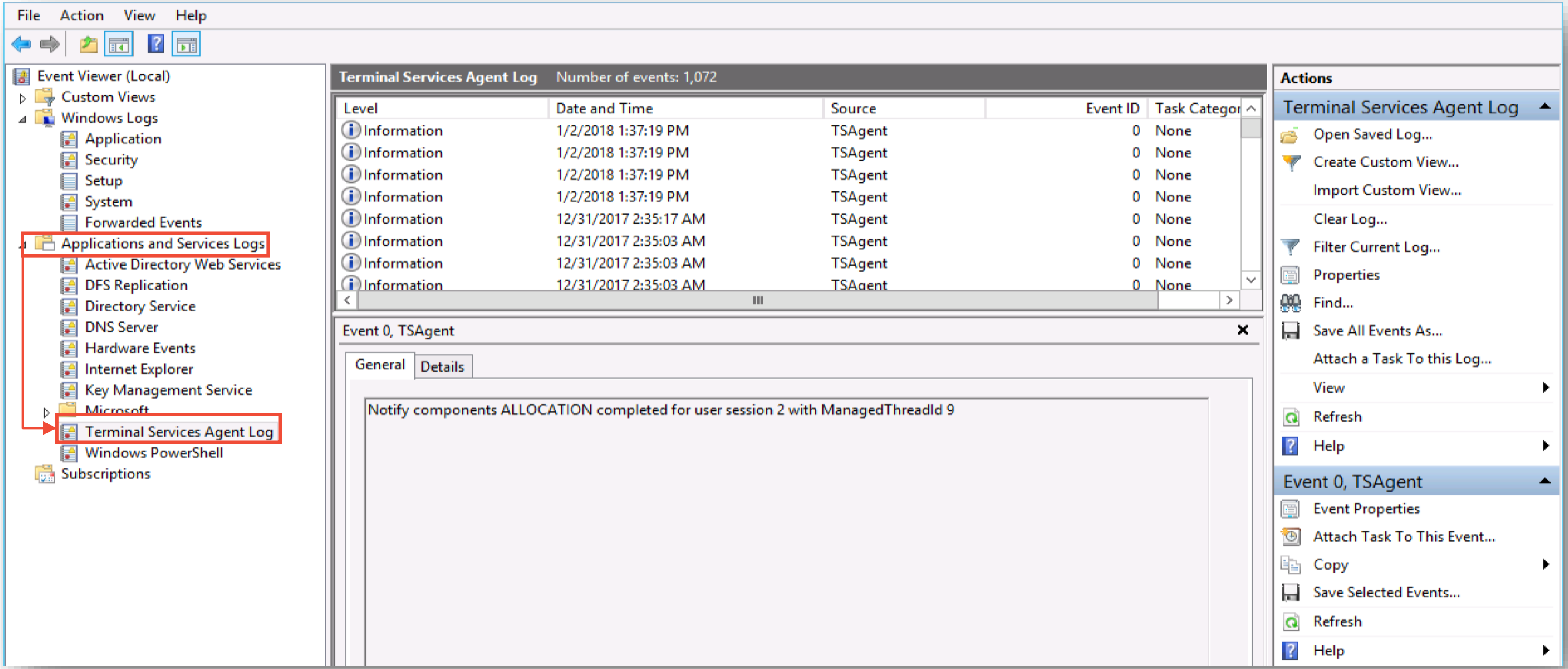
204 No Content response

Revoke token

204 No Content response

Checking the local application logs

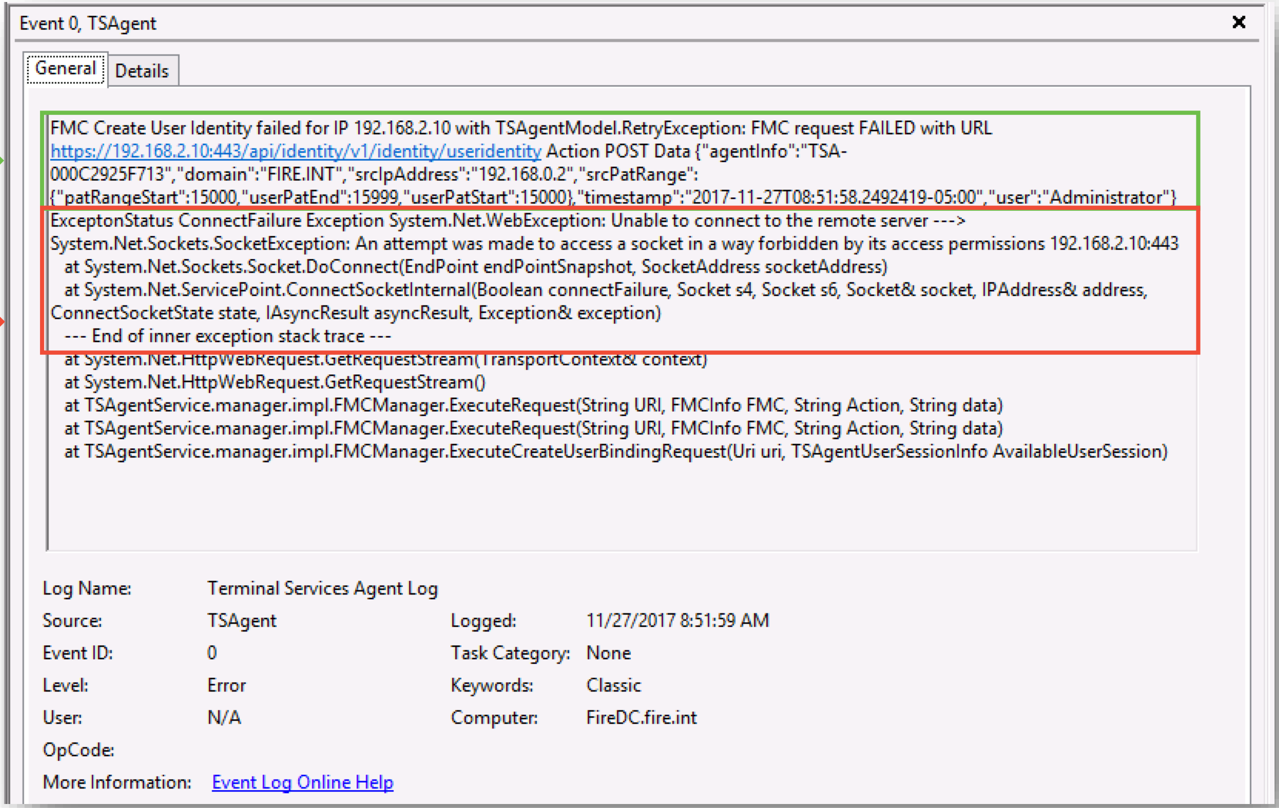
Administrative Tools > Event Viewer



Example of an error for a local issue

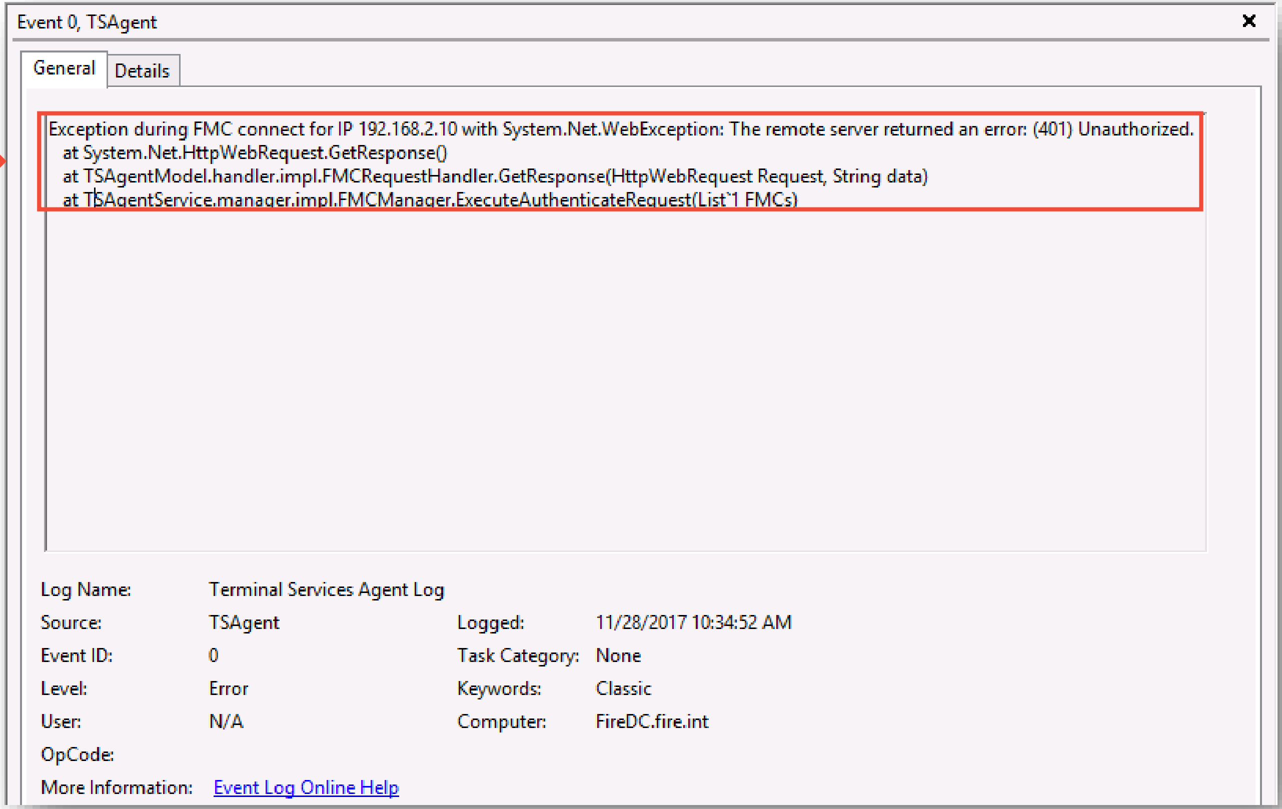
The raw POST request to the FMC

Error in accessing an existing Socket

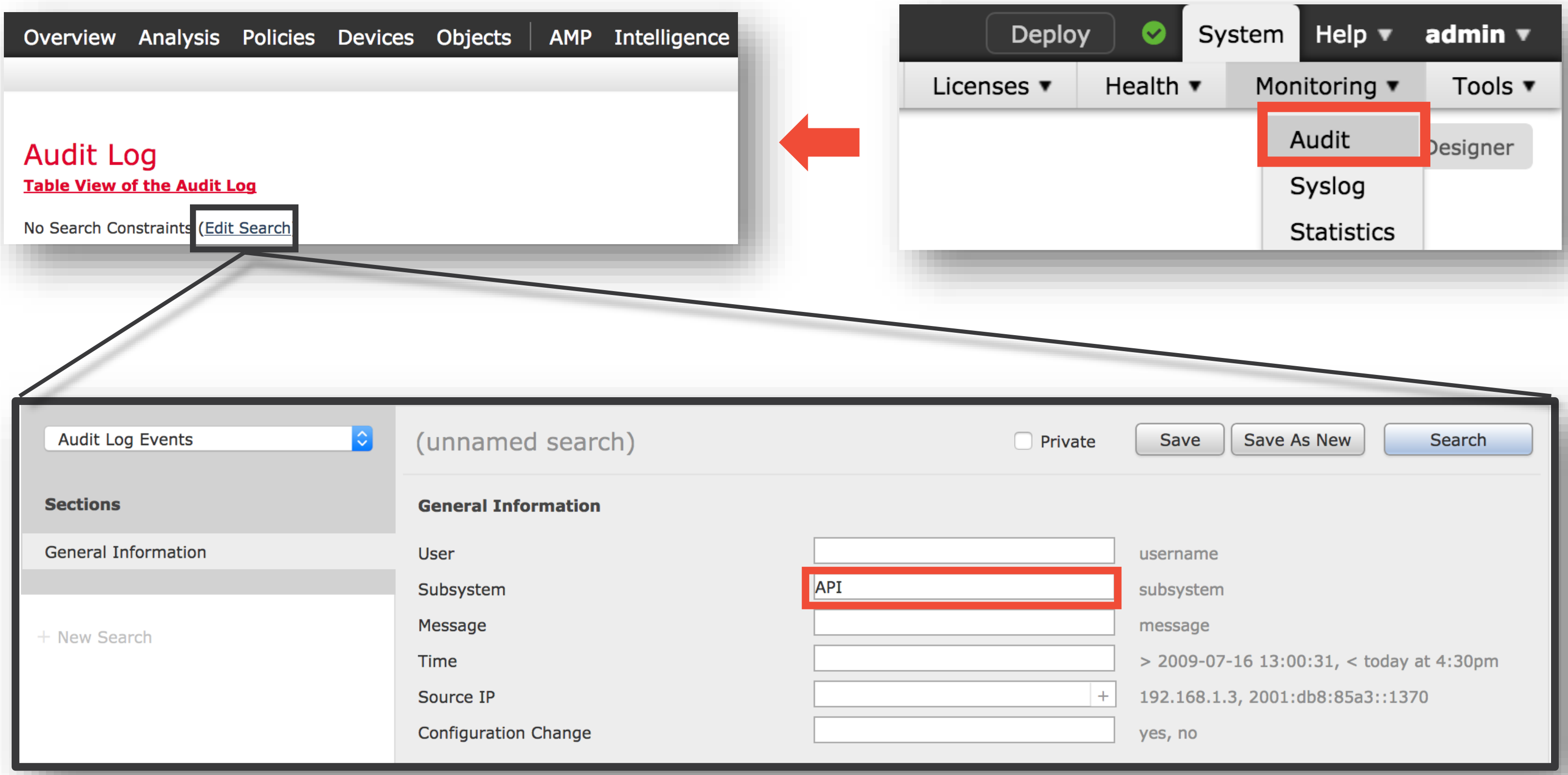


Example of an error for a remote issue

Remote server (FMC) returned a response of 401 Unauthorized



Search the audit log for API activity



View the filtered results

Time	User	Subsystem	Message
2017-12-04 20:19:47		API	POST https://127.0.0.1/api/ui_platform/v1/uiauth/generatetoken No Content (204) - The server has fulfilled the request but does not need to return an entity-body, and might want to return updated meta-information
2017-12-04 19:17:01		API	POST https://127.0.0.1/api/ui_platform/v1/uiauth/generatetoken No Content (204) - The server has fulfilled the request but does not need to return an entity-body, and might want to return updated meta-information
2017-12-04 18:13:01	TSAPI	API	DELETE https://192.168.2.10/api/identity/v1/identity/useridentity/AAAAAAAAAAAAAP__wKgAAgIAAAAAAAAAgD4= OK (200) - The request has succeeded
2017-12-04 18:12:16	TSAPI	API	POST https://192.168.2.10/api/identity/v1/identity/useridentity Created (201) - The request has been fulfilled and resulted in a new resource being created
2017-12-04 18:12:15	TSAPI	API	POST https://192.168.2.10/api/fmi_platform/v1/identityauth/generatetoken No Content (204) - The server has fulfilled the request but does not need to return an entity-body, and might want to return updated meta-information
2017-12-04 18:12:14		API	POST https://127.0.0.1/api/ui_platform/v1/uiauth/generatetoken No Content (204) - The server has fulfilled the request but does not need to return an entity-body, and might want to return updated meta-information
2017-12-04 18:12:06	TSAPI	API	POST https://192.168.2.10/api/identity/v1/identity/useridentity Unauthorized (401) - The request requires user authentication
2017-12-04 17:49:39	TSAPI	API	DELETE https://192.168.2.10/api/identity/v1/identity/useridentity/AAAAAAAAAAAAAP__wKgAAgIAAAAAAAAAgD4= OK (200) - The request has succeeded
2017-12-04 17:32:37		API	POST https://127.0.0.1/api/ui_platform/v1/uiauth/generatetoken No Content (204) - The server has fulfilled the request but does not need to return an entity-body, and might want to return updated meta-information
2017-12-04 17:29:45	TSAPI	API	POST https://192.168.2.10/api/identity/v1/identity/useridentity Created (201) - The request has been fulfilled and resulted in a new resource being created
2017-12-04 17:24:46	TSAPI	API	POST https://192.168.2.10/api/identity/v1/identity/useridentity Created (201) - The request has been fulfilled and resulted in a new resource being created
2017-12-04 17:24:01	TSAPI	API	POST https://192.168.2.10/api/fmi_platform/v1/identityauth/generatetoken No Content (204) - The server has fulfilled the request but does not need to return an entity-body, and might want to return updated meta-information
2017-12-04 17:24:01	TSAPI	API	DELETE https://192.168.2.10/api/identity/v1/identity/useridentity/deleteby?agent_id=TSA-000C2925F713 OK (200) - The request has succeeded
2017-12-04 17:21:52	TSAPI	API	POST https://192.168.2.10/api/fmi_platform/v1/identityauth/generatetoken No Content (204) - The server has fulfilled the request but does not need to return an entity-body, and might want to return updated meta-information
2017-12-04 17:21:50		API	POST https://127.0.0.1/api/ui_platform/v1/uiauth/generatetoken No Content (204) - The server has fulfilled the request but does not need to return an entity-body, and might want to return updated meta-information
2017-12-04 17:21:42		API	DELETE https://192.168.2.10/api/identity/v1/identity/useridentity/AAAAAAAAAAAAAP__wKgAAgIAAAAAAAAAmDo= Unauthorized (401) - The request requires user authentication
2017-12-04 17:17:23	TSAPI	API	POST https://192.168.2.10/api/fmi_platform/v1/identityauth/revokeaccess No Content (204) - The server has fulfilled the request but does not need to return an entity-body, and might want to return updated meta-information
2017-12-04 17:17:22	TSAPI	API	POST https://192.168.2.10/api/fmi_platform/v1/identityauth/generatetoken No Content (204) - The server has fulfilled the request but does not need to return an entity-body, and might want to return updated meta-information
2017-12-04 17:17:20		API	POST https://127.0.0.1/api/ui_platform/v1/uiauth/generatetoken No Content (204) - The server has fulfilled the request but does not need to return an entity-body, and might want to return updated meta-information
2017-12-04 14:55:02		API	POST https://127.0.0.1/api/ui_platform/v1/uiauth/generatetoken No Content (204) - The server has fulfilled the request but does not need to return an entity-body, and might want to return updated meta-information

Page 1 of 1 Displaying rows 1–20 of 20 rows

View Delete

View All Delete All

Once the data is sent to the FMC

Process Check!

- Critical Processes
  - **Tomcat** - Handles REST API requests / responses
  - **adi** - Accepts re-formatted data from Tomcat. Validates data and passes off to SFDataCorrelator
  - **SFDataCorrelator** - Accepts mappings. Marks end of Phase 1

SHELL

```
root@FMC:/# pmtool status | egrep "Tomcat \(|adi \(|SFDataCorrelator \(”
SFDataCorrelator (normal) - Running 1994
Tomcat (system,gui) - Running 5079
adi (normal) - Running 18766
```

TSAgent makes a POST request to the FMC API

SHELL

```
root@FMC:/# less /var/opt/CSCOpx/MDC/tomcat/logs/stdout.logs
…
[ajp-nio-127.0.0.1-9009-exec-3] INFO com.cisco.api.external.rest.common.routing.ExtensionURLFilter - Request for extension URL passed : /identity/useridentity
>>> Permission count for TSAPI [loadOnlyCsm=true] = 5
In API Mode, api.modify_useridentity maps to rest_vdi.modify
In API Mode, api.modify_useridentity maps to rest_vdi.modify
In API Mode, api.modify_useridentity maps to rest_vdi.modify
In API Mode, api.modify_useridentity maps to rest_vdi.modify
[ajp-nio-127.0.0.1-9009-exec-3] INFO BusinessLogicIdentityImpl - User: Test1
[ajp-nio-127.0.0.1-9009-exec-3] INFO BusinessLogicIdentityImpl - Domain: FIRE.INT
[ajp-nio-127.0.0.1-9009-exec-3] INFO BusinessLogicIdentityImpl - SrcIPAddress: 192.168.0.2
[ajp-nio-127.0.0.1-9009-exec-3] INFO BusinessLogicIdentityImpl - Timestamp: 2017-12-01T14:09:46.7458164-05:00
[ajp-nio-127.0.0.1-9009-exec-3] INFO BusinessLogicIdentityImpl - AgentInfo: TSA-000C2925F713
[ajp-nio-127.0.0.1-9009-exec-3] INFO BusinessLogicIdentityImpl - Name: null
[ajp-nio-127.0.0.1-9009-exec-3] INFO BusinessLogicIdentityImpl - Description: null
[ajp-nio-127.0.0.1-9009-exec-3] INFO BusinessLogicIdentityImpl - Id: null
[ajp-nio-127.0.0.1-9009-exec-3] INFO BusinessLogicIdentityImpl - PAT Range:
[ajp-nio-127.0.0.1-9009-exec-3] INFO BusinessLogicIdentityImpl -   PatRangeStart: 15000
[ajp-nio-127.0.0.1-9009-exec-3] INFO BusinessLogicIdentityImpl -   UserPatStart: 16000
[ajp-nio-127.0.0.1-9009-exec-3] INFO BusinessLogicIdentityImpl -   UserPatEnd: 16999
[ajp-nio-127.0.0.1-9009-exec-3] INFO BusinessLogicIdentityImpl -   Name: null
[ajp-nio-127.0.0.1-9009-exec-3] INFO BusinessLogicIdentityImpl -   Description: null
[ajp-nio-127.0.0.1-9009-exec-3] INFO BusinessLogicIdentityImpl -   Id: null
-no timestamp-
[INFO],(MQWrapper.java:149),Attempting to register receiver ipc:///tmp/adireq,com.cisco.ngfw.messagelayer.MQWrapper,ajp-nio-127.0.0.1-9009-exec-3
```

The POST request from the TSAgent

Tomcat parses the JSON

Data from parsed request sent to adi for validation

The JSON that we posted

```
{
        "agentInfo":"TSA-000C2925F713",
        "domain":"FIRE.INT",
        "srcIpAddress":"192.168.0.2",
        "srcPatRange":{
                "patRangeStart":15000,
                "userPatEnd":15999,
                "userPatStart":15000
        },
        "timestamp":"2018-01-02T13:37:19.6950775-05:00",
        "user":"Test1”
}
```

Unique AgentID

The Users Domain

The IP address to map to

The first possible port for ANY user session

The Ending port for this specific users session

The Starting port for this specific users session

The logged in user to create the mapping for

The adi process validates the data

```
SHELL
root@FMC:/# pmtool disablebyid adi
root@FMC:/# adi --debug
...
Dec 04 23:12:16 FMC SF-IMS[15447]: [15452] ADI:adi.RestMsgHandler [DEBUG] adi.cpp:512:HandleLog(): Handling request for creating user binding.
Dec 04 23:12:16 FMC SF-IMS[15447]: [15452] ADI:adi.RealmContainer [DEBUG] adi.cpp:512:HandleLog(): findRealm: Found Realm for domain FIRE.INT
Dec 04 23:12:16 FMC SF-IMS[15447]: [15452] ADI:adi.SubscriberChannel [DEBUG] adi.cpp:512:HandleLog(): Sending request to ADI subscriber
Dec 04 23:12:16 FMC SF-IMS[15447]: [15452] ADI:adi.SubscriberChannel [DEBUG] adi.cpp:512:HandleLog(): Receiving response from DataCorrelator
...
Dec 04 23:13:01 FMC SF-IMS[15447]: [15462] ADI:adi.RestMsgHandler [DEBUG] adi.cpp:512:HandleLog(): Handling request for querying user binding.
Dec 04 23:13:01 FMC SF-IMS[15447]: [15462] ADI:adi.SubscriberChannel [DEBUG] adi.cpp:512:HandleLog(): Sending request to ADI subscriber
Dec 04 23:13:01 FMC SF-IMS[15447]: [15462] ADI:adi.SubscriberChannel [DEBUG] adi.cpp:512:HandleLog(): Receiving response from DataCorrelator
Dec 04 23:13:01 FMC SF-IMS[15447]: [15453] ADI:adi.RestMsgHandler [DEBUG] adi.cpp:512:HandleLog(): Handling request for deleting user binding.
Dec 04 23:13:01 FMC SF-IMS[15447]: [15453] ADI:adi.SubscriberChannel [DEBUG] adi.cpp:512:HandleLog(): Sending request to ADI subscriber
Dec 04 23:13:01 FMC SF-IMS[15447]: [15453] ADI:adi.SubscriberChannel [DEBUG] adi.cpp:512:HandleLog(): Receiving response from DataCorrelator
...
<ctrl+c>

root@FMC:/# pmtool enablebyid adi
```

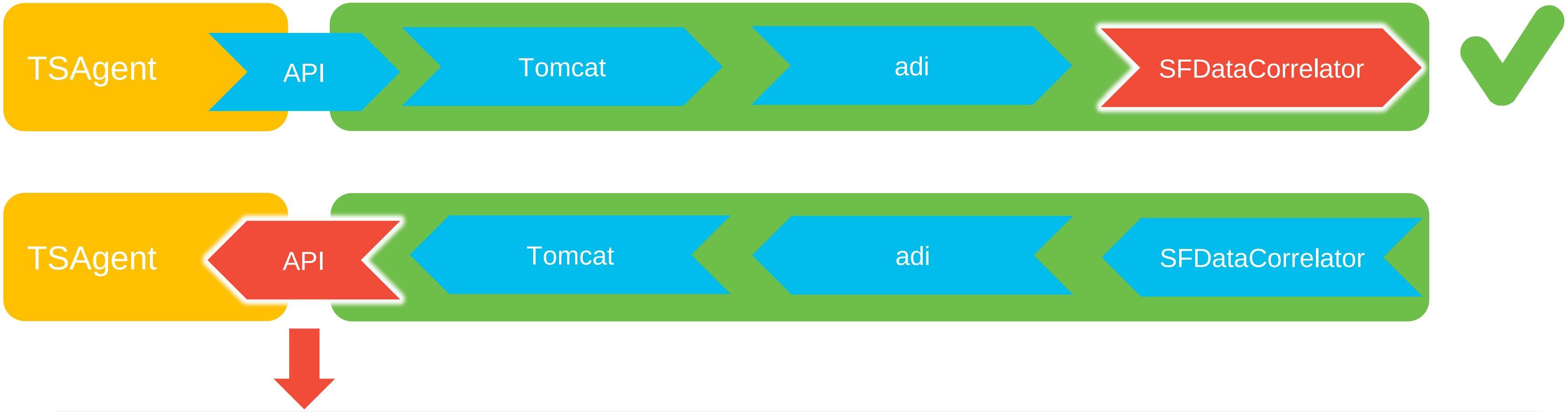
Logon

Logoff

*Remember, to also capture to a log, change the adi debug command to:

adi --debug 2>&1 | tee /var/tmp/adi.log

Responding back to the TSAgent



SHELL

```
root@FMC:/# less /var/opt/CSCOpx/MDC/tomcat/logs/stdout.logs
…
INFO: 192.168.0.2       -       ::1     443     POST    /api/identity/v1/identity/useridentity -        201
        -       222     458     https://192.168.2.10    -       -
…
```

Comparing the agent to the FMC

Monitor | Configure

2 Entries

Filter by Username

REST Server ID	Source IP	Status	Session ID	Username
192.168.2.10	192.168.0.2	Success	2	Administrator
192.168.2.10	192.168.0.2	Success	3	Test1

Additional data hidden by scroll

Domain	Port Range	Login Date
FIRE.INT	15000-15999	11/27/2017 10:23 AM
FIRE.INT	16000-16999	11/27/2017 10:28 AM

Overview | Analysis | Policies | Devices | Objects | AMP | Intelligence

Context Explorer | Connections ▾ | Intrusions ▾ | Files ▾ | Hosts ▾ | Users ▸ User Activity | Vulnerabilities ▾ | Correlation ▾ | Custom ▾ | Lookup ▾ | Search

User Activity

Table View of Events > Users

No Search Constraints (Edit Search)

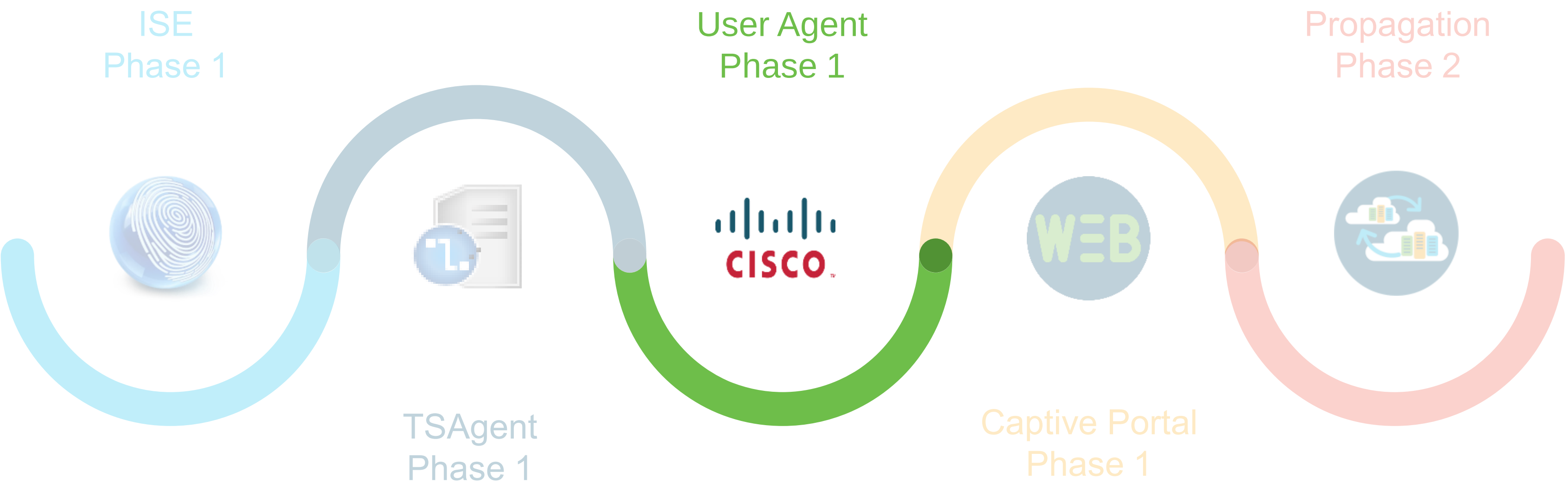
Time	Event	Username	Realm	Discovery Application	Authentication Type	IP Address	Start Port	End Port	Description	VPN Session Type
2017-11-27 10:28:28	User Login	Test1	fire.int	LDAP	Passive Authentication	192.168.0.2	16000	16999		Unknown
2017-11-27 10:23:58	User Login	Administrator	fire.int	LDAP	Passive Authentication	192.168.0.2	15000	15999		Unknown

Page 1 of 1 Displaying rows 1–2 of 2 rows

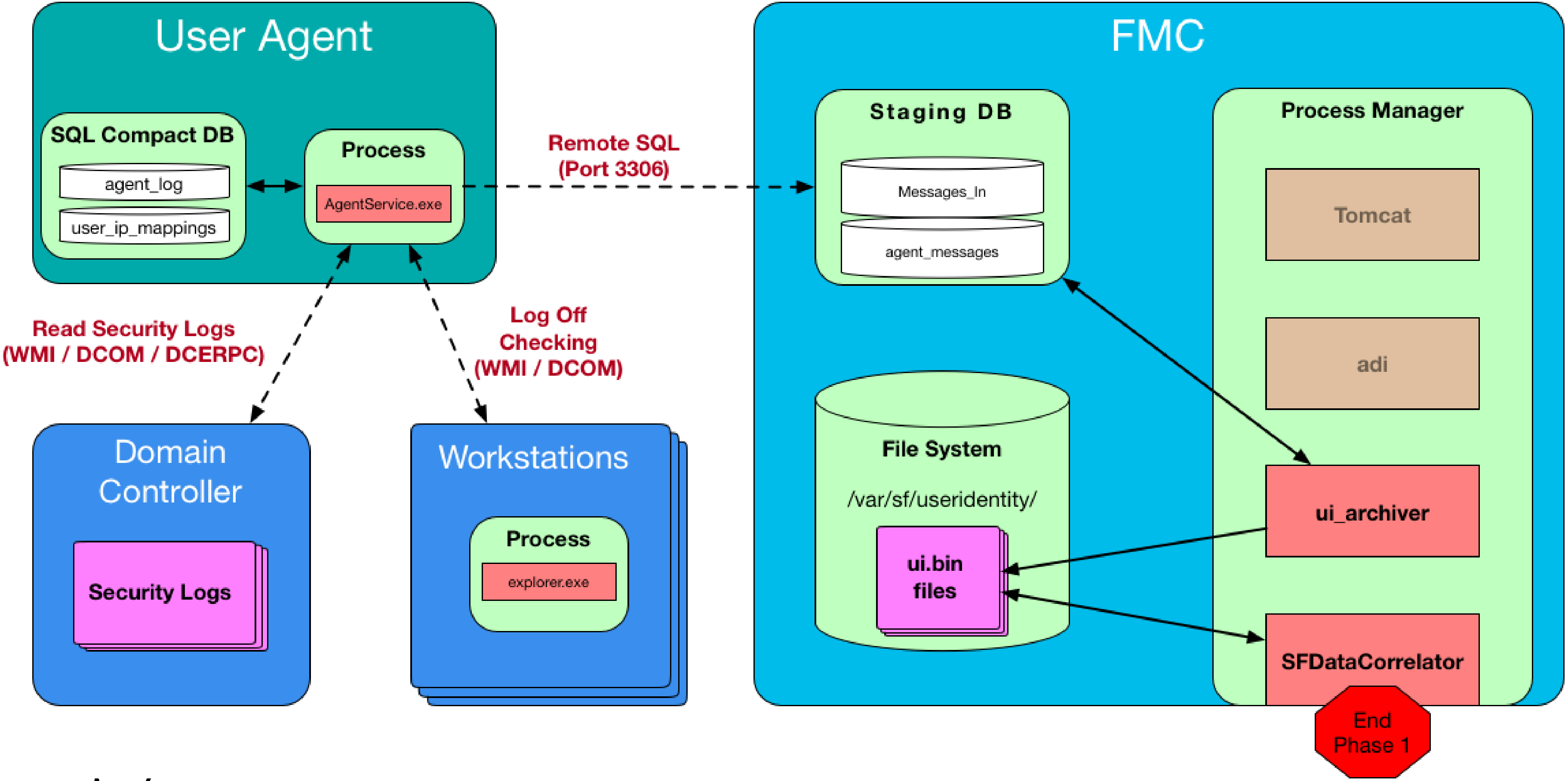
TSAgent Recap

- Ensure the API user is able to authenticate against the FMC REST API
- Check the local Event Viewer logs for the TSAgent for errors
- Confirm the **Tomcat, adi**, and **SFDataCorrelator** processes are up
- Check the API logs:
  - Look at API audit logs in the WebUI for basic information
  - Look at the **Tomcat** logs *(/var/opt/CSCOpx/MDC/tomcat/logs/stdout.log*) for more detailed information
- Put **adi** into debug mode to test

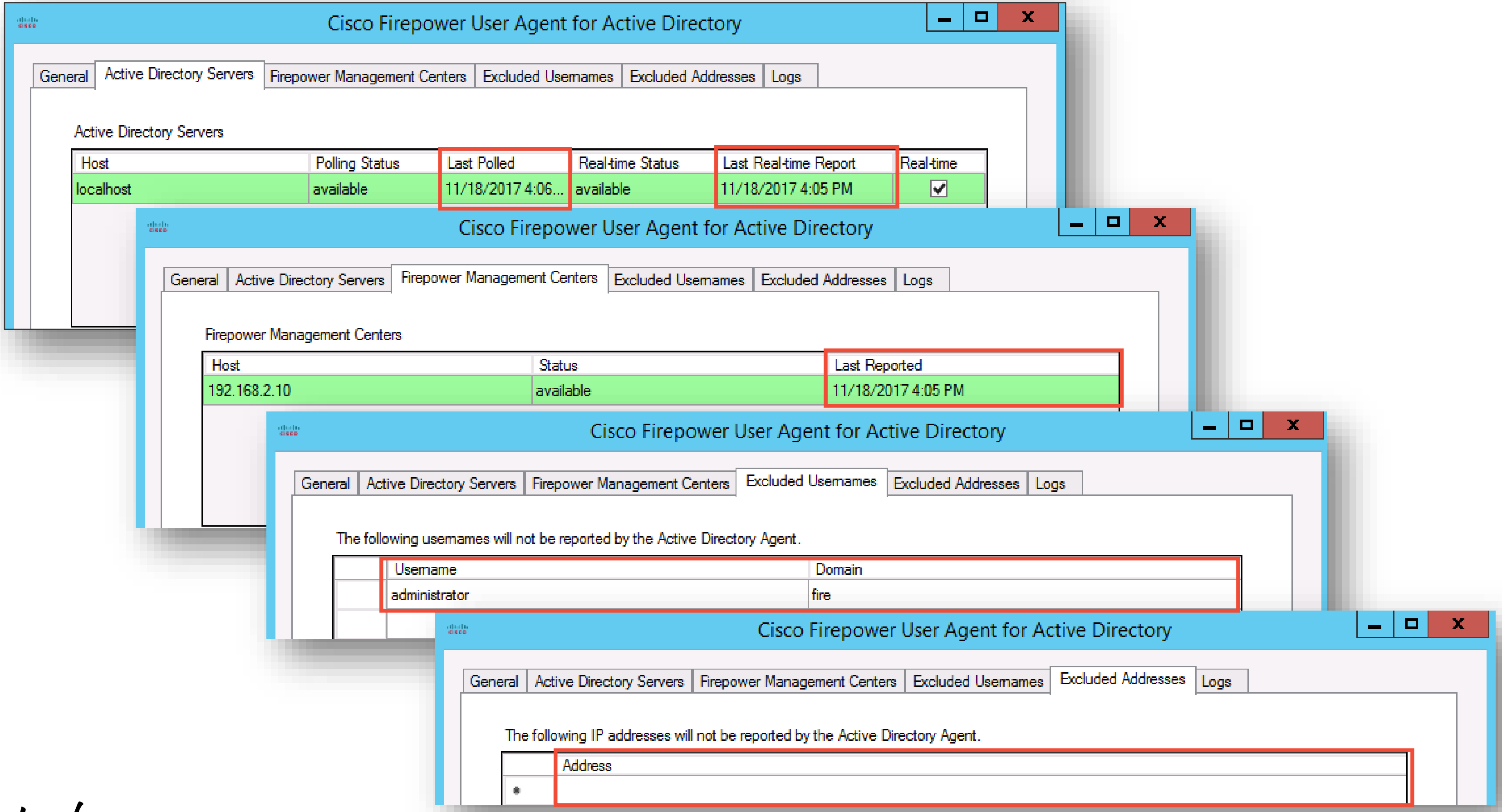
Phase Discussion



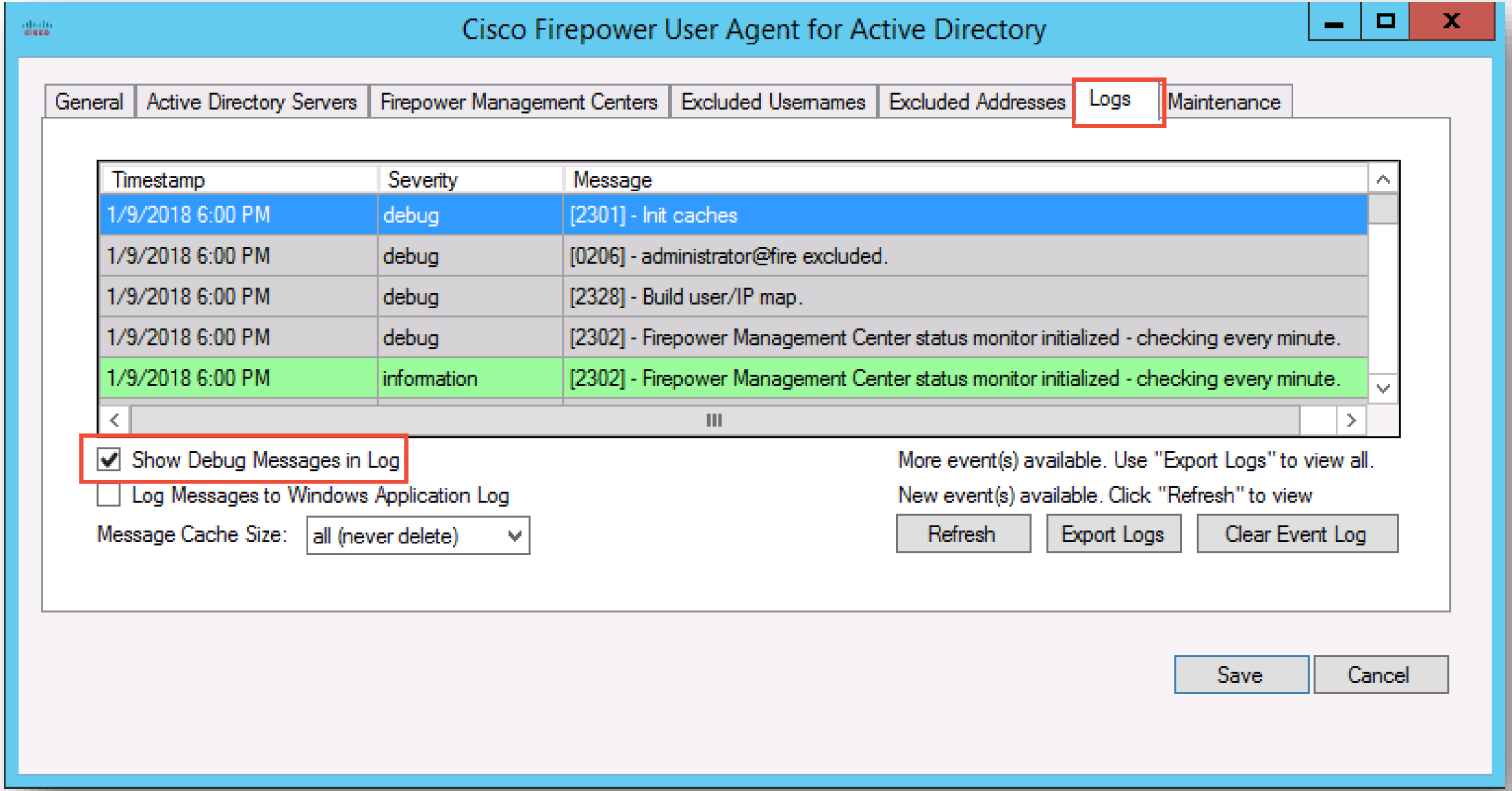
User Agent Diagram



Starting with the basics

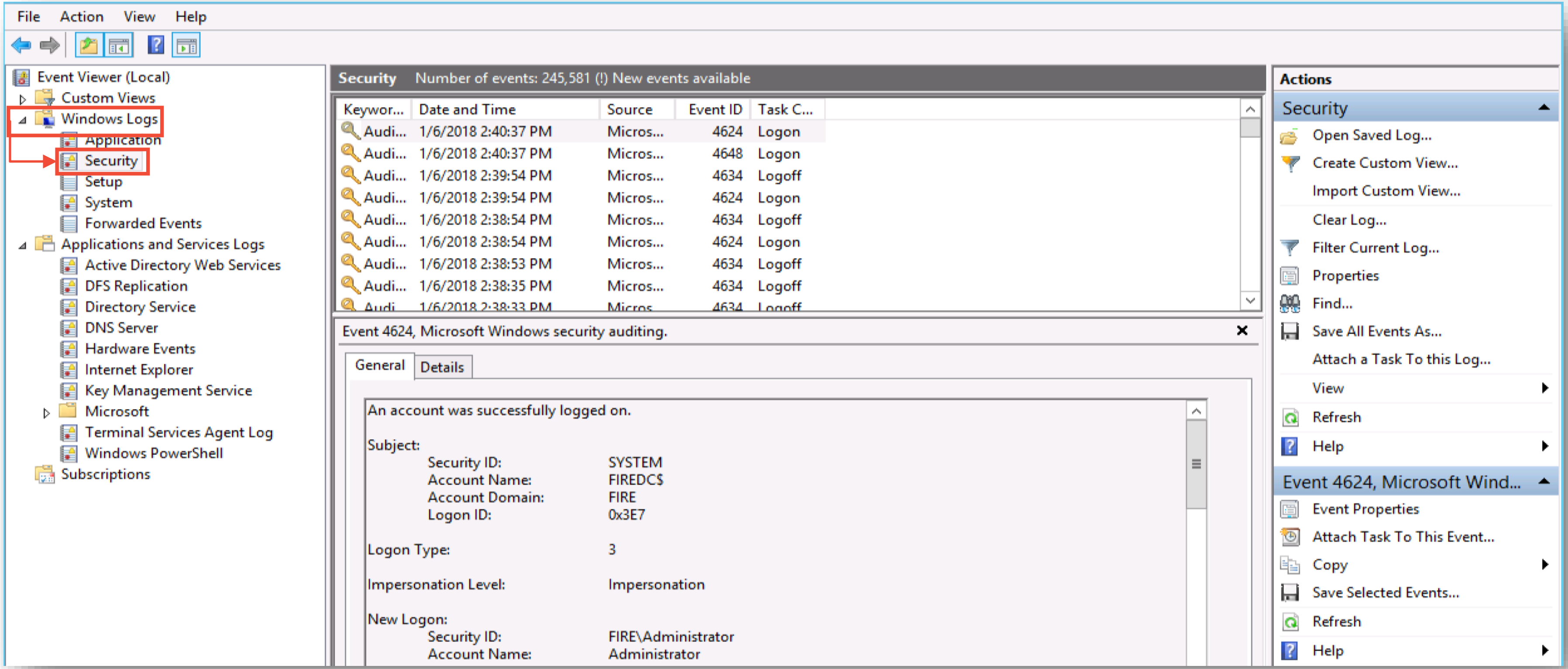


Always check the logs



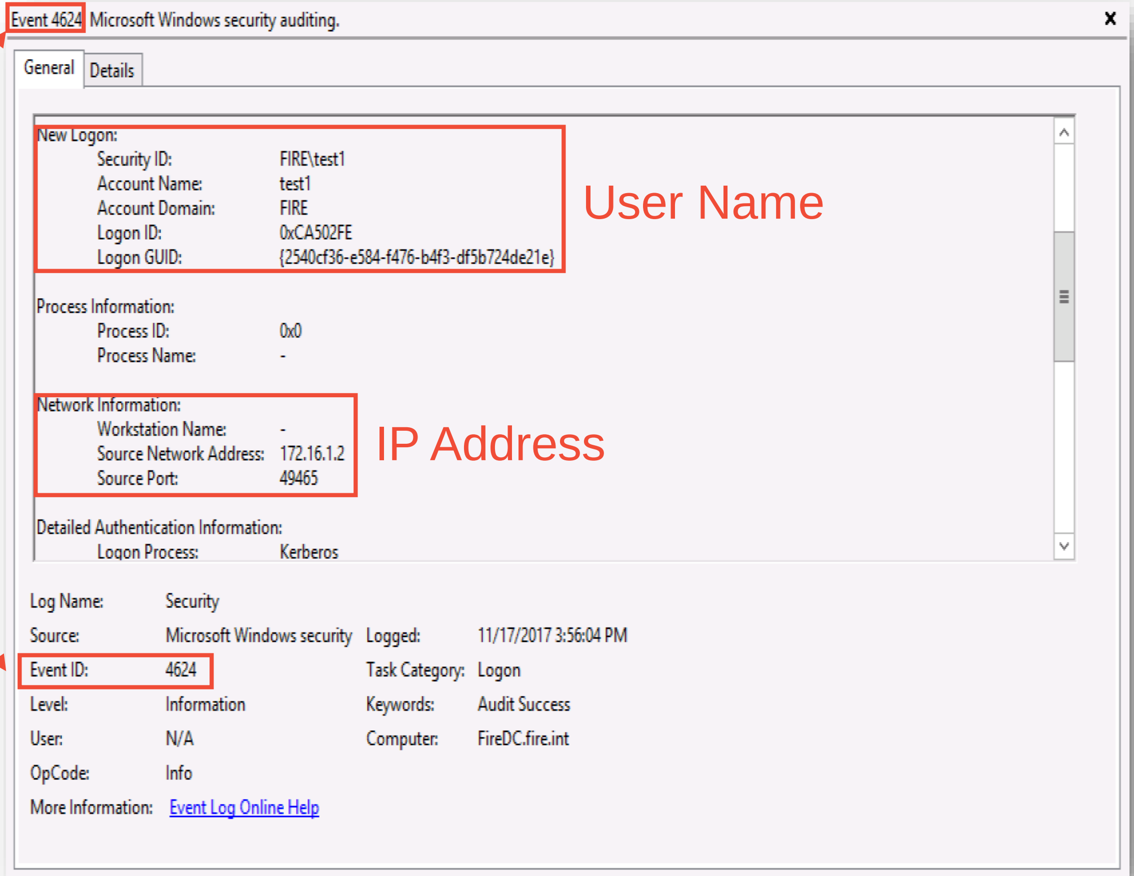
Verify the Security Logs (Local/Remote)

Administrative Tools > Event Viewer



Make sure you have the proper events

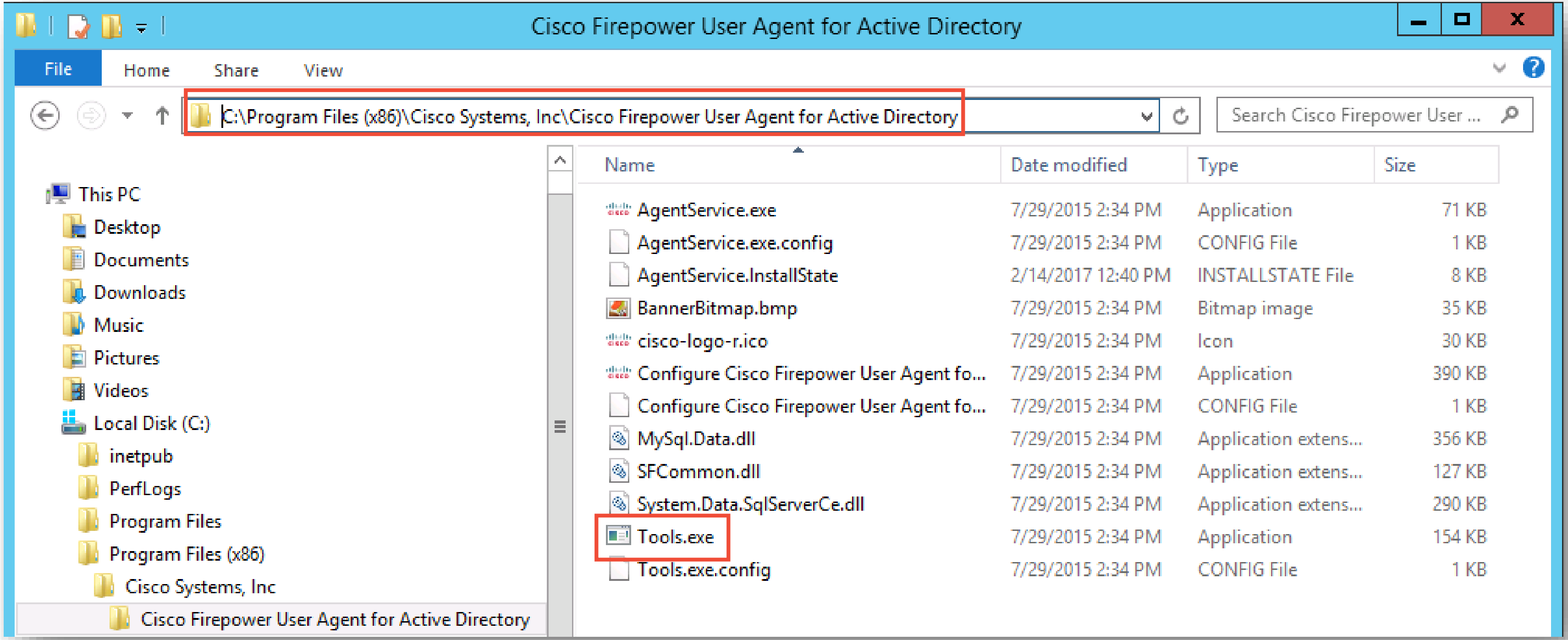
Event ID 4624



User Name

IP Address

There are extra tools available

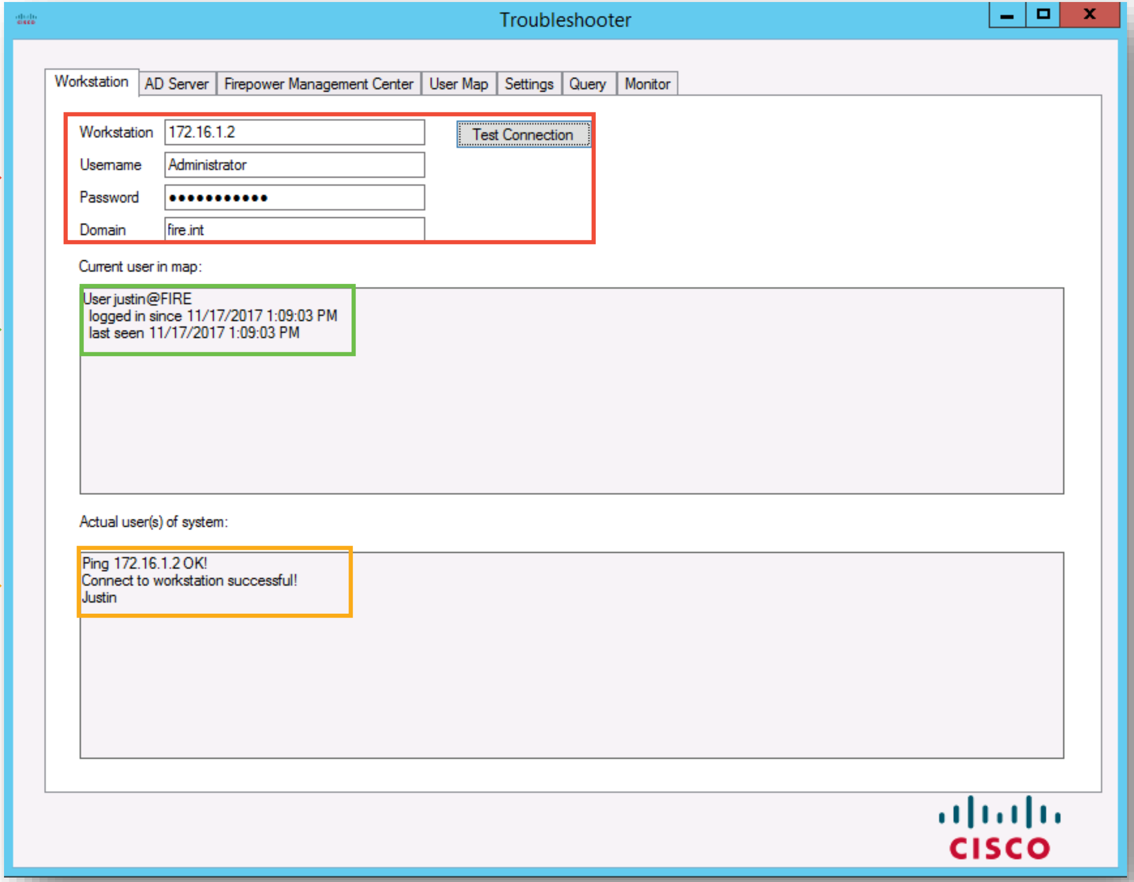


You can query the workstation directly

Connection details
for the test workstation

User Agent databases
current mapping for that IP

Actual logged on user
(WMI/DCOM connection
to endpoint directly)

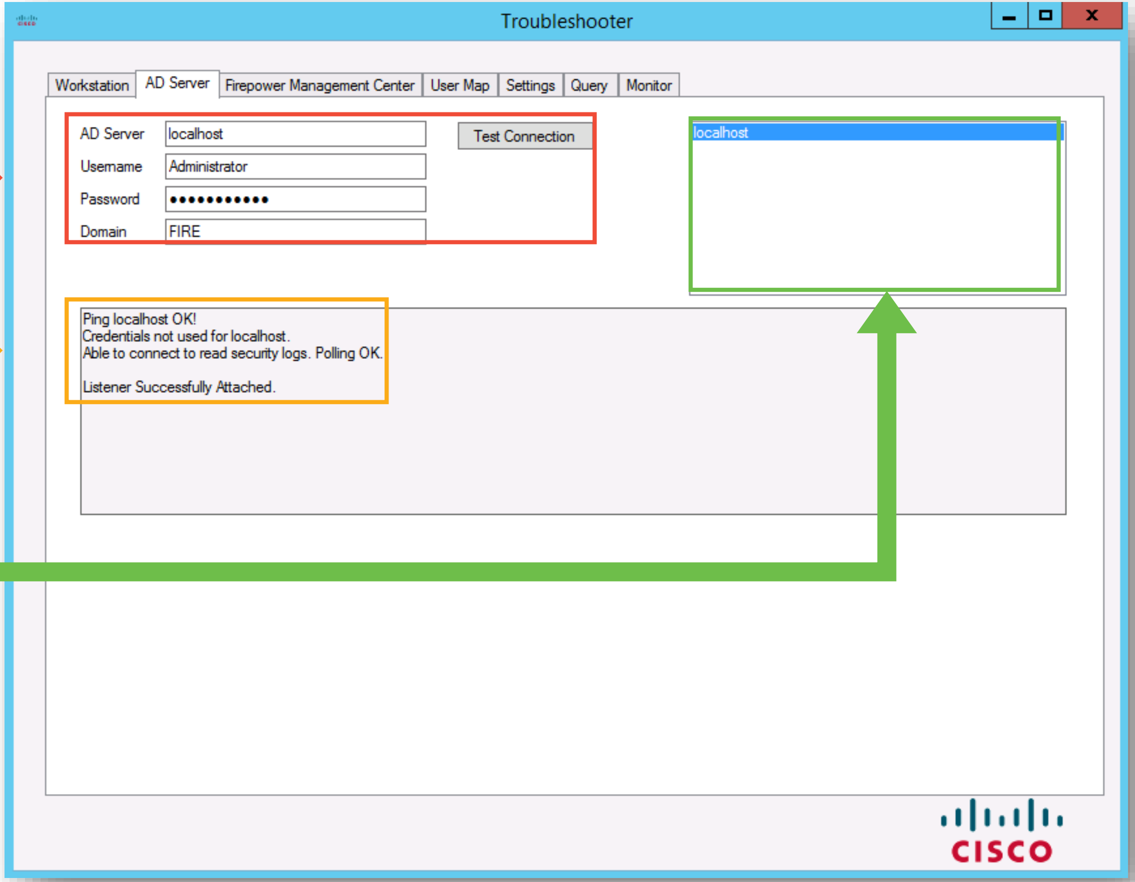


Test the active directory connections

Connection details for the AD server

Output for each connection test step

Presets available for currently configured AD Servers

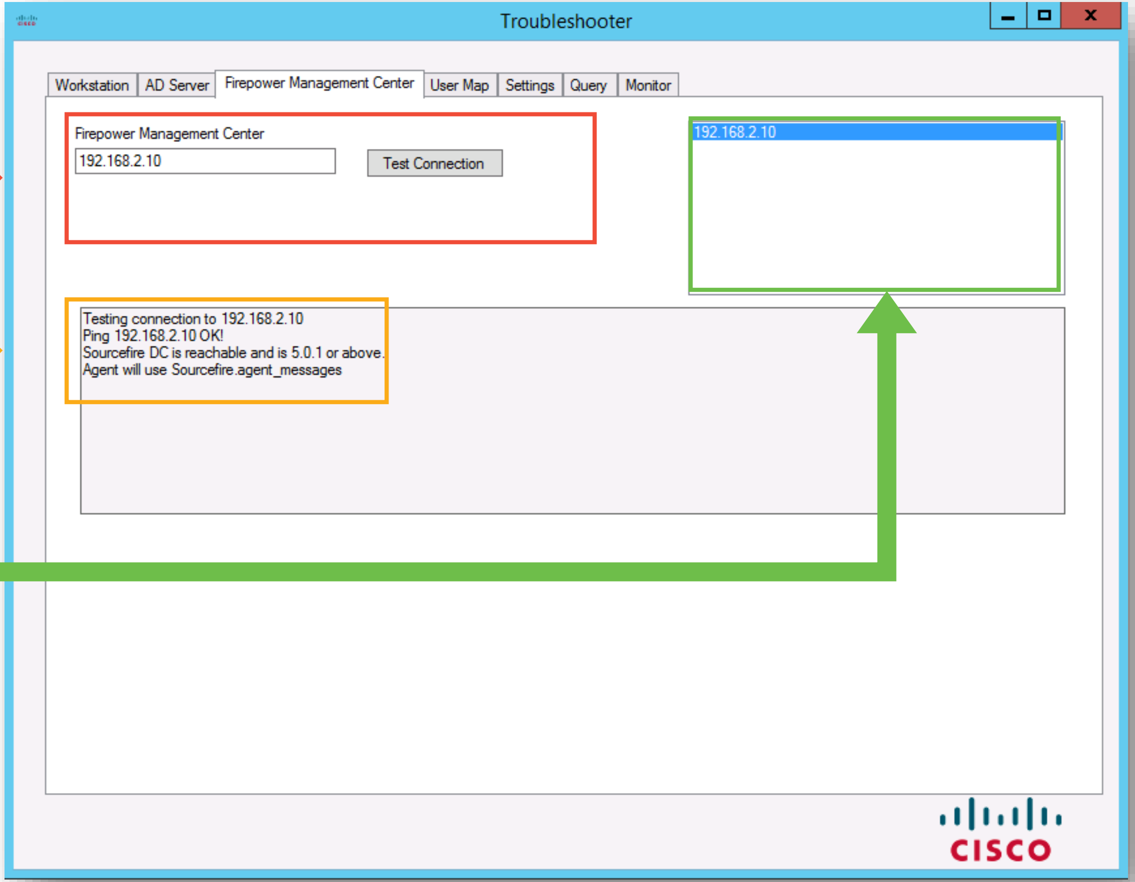


Test connections to the Firepower Managers

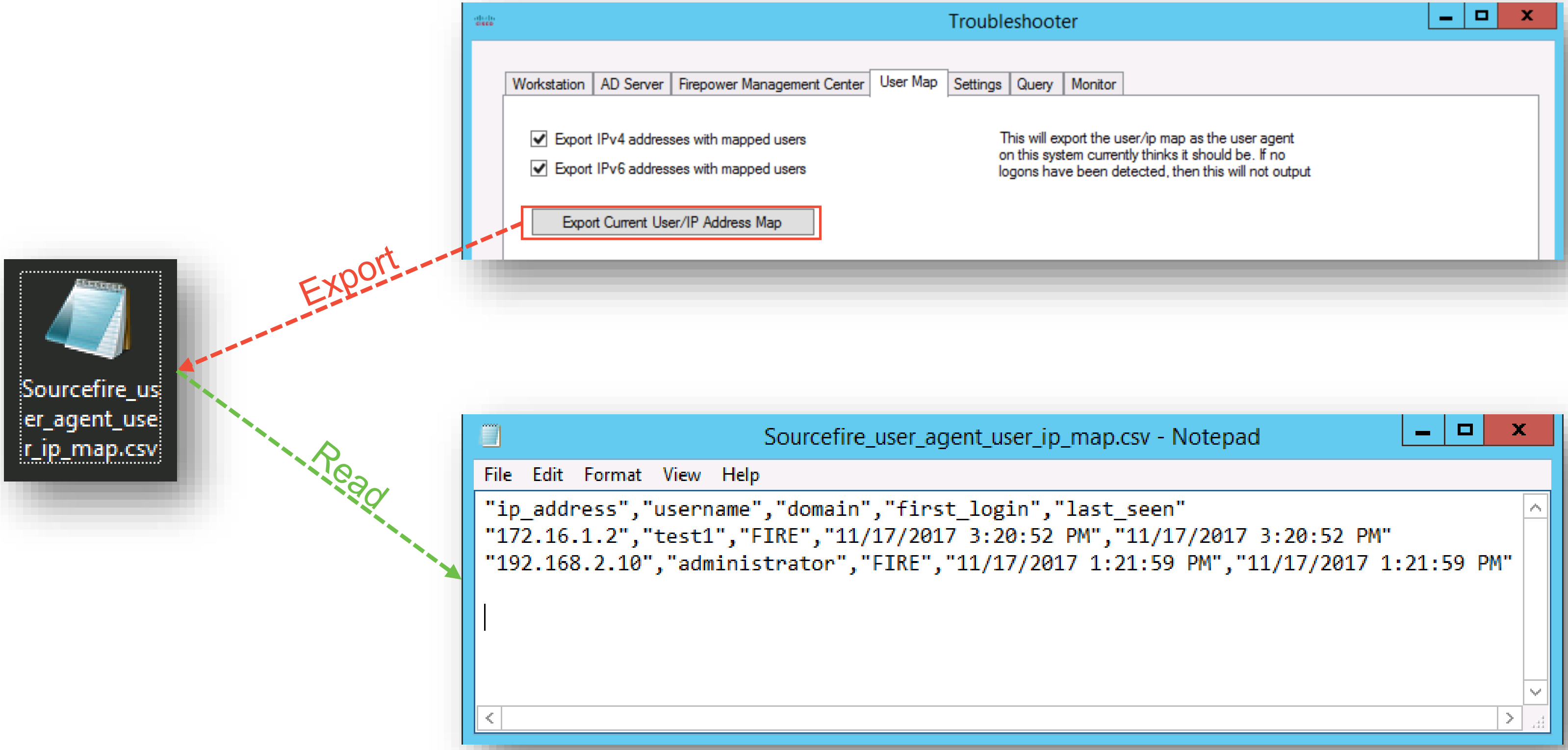
IP Address of the FMC to test

Output for each connection test step

Presets available for currently configured FMC's



See what mappings the agent currently has



Look at the configuration in plaintext

Troubleshooter

Workstation | AD Server | Firepower Management Center | User Map | Settings | Query | Monitor

This reflects the settings table at the time this panel was loaded

setting	value
UniqueName	CiscoFUA
ADServerPollingInterval	1 minute
MessageCacheSize	all (never delete)
DCPollingInterval	60 minutes
WorkstationPollingInterval	5 minutes
ApplicationPath	C:/Program Files (x86)/Cisco Systems, Inc/Cisco Firepower User Agent for Active Directory/
HeartbeatInterval	180000
DBMaintInterval	60000
StaleData	0
ShowDebug	False
MaxADPollLength	1 hour
LogToAppLog	False
SupportUnicode	0
DBSchemaRevision	2.3.1
DebugLogLevel	1
ServiceProcessPriority	Normal
LocalLoginIP	

Once the data is sent to the FMC

Process Check!

- Critical Processes
  - **ui_archiver**
    - Monitors the database that the User Agent is doing remote inserts into
    - Creates **ui.bin.<epoch_tstamp>** files in the /var/sf/useridentity/ directory
  - **SFDataCorrelator**
    - Consumes the ui.bin files in the /var/sf/useridentity/ directory
    - Marks the end of Phase 1

SHELL

```
root@FMC:/# pmtool status | egrep "SFDataCorrelator \(|ui_archiver \(”
SFDataCorrelator (normal) - Running 4842
ui_archiver (normal) - Running 4843
```

The handoff happens very quickly

ui_archiver sees a database update, turns that data into a ui.bin file

SHELL

```
root@FMC:/# less /var/log/messages
…
Nov 18 19:07:43 FMC SF-IMS[4196]: [41 6] CloudAgent:CloudAgent [INFO] IPRep, time to check for updates
Nov 18 19:07:44 FMC SF-IMS[4196]: [42 5] CloudAgent:IPReputation [INFO] The curl option for ip  verify_peer=1
verifyhost=0
Nov 18 19:07:44 FMC SF-IMS[4196]: [42 5] CloudAgent:IPReputation [INFO] The curl option for dns verifypeer=1
verifyhost=0
Nov 18 19:07:58 FMC SF-IMS[4843]: [4843] ui_archiver:OutputFile [INFO] *** Opening
/var/sf/useridentity/ui.bin.1511032078 for output
Nov 18 19:07:58 FMC SF-IMS[4842]: [5903] SFDataCorrelator:UIBinaryFile [INFO] Processed 2875 events from log file
1510683611, new file is /var/sf/useridentity/ui.bin.1511032078 for 1, the local user identity file
Nov 18 19:09:36 FMC Someone connected to me, receiving data
Nov 18 19:09:36 FMC sla_worker : sizeof(msg) : 8192
Nov 18 19:09:36 FMC before recv(), total_bytes_read = 0, hdr_len = 8
```

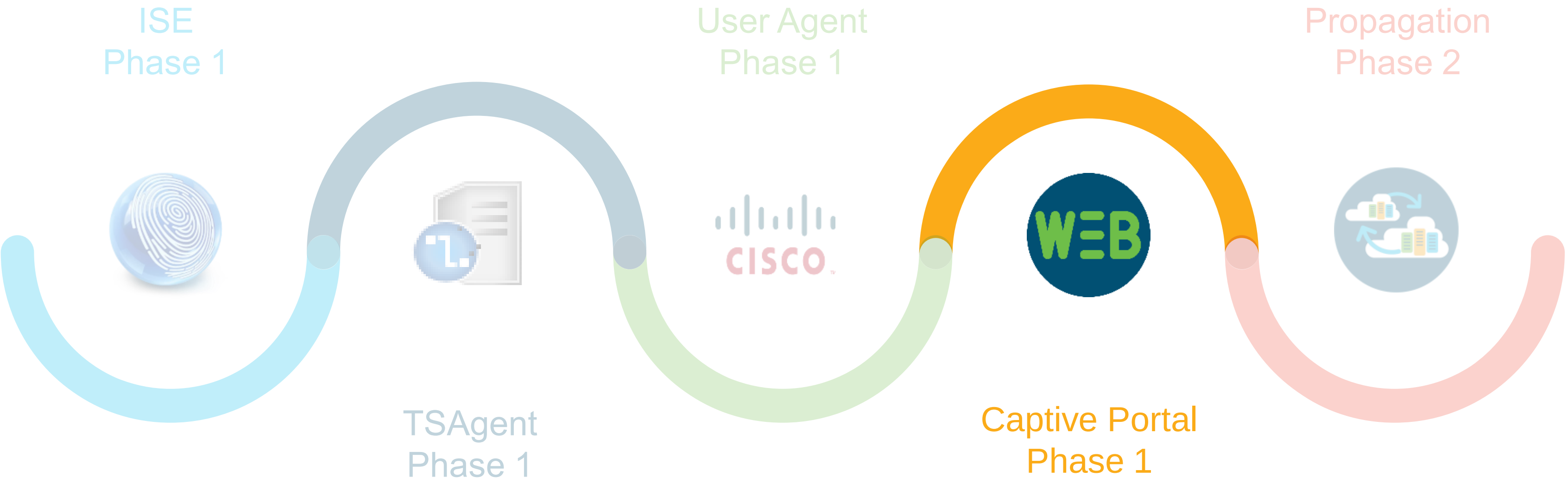
ui.bin file is instantly picked up and processed by SFDataCorrelator

User Agent Recap

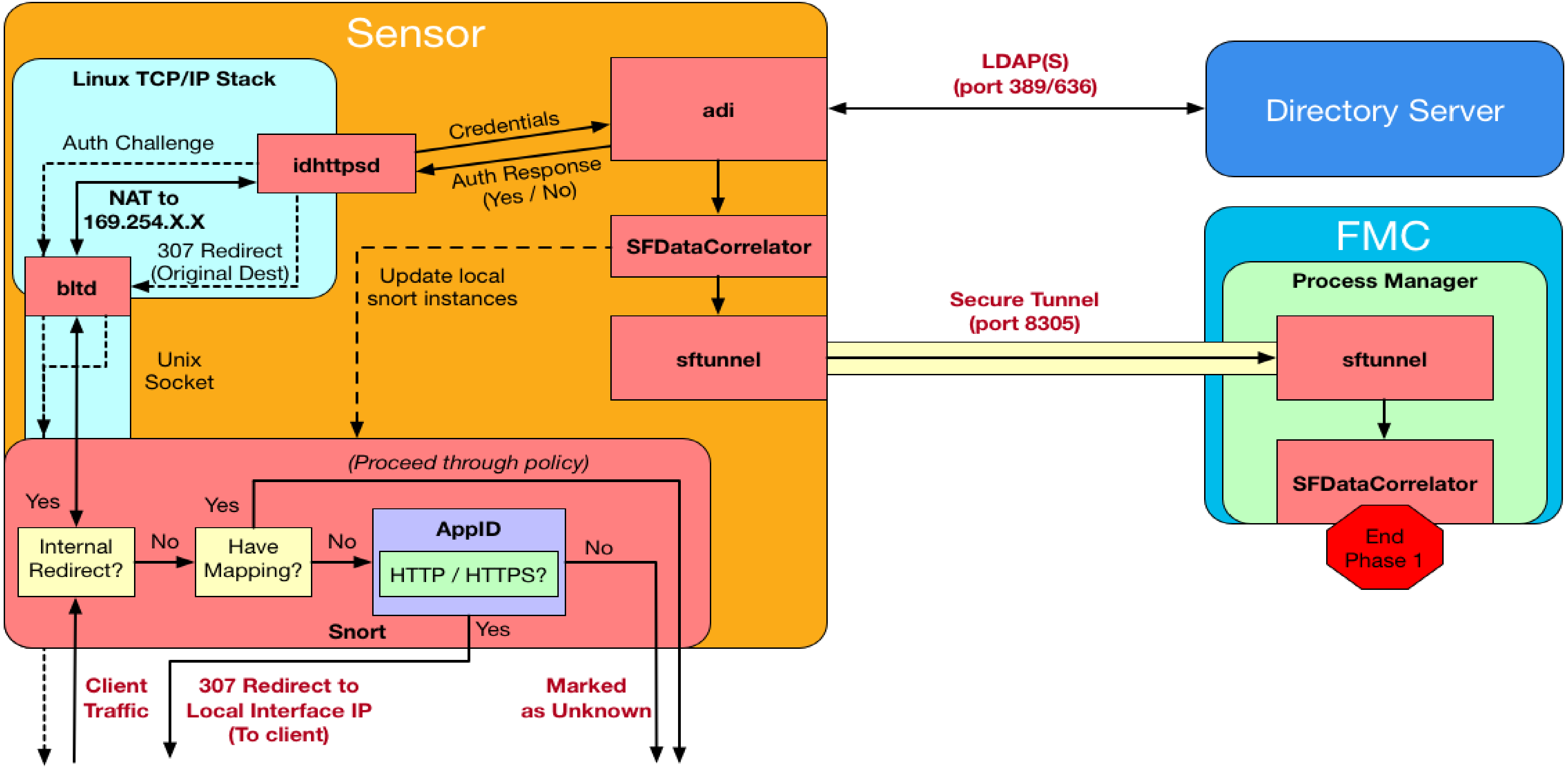
- Sanity check User Agent information and check Logs tab
- Confirm that User Agents are monitoring ALL possible Authentication Points
  - 5 Domain Controllers per agent
  - No Documented maximum on User Agents per FMC
- Ensure that the Domain Controllers are Auditing Logon events (4624 Event ID)
- Troubleshoot with the Tools.exe executable (run as Administrator):
  - Testing FMC, DC, and Endpoint connections
  - Export current User to IP mappings from User Agents database
- Make sure the **ui_archiver** and **SFDataCorrelator** processes are running
- Check FMC syslog for process errors (*/var/log/messages*)

Active Authentication Architecture Deep Dive

Phase Discussion



Captive Portal Diagram



Captive Portal new session walkthrough

1. Client traffic (after coming from the data plane) makes its way to Snort
2. Check for current mappings for the requesting IP address
3. If no mapping, traffic eventually makes it into AppID portion of Snort
4. Traffic is identified as HTTP/HTTPS snort injects a 307 response to client, redirecting them to the sensors interface IP
5. Traffic destined to the sensors local IP forces a flag to be set on the packet that instructs Snort to send this over to bltd
6. The response from the client is sent over to the bltd process via a Unix socket
7. bltd NATs the traffic to a 169.254.X.X IP address to be able to talk to the idhttpsd process
8. idhttpsd receives the GET request from the client (post bltd NAT)
9. idhttpsd challenges the clients authentication (method varies depending on configured authentication mechanism)
10. The challenge response from idhttpsd gets un-natted (by bltd) and sent back to the client (through snort)
11. Client responds to the authentication challenge
12. Response from client comes back through snort, gets re-natted by the bltd process and sent over to idhttpsd
13. idhttpsd passes the credentials it received (from clients response) to the adi process
14. adi tests authentication directly against the configured directory server
    1. adi gets a YES or NO
    2. Regardless of response, adi tells idhttpsd the verdict
    3. Assuming YES, adi will also tell SFDataCorrelator to create a mapping
15. SFDataCorrelator creates the mapping and updates snort with the mappings
16. SFDataCorrelator also sends this information to the FMC to propagate the mappings to other sensors
17. At the same time, idhttpsd will send the client another 307 redirect, redirecting the client to their original destination

Phase 1 Firepower side

Process Check!

- Critical Processes
  - **snort –** Intercepts HTTP / HTTPS traffic and redirects client to auth if there are no current mappings for the requesting IP address
  - **bltd –** NATs traffic internally to be able to talk with the idhttpsd server
  - **idhttpsd –** Internal apache server to handle authentication requests
  - **adi** - Takes credentials received from idhttpsd and validates authentication
  - **SFDataCorrelator –** Creates the user mappings and updates the snort instances

SHELL

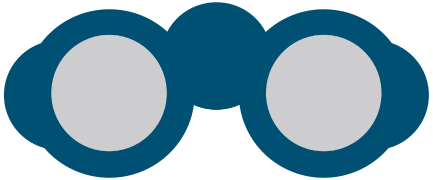
```
root@FTD1:/# pmtool status | egrep "adi \(|SFDataCorrelator \(|idhttpsd \(|bltd \(|snort\)”
SFDataCorrelator (normal) - Running 4497
idhttpsd (system,gui) - Running 18694
adi (normal) - Running 25512
bltd (normal) - Running 4321
6934c232-aaac-11e7-948b-16e77db57e79-d01 (de,snort) - Running 5996
```

Nothing basic about this starting point

1. Look at the logs for errors:
   - /var/log/captive_portal.log
   - /var/log/idhttpsd/error_log

2. Put **adi** into debug mode

3. Take packet captures



Put adi into debug while testing

SHELL

```
root@FTD1:/# adi --debug
```

Put adi into debug mode

```
...
Jan 06 20:53:23 FTD1 SF-IMS[2414]: [2445] ADI:adi.AuthHandler [DEBUG] adi.cpp:512:HandleLog(): auth: received auth request.
```

Auth request from idhttpsd

```
Jan 06 20:53:23 FTD1 SF-IMS[2414]: [2445] ADI:active.retry.counter [DEBUG] adi.cpp:512:HandleLog(): using ipv4 as auth retry key.
Jan 06 20:53:23 FTD1 SF-IMS[2414]: [2445] ADI:active.retry.counter [DEBUG] adi.cpp:512:HandleLog(): new auth retry record created with keyId = 233624236
Jan 06 20:53:23 FTD1 SF-IMS[2414]: [2445] ADI:active.retry.counter [DEBUG] adi.cpp:512:HandleLog(): auth retry increment for simple authentication.
Jan 06 20:53:23 FTD1 SF-IMS[2414]: [2445] ADI:active.retry.counter [DEBUG] adi.cpp:512:HandleLog(): auth request retry count processed (1 out of 3).
```

Create keyId to track auth retries

```
Jan 06 20:53:23 FTD1 SF-IMS[2414]: [2445] ADI:adi.LdapRealm [DEBUG] adi.cpp:512:HandleLog(): auth: using username: 'Test1'
Jan 06 20:53:23 FTD1 SF-IMS[2414]: [2445] ADI:adi.LdapRealm [DEBUG] adi.cpp:512:HandleLog(): ldap: search returned (1) result pages.
Jan 06 20:53:23 FTD1 SF-IMS[2414]: [2445] ADI:adi.LdapRealm [DEBUG] adi.cpp:512:HandleLog(): search '(|(sAMAccountName=Test1))' has the following DN:
'CN=Test1,CN=Users,DC=fire,DC=int'.
Jan 06 20:53:23 FTD1 SF-IMS[2414]: [2445] ADI:adi.LdapRealm [DEBUG] adi.cpp:512:HandleLog(): auth: authenticating using DN: 'CN=Test1,CN=Users,DC=fire,DC=int'
```

Build request body
Make auth request

```
Jan 06 20:53:23 FTD1 SF-IMS[2414]: [2445] ADI:adi.Realm [INFO] adi.cpp:515:HandleLog(): Successful auth request
```

Auth response

```
...
Jan 06 20:53:23 FTD1 SF-IMS[2414]: [2445] ADI:adi.LdapRealm [DEBUG] adi.cpp:512:HandleLog(): ldap: search returned (1) result pages.
Jan 06 20:53:23 FTD1 SF-IMS[2414]: [2445] ADI:adi.LdapRealm [DEBUG] adi.cpp:512:HandleLog(): search '(|(sAMAccountName=Test1))' has the following DN:
'CN=Test1,CN=Users,DC=fire,DC=int'.
Jan 06 20:53:23 FTD1 SF-IMS[2414]: [2445] ADI:adi.LdapRealm [DEBUG] adi.cpp:512:HandleLog(): getUserIdentifier: searchfield sAMAccountName has display naming attr: Test1.
```

Get user info

```
Jan 06 20:53:23 FTD1 SF-IMS[2414]: [2445] ADI:adi.Realm [DEBUG] adi.cpp:512:HandleLog(): session: adding ip: '172.16.1.2' for user:
'cn=test1,cn=users,dc=fire,dc=int', display name 'Test1'.
Jan 06 20:53:23 FTD1 SF-IMS[2414]: [2445] ADI:vdi.radius [DEBUG] adi.cpp:512:HandleLog(): sending session for user::Test1 identity type::4port::52441
Jan 06 20:53:23 FTD1 SF-IMS[2414]: [2454] ADI:infra.ev-rpc [DEBUG] adi.cpp:512:HandleLog(): Server ADI, sending event for subject adi service session directory.
```

Add mapping

Taking packet captures

SHELL

```
> capture ins_captport interface inside buffer 1000000 match tcp host 172.16.1.2 any
> expert

root@FTD1:# tcpdump -i tun1 -s 1518 -w /var/common/captive_portal.pcap
HS_PACKET_BUFFER_SIZE is set to 4.tcpdump:
listening on tun1, link-type RAW (Raw IP), capture size 1518 bytes

[TEST AUTHENTICATION]

^C
99 packets captured
99 packets received by filter
0 packets dropped by kernel

root@FTD1:/home/admin# exit

> capture ins_captport stop
> copy /noconfirm /pcap capture:ins_captport ins_captport.pcap
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
398 packets copied in 0.80 secs
```

File copied to: /mnt/disk0/ins_captport.pcap

Start a capture on the routed interface

Start a second capture on interface tun1

Perform the testing

Stop tun1 capture (CTRL+C)

Stop routed interface capture

Copy it to a ".pcap" file on disk

The captures at an initial glance

ins_captport.pcap

No.	Destination	Source	Protocol	Lengt	Info
261	172.16.1.1	172.16.1.2	TCP	66	52441 → 885 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 W
262	172.16.1.2	172.16.1.1	TCP	66	885 → 52441 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=
263	172.16.1.1	172.16.1.2	TCP	54	52441 → 885 [ACK] Seq=1 Ack=1 Win=65536 Len=0
264	172.16.1.1	172.16.1.2	TCP	233	52441 → 885 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=
265	172.16.1.2	172.16.1.1	TCP	54	885 → 52441 [ACK] Seq=1 Ack=180 Win=15744 Len=0
266	172.16.1.2	172.16.1.1	TCP	723	885 → 52441 [PSH, ACK] Seq=1 Ack=180 Win=15744 Le
267	172.16.1.1	172.16.1.2	TCP	268	52441 → 885 [PSH, ACK] Seq=180 Ack=670 Win=65024
268	172.16.1.2	172.16.1.1	TCP	336	885 → 52441 [PSH, ACK] Seq=670 Ack=394 Win=16768
269	172.16.1.1	172.16.1.2	TCP	571	52441 → 885 [PSH, ACK] Seq=394 Ack=952 Win=64512
270	172.16.1.2	172.16.1.1	TCP	54	885 → 52441 [ACK] Seq=952 Ack=911 Win=17920 Len=0
273	172.16.1.2	172.16.1.1	TCP	816	885 → 52441 [PSH, ACK] Seq=952 Ack=911 Win=17920

Before bltd NAT

Same ports

After bltd NAT

No.	Destination	Source	Protocol	Lengt	Info
63	169.254.0.1	169.254.3.88	TCP	52	52441 → 885 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 W
64	169.254.3.88	169.254.0.1	TCP	52	885 → 52441 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=
65	169.254.0.1	169.254.3.88	TCP	40	52441 → 885 [ACK] Seq=1 Ack=1 Win=65536 Len=0
66	169.254.0.1	169.254.3.88	TCP	219	52441 → 885 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=
67	169.254.3.88	169.254.0.1	TCP	40	885 → 52441 [ACK] Seq=1 Ack=180 Win=15744 Len=0
68	169.254.3.88	169.254.0.1	TCP	709	885 → 52441 [PSH, ACK] Seq=1 Ack=180 Win=15744 Le
69	169.254.0.1	169.254.3.88	TCP	254	52441 → 885 [PSH, ACK] Seq=180 Ack=670 Win=65024
70	169.254.3.88	169.254.0.1	TCP	322	885 → 52441 [PSH, ACK] Seq=670 Ack=394 Win=16768
71	169.254.0.1	169.254.3.88	TCP	557	52441 → 885 [PSH, ACK] Seq=394 Ack=952 Win=64512
72	169.254.3.88	169.254.0.1	TCP	40	885 → 52441 [ACK] Seq=952 Ack=911 Win=17920 Len=0
73	169.254.3.88	169.254.0.1	TCP	802	885 → 52441 [PSH, ACK] Seq=952 Ack=911 Win=17920

captive_portal.pcap

The captures may need to be decoded

Right click..

- Protocol Preferences ▶
- **Decode As...**
- Show Packet in New Window

Choose SSL for each port

Field	Value	Type	Default	Current
TCP port	52441	Integer, base 10	(none)	SSL
TCP port	885	Integer, base 10	(none)	SSL

Raw

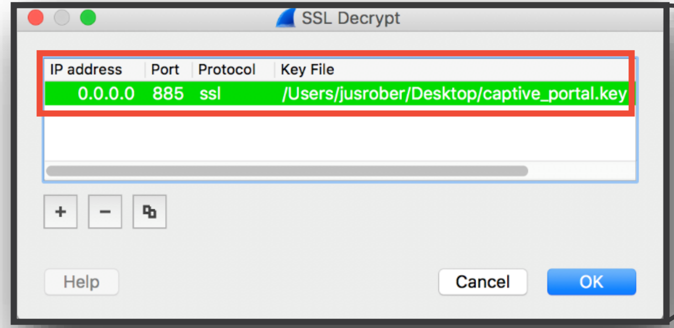
Protocol	Length	Info
TCP	52	52441 → 885 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SA
TCP	52	885 → 52441 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=14
TCP	40	52441 → 885 [ACK] Seq=1 Ack=1 Win=65536 Len=0
TCP	219	52441 → 885 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=179
TCP	40	885 → 52441 [ACK] Seq=1 Ack=180 Win=15744 Len=0
TCP	709	885 → 52441 [PSH, ACK] Seq=1 Ack=180 Win=15744 Len=669
TCP	254	52441 → 885 [PSH, ACK] Seq=180 Ack=670 Win=65024 Len=214
TCP	322	885 → 52441 [PSH, ACK] Seq=670 Ack=394 Win=16768 Len=282
TCP	557	52441 → 885 [PSH, ACK] Seq=394 Ack=952 Win=64512 Len=517
TCP	40	885 → 52441 [ACK] Seq=952 Ack=911 Win=17920 Len=0
TCP	802	885 → 52441 [PSH, ACK] Seq=952 Ack=911 Win=17920 Len=762

Decoded

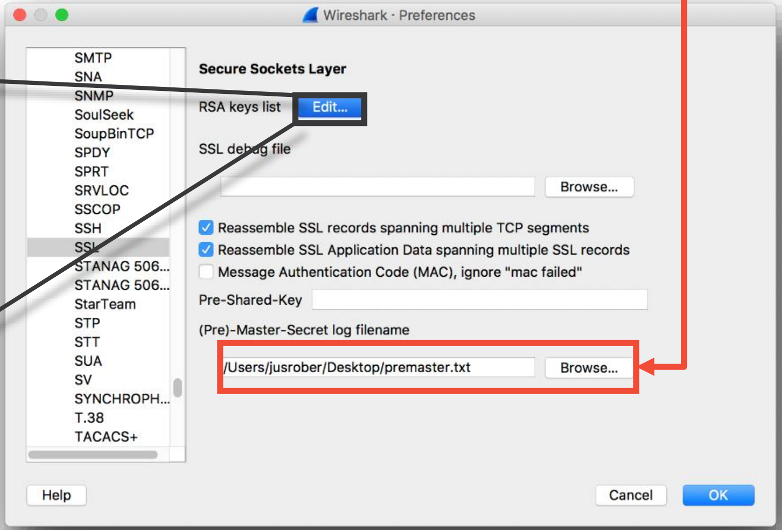
Protocol	Length	Info
TCP	52	52441 → 885 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS
TCP	52	885 → 52441 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0
TCP	40	52441 → 885 [ACK] Seq=1 Ack=1 Win=65536 Len=0
TLSv1.2	219	Client Hello
TCP	40	885 → 52441 [ACK] Seq=1 Ack=180 Win=15744 Len=0
TLSv1.2	709	Server Hello, Certificate, Server Hello Done
TLSv1.2	254	Client Key Exchange, Change Cipher Spec, Finished
TLSv1.2	322	New Session Ticket, Change Cipher Spec, Finished
TLSv1.2	557	Application Data
TCP	40	885 → 52441 [ACK] Seq=952 Ack=911 Win=17920 Len=0
TLSv1.2	802	Application Data, Application Data

Decrypting the captures provides even more insight

1. While testing captive portal, have sessions write out key information (Windows):
   - Set environment variable to create a premaster secret file:
     setx SSLKEYLOGFILE "%HOMEPATH%\Desktop\premaster.txt"
   - Open a private / incognito window and test
2. Use RSA private key (Captive Portal private key)

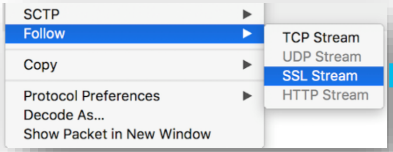


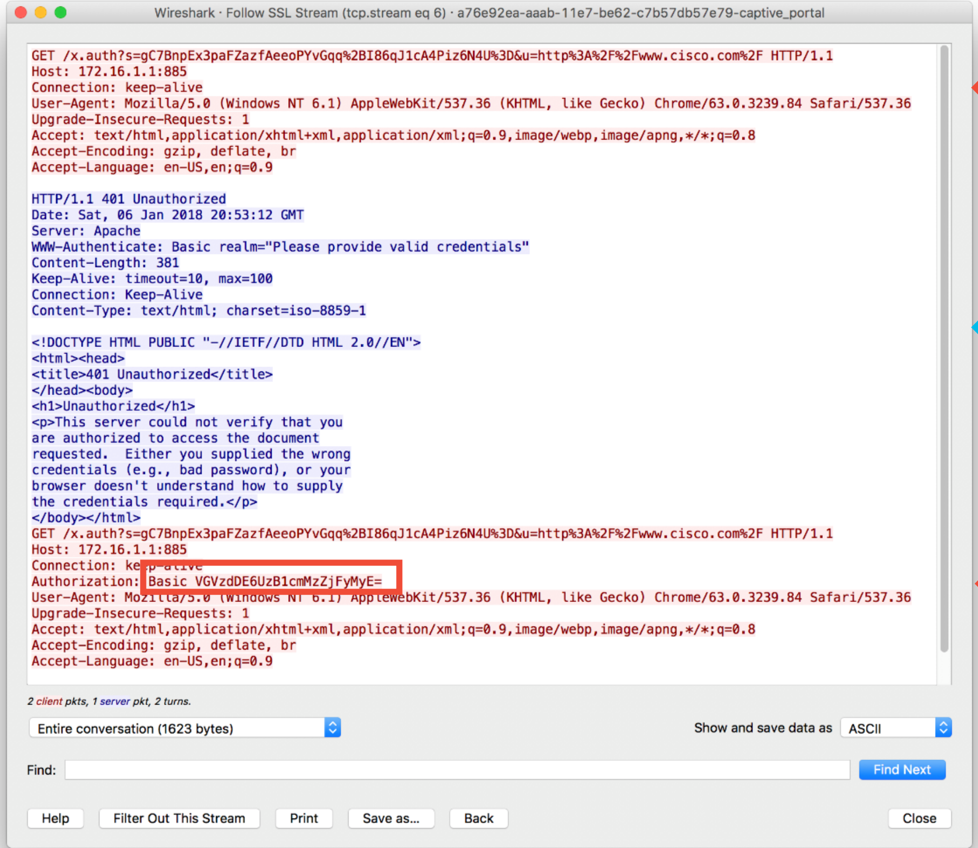
Preferences > Protocols > SSL



You can now follow the SSL Stream

(Right click any SSL Packet)





GET request
after initial redirect

401 Unauthorized
Challenge Response

Captured
Credentials

Redirect back to original destination

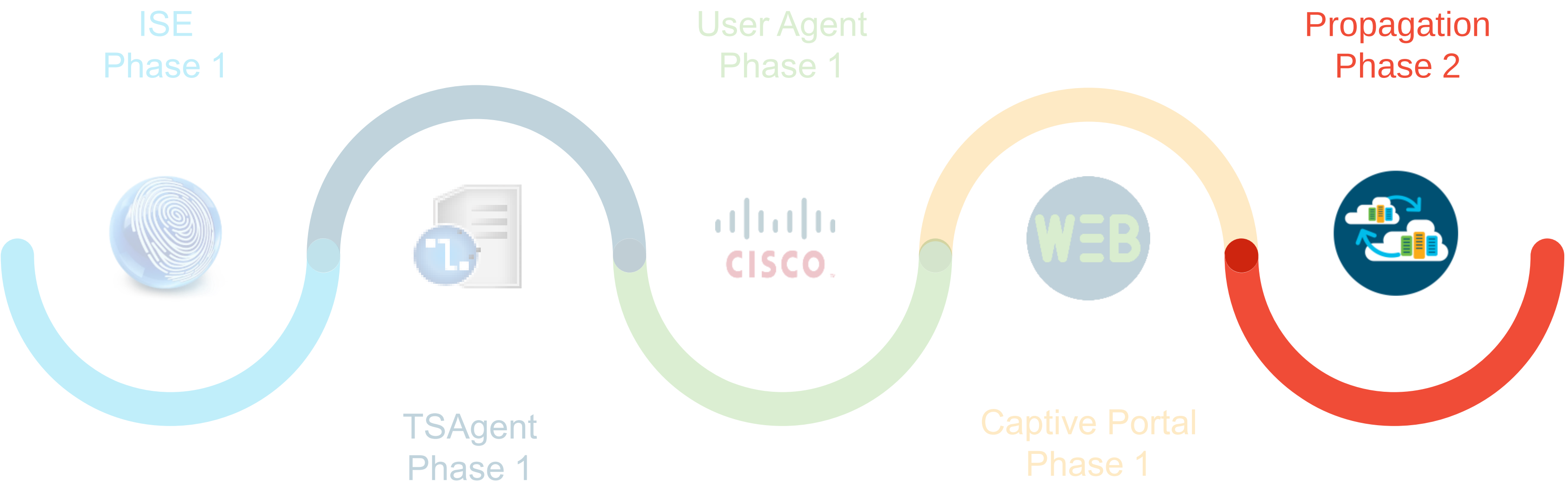
```
GET /x.auth?s=gC7BnpEx3paFZazfAeeoPYvGqq%2BI86qJ1cA4Piz6N4U%3D&u=http%3A%2F%2Fwww.cisco.com%2F HTTP/1.1
Host: 172.16.1.1:885
Connection: keep-alive
Authorization: Basic VGVzdDE6UzB1cmMzZjFyMyE=
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9

HTTP/1.1 307 Temporary Redirect
Date: Sat, 06 Jan 2018 20:53:22 GMT
Server: Apache
Location: http://www.cisco.com/
Content-Length: 231
Keep-Alive: timeout=10, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>307 Temporary Redirect</title>
</head><body>
<h1>Temporary Redirect</h1>
<p>The document has moved <a href="http://www.cisco.com/">here</a>.</p>
</body></html>
```

Original Destination

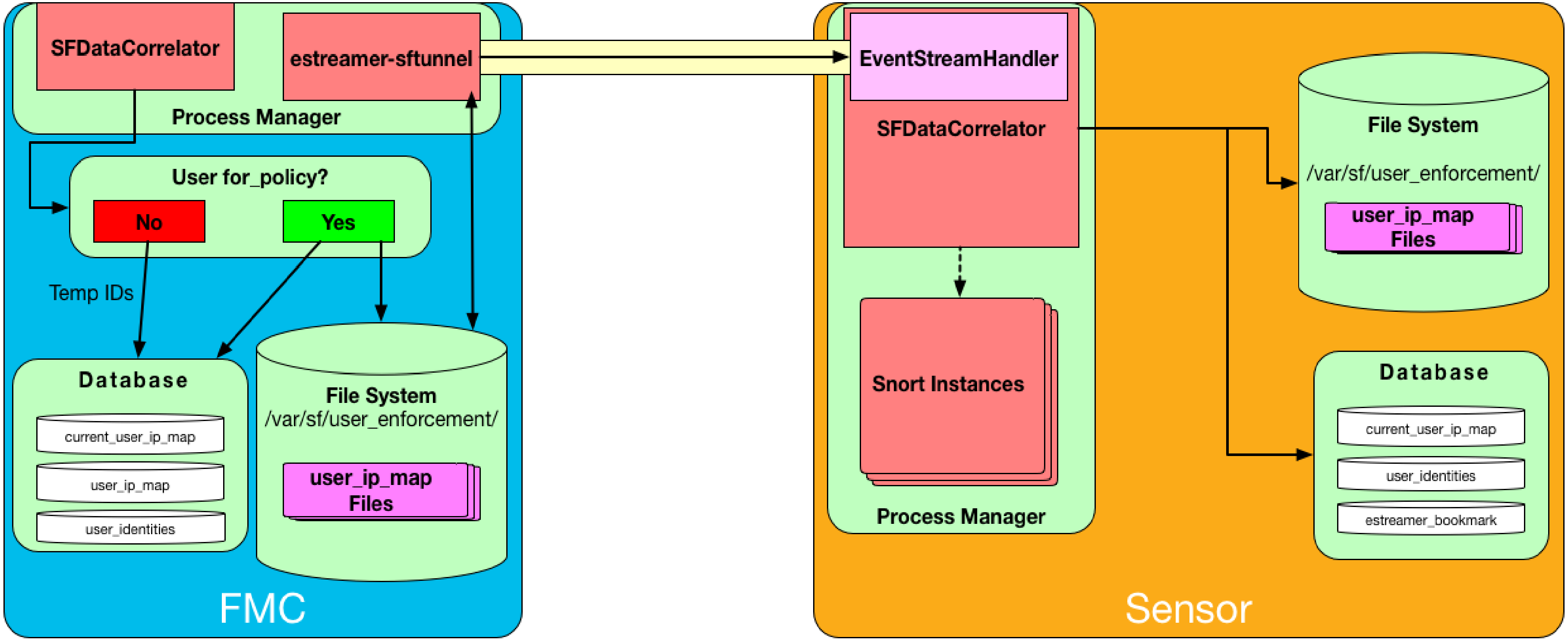
Captive Portal Recap

- Check that all of the relevant processes are up and running
- If you are getting redirected / prompted for credentials:
  - Look for errors in /var/log/captive_portal.log
  - Put **adi** into debug mode
- Problems with redirect / prompt for credentials:
  - Look for errors in /var/log/idhttpsd/error_log
  - Take simultaneous packet captures from routed interface and tunnel interface
    - Prepare to be able to decrypt the captures (Premaster Secret or RSA Key)
- Do all 3 at the same time!

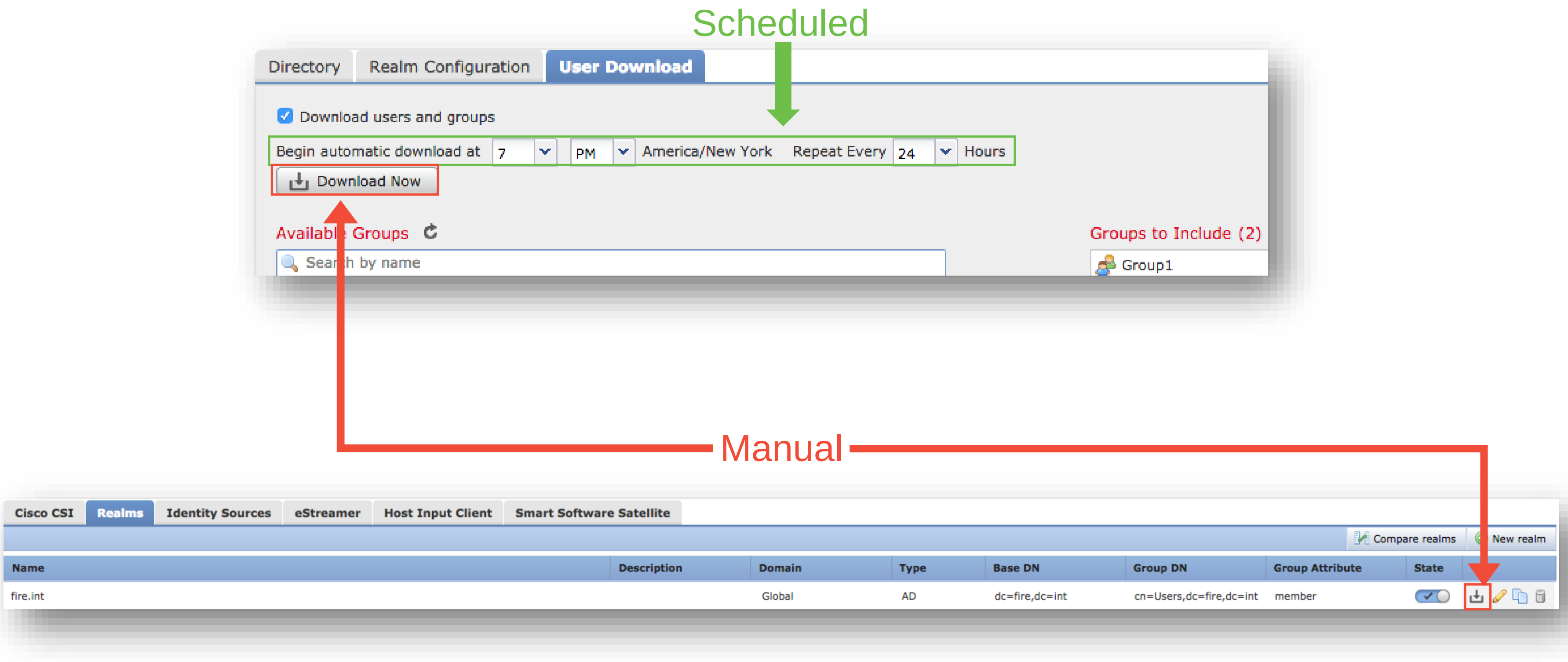
Phase Discussion



Phase 2 Diagram



The user and group downloads



Updates the user_group_map and user_group tables

Script for database interaction
****Read operations ONLY please!****

SHELL

```
root@FMC:/# OmniQuery.pl

sdb> select * from user_group_map;
+----------+------------+----------------+------------------+-------------------------------------------------------+
| user_id | group_id | last_updated | update_status | ldap_uuid                                      |
+----------+------------+----------------+------------------+-------------------------------------------------------+
| 1       | 1          | 1515024128  | new            | a65af96e-c0ba-11e7-ac8f-d697c550d30a |
| 2       | 2          | 1515024128  | new            | a65af96e-c0ba-11e7-ac8f-d697c550d30a |
+----------+------------+----------------+------------------+-------------------------------------------------------+

sdb> select * from user_group;
+-----------+----+----------+---------------+-------------------------------------------------------+--------------+----------+-----------------+
| realm_id | id | name   | last_updated | ldap_uuid                                      | sync_status | deleted | update_status |
+-----------+----+----------+---------------+-------------------------------------------------------+--------------+----------+-----------------+
| 2         | 1  | Group1 | 1515024128 | a65af96e-c0ba-11e7-ac8f-d697c550d30a | local        | 0        | unchanged     |
| 2         | 2  | Group2 | 1515024128 | a65af96e-c0ba-11e7-ac8f-d697c550d30a | local        | 0        | unchanged     |
+-----------+----+----------+---------------+-------------------------------------------------------+--------------+----------+-----------------+
```


Updates the user_identities table

SHELL

```
root@FMC:/# OmniQuery.pl

sdb> select * from user_identities;
+------------+-------------+------------------------------------+-----------------+-----------------+--------------+--------------+------------------------------------+--------------+
| realm_id | id          | username                           | last_seen       | last_updated    | first_name | last_name  | common_name                        | for_policy |
+------------+-------------+------------------------------------+-----------------+-----------------+--------------+--------------+------------------------------------+--------------+
|        2 |        1  | test1                              | 1514491702 |  1514874692 |  test1       |             |                                    |         1 |
|        2 |        2  | test2                              | 1514491742 |  1514874692 |  test2       |             |                                    |         1 |
|        0 |  9999995  | Pending User                       |             0 |          NULL | NULL        | NULL        | Pending User                       |         0 |
|        0 |  9999996  | Guest                              |             0 |          NULL | NULL        | NULL        | Guest                              |         1 |
|        0 |  9999997  | No Authentication Required         |             0 |          NULL | NULL        | NULL        | No Authentication Required         |         1 |
|        0 |  9999998  | Failed Authentication              |             0 |          NULL | NULL        | NULL        | Failed Authentication              |         1 |
|        0 |  9999999  | Unknown                            |             0 |          NULL | NULL        | NULL        | Unknown                            |         1 |
|        2 | 10000001  | administrator                      | 1514706040 |  1514874692 |             |             |                                    |         0 |
|        2 | 10000002  | Test3                              | 1514489481 |  1514878476 | test3       |             |                                    |         0 |
+------------+-------------+------------------------------------+-----------------+-----------------+--------------+--------------+------------------------------------+--------------+
```

- **Downloaded Users -** Downloaded users.
- **Special Identities** - Built in identities for special use. (also, 9999993 “Pending”)
- **Temporary Users** - Users that were seen, but were not part of the downloaded groups are given a temporary ID (10000000+).

Create unified files to update the sensors

SHELL

```
root@FMC:/# less /var/log/messages
…
Nov 29 22:52:42 FMC SF-IMS[4339]: [4313] ADI:adi.DirectoryTestHandler [INFO] test: directory LDAP bind.
Nov 29 22:52:42 FMC SF-IMS[4339]: [4313] ADI:adi.Directory [INFO] Directory server ldap://192.168.0.2:389 changed state to up
Nov 29 22:52:42 FMC SF-IMS[4339]: [4313] ADI:adi.DirectoryTestHandler [INFO] test: LDAP bind succeeded.
Nov 29 22:52:42 FMC SF-IMS[4339]: [21583] ADI:adi.LdapRealm [WARN] ldap: search failed: Can't contact LDAP server, attempting rebind
Nov 29 22:52:42 FMC SF-IMS[4842]: [21596] SFDataCorrelator:ControlHandler [INFO] Handling control connection from sudo_user '', cmd '/usr/bin/perl /usr/local/sf/bin/ActionQueueScrape.pl', pid 21557 (uid 0, gid 0)
Nov 29 22:52:43 FMC SF-IMS[6745]: [6748] Event Streamer:Unified2Iterator [INFO] Opened /var/sf/user_enforcement/user_group_map.1511995962
```

File gets created on disk

SHELL

```
root@FMC:/# ls -lh /var/sf/user_enforcement/
total 128K
-rw-r--r-- 1 root root 156 Nov 26 00:02 user_group_map.1511654525
-rw-r--r-- 1 root root 156 Nov 27 00:02 user_group_map.1511740924
-rw-r--r-- 1 root root 156 Nov 28 00:02 user_group_map.1511827326
-rw-r--r-- 1 root root 156 Nov 29 00:02 user_group_map.1511991421
-rw-r--r-- 1 root root 156 Nov 29 22:52 user_group_map.1511995962
```

View it!

SHELL

```
# u2dump user_group_map.1511995962

Unified2 Record at offset 0
    Type: 153(0x00000099)
    Timestamp: 1511995962
    Length: 48 bytes
Unified2UserGroupMapUpdate
    Group ID:          1
    Group Name:        Group1
    Added Users:       1  2
    Removed Users:
…
```

The sensors consume the data

SHELL

```
root@FTD1:/# less /var/log/messages
…
Nov 29 22:52:43 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:EventStreamHandler [INFO] USER_GROUP_CTRL_MSG (1)
Nov 29 22:52:43 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:UserIdentity [INFO] Creating User IP Map snapshots snapshot_flag = 1
Nov 29 22:52:43 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:Unified2Archive [INFO] Opened archive file
'/ngfw/var/sf/user_enforcement/user_ip_map.snapshot.1511995963'
```

File gets created on disk

SHELL

```
root@FTD1:/# ls -lh /var/sf/user_enforcement/
total 16K
-rw-r--r-- 1 root root  92 Nov 29 23:00 user_ip_map.1511996419
-rw-r--r-- 1 root root 190 Nov 30 17:58 user_ip_map.1512053716
-rw-r--r-- 1 root root 159 Nov 29 22:52 user_ip_map.snapshot.1511995963
```

View it!

SHELL

```
# u2dump user_ip_map.snapshot.1511995963

Unified2 Record at offset 0
 Type: 156(0x0000009c)
Timestamp: 1511995963
Length: 40 bytes
Unified2UserGroupSnapshot
Groups:         1 2
…
```

Mapping users to IP addresses

Phase 2 - SFDataCorrelator

Writes the updates it receives into the database directly

- Updates multiple tables
- There is no log of this action

Writes out raw unified files to disk

- Also stored in the /var/sf/user_enforcement/ directory
- Follow a naming scheme of **user_ip_map.<epoch_tstamp>**
- Only users intended for use in policy are included (for_policy = 1)

SFDataCorrelator opening the unified to write to

SHELL

```
root@FMC:/# less /var/log/messages
…
Nov 13 18:23:06 FMC SF-IMS[4842]: [23574] SFDataCorrelator:MySQLEvent [INFO] Created temporary merge table: temp_SFD_update_rua_event_23574
Nov 13 18:23:06 FMC SF-IMS[4842]: [23574] SFDataCorrelator:MySQLEvent [INFO] Drop temporary merge table: temp_SFD_update_rua_event_23574
Nov 13 18:23:06 FMC SF-IMS[4842]: [23574] SFDataCorrelator:UserIdentity [INFO] GetUserIdentityByUserKey() found no record for Realm:2, Username:test1, Protocol:788
Nov 13 18:23:06 FMC SF-IMS[4842]: [23574] SFDataCorrelator:UserIdentity [INFO] GetUserIdentityByUserKey() found no record for Realm:2, Username:test1, Protocol:683
Nov 13 18:23:06 FMC SF-IMS[4842]: [23574] SFDataCorrelator:UserIdentity [INFO] GetUserIdentityByEmailKey() found no record for Realm:2, Email:test1@fire.int, Protocol:788
Nov 13 18:23:06 FMC SF-IMS[4842]: [23574] SFDataCorrelator:UserIdentity [INFO] GetUserIdentityByEmailKey() found no record for Realm:2, Email:test1@fire.int, Protocol:683
Nov 13 18:23:06 FMC SF-IMS[4842]: [23574] SFDataCorrelator:Unified2Archive [INFO] Opened archive file '/var/sf/user_enforcement/user_ip_map.1510597386'
```

The user_ip_map files

File on the FMC

```
SHELL
root@FMC:/# ls -lh /var/sf/user_enforcement/
total 36K
-rw-r--r-- 1 root root  156 Nov 13 18:23 user_group_map.1510597386
-rw-r--r-- 1 root root  156 Nov 14 00:02 user_group_map.1510617725
-rw-r--r-- 1 root root  156 Nov 15 00:02 user_group_map.1510704128
-rw-r--r-- 1 root root  156 Nov 16 00:02 user_group_map.1510790524
-rw-r--r-- 1 root root  156 Nov 17 00:02 user_group_map.1510876924
-rw-r--r-- 1 root root  156 Nov 18 00:02 user_group_map.1510963325
-rw-r--r-- 1 root root  156 Nov 19 00:02 user_group_map.1511049727
-rw-r--r-- 1 root root  156 Nov 20 00:02 user_group_map.1511136124
-rw-r--r-- 1 root root 1.4K Nov 20 17:48 user_ip_map.1510597386
```

File on the FTD

```
SHELL
root@FTD1:/# ls -lh /var/sf/user_enforcement/
total 16K
-rw-r--r-- 1 root root 190 Nov 19 01:19 user_ip_map.1511053578
-rw-r--r-- 1 root root 190 Nov 20 17:48 user_ip_map.1511195137
-rw-r--r-- 1 root root  56 Nov 19 00:02 user_ip_map.snapshot.1511049728
-rw-r--r-- 1 root root  56 Nov 20 00:02 user_ip_map.snapshot.1511136126
```

Using u2dump to read the user_ip_map files

SHELL

```
# u2dump user_ip_map.1510597386

Unified2 Record at offset 956
  Type: 151(0x00000097)
  Timestamp: 1511053577
  Length: 82 bytes
Unified2UserIpMapUpdate
  User ID:        1
  Realm ID:       2
  User Name:      test1
  IP Address:     ::ffff:172.16.1.2
  Timestamp:      1511053233
  Flag:           1
  Authentication:  1
  Endpoint ID:    0
  Security Tag ID: 0
  Location IP:    ::
  PAT Range Start: 0
  User PAT Start:  0
  User PAT End:    0
…
```

Logon Event

Logoff Event

SHELL

```
# u2dump user_ip_map.1510597386
…
Unified2 Record at offset 1054
 Type: 151(0x00000097)
  Timestamp: 1511054342
  Length: 76 bytes
Unified2UserIpMapUpdate
  User ID:        0
  Realm ID:       2
  User Name:      (null)
  IP Address:     ::ffff:172.16.1.2
  Timestamp:      1511053998
  Flag:           0
  Authentication:  1
  Endpoint ID:    0
  Security Tag ID: 0
  Location IP:    ::
  PAT Range Start: 0
  User PAT Start:  0
  User PAT End:    0
```

Transferring information to the sensor

Process check!

- The **estreamer-sftunnel** process
  - Responsible for the transfer of data to the sensors
  - Has a dedicated sftunnel channel that is used for the transfers
  - Logs to syslog as ”Event Streamer”
- New data is actively sent to the sensors when received
- Old data can be streamed again at sensors request

SHELL

```
root@FMC:/# pmtool status | grep "estreamer-sftunnel ”
estreamer-sftunnel (normal) - Running 6745
```

Estreamer-sftunnel opening the unifieds

SHELL

```
root@FMC:/# less /var/log/messages
…
Nov 13 18:23:06 FMC SF-IMS[4842]: [23574] SFDataCorrelator:MySQLEvent [INFO] Created temporary merge table: temp_SFD_update_rua_event_23574
Nov 13 18:23:06 FMC SF-IMS[4842]: [23574] SFDataCorrelator:MySQLEvent [INFO] Drop temporary merge table: temp_SFD_update_rua_event_23574
Nov 13 18:23:06 FMC SF-IMS[4842]: [23574] SFDataCorrelator:UserIdentity [INFO] GetUserIdentityByUserKey() found no record for Realm:2, Username:test2,
Protocol:788
Nov 13 18:23:06 FMC SF-IMS[4842]: [23574] SFDataCorrelator:UserIdentity [INFO] GetUserIdentityByUserKey() found no record for Realm:2, Username:test2,
Protocol:683
Nov 13 18:23:06 FMC SF-IMS[4842]: [23574] SFDataCorrelator:UserIdentity [INFO] GetUserIdentityByEmailKey() found no record for Realm:2,
Email:test2@fire.int, Protocol:788
Nov 13 18:23:06 FMC SF-IMS[4842]: [23574] SFDataCorrelator:UserIdentity [INFO] GetUserIdentityByEmailKey() found no record for Realm:2,
Email:test2@fire.int, Protocol:683
Nov 13 18:23:07 FMC SF-IMS[4829]: [4841] Event Streamer:Unified2Iterator [INFO] Opened /var/sf/user_enforcement/user_group_map.1510597386
Nov 13 18:23:07 FMC SF-IMS[4829]: [4841] Event Streamer:Unified2Iterator [INFO] Opened /var/sf/user_enforcement/user_ip_map.1510597386
```

Receiving data on the sensor

Process Check!

- Sensor has its own SFDataCorrelator process
  - **EventStreamHandler** thread connects to estreamer-sftunnel and receives data
  - **UserIdentity** thread processes the data
  - **Unified2Archive** thread creates and updates the local user_ip_map files
  - Also updates the local sensor database

SHELL

```
root@FTD1:/# pmtool status | grep SFDataCorrelator
SFDataCorrelator (normal) - Running 3715

root@FTD1:/# less /var/log/messages
…
Nov 13 18:23:07 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:EventStreamHandler [INFO] Init sequence to 1
Nov 13 18:23:08 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:UserIdentity [INFO] GetUserIdentityByUserKey() found no record for (ID 1)
Nov 13 18:23:08 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:UserIdentity [INFO] GetUserIdentityByUserKey() found no record for Realm:2, Username:test1,
Protocol:0
Nov 13 18:23:08 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:Unified2Archive [INFO] Opened archive file
'/ngfw/var/sf/user_enforcement/user_ip_map.1510597388'
```


Snort loads the snapshot and the incremental file

SHELL

```
root@FTD1:/# less /var/log/messages
```

Information is logged in syslog

```
...
Nov 13 18:23:08 FTD1 SF-IMS[5500]: [5506] sfpreproc:UserGroupMapReload [INFO] update tpye UPDATE_GROUPS, deleting old ug_hash
Nov 13 18:23:08 FTD1 SF-IMS[5500]: [5506] sfpreproc:UserGroup [INFO] loading snapshot: /var/sf/user_enforcement/user_ip_map.snapshot.1510597388
```

Snort loads snapshot

```
Nov 13 18:23:08 FTD1 SF-IMS[5500]: UserGroup [INFO] User/Group counts:
Nov 13 18:23:08 FTD1 SF-IMS[5500]: UserGroup [INFO]    num hosts:              0
Nov 13 18:23:08 FTD1 SF-IMS[5500]: UserGroup [INFO]    num groups:             0
Nov 13 18:23:08 FTD1 SF-IMS[5500]: UserGroup [INFO]    num user/group mappings:  0
Nov 13 18:23:08 FTD1 SF-IMS[5500]: UserGroup [INFO]    num users:              0
Nov 13 18:23:08 FTD1 SF-IMS[5500]: UserGroup [INFO]    num skipped:            0
Nov 13 18:23:08 FTD1 SF-IMS[5500]: UserGroup [INFO]    num cache misses:       0
Nov 13 18:23:08 FTD1 SF-IMS[5500]: UserGroup [INFO]    num cache updates:      0
Nov 13 18:23:08 FTD1 SF-IMS[5500]: UserGroup [INFO] User/Group mem usage:
Nov 13 18:23:08 FTD1 SF-IMS[5500]: UserGroup [INFO]    group_bit_hash:  65616
Nov 13 18:23:08 FTD1 SF-IMS[5500]: UserGroup [INFO]    user_group_hash: 65720
Nov 13 18:23:08 FTD1 SF-IMS[5500]: UserGroup [INFO]    host_hash:      262224
Nov 13 18:23:08 FTD1 SF-IMS[5500]: UserGroup [INFO]    user_ip_hash:    0
Nov 13 18:23:08 FTD1 SF-IMS[5500]: UserGroup [INFO]    total:          393560
Nov 13 18:23:08 FTD1 SF-IMS[5500]: UserGroup [INFO]    memcap:         903150
Nov 13 18:23:08 FTD1 SF-IMS[5500]: UserGroup [INFO]    groupMemcap:     100350
```

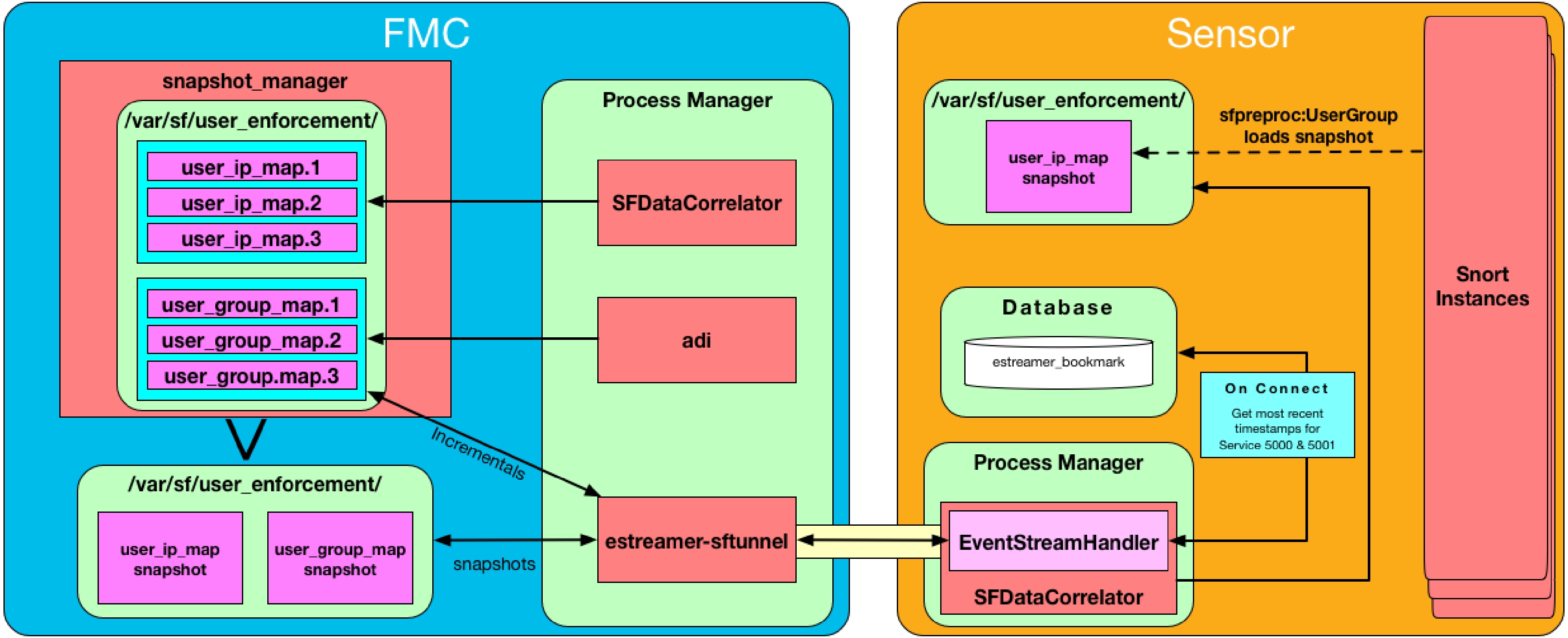
Summary of the user/group load

```
Nov 13 18:23:08 FTD1 SF-IMS[5500]: [5506] sfpreproc:Unified2Iterator [INFO] Opened /var/sf/user_enforcement/user_ip_map.1510597388
```

Snort opens the Incremental file

Let’s rewind

…and talk more about snapshots



FMC Snapshots

Process Check!

- Critical Processes:
  - **SFDataCorrelator** – Responsible for creating user_ip_map snapshots
  - **snapshot_manager**:
    - Creates snapshots for user_group_map files (snapshot_manager.pl)
    - Prunes old user_ip_map and user_group_map files (*/var/log/snapshot_manager.log*)

SHELL

```
root@FMC:/# pmtool status | egrep "SFDataCorrelator \(|snapshot_manager \(”
SFDataCorrelator (normal) - Running 11317
snapshot_manager (normal) - Running 4947
```

When do FMC snapshots happen?

File Count	If there are more than 20 user_ip_map or user_group_map files on the file system
File Size	If there are more than 5MB of incremental updates
Manual	If the snapshot job is invoked manually (TAC)

FMC Snapshots

SHELL

```
root@FMC:/# less /var/log/messages

…
Nov 28 20:54:18 FMC SF-IMS[4842]: [17628] SFDataCorrelator:HandleUserMessage [INFO] CHANGE_USER_CREATE_SNAPSHOT message
Nov 28 20:54:18 FMC SF-IMS[4842]: [17628] SFDataCorrelator:UserIdentity [INFO] Creating User IP Map snapshots snapshot_flag = 0
Nov 28 20:54:18 FMC SF-IMS[4842]: [17628] SFDataCorrelator:Unified2Archive [INFO] Opened archive file
'/var/sf/user_enforcement/user_ip_map.snapshot.1511902458'
Nov 28 20:54:18 FMC SF-IMS[4842]: [17628] SFDataCorrelator:Unified2Archive [INFO] Opened archive file
'/var/sf/user_enforcement/user_ip_map.snapshot-v2.1511902458'
Nov 28 20:54:18 FMC SF-IMS[4842]: [17628] SFDataCorrelator:Unified2Archive [INFO] Opened archive file
'/var/sf/user_enforcement/user_ip_map.snapshot-v1.1511902458'
…
```

Resulting files on FMC

SHELL

```
root@FMC:/# ls -lh /var/sf/user_enforcement/*user_ip*snapshot*
-rw-r--r-- 1 root root 62 Nov 28 20:54 user_ip_map.snapshot-v1.1511902458
-rw-r--r-- 1 root root 91 Nov 28 20:54 user_ip_map.snapshot-v2.1511902458
-rw-r--r-- 1 root root 97 Nov 28 20:54 user_ip_map.snapshot.1511902458
```

When do Sensor snapshots happen?

Group Download	Every time the sensor gets Group data (usually User/Group downloads)
Re-connect to estreamer-sftunnel	Every time SFDataCorrelator:EventStreamHandler thread re-connects to FMC's estreamer-sftunnel instance
Manual	If the snapshot job is invoked manually (TAC)

Sensor snapshots

SHELL

```
root@FTD1:/# less /var/log/messages
…
Nov 20 00:02:06 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:EventStreamHandler [INFO] USER_GROUP_CTRL_MSG (1)
Nov 20 00:02:06 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:UserIdentity [INFO] Creating User IP Map snapshots snapshot_flag = 1
Nov 20 00:02:06 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:Unified2Archive [INFO] Opened archive file
'/ngfw/var/sf/user_enforcement/user_ip_map.snapshot.1511136126'
```

Resulting file on FTD

SHELL

```
root@FTD1:/# ls -lh /var/sf/user_enforcement/
total 16K
-rw-r--r-- 1 root root 190 Nov 19 01:19 user_ip_map.1511053578
-rw-r--r-- 1 root root 190 Nov 20 17:48 user_ip_map.1511195137
-rw-r--r-- 1 root root  56 Nov 19 00:02 user_ip_map.snapshot.1511049728
-rw-r--r-- 1 root root  56 Nov 20 00:02 user_ip_map.snapshot.1511136126
```

The sensor establishes a connection to estreamer

SHELL

```
root@FTD1:/# less /var/log/messages
```

Information is logged in syslog

```
...
Nov 29 15:55:37 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:EventStreamHandler [INFO] Established estreamer connection to 192.168.2.10
Nov 29 15:55:37 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:EventStreamHandler [INFO] sending User Enforcement request message
```

Connected to estreamer-sftunnel

```
...
Nov 29 15:55:37 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:EventStreamHandler [INFO] Published service 5001 data size 8
Nov 29 15:55:37 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:EventStreamHandler [INFO] Service/type 5001 is available. remains 32 bytes
Nov 29 15:55:37 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:EventStreamHandler [INFO] Published service 5000 data size 8
Nov 29 15:55:37 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:EventStreamHandler [INFO] Service/type 5000 is available. remains 16 bytes
```

Services 5000 & 5001 are published to client

```
...
Nov 29 15:55:37 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:EventStreamHandler [INFO] requesting service
SF_USER_ENFORCEMENT (5000) initial timestamp 1511883672
Nov 29 15:55:37 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:EventStreamHandler [INFO] REQ_SEND_USER_IP_MAP_EVENTS version 3
```

Build request for Service 5000 (User)

```
Nov 29 15:55:37 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:EventStreamHandler [INFO] requesting service
SF_GROUP_ENFORCEMENT (5001) initial timestamp 1511827326
Nov 29 15:55:37 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:EventStreamHandler [INFO] REQ_SEND_USER_GROUP_SNAPSHOTS version 1
```

Build request for Service 5001 (Group)

```
Nov 29 15:55:37 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:EventStreamHandler [INFO] SEND FULL REQUEST 2049 length 72 bytes
Nov 29 15:55:37 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:EventStreamHandler [INFO] SEND FULL REQUEST 2049 length 72 bytes
```

Send both requests

The FMC receives the initial request

SHELL

```
root@FMC:/# less /var/log/messages
```

Information is logged in syslog

```
…
Nov 29 15:55:37 FMC SF-IMS[6745]: [6748] Event Streamer:sfestreamer [INFO] Got UEC_STREAM_REQUEST length 72
```

Requests received

```
Nov 29 15:55:37 FMC SF-IMS[6745]: [6748] Event Streamer:ConnectionHandler [INFO] requested service [5000] timestamp [1511883672]
Nov 29 15:55:37 FMC SF-IMS[6745]: [6748] Event Streamer:ConnectionHandler [INFO] Got Event type 121, version 3
Nov 29 15:55:37 FMC SF-IMS[6745]: [6748] Event Streamer:ConnectionHandler [INFO] user_ip_map events version 3
```

Parsed request for service 5000 (User)

```
Nov 29 15:55:37 FMC SF-IMS[6745]: [6748] Event Streamer:ConnectionHandler [INFO] requested service [5001] timestamp [1511827326]
Nov 29 15:55:37 FMC SF-IMS[6745]: [6748] Event Streamer:ConnectionHandler [INFO] Got Event type 122, version 1
Nov 29 15:55:37 FMC SF-IMS[6745]: [6748] Event Streamer:ConnectionHandler [INFO] user_group_snapshots version 1
```

Parsed request for service 5001 (Group)

```
Nov 29 15:55:37 FMC SF-IMS[6745]: [6748] Event Streamer:ConnectionHandler [INFO] creating iterator for service
[5001] prefix [user_group_map.] timestamp [1511827326]
Nov 29 15:55:37 FMC SF-IMS[6745]: [6748] Event Streamer:ConnectionHandler [INFO] creating iterator for service
[5000] prefix [user_ip_map.] timestamp [1511883672]
```

Iterator called to search local files for more recent data

```
…
Nov 29 15:55:37 FMC SF-IMS[6745]: [6748] Event Streamer:ConnectionHandler [INFO] NeedSendSnapshot:
oldest file [user_ip_map.1511969667] newest snapshot [user_ip_map.snapshot.1511902458]
Nov 29 15:55:37 FMC SF-IMS[6745]: [6748] Event Streamer:ConnectionHandler [INFO] need snapshot for service 5000
```

More recent data is available

```
Nov 29 15:55:37 FMC SF-IMS[6745]: [6748] Event Streamer:ConnectionHandler [INFO]
/usr/local/sf/bin/send_user_group_snapshots.pl a76e92ea-aaab-11e7-be62-c7b57db57e79 '
/var/sf/user_enforcement/user_ip_map.snapshot.1511902458' 'user_ip_map.snapshot.1511902458' '' '' /var/sf/run/estreamer-sftunnel.pid
```

Perl script called to copy the snapshot file to the sensor

The sensor loads the snapshot, requests more data

SHELL

```
root@FTD1:/# less /var/log/messages

…
Nov 29 15:55:52 FTD1 SF-IMS[4497]: [7722] SFDataCorrelator:HandleUserMessage [INFO] CHANGE_USER_GROUP_LOAD_SNAPSHOT message
Nov 29 15:55:52 FTD1 SF-IMS[4497]: [7722] SFDataCorrelator:UserIdentity [INFO] loading snapshot /var/sf/peers/a76e92ea-aaab-11e7-be62-c7b57db57e79/user_ip_map.snapshot.1511902458
Nov 29 15:55:53 FTD1 SF-IMS[4497]: [7722] SFDataCorrelator:UserIdentity [INFO] done loading snapshot /var/sf/peers/a76e92ea-aaab-11e7-be62-c7b57db57e79/user_ip_map.snapshot.1511902458
Nov 29 15:55:53 FTD1 SF-IMS[4497]: [7722] SFDataCorrelator:EventStreamHandler [INFO] Received snapshot for peer e4c2196e-aaab-11e7-aaa5-3f8a1e9cd00e
```

Snapshot Loaded

```
…
Nov 29 15:55:53 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:EventStreamHandler [INFO]
snapshot loaded, sending new user enforcement request message
Nov 29 15:55:53 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:EventStreamHandler [INFO] sending User Enforcement request message
```

Create new request for incremental data

```
…
Nov 29 15:55:53 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:EventStreamHandler [INFO] requesting service
SF_USER_ENFORCEMENT (5000) initial timestamp 1511902458
Nov 29 15:55:53 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:EventStreamHandler [INFO] REQ_SEND_USER_IP_MAP_EVENTS version 3
```

New request for service 5000 (User)

```
Nov 29 15:55:53 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:EventStreamHandler [INFO] requesting service
SF_GROUP_ENFORCEMENT (5001) initial timestamp 1511827326
Nov 29 15:55:53 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:EventStreamHandler [INFO] REQ_SEND_USER_GROUP_SNAPSHOTS version 1
```

New request for service 5001 (Group)

```
Nov 29 15:55:53 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:EventStreamHandler [INFO] SEND FULL REQUEST 2049 length 72 bytes
Nov 29 15:55:53 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:EventStreamHandler [INFO] SEND FULL REQUEST 2049 length 72 bytes
```

Send both requests

The FMC receives the request for incrementals

SHELL

```
root@FMC:/# less /var/log/messages

…
Nov 29 15:55:54 FMC SF-IMS[6745]: [6748] Event Streamer:sfestreamer [INFO] Got UEC_STREAM_REQUEST length 72

Nov 29 15:55:54 FMC SF-IMS[6745]: [6748] Event Streamer:ConnectionHandler [INFO] requested service [5000] timestamp [1511902458]
Nov 29 15:55:54 FMC SF-IMS[6745]: [6748] Event Streamer:ConnectionHandler [INFO] Got Event type 121, version 3
Nov 29 15:55:54 FMC SF-IMS[6745]: [6748] Event Streamer:ConnectionHandler [INFO] user_ip_map events version 3

Nov 29 15:55:54 FMC SF-IMS[6745]: [6748] Event Streamer:ConnectionHandler [INFO] requested service [5001] timestamp [1511827326]
Nov 29 15:55:54 FMC SF-IMS[6745]: [6748] Event Streamer:ConnectionHandler [INFO] Got Event type 122, version 1
Nov 29 15:55:54 FMC SF-IMS[6745]: [6748] Event Streamer:ConnectionHandler [INFO] user_group_snapshots version 1

Nov 29 15:55:54 FMC SF-IMS[6745]: [6748] Event Streamer:ConnectionHandler [INFO] creating iterator for service
[5001] prefix [user_group_map.] timestamp [1511827326]
Nov 29 15:55:54 FMC SF-IMS[6745]: [6748] Event Streamer:ConnectionHandler [INFO] creating iterator for service
[5000] prefix [user_ip_map.] timestamp [1511902458]

Nov 29 15:55:54 FMC SF-IMS[6745]: [6748] Event Streamer:Unified2Iterator [INFO] Opened /var/sf/user_enforcement/user_group_map.1511827326
Nov 29 15:55:54 FMC SF-IMS[6745]: [6748] Event Streamer:Unified2Iterator [INFO] Opened /var/sf/user_enforcement/user_ip_map.1510597386
Nov 29 15:55:55 FMC SF-IMS[6745]: [6748] Event Streamer:Unified2Iterator [INFO] Opened /var/sf/user_enforcement/user_group_map.1511913727
Nov 29 15:55:55 FMC SF-IMS[6745]: [6748] Event Streamer:Unified2Iterator [INFO] Opened /var/sf/user_enforcement/user_ip_map.1511969667
```

Request received

Parsed request for service 5000 (User)

Parsed request for service 5001 (Group)

Iterator called to search local files for more recent data

Open newer files to stream to sensor

The new data is written out and picked up by snort

SHELL

```
root@FTD1:/# less /var/log/messages

...
Nov 29 15:55:55 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:EventStreamHandler [INFO] USER_GROUP_CTRL_MSG (1)

Nov 29 15:55:55 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:UserIdentity [INFO] Creating User IP Map snapshots snapshot_flag = 1
Nov 29 15:55:55 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:Unified2Archive [INFO] Opened archive file
'/ngfw/var/sf/user_enforcement/user_ip_map.snapshot.1511970955'
Nov 29 15:55:55 FTD1 SF-IMS[4497]: [4702] SFDataCorrelator:Unified2Archive [INFO] Opened archive file '/ngfw/var/sf/user_enforcement/user_ip_map.1511970955'

Nov 29 15:55:55 FTD1 SF-IMS[335]: [336] sfpreproc:UserGroupMapReload [INFO] update tpye UPDATE_GROUPS, deleting old ug_hash
Nov 29 15:55:55 FTD1 SF-IMS[335]: [336] sfpreproc:UserGroup [INFO] loading snapshot: /var/sf/user_enforcement/user_ip_map.snapshot.1511970955

Nov 29 15:55:55 FTD1 SF-IMS[335]: UserGroup [INFO] User/Group counts:
Nov 29 15:55:55 FTD1 SF-IMS[335]: UserGroup [INFO]    num hosts:                    1
Nov 29 15:55:55 FTD1 SF-IMS[335]: UserGroup [INFO]    num groups:                   2
Nov 29 15:55:55 FTD1 SF-IMS[335]: UserGroup [INFO]    num user/group mappings:      1
Nov 29 15:55:55 FTD1 SF-IMS[335]: UserGroup [INFO]    num users:                    1
Nov 29 15:55:55 FTD1 SF-IMS[335]: UserGroup [INFO]    num skipped:                  0
Nov 29 15:55:55 FTD1 SF-IMS[335]: UserGroup [INFO]    num cache misses:             0
Nov 29 15:55:55 FTD1 SF-IMS[335]: UserGroup [INFO]    num cache updates:            0
Nov 29 15:55:55 FTD1 SF-IMS[335]: UserGroup [INFO] User/Group mem usage:
Nov 29 15:55:55 FTD1 SF-IMS[335]: UserGroup [INFO]    group_bit_hash:               65688
Nov 29 15:55:55 FTD1 SF-IMS[335]: UserGroup [INFO]    user_group_hash:              65852
Nov 29 15:55:55 FTD1 SF-IMS[335]: UserGroup [INFO]    host_hash:                    262296
Nov 29 15:55:55 FTD1 SF-IMS[335]: UserGroup [INFO]    user_ip_hash:                 40
Nov 29 15:55:55 FTD1 SF-IMS[335]: UserGroup [INFO]    total:                        393876
Nov 29 15:55:55 FTD1 SF-IMS[335]: UserGroup [INFO]    memcap:                       905734
Nov 29 15:55:55 FTD1 SF-IMS[335]: UserGroup [INFO]    groupMemcap:                  100637

Nov 29 15:55:56 FTD1 SF-IMS[335]: [336] sfpreproc:Unified2Iterator [INFO] Opened /var/sf/user_enforcement/user_ip_map.1511970955
```

SFDataCorrelator receives data

Snapshot / Incremental files written out

Snort loads snapshot

Summary of the user/group load

Snort loads new incremental file

Advanced Troubleshooting and Failure Identification

The user_map_query script

SHELL

```
# user_map_query.pl --help

Usage: user_map_query.pl [OPTIONS] [ITEMS]...

Version: 4.0
This script will return current information about users, groups and IP addresses.
This will only show user to IP address assoiciations to IP addresses that currently belong to a user.It does not show all IP addresses that the user was associated with in the past.


You must provide one (and only one) of the following options:
-g, -i, -u

Examples:

user_map_query.pl -u jsmith                # displays the information for the user jsmith

user_map_query.pl -i 10.1.2.3              # displays users associated to the IP address 10.1.2.3

user_map_query.pl -g myGroup               # displays all users associated to group myGroup

user_map_query.pl --dump-data sensor       # dumps troubleshooting data and stores it in file sensor_utd.uuid.timestamp.tar.gz


Options:
--dump-data <pre_str>     Dumps all troubleshooting data for user/group mapping. If provided, the output files will be prepended with "<pre_str>_”
-d, --debug               enable debug logging (off by default)
-g, --group               Displays the users associated to the group(s) specified (can not be passed with -i or -u)
-h, -?, --help            Print usage information
-i, --ip-addr             Displays the users associated to the IPv4 address(es) specified (can not be passed with -g or -u)
--iu                      Include unified file data
--outfile                 Dumps the output to the specified file
-s, --snort               Include data from snort's mapping
-u, --user                Displays the IP addresses associated to the user(s) specified (can not be passed with -g or -i)
--unified-all             Displays all of the unified data per record regardless of the type of query
--unified-dir             The directory to look for unified files (default is /var/sf/user_enforcement)
--use-id                  Treats the values passed as IDs (only relevant for user and group queries)
```

Querying for a specific user by name

SHELL

```
root@FMC:/# user_map_query.pl -u test1

Current Time: 11/20/2017 21:33:36 UTC

Getting information on username(s)...

___
User #1: test1
---
        ID:         1
        Last Seen:  Unknown
        for_policy: 1
        Realm ID:   2

==============================
|          Database          |
==============================

##) IP Address [Realm ID]
1)   ::ffff:172.16.1.2 [2]

##) Group Name (ID) [realm: Realm Name (ID)]
 1) Group1 (1) [realm: fire.int (2)]
```

FMC

FTD

SHELL

```
root@FTD1:/# user_map_query.pl -u test1

Current Time: 11/20/2017 21:33:44 UTC

Getting information on username(s)...

___
User #1: test1
---
        ID:         1
        Last Seen:  Unknown
        for_policy: 0
        Realm ID:   2

==============================
|          Database          |
==============================

##) IP Address [Realm ID]
1)   ::ffff:172.16.1.2 [2]

##) Group Name (ID)
 1) Group1 (1)
```

Querying for a specific IP address

SHELL

```
root@FMC:/# user_map_query.pl -i 172.16.1.2

Current Time: 11/20/2017 21:56:21 UTC

Getting information on IP Address(es)...

____
IP #1: 172.16.1.2
---

================================
|            Database           |
================================

##) Username (ID) [Realm ID]
 1) test1 (1) [2]
          for_policy: 1
          Last Seen: Unknown
          Realm Name: fire.int
```

FMC

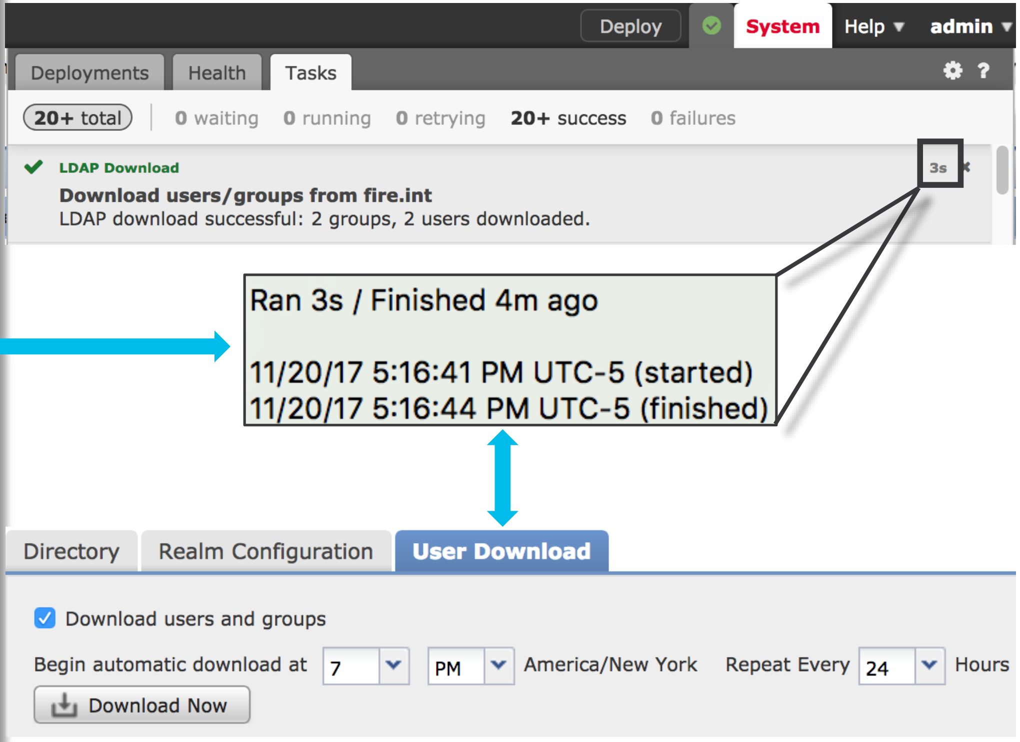
FTD

SHELL

```
root@FTD1:/# user_map_query.pl -i 172.16.1.2

Current Time: 11/20/2017 21:56:26 UTC

Getting information on IP Address(es)...

____
IP #1: 172.16.1.2
---

================================
|            Database           |
================================

##) Username (ID) [Realm ID]
 1) test1 (1) [2]
          for_policy: 0
          Last Seen: Unknown
          Realm Name: Unknown
```

Look at group information on the FMC

```
SHELL
root@FMC:/# user_map_query.pl -g Group1

Current Time: 11/20/2017 22:17:20 UTC

Getting information on Group(s)...

___
Group #1: Group1
---

ID: 1
Group Updated: 11/20/2017 22:16:43 UTC
Realm ID: 2
Realm Name: fire.int

==============================
|          Database          |
==============================

##) Username (ID)
1)   test1 (1)
        for_policy:          1
        Last Seen:           11/20/2017 21:25:47 UTC
        Group Map Update:    01/01/1970 00:00:00 UTC
        Has Auth Login:      1
        Realm Name:          fire.int
        Realm ID:            2
```



Looking at snort related information on FTD

SHELL

```
root@FTD1:/# user_map_query.pl -s -u test1

...

Would you like to dump user data from snort now? (Current Time: 11/20/2017 22:11:12 UTC) [y,n]: y

Successfully commanded snort.

...

Snort identitiy files read:
user_identity.dump file info for snort data:
File time                                   instance(s)
1511215876 (11/20/2017 22:11:16 UTC)        instance 1
____
User #1: test1
---
            ID:        1
            Last Seen:  Unknown
            for_policy: 0
            Realm ID:   2
==============================                              ==============================
|          Database          |                              |           Snort            |
==============================                              ==============================

##) IP Address [Realm ID]                                   ##) IP Address [Realm ID] (instances)
  1) ::ffff:172.16.1.2 [2]                                    1) ::ffff:172.16.1.2 [2] (instance 1)
                                   ...
##) Group Name (ID)                                         ##) Group Name (ID) (instances)
  1) Group1 (1)                                               1) Group1 (1) (instance 1)
```

Note: Snort will only have mapping of user to group if has seen traffic that matched an AC rule that had to do a lookup.

Because of this you may see that some instances have a mapping and others do not and this is normal.

The access control policy

1 **Block** traffic from members of **Group1** destined to ports 80 or 443

2 **Allow** but inspect traffic (intrusion and file) from members of **Group2**

3 **Default** inspect **everything else** against the Security Over Connectivity policy

Filter by Device | Show Rule Conflicts | Add Category | Add Rule | Search Rules

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	ISE/SGT Attributes	Action	
Mandatory - Lab (1-2)														
1	Block_Group1	Any	Any	Any	Any	Any	fire.int/Group1	Any	Any	HTTP HTTPS	Any	Any	Block	0
2	Allow_Group2	Any	Any	Any	Any	Any	fire.int/Group2	Any	Any	Any	Any	Any	Allow	0
Default - Lab (-)														
There are no rules in this section. Add Rule or Add Category														
Default Action													Intrusion Prevention: Security Over Connectivity	

The firewall-engine-debug tool

SHELL

```
> system support firewall-engine-debug

Please specify an IP protocol: tcp
Please specify a client IP address: 172.16.1.2
Please specify a client port:
Please specify a server IP address: 192.168.0.10
Please specify a server port: 8081

Monitoring firewall engine debug messages

172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 New session
172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 Starting with minimum 4, 'Allow_Group2', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 1, icmpType 0, icmpCode 0
172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 rule order 4, 'Allow_Group2', did not match group 2
172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 no match rule order 4, 'Allow_Group2', user 1, realm 2
172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 match rule order 5, id 268434432 action Allow
172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 allow action
172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 URL SI: ShmDBLookupURL("http://192.168.0.10:8081/") returned 0
172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 Starting with minimum 4, 'Allow_Group2', and IPProto first with zones 1 -> 2, geo 0(0) -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 676, payload 0, client 589, misc 0, user 1, url http://192.168.0.10:8081/, xff
172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 rule order 4, 'Allow_Group2', did not match group 2
172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 no match rule order 4, 'Allow_Group2', user 1, realm 2
172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 match rule order 5, id 268434432 action Allow
172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 allow action
172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 no file policy
172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 Deleting session
```

Run the tool from the restricted shell

Enter test parameters
(leave blank for "any")

The UserID can be
found in the metadata

What if you get too much output?

 # grep -i ngfwdbg /var/log/messages | grep <ephemeral_port>

SHELL

```
root@FTD1:/# grep -i ngfwdbg /var/log/messages | grep 54255
Dec  4 19:21:59 FTD1 SF-IMS[31901]: NGFWDbg 172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 New session
Dec  4 19:21:59 FTD1 SF-IMS[31901]: NGFWDbg 172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 Starting with minimum 4, id 268435458 and
IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 1, icmpType 0,
icmpCode 0
Dec  4 19:21:59 FTD1 SF-IMS[31901]: NGFWDbg 172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 rule order 4, id 268435458 did not match group
2
Dec  4 19:21:59 FTD1 SF-IMS[31901]: NGFWDbg 172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 no match rule order 4, id 268435458 user 1,
realm 2
Dec  4 19:21:59 FTD1 SF-IMS[31901]: NGFWDbg 172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 match rule order 5, id 268434432 action Allow
Dec  4 19:21:59 FTD1 SF-IMS[31901]: NGFWDbg 172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 allow action
Dec  4 19:21:59 FTD1 SF-IMS[31901]: NGFWDbg 172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 URL SI:
ShmDBLookupURL("http://192.168.0.10:8081/") returned 0
Dec  4 19:21:59 FTD1 SF-IMS[31901]: NGFWDbg 172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 Starting with minimum 4, id 268435458 and
IPProto first with zones 1 -> 2, geo 0(0) -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 676, payload 0, client 589, misc 0, user 1, url
http://192.168.0.10:8081/, xff
Dec  4 19:21:59 FTD1 SF-IMS[31901]: NGFWDbg 172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 rule order 4, id 268435458 did not match group
2
Dec  4 19:21:59 FTD1 SF-IMS[31901]: NGFWDbg 172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 no match rule order 4, id 268435458 user 1,
realm 2
Dec  4 19:21:59 FTD1 SF-IMS[31901]: NGFWDbg 172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 match rule order 5, id 268434432 action Allow
Dec  4 19:21:59 FTD1 SF-IMS[31901]: NGFWDbg 172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 allow action
Dec  4 19:22:18 FTD1 SF-IMS[31901]: NGFWDbg 172.16.1.2-54255 > 192.168.0.10-8081 6 AS 1 I 0 Deleting session
```

The detection engine

- Enforces policy and performs inspection on traffic traversing the device
  - Snort is the main component
  - Snort stores events here!

SHELL

```
root@FTD1:/# de_info.pl
____________________________________________________________________________
DE Name                : Primary Detection Engine (a76e92ea-aaab-11e7-be62-c7b57db57e79)
DE Type                : ids
DE Description         : Primary detection engine for device a76e92ea-aaab-11e7-be62-c7b57db57e79
DE Resources           : 1
DE UUID                : 6934c232-aaac-11e7-948b-16e77db57e79
____________________________________________________________________________
```

Make note of this for the next slide

Looking at snort related information on FTD

SHELL

```
root@FTD1:/# ls -lh /var/sf/detection_engines/
total 4.0K
drwxr-xr-x 12 root root 4.0K Dec  4 00:00 6934c232-aaac-11e7-948b-16e77db57e79
```

The UUID from the Previous slide

SHELL

```
root@FTD1:/# ls -lh /var/sf/detection_engines/6934c232-aaac-11e7-948b-16e77db57e79/instance-1/unified_events*
-rw------- 1 root root 1.8K  Oct 17   16:32 unified_events-1.log.1508257610
-rw------- 1 root root 4.2K  Oct 19   16:33 unified_events-1.log.1508353958
-rw------- 1 root root 9.3K  Oct 20   17:33 unified_events-1.log.1508448227
-rw------- 1 root root 1.3K  Oct 28   04:21 unified_events-1.log.1509164197
-rw------- 1 root root 1.3K  Oct 31   10:01 unified_events-1.log.1509443741
-rw------- 1 root root 8.4K  Nov  4   09:46 unified_events-1.log.1509707155
-rw------- 1 root root 1.4K  Nov  8.  05:09 unified_events-1.log.1510117403
-rw------- 1 root root 3.8K  Nov 10   13:43 unified_events-1.log.1510273622
-rw------- 1 root root 7.5K  Nov 15.  06:03 unified_events-1.log.1510652304
-rw------- 1 root root 1.1K  Nov 17   09:38 unified_events-1.log.1510907848
-rw-r--r-- 1 root root     23 Nov 24   22:38 unified_events-1.log.bookmark.e4c2196e-aaab-11e7-aaa5-3f8a1e9cd00e
-rw------- 1 root root 876K Dec  4   19:03 unified_events-2.log.1512349944
-rw-r--r-- 1 root root     23 Dec  4   19:02 unified_events-2.log.bookmark.e4c2196e-aaab-11e7-aaa5-3f8a1e9cd00e
```

Each instance of snort gets its own directory

The file with the Connection event

Reading the raw connection event

SHELL

```
root@FTD1:/# u2dump /var/sf/detection_engines/6934c232-aaac-11e7-948b-16e77db57e79/instance-1/unified_events-2.log.1512349944 | less
...
Unified2 Record at offset 251314
  Type: 210(0x000000d2)
  Timestamp: 0
  Length: 877 bytes
Forward to DC: Yes
FlowStats:
...
        Initiator: 172.16.1.2
        Responder: 192.168.0.10
        Original Client: ::
        Policy Revision: 00000000-0000-0000-0000-00005a1099ed
        Rule ID: 268434432
        Tunnel Rule ID: 0
        Monitor Rule ID: <none>
        Rule Action: 2
        Rule Reason: 0
        NetFlow Source: ::
        User ID: 1
        Application ID: 676
        Client ID: 589
        Client Version (12): 62.0.3202.94
        Location IP: ::
        Endpoint Profile ID: 0
        Security Group ID: 0
        URL Category: 0
        URL Reputation: 0
        URL (65): http://192.168.0.10:8081/resources/themes/bootstrap/css/style.css
...
```

Dump the contents with u2dump

IP addresses for for the event

Internal Rule ID for the AC rule that we matched

The ID of the User for the event

The URL data from the triggering packet

The connection in the FMC

	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Initiator User	Responder IP	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
	2017-12-04 14:21:58	2017-12-04 14:22:17	Allow		172.16.1.2		test1 (fire.int\test1, LDAP)	192.168.0.10	inside	outside	54256 / tcp	8081 / tcp
	2017-12-04 14:21:58	2017-12-04 14:22:17	Allow		172.16.1.2		test1 (fire.int\test1, LDAP)	192.168.0.10	inside	outside	54257 / tcp	8081 / tcp
	2017-12-04 14:21:58	2017-12-04 14:22:17	Allow		172.16.1.2		test1 (fire.int\test1, LDAP)	192.168.0.10	inside	outside	54255 / tcp	8081 / tcp
	2017-12-04 14:21:58	2017-12-04 14:22:17	Allow		172.16.1.2		test1 (fire.int\test1, LDAP)	192.168.0.10	inside	outside	54258 / tcp	8081 / tcp

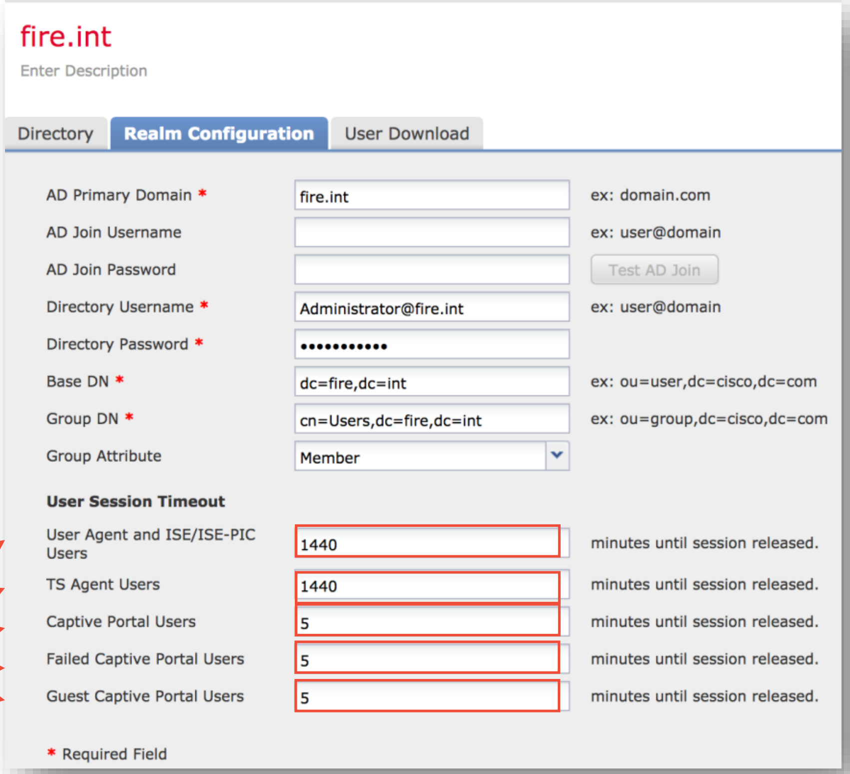
Page 1 of 1 Displaying rows 1–4 of 4 rows

Application Protocol	Client	Client Version	Web Application	Application Risk	Business Relevance	URL	Access Control Policy	Access Control Rule	Network Analysis Policy	Prefilter Policy
							Lab	Default Action	NAP_Time	Lab-Prefilter
							Lab	Default Action	NAP_Time	Lab-Prefilter
HTTP	Chrome	62.0.3202.94	Web Browsing	Medium	Medium	http://192.168.0.10:8081/	Lab	Default Action	NAP_Time	Lab-Prefilter
							Lab	Default Action	NAP_Time	Lab-Prefilter

Change the session timeout values

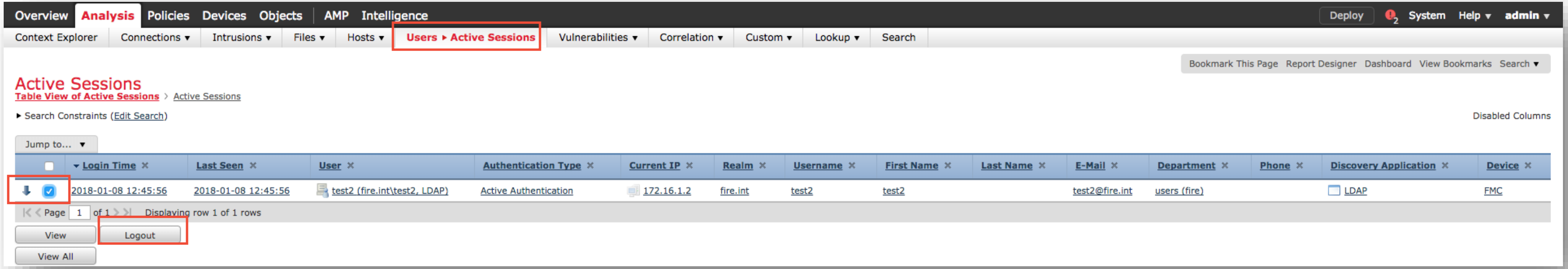
Default 1440

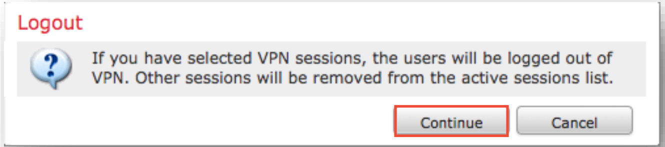
(1 day)

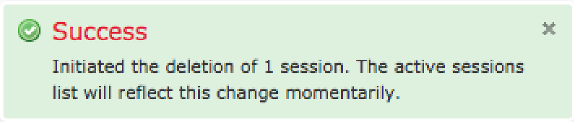


Manually Logout a user on the FMC

Analysis > Users > Active Sessions







Common Issues

Extra Content!

- Cheat Sheet:
  - https://cisco.box.com/s/6a3m93y5zx2t1fsls82xxdc99cgmnv6h

- Identity PCAPS:
  - ins_captout.pcap - https://cisco.box.com/s/qcacl8g2b8l60rc561tpxyx5nwief2a9
  - captive_portal.pcap - https://cisco.box.com/s/lelz4gdt8d4vebzwucbz1udpgng6e754
  - Premaster.txt - https://cisco.box.com/s/d09xorhkualx6mow0o2f7asi6q6yufls

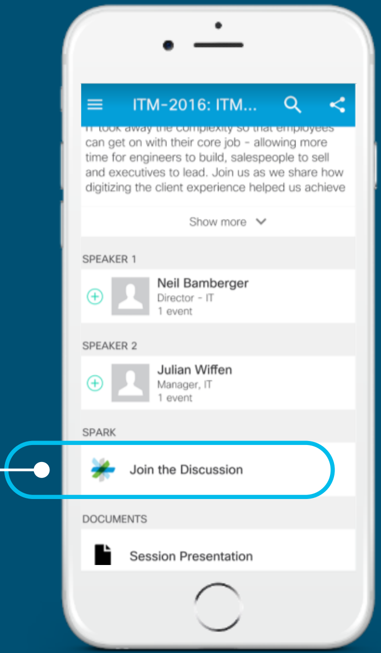
Cisco Spark

Questions?

Use Cisco Spark to communicate with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space



cs.co/ciscolivebot#BRKSEC-3227

Complete Your Online Session Evaluation

- Please complete your Online Session Evaluations after each session
- Complete 4 Session Evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Live T-shirt
- All surveys can be completed via the Cisco Live Mobile App or the Communication Stations

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at www.ciscolive.com/global/on-demand-library/.

Continue Your Education

- Demos in the Cisco campus
- Walk-in Self-Paced Labs
- Tech Circle
- Meet the Engineer 1:1 meetings
- Related sessions

Thank you

You're

iT