Identity, Credential, and Access Management (ICAM) Implementation Guide

Science and Technology Directorate
Identity, Credential, and Access Management (ICAM) Implementation Guidance

July 2018

Version 1

Prepared for
Department of Homeland Security
Science and Technology Directorate
Dedicated to the memory of:

Tom Sorley
1965-2018

The Identity, Credential, and Access Management (ICAM) document series is dedicated to the memory of Tom Sorley. Tom was a member of the Executive Leadership of the Public Safety Communications ICAM Working Group that sponsored this document. He was the Chief Information Officer and Deputy Director of the Information Technology Department for Public Safety for the City of Houston, Texas, and National Chair of the Public Safety Advisory Committee (PSAC). Tom was a thought leader in public safety communications and his vision is reflected in this ICAM Educational Series.
DISCLAIMER OF LIABILITY

The Identity, Credential, and Access Management (ICAM) Educational Series is provided by the Public Safety Communications ICAM Working Group (PSC ICAM WG) “as is” with no warranty of any kind, either expressed or implied, including, but not limited to, any warranty of merchantability or fitness for a particular purpose. This material is provided to support the efforts of public safety information sharing, situational awareness and key decision making. These documents are intended to guide users for making informed decisions on improving the security posture of their information systems by using ICAM principles.

The ICAM Educational Series is intended to provide guidance for implementing ICAM principles, and does not contain or infer any official requirements, policies, or procedures, nor does it supersede any existing official emergency operations planning guidance or requirements documents. As a condition of the use of the Series, the recipient agrees that in no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages, arising out of, resulting from, or in any way connected to the Series or the use of information from the Series for any purpose. It is recommended that organizations align their resources with tools that would best fit their infrastructure as well as their own standards and requirements.

The PSC ICAM WG does not endorse any commercial product or service referenced in the ICAM Educational Series, either explicitly or implicitly. Any reference herein to any specific commercial product, process, or service by service mark, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the PSC ICAM WG. The views and opinions of authors expressed herein do not necessarily state or reflect those of the PSC ICAM WG and shall not be used for advertising or product endorsement purposes.
EXECUTIVE SUMMARY

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) created systems implementing Identity, Credential, and Access Management (ICAM) products within a sandbox for the Public Safety Communications (PSC) Identity, Credential, and Access Management (ICAM) Working Group (WG). This document provides implementation guides to the Public Safety Community (Community) to enhance existing ICAM efforts. PSC ICAM WG worked to discover gaps in publicly available documentation that affect an engineer’s ability to effectively implement an ICAM-enabled system. These gap analyses and assessments provided the foundation for these ICAM Implementation Guides.

The Community’s goal is to have the ability to appropriately share critical information among its members, which can aid in saving lives and protecting property. This critical information is at times highly sensitive and can include law enforcement information, as well as personally identifiable information (PII) and protected health information (PHI), so each organization must have assurance the right person with the right credentials is accessing information at the right time. This is where ICAM comes in.

To support the Community with its mission-critical tasks, ICAM helps address the growing data management, interoperability and cybersecurity challenges facing public safety today. ICAM solutions, especially federated ones, align public safety communities around common identity and access management practices.

It is also important for Community members who are sharing information between different organizations to make sure the information does not fall into the wrong person’s hands. This is where ICAM is essential for the Community. Identity proofing an organization’s employees and volunteers, providing strong credentials for system access and enabling the use of multifactor authentication, using attributes to provision resources, and creating strong access management all help an organization ensure that the right person is accessing an organization’s information through a secure and seamless federation.

The intent of this document is to provide implementation guides for ICAM-enabled systems. This document does not recommend specific ICAM products, but does strive to create useable aids for the implementation of ICAM products and encourage the adoption of multifactor authentication with a focus on the use of open source products. This document is paired with the ICAM Executive Primer and ICAM Acquisition Guidance.

![Figure 1 - Steps to Secure and Seamless Information Sharing (Federation)](image-url)
**Intended Audience**

This document provides guidance to implement the ICAM products. The document teaches each of the following stakeholders\(^1\) about ICAM solutions:

<table>
<thead>
<tr>
<th>Stakeholder Group</th>
<th>Responsibilities</th>
<th>Documents to Read</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Leadership</td>
<td>...is the responsible authority for the Department, State or Agency’s fiscal and human resources for ICAM investments. This stakeholder group will use the document to understand the importance of ICAM investments, and to translate the value proposition of ICAM solutions to their mission needs.</td>
<td>ICAM Executive Primer</td>
</tr>
<tr>
<td>Program Managers</td>
<td>...are responsible for the operational implementation and oversight of ICAM capabilities to ensure they meet the functional mission requirements defined by the intended users. They must communicate to both the Executive Leadership and Solutions Architects to ensure understanding and expectations of the requirements for interoperable ICAM investments. Managers are required to quantify the benefit and resource impacts, including cost and integration savings, to Executive Leadership to ensure continued support and resource sustainment. This document provides Program Managers with a description of the key capabilities, processes, services, infrastructure, standards and procurement language samples that are required of an interoperable ICAM architecture solution.</td>
<td>ICAM Executive Primer &amp; ICAM Acquisition Guidance</td>
</tr>
<tr>
<td>Solution Architects</td>
<td>...are responsible for acquisition requirements and the design/development/integration of ICAM solutions in accordance with their respective organization’s enterprise architecture technical and management requirements. The Solution Architects will be required to compare and quantify the technical implementation options, alternatives and cost constraints to the Program Managers. This document provides structured technical guidance and reference artifacts to assist in achieving an ICAM-enabled system.</td>
<td>This document series, ICAM Executive Primer &amp; ICAM Acquisition Guidance</td>
</tr>
</tbody>
</table>

---

CONTENTS

Disclaimer of Liability ................................................................................................................................... i
Executive Summary ...................................................................................................................................... ii
Contents ....................................................................................................................................................... iv
Table of Figures ........................................................................................................................................... iv

1 Introduction ............................................................................................................................................ 1
  1.1 Purpose ...................................................................................................................................... 1
  1.2 Background ............................................................................................................................... 1
  1.3 Approach ................................................................................................................................... 2
  1.4 Enabling Multifactor Authentication ........................................................................................ 2
  1.5 How to Use ............................................................................................................................... 2
  1.6 What’s in this Document ........................................................................................................... 3

2 AuthLite Implementation Guide ............................................................................................................. 4

3 Shibboleth IdP 3 & SP 2 Windows Installation Guide ......................................................................... 36

4 Duo Access Gateway Implementation Guide ....................................................................................... 73

5 Okta Identity Cloud Implementation Guide ......................................................................................... 75

TABLE OF FIGURES

Figure 1 - Steps to Secure and Seamless Information Sharing (Federation) ................................................ ii
Figure 2 - System Configured for Multifactor Authentication Using Yubikey HOTP (HMAC-based one-
time password), AuthLite & MS Windows Active Directory........................................................................ 4
Figure 3 - System Configured for Multifactor Authentication Using Duo TOTP (Time-based One-Time
password), Shibboleth IdP, Shibboleth SP & MS Windows Active Directory.................................................. 36
Figure 4 - Duo Access Gateway SSO ......................................................................................................... 73
Figure 5 - Okta Identity Cloud SSO Build Architecture ............................................................................ 75
1 INTRODUCTION

This document serves as a source of Identity, Credential, and Access Management (ICAM) Implementation Guides resulting from the evaluation of publicly available documents and the implementation of ICAM-enabled systems in a sandbox. The ICAM landscape is complex and there are many elements to consider. ICAM policies are important to have in enabling technology to share data within a wide variety of applications, including an organization’s existing legacy systems as well as emerging nationwide initiatives, such as the Nationwide Public Safety Broadband Network (NPSBN), Next Generation 911 services and the First Responder Network Authority (FirstNet).

While this document is focused on assisting state, local, tribal and territorial (SLTT) Public Safety Community (Community) entities in improving the security posture of their systems so they can safely and securely share information with each other, this document can be used for any organization implementing the products discussed within this document. Instead of considering both single and multifactor authentication, this document focuses on implementing multifactor authentication on an organization’s systems. Adopting multifactor authentication when upgrading an ICAM-enabled system is highly recommended for any organization, but it is especially recommended based on a risk assessment of the typical information stored in the Community’s systems. This document is the third of a series of ICAM educational tools, including the ICAM Executive Primer and ICAM Acquisition Guidance.

1.1 PURPOSE

The goal of this document is to enable any organization, including the SLTT Community, to spend its resources wisely on thoughtful and well-specified ICAM implementation activities that result in an ICAM-enabled system that includes multifactor authentication. This document provides ICAM implementation guides for the Community and seeks to leverage existing efforts to avoid duplication and maximize the value of existing ICAM products and solutions. While it does use specific vendors to complete the builds, this document does not endorse any specific vendor, technology or software. The implementation guidance within this document aids the Community in creating ICAM-enabled systems and adopting multifactor authentication. Further, each organization is responsible for its own cybersecurity measures, and they should make decisions based on their own requirements, laws and experience.

1.2 BACKGROUND

The Public Safety Communications Identity, Credential, and Access Management Working Group (PSC ICAM WG) is a subsidiary group of the Information Sharing Council (ISC) with a Federal Advisory Committee Act (FACA) exempt status under Section 1016(g)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (as amended). Its members include the Department of Homeland Security (DHS) Science and Technology Directorate (S&T), Partner Engagement Information Sharing Environment (P-ISE), DHS Office of Emergency Communications (OEC), FirstNet, as well as National Institute of Standards and Technology (NIST) Public Safety Communications Research Division (PSCR). The PSC ICAM WG supports the ISC in fulfilling the ISC’s duties (with a focus on public safety) pertaining to the interchange of information between public safety agencies by addressing policy, governance, standards, technology and acquisition guidance on ICAM capabilities for the public safety community.
1.3 APPROACH
Through outreach to various communities (including FirstNet stakeholders, the Federal ICAM Subcommittee, DHS Cyber and the Office of the Director of National Intelligence’s Sensitive But Unclassified [SBU] Technical Advisory Committee [STAC]) and utilization of the capabilities of the Tech Foraging group at DHS, S&T and the PSC ICAM WG gathered existing ICAM documents and collected information from building ICAM-enabled systems in a test environment (i.e., sandbox) to distill the information into these implementation guides.

1.4 ENABLING MULTIFACTOR AUTHENTICATION
Most people are familiar with ICAM concepts. When leaving their houses or cars, most choose to lock their doors and restrict access only to those with a key. Likewise, anyone who accesses the internet is familiar with single factor authentication, such as gaining access to a computer system, email or social network with a username and password.

Single factor authentication is a weaker form of protection for computer systems and applications because a password can be obtained easily (i.e., through email phishing or other hacking means) and easily shared. Weak credentials played a factor in 81% of the systems that were hacked in 2016; weak credentials include the use of username and password.

Multifactor authentication uses stronger credentials that can provide an organization with a higher assurance that the user attempting to access an organization’s resources is the intended person. To create this higher assurance, multifactor authentication requires the use of two of three “factors”: something you have (a credential), something you are (fingerprint or other biometric) and something you know (password or personal identification number (PIN)).

When organizations connect their systems with others within their community, that community will need to know who is accessing which pieces of information at what times to ensure only authorized users are within the system. Multifactor authentication becomes useful in information sharing scenarios. After performing a risk assessment based on the type of information held in the SLTT Community’s systems, it was determined that multifactor authentication would reduce the risk of a system intrusion. As a result, this document, as well as the implementation and procurement guides, are all tailored towards ICAM systems with multifactor authentication.

1.5 HOW TO USE
The content within this document provides a deeper view for Solutions Architects into an ICAM-enabled system configured with multifactor authentication through implementation guides. This document is part of a progressive series that begins with the ICAM Executive Primer, a high-level, educational dive into ICAM for Executive Leadership and others through ICAM concepts and real-world scenarios of ICAM principles in action. The ICAM Acquisition Guidance is the second in the series and gives an overview to Program Managers of what to look for while acquiring ICAM products, and advises Solutions Architects about lessons learned from sandbox builds of ICAM-enabled systems with multifactor authentication. This document is the third in the series.

---

2 Most public safety communications systems, radio sites, public safety facilities, data centers and radios are physically secured against internal and external threats.

Beyond a progressively deeper dive into the world of ICAM for stakeholders, this series also contains several helpful sections and appendices, including a high-level executive overview of ICAM and procurement language.

This document was developed by the PSC ICAM WG; questions and comments can be sent to DHS S&T at: SandTFRG@hq.dhs.gov.

1.6 WHAT’S IN THIS DOCUMENT

To collect data for these Implementation Guides, DHS S&T created ICAM-enabled systems configured with multifactor authentication in a sandbox. Each build used different software and credentials that could be used in a build by the Community. The AuthLite Implementation Guide used low-cost products associated with the FIDO Alliance within its system. The Shibboleth IdP 3 & SP 2 Windows Installation Guide used a free, open source product that was mentioned on the Global Federation Identity and Privilege Management (GFIPM) website.

Based on the installation procedures and associated outcomes of these two builds, PSC ICAM WG created the below reference architecture and implementation guides. In no way does the PSC ICAM WG endorse or favor the vendors and software implemented below. These guides are for educational purposes only. And as such, each organization is responsible for its own cybersecurity measures, and should make decisions based on the requirements, laws and experiences of the organization.
This build was conducted in an Amazon Web Services (AWS) environment and, as such, its guide contains implementation instructions specific to AWS. It is based on FIDO Alliance-approved products. The Yubikey, a FIDO Alliance-approved credential, is a hard token that can be plugged into a universal serial bus (USB) port or used with another near field communication (NFC) device and touched to release a certificate. Its cost varies on the type of Yubikey chosen and the device can be configured several different ways – it could be used as a single-factor authenticator, as a one-time password (OTP) device, or even as a public key infrastructure (PKI) token. In this build, the Yubikey is configured for two-factor authentication as a keyed-hash message authentication code (HMAC)-based one-time password (HOTP).

To use the Yubikey in an AWS environment, USB hardware needs to be accessible by the Amazon elastic compute cloud (EC2) instances. One way to accomplish this is by setting up a publicly accessible virtual private network (VPN) tunnel into AWS. Because USB credentials cannot be passed through directly to EC2 instances, this allows the user to provide two authentication factors to gain access to the VPN (or virtual private cloud [VPC] in this case). In this build, OpenVPN was chosen for this purpose and setup to use a Microsoft domain controller as its user directory. Microsoft Active Directory does not natively support multifactor authentication, so AuthLite was used as a middleware to provide multifactor authentication. AuthLite is relatively inexpensive, FIDO Alliance-approved, and interacts seamlessly with the Yubikey.
and Active Directory. In this build, Yubikey and Active Directory username/password provide the two factors needed to access the VPC via the OpenVPN (and AuthLite) software.
CREATING A DOMAIN CONTROLLER

STEPS TO CREATE DOMAIN CONTROLLER

1. Login to your Windows Server instance.
2. Open “Action Center.”
3. Click “Windows Update.”
4. Click “Check for updates.”
5. Install updates (do not install any roles or features until this step is complete).
6. Open “Server Manager.”
7. Under “Local Server,” change the server name (double click “Computer Name”) to DC01 (or the preferred server name of choice) and the internet protocol (IP) address to private (avoid using default 192.168.0.1).
8. Click “Add roles and features” (located under configure this local server), to create a Domain Controller by installing the Active Directory Domain Services (AD DS) role.
9. The “Before you begin” screen provides you basic information, such as configuring strong passwords, IP addresses and Windows updates.

10. On the Installation Type page, select the first option “Role-based or Feature-based Installation.” The Scenario-based Installation option applies only to Remote Desktop services.
11. On the “Server Selection” page, select a server from the server pool, and then click “Next.”

12. To install AD DS, select “Active Directory Domain Services.” There will be a pop-up that allows you to add other AD DS related tools. Click “Add Features.”
13. After clicking “Add Features” above, click “Next.”

14. On the “Select Features” page (the Group Policy Management feature is automatically installed during the promotion), click “Next.”
15. On the “Active Directory Domain Services” page, it gives basic information about AD DS. Click “Next.”

16. On the “Confirmation” page, you need to confirm to continue with this configuration. It will provide you an option to export the configuration settings and to restart the server automatically as required.
17. After clicking “Install,” the selected role binaries will be installed on the server.

18. After “Active Directory Domain Services” role binaries have been installed, the server can be promoted to a Domain Controller.

19. Place your cursor over the flag and warning symbol, and when the drop-down displays, click “Promote the server to a Domain Controller.”
20. To create a new AD forest (an Active Directory forest is the highest level of organization within Active Directory), select “Add a new forest” (for the purposes of this guide we created a forest named “dhs-st-lab.local”).

21. Type in the forest name as the Root domain name.
22. Specify the FFL (“Forest functional level”), DFL (“Domain functional level”), whether it should be a domain name system (DNS) Server and the DSRM (“Directory Services Restore Mode”) administrator password. Click “Next.” AD automatically selects the Global Catalog (GC) option by default and you cannot deselect it (the reason for this is that GC is the very first domain controller [DC] of the AD forest and at least one needs to be a GC).

23. Ignore the DNS delegation warning, and click “OK.”
24. Check the NetBIOS name already assigned. Click “Next.”

25. Specify the location of the AD related folders and then click “Next.”
26. Read the summary of all installation options/selections. Click “Next.”

27. Before the actual install of AD, all prerequisites are checked. If “All prerequisite checks passed successfully,” then click “Install.”
28. When you click Install, DNS and the group policy management console (GPMC) are installed automatically.

29. After the promotion of the server to a DC finished server, the server will restart automatically.

30. Once the server is booted, login and click on “Server Manager” | “Tools.” You should see that the following have been installed:
   - “Active Directory Administrative Center”
   - “Active Directory Domains and Trusts”
   - “Active Directory Module for Windows PowerShell”
   - “Active Directory Sites and Services”
   - “Active Directory Users and Computers”
   - “ADSI Edit”
   - “DNS”
   - “Group Policy Management”
CREATE DOMAIN ADMIN USER

1. From Server Manager, click on “Active Directory Users and Computers.”
2. Click on the “Domain” on the left pane and click the “Add User” button as shown.

3. Add a Domain admin user listed here as “AD ADMIN.”
4. Right click your new user and add groups “Domain Admins” and “Administrators.”

**OpenVPN Install/Configuration**

**Server Side**


   OpenVPN Access Server  
   *Version 2.1.9 | Sold by OpenVPN Technologies, Inc.*  
   OpenVPN Access Server is a full featured SSL VPN software solution that integrates OpenVPN server capabilities, enterprise management capabilities, simplified OpenVPN Connect UI, and OpenVPN Client software packages that accommodate Windows, MAC, and Linux, mobile OS (Android and iOS) environments. OpenVPN Access Server supports a wide range of configurations, including secure and granular remote access to internal network and/or private cloud network resources and applications with fine-grained access control.

2. Click the link “OpenVPN Access Server” and follow to the next page.
3. Click “Continue” and follow to the next page. On this page, you will choose the options that best suit your requirements for the instance and click “Launch with 1-click.” The instance will then be launched in your AWS EC2 Dashboard.

4. Login to the virtual machine (VM) using Putty with the credentials you specified in the 1-click launch window.
5. Create a new user for use with the OpenVPN console using the command “sudo adduser TheUserName”.
6. Run the OpenVPN initialization program with the following command: sudo ovpn-init --ec2.
7. Answer the questions for your needs and use the previously created user name when asked by the init program.
8. Once the instance passes system checks and launches, navigate to the user interface via web browser using the VPN instance public IP address (which will be different from the one shown below). It will take you to the admin OpenVPN logon page.
9. Logon to OpenVPN with the default credentials; change those credentials on the user interface.
1. Download the OpenVPN Connect Client. (You may also use the Client from OpenVPN; however, the steps you will need to undertake would differ from the ones included here.)

2. Download the OpenVPN Config file and save it on your computer. You may need to right-click and “Save as.” Double-clicking the Config file should open the Desktop Client and automatically load the file.

3. **If the config file does not open** - Run the OpenVPN Client. Click on the “+” button to add a new Connection Profile.
4. Choose “Local File” and click “Import.”

5. Locate your OpenVPN configuration file and Open it.
6. Enter a name for the VPN Profile, or leave it as is and click “Save” to add the Profile.

7. **If the config file opens** - Click on the newly created Connection Profile to make a connection to the VPN server.
8. Enter your Username and Password when prompted and click “Login.” Note: Username and password are case sensitive.

9. Upon successful connection, you will see a similar window:

**ADDITIONAL INSTRUCTIONAL RESOURCES:**

https://docs.openvpn.net/how-to-tutorialsguides/virtual-platforms/amazon-ec2-appliance-ami-quick-start-guide/
OPENVPN LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP) CONFIGURATION

1. Login to OpenVPN Access Server Admin UI.

2. Click on the LDAP link under the “Authentication” menu.
3. On the “LDAP Settings” page, enter the following:
   a. Enter the LDAP Server hostname/IP address in “Primary server” field. You may also enter a “Secondary server” if you have a secondary server (Note that in our case: 10.0.1.87 is the Active Directory [AD] server).
   b. Select “Use these credentials.”
   c. Enter the “Bind DN” – this will be the admin account that was previously created on your LDAP/Active Directory server.
   d. Input the “Password” for the Admin User.
   e. Enter the “Base DN for User Entries” – this is where user information is stored. It is important to note here that the “Base DN” needs to point to a “VPN Users” (or similarly named) group in AD, not the AuthLite Users group. “AuthLite Users” is a special group used by AuthLite only; the build does not work when that group is included as part of the “Base DN” here.
   f. Once you complete the settings above, click “Save Settings.”

<table>
<thead>
<tr>
<th>Configuration</th>
<th>LDAP Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td></td>
</tr>
<tr>
<td>SSL Settings</td>
<td></td>
</tr>
<tr>
<td>Server Network Settings</td>
<td></td>
</tr>
<tr>
<td>VPN Mode</td>
<td></td>
</tr>
<tr>
<td>VPN Settings</td>
<td></td>
</tr>
<tr>
<td>Advanced VPN</td>
<td></td>
</tr>
<tr>
<td>Web Server</td>
<td></td>
</tr>
<tr>
<td>Client Settings</td>
<td></td>
</tr>
<tr>
<td>Failover</td>
<td></td>
</tr>
<tr>
<td><strong>User Management</strong></td>
<td></td>
</tr>
<tr>
<td>User Permissions</td>
<td></td>
</tr>
<tr>
<td>Group Permissions</td>
<td></td>
</tr>
<tr>
<td>Revoke Certificates</td>
<td></td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td></td>
</tr>
<tr>
<td>General</td>
<td></td>
</tr>
<tr>
<td>PAM</td>
<td></td>
</tr>
<tr>
<td>RADIUS</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td></td>
</tr>
<tr>
<td><strong>Tools</strong></td>
<td></td>
</tr>
<tr>
<td>Profiles</td>
<td></td>
</tr>
<tr>
<td>Connectivity Test</td>
<td></td>
</tr>
</tbody>
</table>
4. Click “Update Running Server” so the settings can take effect.

5. Click “General” under “Authentication,” select LDAP and click “Save Settings.”

6. Click “Update Running Server” again so the changes can take effect.

7. You should now have OpenVPN Access Server configured to use LDAP.
INSTALLING AUTHLITE

AuthLite is software that integrates multifactor authentication into existing Active Directory configurations. We used the version 2.2 installer for 64-bit Windows. AuthLite installs two programs that are used to manage the software: AuthLite Configuration and AuthLite Token Manager. Note: The user who performs the installation on the Domain Controller must be a member of both the Domain Admins and Schema Admins groups.4

1. Download and install the software from the AuthLite website:
   http://www.authlite.com/downloads/
2. Before beginning to use the product, enter a license key (evaluation licenses are free):

   ![AuthLite Configuration Interface](image)

4 https://www.authlite.com/capabilities/
AUTHLITE CONFIGURATION

The AuthLite Configuration application is where you configure most of the global parameters for the software. For AuthLite to work, the proper AD user groups must be configured. The default AuthLite user group must be called “AuthLite Users.” Any user that needs to have multifactor authentication capabilities must be a member of this group, otherwise AuthLite will not recognize them. AuthLite only controls access for users who are members of this group. Anyone else is still managed using default Windows behavior.5

AuthLite recommends the group should be configured as follows:

1. To mirror the above, create three identical security groups.
2. The 1F tag group should have AuthLite Users as a member.

5http://s3.authlite.com/downloads/2.3/AuthLite.pdf?_ga=2.26861055.395576150.1523451294-1824266537.1519826533
3. Once all this is in place, AuthLite needs to know about your new groups. Add the group pair to the AuthLite configuration:

4. To have everything work as intended, modify two settings in the configuration so that AuthLite/AD will limit AuthLite Users LDAP requests for authentication to 2-factor only.
5. Within “Forced 2 Factor Computers” and “LDAP Permissions,” add the IP range for the OpenVPN server as well as the DC computer name itself (both of which will differ from the ones listed below).
**Yubikey and AuthLite Token Manager HOTP Configuration**

Finally, a token must be mapped to one or more members of the AuthLite Users group for multifactor authentication to occur. To configure Yubikey, add one on the appropriate tab in AuthLite. Since we worked remotely in an AWS lab instance, this required an export of the Yubikey XML, which is then imported into the AuthLite configuration because AWS does not allow remote mapping of local USB ports.

Yubikey exportation is fully outlined in the AuthLite 2.2 documentation, beginning on page 19.

In summary, to export:

1. Download and install the Yubikey Programmer application from the AuthLite downloads website (on your local machine).
2. Go to the “Choose Ports” tab. Plug in one or more Yubikeys to identify which USB ports will be used during this programming session. If you plug them in one at a time and wait for each port to be recognized, you will know which port corresponds to which key. This will in turn make it easier to find which key to unplug/re-plug in the event of a programming error. (Note: Due to Windows slow USB enumeration, there is not much speed advantage to using many ports at once).
3. When ready, click “Start Programming” – each time you plug in a Yubikey to one of the ports you chose, it will be programmed.
4. Remove each key when the status reads “DONE (remove key).” Do not click “Finish” at this point if you have more keys to program. You can continue to plug in new keys and program them. When finished with all keys, click the “Finish” button.
5. Save the resulting XML file. This file should be considered sensitive information, as it contains all the secret values programmed into the keys. Treat this with the same security measures you would use for a password list or other secure document.

To import and assign:

1. On the Domain Controller, launch the AuthLite Token Manager and select “Import Keys” from the File menu.
2. Select the XML file generated when you programmed your keys, and click “Open.”
3. The key records will be imported.
4. You should then see new unassigned Yubikey records in the list.
5. Now that the file is imported, you should DELETE the XML file from your workstation and the DC. It is no longer needed once the keys are imported. This file should be considered sensitive information, as it contains all the secret values programmed into the keys.
6. Right-click an unassigned Yubikey record and select “Reassign.”
7. Input the information about the user to which you want to assign the token.
LOGGING INTO OPENVPN CLIENT USING YUBIKEY

1. Open the OpenVPN client login screen and select the user name field.
2. Insert the YubiKey device and press the Gold center button on the device.

3. The YubiKey will generate a token for the username.
4. Enter the Active Directory password for the user assigned to the YubiKey in previous steps and press enter.
5. The OpenVPN will connect your computer to the VPN network.
INBOUND/OUTBOUND RULES (PERTAINING TO INSTANCES CREATED WITH AWS)

DOMAIN CONTROLLER INBOUND/OUTBOUND RULES

Domain Controller Inbound/Outbound rules should resemble the following:

**Outbound rules**

![Outbound rules table]

**Inbound rules**

![Inbound rules table]
OPENVPN INBOUND/OUTBOUND RULES

OpenVPN Inbound/Outbound rules should resemble the following:

**Outbound rules**

<table>
<thead>
<tr>
<th>Type</th>
<th>Protocol</th>
<th>Port Range</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>All traffic</td>
<td>All</td>
<td>All</td>
<td>0.0.0.0/0</td>
</tr>
</tbody>
</table>

**Inbound rules**

<table>
<thead>
<tr>
<th>Type</th>
<th>Protocol</th>
<th>Port Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom UDP Rule</td>
<td>UDP</td>
<td>1194</td>
</tr>
<tr>
<td>Custom UDP Rule</td>
<td>UDP</td>
<td>1194</td>
</tr>
<tr>
<td>SSH</td>
<td>TCP</td>
<td>22</td>
</tr>
<tr>
<td>Custom ICMP Rule - IPv6</td>
<td>All</td>
<td>N/A</td>
</tr>
<tr>
<td>Custom ICMP Rule - IPv6</td>
<td>All</td>
<td>N/A</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>9443</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>9443</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>943</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>3389</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>3389</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>443</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>443</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>443</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>443</td>
</tr>
<tr>
<td>All ICMP - IPv4</td>
<td>All</td>
<td>N/A</td>
</tr>
<tr>
<td>All ICMP - IPv4</td>
<td>All</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Figure 3 - System Configured for Multifactor Authentication Using Duo TOTP (Time-based One-Time password), Shibboleth IdP, Shibboleth SP & MS Windows Active Directory.

Shibboleth is a federated identity solution that provides simplified sign-on (SSO) capabilities, along with multifactor authentication. Because the GFIPM website provides a link to implementation documentation for Shibboleth (a free, open source product), Shibboleth was used as an identity provider and simplified sign-on solution, as well as a service provider.

This build includes a time-based one-time password (TOTP) credential on your phone. Duo was chosen because it interoperates with Shibboleth and is free (for up to 10 users). Duo's mobile phone TOTP application allows for a 6-digit number found on the phone, a phone call, or a button that pops up on your phone to prove you have access to the credential.
ABOUT
This implementation guide has been created to assist organizations with installing and configuring Shibboleth Identity Provider v3 and Service Provider 2 to authenticate users over LDAP against Microsoft Active Directory. Additionally, it outlines how to add a second factor to authentication using Duo TOTP. While researching Shibboleth, it was found that much of the publicly available documentation for installing and configuring Shibboleth was not straightforward, especially for those who may be unfamiliar with the software. This guide will offer clear-cut instructions on how to implement the Shibboleth software in an AWS cloud environment, and should be used as a reference in conjunction with the current publicly available Shibboleth documentation. Throughout this guide, links have been provided to offer additional assistance and information.

WHAT IS THE SHIBBOLETH SOFTWARE?
This step by step guide provides detailed instructions on how to successfully implement the Shibboleth software components in an AWS cloud environment. The Shibboleth software is a web-based SSO system made up of three components:

- The Identity Provider (IdP) is responsible for user authentication and providing user information to the Service Provider (SP). It is located at the home organization, which is the organization that maintains the user's account.
- The SP is responsible for protecting an online resource and consuming information from the IdP. It is located at the resource organization, which is the organization that keeps records that will be shared.
- The Discovery Service (DS) helps the SP discover the user’s IdP. It may be located anywhere on the web and is not required in all cases.\(^6\)

Shibboleth has two major halves: an IdP and a SP. The IdP supplies information about users to applications, and the SP gathers information about users to protect resources. In the typical use case, a web browser accesses a protected resource, authenticates at the identity provider and once authenticated, is logged into the resource.\(^7\)

- **Web Browser** – represents the user within the SSO process.
- **Resource** – contains restricted access content that the user wants to access.
- **Identity Provider (IdP)** – authenticates the user.
- **Service Provider (SP)** – performs the SSO process for the resource.\(^8\)

---


\(^8\) How Shibboleth Works: Basic Concepts, [https://www.shibboleth.net/index/basic](https://www.shibboleth.net/index/basic).
BEFORE YOU BEGIN – A LIST OF HELPFUL TIPS:

- Although it is encouraged to do so, always be careful when/if copy and pasting code from this guide, and double-check that you have substituted the correct values.
- Always double-check that you are downloading the correct version of any software.
- Sometimes simple missteps can cause big problems; remember to check the logs included with all software utilized during this process to determine the cause of any issues you encounter.
- There are multiple ways to configure Shibboleth depending on what you are doing – one configuration/integration will not necessarily work for everyone.
- There is very limited documentation available for troubleshooting.
- Document the steps you have taken as you go, just in case a component breaks – this will allow you to compare the documentation of your build with the documentation of this guide.
- Setting up a system that utilizes the Shibboleth IdP and/or SP is a long process. It will take a lot of time and resources and will require the assistance of senior-level engineers.
- Remember that https://www.testshib.org/ is a very useful troubleshooting tool during the latter steps of the Shibboleth software configuration.

INITIAL CONFIGURATION

CREATE THREE EC2 INSTANCES WITHIN AWS (WINDOWS 2012 BASE SERVER, 2GB+ OF RAM & 2X 160GB/ 1X 30GB STORAGE):

1. Enter the EC2 Dashboard, select or search for EC2, then click the launch an EC2 instance button.
3. Select the t2.medium instance type.
4. On the “Configure Instance Details” page, make changes as needed (add EC2 to the desired VPC, subnet, security group, etc.)
5. Add storage to your instance.
6. Accept all defaults.
7. Review Configuration Settings, launch instance, and select or create key pair.
8. Attempt to connect to your instance, create a key pair, decrypt the key and save your password.
9. After creating the first instance, click “Actions” then select “Create More Like This” and create two more instances, one with less storage (the instance with less storage will be used as the Domain Controller).

CREATE A DOMAIN CONTROLLER (IF NEEDED)

1. Login to your Windows Server instance.
2. Open “Action Center.”
3. Click “Windows Update.”
4. Click “Check for updates.”
5. Install updates (do not install any roles or features until this step is complete).
6. Open “Server Manager.”
7. Under “Local Server,” change the server name (double click “Computer Name”) to DC01 (or desired server name) and the IP address to private (avoid using default 192.168.0.1).
8. Repeat steps 1-7 on the SP and IdP EC2 instances.
9. Click “Add roles and features” (located under configure this local server) to create a Domain Controller by installing the AD DS (Active Directory Domain Services role).

10. The “Before You Begin” screen provides you basic information, such as configuring strong passwords, IP addresses and Windows updates.
11. On the Installation Type page, select the first option “Role-based or Feature-based Installation.” Scenario-based Installation option applies only to Remote Desktop services.

12. On the “Server Selection” Page, select a server from the server pool. Click “Next.”
13. To install AD DS, select “Active Directory Domain Services,” in turn there will be a pop-up that allows you to add other AD DS related tools. Click “Add Features.”

14. After clicking “Add Features” above, click “Next.”
15. On the “Select Features” Page, the Group Policy Management feature is automatically installed during the promotion. Click “Next.”

16. On the “Active Directory Domain Services” page, it gives basic information about AD DS. Click “Next.”
17. On the “Confirmation” Page, you need to confirm the configuration settings to continue. The wizard will provide you an option to export the configuration settings. Additionally, you can specify whether you want to restart the server automatically as required.

18. After clicking “Install,” the selected role binaries will be installed on the server.
19. After “Active Directory Domain Services” role binaries have been installed, the server can be promoted to a Domain Controller.

20. To promote Windows 2012 Server to Domain Controller, click “Promote the server to a Domain Controller.”

21. To create a new AD forest, select “Add a new forest” (for the purposes of this guide we created a forest named “dhs-st-lab.local”).
22. Type in the forest name as the Root domain name.

23. Specify the FFL, DFL, whether it should be a DNS Server and the DSRM (Directory Services Restore Mode) administrator password, click “Next.” AD automatically selects the GC option by default and you cannot deselect it. (The reason for this is that GC is the very first DC of the AD forest and at least one needs to be a GC).
24. Ignore the DNS delegation warning. Click “OK.”

25. Checks the NetBIOS name already assigned, click “Next.”
26. Specify the location of the AD related folders and then click “Next.”

27. Read the summary of all installation options/selections. Click “Next.”
28. Before the actual install of AD, all prerequisites are checked. If all prerequisite checks are passed successfully, then click “Install.”

![Prerequisites Check](image1)

29. When you click Install, DNS and the GPMC are installed automatically.

![Installation](image2)
After the promotion of the server to a DC finished server, the server will restart automatically. Once the server is booted, login, click on “Server Manager” | “Tools,” you should see that following have been installed:

- “Active Directory Administrative Center”
- “Active Directory Domains and Trusts”
- “Active Directory Module for Windows PowerShell”
- “Active Directory Sites and Services”
- “Active Directory Users and Computers”
- “ADSI Edit”
- “DNS”
- “Group Policy Management”

**CREATE A LOCAL ADMIN ACCOUNT ON EACH INSTANCE**

1. Open “Computer Management” by pressing Win + X.
2. In the console tree, click “Users.”
4. Type the appropriate information in the dialog box twice.
5. Select/clear (as per your need) the checkboxes for:
   - “User must change password at next logon”
   - “User cannot change password”
   - “Password never expires”
6. Click “Create,” and then click “Close.”
7. Choose “Groups,” and right-click “Add to Group” on Administrators. Then select the user account to add to this group.
JOIN THE IDP AND SP SERVERS TO THE DOMAIN (PERFORM THESE STEPS ON THE IDP AND SP EC2s):

1. Open “Server Manager.”
2. On the left side pane, click “Local Server.”
3. System properties will open, click “change.”
4. Under “Member of,” select “Domain,” and type the domain name of your choice, click “OK.”
5. You will be asked to enter your credentials. Login using a domain admin account.
6. You will be prompted to restart your computer, click “OK.”
7. Open “Network and Sharing Center.”
8. Click “Change Adapter settings.”
9. Right click the wireless network adapter.
10. Select IPV4 and click “Properties.”
11. Under Use Following DNS addresses, add in the IP address of the Domain Controller.
12. Check “Validate Settings” upon exit.
13. Click “OK.”
ADD ACTIVE DIRECTORY CERTIFICATE SERVICES

1. Open “Server Manager.”
2. Click “Local Server.”
3. Click “Add roles and features” (located under configure this local server).
4. On the Installation Type page, select the first option “Role-based or Feature-based Installation.” Scenario-based Installation option applies only to Remote Desktop services.

5. On the “Server Selection” Page, select a server from the server pool, click “Next.”

7. Enter Restore mode user and password, and press next.
8. Accept default items, press next and then finish.
CREATE DOMAIN ADMIN USER

1. From Server Manager, click on Active Directory Users and Computers.
2. Click on the Domain on the left pane and click the Add User button as shown.

3. Add a Domain admin user listed here as “AD ADMIN.”
4. Right click your new user and add groups “Domain Admins” and “Administrators.”

CONFIGURE CERTIFICATE SERVICES

2. Supply the credentials that we just created in the step above.

3. Press Next.
4. Select Enterprise CA and press Next.

5. Select Root CA and press Next.

7. Press Configure.
ICAM Implementation Guidance v.1

EXPORT CERTIFICATE TO IDP

1. Launch a Power Shell session and enter Microsoft management console (MMC) command / Open File menu, and select Add or Remove Snap In and select Certificate Snap In and launch.

2. Select the Certificate that has the name of your AD Domain, right click and select Export.
3. Press Next and save the file (Choose a name easy to remember and find, i.e., ADCERT).

4. Copy the newly created file to the IdP desktop through the Remote Desktop clipboard functionality.

CONFIGURING THE IDP SERVER

DISABLE INTERNET EXPLORER (IE) ENHANCED SECURITY

1. On your IdP instance navigate to “Server Manager.”
2. Click “Local Server.”
3. Click “IE enhanced security” and disable for both administrators and users.
4. Restart the server.

Sometimes this process must be repeated a few times before it works.

DISABLE FIREWALL

1. Go to “Server Manager.”
2. On the left side pane, click “Local Server.”
3. Click “Windows Firewall.”
4. Click “Turn Windows Firewall on or off.” Click “Turn off Windows Firewall.”
5. Choose “Turn off Windows Firewall” from Domain network settings, Private network settings and Public network settings, and click “OK” to finish turning off firewall.

DOWNLOAD CHROME

1. Navigate to Internet Explorer.
2. Search “Download Chrome.”
3. Download and install Google Chrome.
DOWNLOAD NOTEPAD++

1. Navigate to Chrome.
2. Search “Download Notepad ++.”
3. Download and install Notepad ++.

DOWNLOAD AND INSTALL JAVA 8

1. Download Java JDK for Windows 64 bit and install.
2. Set JAVA_HOME system variable to JDK install path (i.e., c:\Program Files\Java\jdkxx).
   a. From the Start Menu right click computer.
   b. Click “Properties.”
   c. Click “Advanced System Settings.”
   d. Click “Environment Variables.”
   e. Under System Variables, click “New…”
   f. Name the variable JAVA_HOME and point it to your JDK install directory.

DOWNLOAD AND INSTALL TOMCAT 8.5

The identity provider is a standard Java web application and runs on a compatible servlet container. Tomcat 8.5 is the container documented in this guide to deploy and run the IdP within our environment.

1. Download Tomcat 8.5 32-bit/64-bit Windows Service Installer.
2. Run the installer, set administrator username/password, and accept all other defaults.
3. Navigate to your Tomcat 8.5 install directory (default is C:\Apache Software Foundation).
4. Click the checkbox that enables Tomcat to run immediately after install.
5. Open http://localhost:8080/ with your browser (if you can see the Tomcat homepage, then you have successfully installed Tomcat 8.5).
INSTALLING THE SHIBBOLETH IDP V3

1. **Download** Shibboleth IdP v3 onto your IdP server instance with Tomcat 8.5 installed on it.
2. Run IdP Windows Installer. Set the install path to `C:\opt\shibboleth-idp`.

3. Check the “Configure for Active Directory” checkbox.
4. Specify the DNS name for your IdP (i.e., SHIB-IDP.dhs-st-lab.local).
5. Specify the scope (i.e., dhs-st-lab.local).
6. Click “Next.”

7. Specify the Active Directory Domain (i.e., dhs-st-lab.local).
8. Leave the “Use Global Catalog” checkbox unchecked.
9. Enter the credentials for the Active Directory Admin account that will be used to perform LDAP lookups.
10. Click “Next.”
ICAM Implementation Guidance v.1

**CONFIGURING SSL ON TOMCAT**

1. Create and initialize Java keystore.
   a. Open cmd (Command Prompt) as Administrator and run the following keytool command:
      ```
      if (OS == Windows) {
          "%JAVA_HOME%\bin\keytool" -genkey -alias tomcat -keyalg RSA
      }
      else {
          "$JAVA_HOME/bin/keytool" -genkey -alias tomcat -keyalg RSA
      }
      
      Set a password (in our example we used “changeit”).
   
2. Provide answers to the questions asked when creating the certificate store.
   a. Enable secure sockets layer (SSL) by adding the following connector to server.xml:
      ```
      <Connector
          port="8443"
          maxThreads="200"
          scheme="https"
          secure="true"
          SSLEnabled="true"
          keystoreFile="<PATH TO KEYSTORE>"
          keystorePass="<PASSWORD>"
          clientAuth="false"
          sslProtocol="TLS"/>
      
      b. Open “Services” and restart Tomcat.
   
   c. To check if https is enabled, navigate to https://localhost:8443.

**CONFIGURING THE SHIBBOLETH IDP V3**

1. Create an xml file named idp.xml used to dynamically deploy the idp.war file when it is rebuilt.
   a. Copy and paste the following into idp.xml
      ```
      <Context docBase="C:/opt/shibboleth-idp/war/idp.war"
          privileged="true"
          antiResourceLocking="false"
          swallowOutput="true">
          <!-- Work around lack of Max-Age support in IE/Edge -->
          <CookieProcessor alwaysAddExpires="true" />
          </Context>
      
      <CookieProcessor alwaysAddExpires="true" />
      </Context>
      
      Save idp.xml into <tomcat dir>/conf/Catalina/localhost/.

2. Modify ldap.properties – make sure AD server name and ldapURL are correct. Check to ensure all other values look OK.

3. Modify C:\opt\shibboleth-idp\webapp\WEB-INF\web.xml to include:
   ```
   <context-param>
       <param-name>idp.home</param-name>
       <param-value>/opt/shibboleth-idp</param-value>
   </context-param>
   
   a. [Download](http://tomcat.apache.org/download-taglibs.cgi) latest .jar files:
      - Impl: [taglibs-standard-impl-1.2.5.jar](http://tomcat.apache.org/download-taglibs.cgi) (pgp, md5)
      - Spec: [taglibs-standard-spec-1.2.5.jar](http://tomcat.apache.org/download-taglibs.cgi) (pgp, md5)
      - EL: [taglibs-standard-jstl-1.2.5.jar](http://tomcat.apache.org/download-taglibs.cgi) (pgp, md5)
      - Compat: [taglibs-standard-compat-1.2.5.jar](http://tomcat.apache.org/download-taglibs.cgi) (pgp, md5)
   
   c. Run cmd as an administrator.
   d. Run build.bat within the Shibboleth bin/ directory to generate a new war file.
   e. Open “Services,” restart the Tomcat service. Next, navigate to https://<server URL>:8443/idp/shibboleth. The IdP metadata page should now display.
CONFIGURING THE SP SERVER

DISABLE IE ENHANCED SECURITY
1. On your SP instance navigate to “Server Manager.”
2. Click “Local Server.”
3. Click “IE enhanced security” and disable for both administrators and users.
4. Restart the server.
Sometimes this process must be repeated a few times before it works.

DISABLE FIREWALL
1. Go to “Server Manager.”
2. On the left side pane, click “Local Server.”
3. Click “Windows Firewall.”
4. Click “Turn Windows Firewall on or off.” Click “Turn off Windows Firewall.”
5. Choose “Turn off Windows Firewall” from Domain network settings, Private network settings and Public network settings, and click “OK” to finish turning off firewall.

DOWNLOAD CHROME
1. Navigate to Internet explorer.
2. Search “Download Chrome.”
3. Download and install Google Chrome.

DOWNLOAD NOTEPAD++
1. Navigate to Chrome.
2. Search Download “Notepad ++”.
3. Download and install “Notepad ++.”

DOWNLOAD AND INSTALL APACHE (ON SP SERVER)
Apache is an open-source HTTP server for modern operating systems, including UNIX and Windows. The Service Provider is a web server module (installed and configured to work with a web server, such as Apache) that intercepts the user’s request to access a protected resource. Windows may present an error stating that the version of the software is not compatible with your system. If this happens and you have already verified the version downloaded, then re-download it and try installing it again.
1. Install Apache from Apache Lounge (Apache Lounge is an organization that provides pre-package installation bundles for Windows systems; this download of Apache will include openssl).
2. Download and install C++ redistributable library.
3. Extract the folder to C:/Apache24.
   a. Run cmd (Command Prompt) as an Administrator and install Apache 2.4 as a service.
      httpd.exe -k install
b. Create an `OPENSSL_CONF` Windows System environment variable to point to `openssl.cnf` (located within the Apache bin/install directory).
   i. From the Start Menu, right click “Computer.”
   ii. Click “Properties.”
   iii. Click “Advanced System Settings.”
   iv. Click “Environment Variables.”
   v. Under “System Variables”, click “New...”

c. Create a SSL self-signed certificate using the following OpenSSL commands (use “changeit” as a password where needed). Make sure that you input your fully qualified domain name as the common name when you respond to the prompts to create your ssl certificate information:
   
   ```
   openssl genrsa -des3 -out server.key 1024
   openssl req -new -key server.key -out server.csr
   copy server.key server.key.org
   openssl rsa -in server.key.org -out server.key
   openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
   ```

d. Create a folder within the Apache install directory named certificates. Move the four files that you just created into this directory from the conf folder (if you sort the conf folder by date modified, these files should come to the top).

e. Open `conf/http.conf` and modify virtual host at port 553 where the SP is called to resemble the following:

   ```
   <VirtualHost *:553>
   ServerName <SERVERNAME>
   # Include C:\opt\shibboleth-sp\etc\shibboleth\apache24.config
   DocumentRoot C:/Apache24/htdocs
   ErrorLog C:/Apache24/logs/error_ssl.log
   CustomLog C:/Apache24/logs/access_ssl.log combined
   SSLEngine on
   SSLCertificateFile "C:/Apache24/certificates/server.crt"
   SSLCertificateKeyFile "C:/Apache24/certificates/server.key"
   </VirtualHost>
   ```

f. Enable the `mod_ssl.so` module in htd.conf:

   ```
   LoadModule ssl_module modules/mod_ssl.so
   ```

   (uncomment the corresponding LoadModule line )

g. Setup to listen on port 553

   ```
   By adding Listen 553
   ```

h. Now create a folder within htdocs named secure and place a protected resource within it (in our example, we created secure.html within the folder).

i. Restart Apache. At this point, Apache should start without error and you should be able to access the webpage by navigating to:

   ```
   http://localhost/secure/secure.html
   https://localhost:553/secure/secure.html
   ```

At this point, you can access secure.html page without logging in because it is not protected by Shibboleth.
Final IDP Configuration

1. Navigate to the IdP metadata folder (the default path to C:\shibboleth install directory\metadata).
2. Modify idp-metadata.xml.
3. Be sure to make sure all the “Location=” attributes point to IdP app on Tomcat 8 (port 8443) (https://<idp server>:8443/idp...).
4. Modify conf/metadata-providers.xml.
   a. Add a similar metadata-provider to the one below for SP metadata provider:
      ```xml
      <MetadataProvider xsi:type="FilesystemMetadataProvider"
       xmlns="urn:mace:shibboleth:2.0:metadata"
       id="MyMetadata1"
       metadataFile="C:/opt/shibboleth-idp/metadata/<sp servername>-metadata.xml" />
      ```
5. From your browser, launch https://<sp server>/Shibboleth.sso/Metadata.
6. Save the xml content that is returned to C:/opt/shibboleth-idp/metadata/<sp server>-metadata.xml.
7. Add connection to your SSL certificate in the ldap.properties file on the IdP serve, add certificate file we previously placed on the desktop, and make sure the user and password in the file are the AD Admin user we created in the previous steps.
8. Rebuild the WAR by running build.bat again.
9. Restart Tomcat service.

Installing/Configuring the Shibboleth SP

1. Download and install Shibboleth SP onto your SP server instance with Apache installed on it as instructed by its msi (shibboleth-sp-2.4.2-win32.msi).
2. Install to default location, which is C:\opt\shibboleth-sp.
3. Once the SP is installed, go to etc\shibboleth directory.
4. Modify the shibboleth2.xml file.
   a. Remove or comment the "<InProcess logger="native.logger">..</InProcess>" block.
   b. Modify <Host> to include hostname
      ```xml
      <Host name="<SP SERVERNAME>">
      <Path name="secure" authType="shibboleth" requireSession="true"/>
      </Host>
      ```
   c. Provide Application Defaults by modifying the entityID portion of that tag to be the FQDN (Fully Qualified Domain Name).
   d. Provide SSO attributes (do not add port 553 to the following entry)
      ```xml
      <SSO entityID="https://<IdP SERVERNAME>/idp/shibboleth">
      SAML2 SAML1
      </SSO>
      ```
   e. Enter MetaData provider
      ```xml
      <MetadataProvider type="XML" file="<IdP SERVERNAME>-metadata.xml"/>
      ```
      Once the IdP is a running file, you should be able to navigate to this address and it will return a metadata file: https://<IdP SERVERNAME>:8443/idp/shibboleth
   f. Save the metadata (i.e., C:\opt\shibboleth-sp\etc\shibboleth\metadata\my-metadata.xml).
5. Change showAttributeValues="true".
6. Modify the apache24.config file. This way you will be able to test the header content.
   a. Replace
      
      ```
      <Location /secure>
      AuthType shibboleth
      ShibRequestSetting requireSession 1
      require valid-user
      </Location>
      ```
      with
      
      ```
      <Location /secure>
      AuthType shibboleth
      ShibRequestSetting requireSession 1
      require shib-session
      ShibRequireSession On
      ShibUseHeaders On
      </Location>
      ```
   
7. Modify the attribute-map.xml file.
   a. Add an entry for uid similar to the following (you can copy it from under the LDAP examples)
      
      ```
      <Attribute name="urn:oid:0.9.2342.19200300.100.1.1" id="uid"/>
      ```
   
8. Uncomment the following line from httpd.conf:
      ```
      Include C:\opt\shibboleth-sp\etc\shibboleth\apache24.config
      ```

9. Go to Windows services and restart the Shibboleth 2 Daemon(Default).
10. Restart the Apache 2.4 service.

**TESTING YOUR CONFIGURATION**

1. Now that your IdP and SP have been configured, navigate to https://<your hostname>:553/secure/secure.html.
2. If you have been successful, you should be able to see a login screen.
3. Enter Active Directory account credentials for a valid user.
4. If you can see the secure.html webpage, then you have successfully installed/configured the Shibboleth IdP and SP.

**DUO INSTALL AND CONFIGURATION**

1. [Sign up for a Duo account](https://<your hostname>:553/secure/secure.html).
2. Log in to the [Duo Admin Panel](https://<your hostname>:553/secure/secure.html) and navigate to Applications.
3. Click “Protect an Application” and locate Shibboleth in the applications list. Click “Protect this Application” to get your integration key, secret key and API hostname.
4. Generate an akey. Your application secret key (or akey) is a string that you should generate and keep secret from Duo. It should be at least 40 characters long and stored alongside your integration key and secret key.
   a. Create a random string of 40 characters (akey value).
5. Configure [idp]/conf/authn/duo.properties
   a. Input the following keys and the API unique to your install.
      i. ikey (idp.duo.integrationKey)
      ii. skey (idp.duo.secretKey)
      iii. akey (idp.duo.applicationKey)
      iv. API hostname (idp.duo.apiHost)
6. Use [NTP](https://<your hostname>:553/secure/secure.html) to ensure that your server’s time is correct.
7. Next, make sure that the properties file is being referenced by the top level [idp]/conf/idp.properties. The variable idp.additionalProperties should contain /conf/authn/duo.properties.
8. Set idp.authn.identitySwitchIsError = true in idp.properties.
9. Within `idp.properties` set `idp.authn.flows = MFA`

10. Within `[idp]/conf/authn/mfa-authn-config.xml` replace the current content with the following:

```xml
<util:map id="shibboleth.authn.MFA.TransitionMap">
  <!-- First rule runs the Password login flow. -->
  <entry key="">
    <bean parent="shibboleth.authn.MFA.Transition" p:nextFlow="authn/Password" />
  </entry>
  <!-- Second rule runs a function if Password succeeds, to determine whether an additional factor is required. -->
  <entry key="authn/Password">
    <bean parent="shibboleth.authn.MFA.Transition" p:nextFlowStrategy-ref="checkSecondFactor" />
  </entry>
  <!-- An implicit final rule will return whatever the final flow returns. -->
</util:map>

<!-- Example script to see if second factor is required. -->
<bean id="checkSecondFactor" parent="shibboleth.ContextFunctions.Scripted" factory-method="inlineScript">
  <constructor-arg>
    <![CDATA[
      nextFlow = "authn/Duo";
      nextFlow; // pass control to second factor or end with the first
    ]]]>
  </constructor-arg>
</bean>
```
11. Place the following beans into `idp]/conf/authn/general-authn.xml`:

   ```xml
   <bean id="authn/Duo" parent="shibboleth.AuthenticationFlow"
       p:forcedAuthenticationSupported="true" p:nonBrowserSupported="false">
     <!--
     The list below should be changed to reflect whatever locally- or
     community-defined values are appropriate to represent MFA. It is
     strongly advised that the value not be specific to Duo or any
     particular technology.
     -->
     <property name="supportedPrincipals">
       <list>
         <bean parent="shibboleth.SAML2AuthnContextClassRef"
               c:classRef="http://example.org/ac/classes/mfa" />
         <bean parent="shibboleth.SAML1AuthenticationMethod"
               c:method="http://example.org/ac/classes/mfa" />
       </list>
     </property>
   </bean>
   
   <bean id="authn/MFA" parent="shibboleth.AuthenticationFlow"
       p:passiveAuthenticationSupported="false"
       p:forcedAuthenticationSupported="true" p:nonBrowserSupported="false">
     <!--
     The list below almost certainly requires changes, and should
     generally be the
     union of any of the separate factors you combine in your particular
     MFA flow
     rules. The example corresponds to the example in mfa-authn-config.xml
     that
     combines IPAddress with Password.
     -->
     <property name="supportedPrincipals">
       <list>
         <bean parent="shibboleth.SAML2AuthnContextClassRef"
               c:classRef="urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport" />
         <bean parent="shibboleth.SAML2AuthnContextClassRef"
               c:classRef="urn:oasis:names:tc:SAML:2.0:ac:classes:Password" />
         <bean parent="shibboleth.SAML1AuthenticationMethod"
               c:method="urn:oasis:names:tc:SAML:1.0:am:password" />
         <bean parent="shibboleth.SAML2AuthnContextClassRef"
               c:classRef="http://example.org/ac/classes/mfa" />
         <bean parent="shibboleth.SAML1AuthenticationMethod"
               c:method="http://example.org/ac/classes/mfa" />
       </list>
     </property>
   </bean>
   
   12. Use a mobile device to download the Duo Mobile application and configure for TOTP/push usage
       with your Duo account.
   
   13. Rebuild the WAR by running `build.bat` again.
   
   
   15. Try to access the protected resource again. This time, there should be a second factor prompt
       using Duo.

   Duo configuration is now complete. Refer to this [page](#) on the Shibboleth wiki for additional information.
STILL NOT SEEING A LOGIN SCREEN?

- Ensure that all entity IDs match up in metadata files.
- Use Test-Shib.org to verify the operation of both SP and IdP.
- We have found that sometimes Java and Tomcat do not automatically install system level variables and this can cause many issues during the Shibboleth install.
  - Within this guide, we tell you to self-install system level variables.
  - If you may have forgotten to do this, double check that you have followed these steps and/or have the correct variable name/path inputted.
- Use Tomcat 8.5 as opposed to Tomcat 9 (Tomcat 9 appears to have bugs that prevent Shibboleth from working properly).

RESOURCES


4 DUO ACCESS GATEWAY IMPLEMENTATION GUIDE

Public Safety Community

Duo Access Gateway (DAG) adds two-factor authentication, complete with inline self-service enrollment, to popular cloud services. DAG’s capabilities include SSO and Microsoft (MS) AD/LDAP integration. This build was performed in an AWS environment and used MS AD as its connected user source. For the purposes of this build, DAG facilitated multifactor authentication and provided a user-friendly SSO dashboard with access to Slack, Dropbox and G Suite SPs. Duo Mobile was used for the second authentication factor and each SP was configured for SSO using security assertion markup language (SAML) 2.0 protocol.

Because DAG has robust, publicly available documentation, this Implementation Guide provides links that send the reader to the Duo website as a reference for most of the build steps.

Figure 4 - Duo Access Gateway SSO
BEFORE YOU BEGIN – A LIST OF HELPFUL TIPS

- Ensure that all pre-configuration is accurate to avoid errors throughout setup process.
- For many commercial applications, organizations need to have the right commercial plan to implement SSO.
- Remove any conflicting metadata that may interfere with configuration.

TO BEGIN

Before setting up DAG, organizations should first review all documentation to fully understand the system requirements and prerequisites required for a successful implementation of the software. A good starting point can be found on the Duo Access Gateway for Windows Overview page.

INSTALL AND CONFIGURE DAG

Before installation, DAG installer verifies the system prerequisites and exits if any are missing. Installation and configuration documentation, including steps for configuring the organization’s authentication source, can be found under the Install Duo Access Gateway header, on the Duo Access Gateway for Windows page.

CONNECT CLOUD APPLICATIONS

Create, add and configure your cloud applications to the DAG.

CONFIGURE DAG FOR MULTIFACTOR AUTHENTICATION

DAG allows for an organization’s users to self-enroll in multifactor authentication with their own factors. An organization must first enable the self-service portal. Once enabled, an organization’s users can register their devices and other factors for multifactor authentication; documentation can be found on the Duo Guide to Two-Factor Authentication page under the Adding a new device header.

ENABLE DUO ACCESS GATEWAY LAUNCHER APPLICATION

Duo Access Gateway Launcher is an application internal to DAG that, when enabled, provides a user-friendly SSO portal from which users can access their personal DAG-protected service provider applications. The Launcher itself can also be configured to require multifactor authentication. The Launcher was set up and used as part of this build. Specific information on the configuration of DAG Launcher can be found on the Duo Access Gateway for Windows Overview page under the Enable the Duo Access Gateway Launcher.
Okta Identity Cloud (Okta) is a cloud-based IdP that integrates with on-premises and other cloud-based applications. Okta’s capabilities include provisioning, SSO and MS AD/LDAP integration. The build created by our engineering team used MS AD within an AWS environment as its user source. The users on the domain controller were synced to Okta Identity Cloud via the Okta agent software. Okta facilitated multifactor authentication and provided an SSO dashboard with user access to Slack, Dropbox and G Suite SPs. A personal identity verification interoperable (PIV-I) card with a PIN was used as the second authentication factor, and each SP was configured for SSO using SAML 2.0 protocol.

Okta has a robust library of documentation, so instead of specifying every detail, this implementation guide discusses the proper order for installation and configuration, with supplemental links to the relevant Okta pages.
BEFORE YOU BEGIN – A LIST OF HELPFUL TIPS

- Familiarize yourself with Okta terminology through the Okta Help Center, Okta Terminology page.
- Remove any conflicting metadata that may interfere with configuration.
- Customize your organization’s parameter values before configuring SAML 2.0.
- Enable the “Multiple Sign-In” feature in G-Suite and use a “Backdoor URL” to allow the administrator access without a SAML assertion.9
- Okta supports PIV and PIV-I cards, but that feature needs to be enabled by Okta.

TO BEGIN

Okta is a cloud-based identity management solution. Once a plan is purchased, Okta sends the organization’s administrator a link to the application. A good place to begin is on the Okta Help Center's Getting Started as a New Okta Administrator page.

CONNECTING A DOMAIN CONTROLLER

If you do not already have a domain controller installed and configured, you can find information on how to create one in the first step of the Authlite Implementation Guide.

Once your domain controller is configured and installed for your organization, follow Okta’s installation and configuration guide for the Okta Active Directory Agent, found on the Okta Help Center's Install and Configure the Okta Active Directory Agent page.

SERVICE PROVIDER CONFIGURATION

Now that Okta is connected to your domain controller, you need to configure your service providers. The three selected below are available, along with thousands of pre-integrated apps.

1. **Slack Configuration**
   a. Configure Slack for SAML 2.0. Documentation can be found on Okta's How to Configure SAML 2.0 for Slack page.
   b. Configure provisioning within Okta for Slack. Documentation can be found on Okta's Configuring Provisioning for Slack page.

2. **Dropbox Configuration**
   a. Configure Dropbox. Documentation can be found on Okta's Configuring Provisioning for Dropbox Business page.

3. **G Suite Configuration**
   a. Configure G Suite for SAML 2.0. Documentation can be found on Okta's How to Configure SAML 2.0 for G Suite.
   b. Configure provisioning within Okta for G Suite. Documentation can be found on Okta Help Center's Configuring Provisioning for G Suite page.

---
Once everything is properly configured, your Okta dashboard will look like this:

![Okta Dashboard Screenshot]

**PIV-I CONFIGURATION**

Once your service providers are configured, the addition of a second authentication factor is strongly recommended before users obtain access to Okta. We used a PIV-I card. Steps for PIV configuration can be found on Okta's Identify Providers page (click on “Add a PIV card”).

**CHANGE MANAGEMENT**

[Okta Help Center's End User Adoption Toolkit](https://www.okta.com/help/end-user-adoption-toolkit) provides helpful information to download the End User Adoption kit.