Configuring Kerberos Constrained Delegation

Welcome to the F5 deployment guide on configuring Kerberos constrained delegation through BIG-IP APM. This guide was created to supplement other F5 deployment guides which contain configuration guidance for specific applications, but do not include Kerberos constrained delegation configuration.

Products and applicable versions

<table>
<thead>
<tr>
<th>Product</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIG-IP LTM, APM</td>
<td>11.0 - 12.0</td>
</tr>
<tr>
<td>Deployment Guide version</td>
<td>1.1 (see Document Revision History on page 19)</td>
</tr>
<tr>
<td>Last updated</td>
<td>09-23-2015</td>
</tr>
</tbody>
</table>

Visit the Microsoft page of F5’s online developer community, DevCentral, for Microsoft forums, solutions, blogs and more: http://devcentral.f5.com/Microsoft/.

Important: Make sure you are using the most recent version of this deployment guide, available at http://www.f5.com/pdf/deployment-guides/kerberos-constrained-delegation-dg.pdf
Contents

Prerequisites and configuration notes 3

Configuring the Active Directory domain controller 4
  Creating the APM Delegation Account on the Windows Domain Controller 4
  Modifying the account to be trusted for delegation 5
  Configuring Trust for the Active Directory user 7
  Disabling anonymous authentication and enabling Windows authentication 7

Configuring the BIG-IP APM for Kerberos Delegation Authentication 8
  Editing the Access Policy 10
  Creating the BIG-IP LTM objects 12

Using the logs for information and troubleshooting 13

Configuration Example: Customizing APM Access Policy to support alternative UPN suffixes when using client-side NTLM authentication for Outlook Anywhere 14
  Troubleshooting Kerberos SSO 17

Appendix: Configuring additional BIG-IP settings 18

Document Revision History 19
Prerequisites and configuration notes

- DNS Reverse Lookup Zone(s) with appropriate PTR record(s) are critical for successful configuration of Kerberos SSO Constrained Delegation.

- All of the Active Directory domains involved in Kerberos Delegated authentication must be at a Microsoft Windows Server 2003 Functional Level or higher. If the domain less than the Windows 2003 Server level (such as Windows 2000 compatible mode), you will not be able to find the Delegation Tab in the properties of APM Delegation Account created on the Windows Domain Controller.

Additionally, /var/log/apm will record the following error:

bigip1 err /usr/bin/websso[17269]: 01490000:3:
Kerberos: can't get S4U2Proxy ticket for server HTTP/REVOLVER.ESX-LAB.NET@REVOLVER.ESX-LAB.NET - Requesting ticket can't get forwardable tickets (-1765328163)

- Be aware that if you are using BIG-IP v11.1, the system records log messages in MySQL Database, instead of sending them to the regular /var/log/apm logfile, by default. You must modify this default behavior by executing the following command from the command line:
  
  # tmsh modify sys db log.access.syslog value enable

- When there are multiple back-end realms, being front-ended by BIG-IP APM, the Server Domain(s) must have bidirectional transitive trusts with the users’ domain(s). You must create an APM Delegation Account in each realm whose users will be accessing websites through the APM.

A domain and a Kerberos Realm are different in that for Kerberos, a realm is a set of users and the authentication methods for those users to access that realm. A realm resembles a fully-qualified domain name and can be distributed across either a single server or a single domain across multiple machines. A single server instance can also support multiple realms.
Configuring the Active Directory domain controller

In this section, the configuration procedures take place on the Active Directory domain controller. This section contains the following tasks:

- Creating the APM Delegation Account on the Windows Domain Controller, on this page
- Modifying the account to be trusted for delegation on page 5
- Configuring Trust for the Active Directory user on page 7
- Disabling anonymous authentication and enabling Windows authentication on page 7

Note: This section provides guidance only; for specific instructions, consult the appropriate documentation. F5 cannot be responsible for improper configuration of Active Directory or Microsoft devices.

Creating the APM Delegation Account on the Windows Domain Controller

In order to use Kerberos SSO, the BIG-IP APM user account must be created in Active Directory and modified to be trusted for delegation.

You can either create the APM Delegation account from the Windows Domain controller using either the UI or PowerShell commands. If you want to use PowerShell, see To create the APM delegation account using a PowerShell command on page 5.

To create the APM delegation account from the UI

1. From the Windows Domain controller, from the Administrative Tools menu, open Active Directory Users and Computers.

2. To create a new user (recommended), use the following guidance. If you are modifying an existing user, continue with Step 3.
   a. In the left navigation pane, right-click Users, and then from the New menu, click User.
   b. In the First and Last name boxes, type the appropriate names.
   c. In the User logon name field, type host/ and then a unique name. The user logon name must begin with host/. In this case, host is a literal string that later matches the Type of Service in Service Principal Name (SPN). The name is any name that needs to be matched while configuring APM SSO object, and the domain is the DNS FQDN for the realm containing your web resources to be accessed. The domain for the Sever can be found either from System Properties, or by running the set command from the command prompt.
   d. Click Next.
   e. Type and confirm the password, and then uncheck User must change password at next logon. Check the boxes for User cannot change password and Password never expires.
   f. Review the information and then click Finish.

3. In either the left pane or the main pane, right-click the user you just created (or the existing user) and then click Properties.

4. Ensure the User logon name is correct, including the host/ prefix.

5. In the Account options area, ensure the boxes for User cannot change password and Password never expires are checked.

6. In the Account expires area, make sure Never is selected.

7. Click Ok.

When properly configured, the Account tab of your user account should look like Figure 1 on the next page.
To create the APM delegation account using a PowerShell command

Use this guidance if you prefer to create the user account using a PowerShell command.

To create the delegation account using PowerShell commands, use the following syntax, replacing the account username information in red with the appropriate values for your configuration.

```
New-ADUser -Name "APM Delegation Account" -UserPrincipalName host/account-username.example.com@example.com -SamAccountName "account-username" -PasswordNeverExpires $true -Enabled $true -AccountPassword (Read-Host -AsSecureString "Account Password")
```

Modifying the account to be trusted for delegation

Next step is to modify this the user account you just created to be a Delegate Account (meaning it is able to obtain Kerberos tickets from the KDC on behalf of other valid domain users). There are three methods of achieving this, either using the command line, the adsiedit UI, or a PowerShell commands. Use the method appropriate for your environment, and only use one method.

- `setspn` - CLI-based, easier, but takes a while to complete execution
- `adsiedit` - Opens up a graphical interface and involves multiple steps
- `PowerShell` - A single command for PowerShell users

These utilities should be included in the service pack support tools and are installed by default in Windows Server 2008 DC. If using Windows 2003 SP1, setspn is present but it is inside a toolkit that needs to be installed first to access it.

To modify the account using the command line

Use the following syntax to modify the account using the command line. This command includes the User logon name and also the pre-Windows logon name:

```
setspn -A host/bigip_user.exetst.local host.apm
```

When successful, the command returns an Updated Object message. Continue with Configuring Trust for the Active Directory user on page 7.
To modify the account using ADSIEdit

Use the following guidance to modify the account using ADSIEdit. This modifies the `servicePrincipalName` attribute of the Delegation Account from ADSIEdit (Default Context).

1. Run `adsiEdit.msc`,

2. Navigate to the domain user accounts (CN=Users), right-click the Delegation account you created, and then click Properties.

![ADSI Edit utility](image1)

Figure 2: ADSI Edit utility

3. From the Attribute column, click `servicePrincipalName`, and then click the Edit button.

![Editing the servicePrincipalName](image2)

Figure 3: Editing the servicePrincipalName

4. In the Value to add field, type the user logon name of the delegation account you created.

![Adding the user to the servicePrincipalName](image3)

Figure 4: Adding the user to the servicePrincipalName

5. Click the Ok button on both dialog boxes to complete the procedure.

Continue with Configuring Trust for the Active Directory user on page 7.
To modify the account using PowerShell

Use the following guidance to modify the account using a PowerShell command. Replace the account-username and domain information the values from your environment.

```
Set-AdUser -Identity account-username -ServicePrincipalNames @{Add="host/account-username.example.com"}
```

Configuring Trust for the Active Directory user

In this section, you configure the trust for specific services for the user you created.

1. From the Windows Domain controller, from the Administrative Tools menu, open Active Directory Users and Computers.
2. Right-click the user account you created.
3. Click the Delegation tab.
4. Click Trust this user for delegation to specified services only. This enables Kerberos constrained delegation.
5. Under Trust this user for delegation to specified services only, click Use any authentication protocol. This enables Kerberos protocol transition on the server-side.
6. In the Services to which this account can present delegated credentials area, click the Add button to add services to the list.
7. From the Add Services dialog box, click Users or Computers.
8. From the Select Users or Computers dialog, in the Enter the object names to select field, type the computer/server where the desired Web service is running. You can add multiple devices separated by a semi-colon. Click Check Names.
9. Click the OK button.
10. From the Available Services area, select the service(s) you want to delegate to this account.
11. Click the OK button on each of the dialog boxes to exit.

This concludes the configuration of the APM Delegation Account.

Disabling anonymous authentication and enabling Windows authentication

The next task is to disable Anonymous authentication, and then enable Windows authentication on the default web site running on the IIS server

To disable anonymous authentication

1. Open IIS Manager, and then browse to Sites > (your-site-name).
2. In the main pane, in the IIS section, double-click Authentication to reveal all the available Authentication methods.
3. Click Anonymous Authentication (enabled by default) to highlight it, and then in the Actions pane, click Disable. Anonymous Authentication must disabled for testing Kerberos in operation.
4. Click Windows Authentication to highlight it, and then in the Actions pane, click Enable.
5. Optional: You may want to remove the NTLM option in order to ensure that Kerberos is the only type of Authentication method currently supported for accessing your web site.
   a. Click Windows Authentication to highlight it, and then in the Actions pane, click Providers.
   b. In the Providers dialog box, select NTLM and Negotiate, and then click Remove.
   c. From the Available Providers list, click Negotiate:Kerberos. This ensures that only Kerberos is the only available authentication mechanism for this website.
   d. Click Ok.
6. From the command prompt, run the commend `iisreset /noforce`.

Now, when you try to access this web site without implementing Kerberos SSO configuration (such as with LTM only configuration), you see a 401 response from the web server.
## Configuring the BIG-IP APM for Kerberos Delegation Authentication

Use the following table for guidance on configuring the BIG-IP APM objects necessary for this configuration. For specific instructions on configuring individual objects, see the Help tab or APM documentation.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Description/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Type a unique name, such as sso-kerberos</td>
<td></td>
</tr>
<tr>
<td><strong>SSO Method</strong></td>
<td>Kerberos</td>
<td></td>
</tr>
<tr>
<td><strong>Kerberos Realm</strong></td>
<td>Type the Kerberos Realm.</td>
<td>This must be uppercase, such as MYDOMAIN.COM. If your servers are located in multiple realms, each realm requires a separate SSO configuration. The user’s Realm can be obtained from the logon page by specifying the “session.logon.last.domain” session variable. In case this variable is not set, the user’s realm is assumed to be the same as Server’s realm.</td>
</tr>
<tr>
<td><strong>KDC</strong></td>
<td>Type the IP address or FQDN of the Kerberos Key Distribution Center (KDC).</td>
<td>This normally is the Active Directory Domain Controller for the user’s domain. KDC, being an optional field, can be omitted, in which case it should be discoverable through SRV records for the Server realm’s domain (usually same as realm’s name). Kerberos SSO processing is fastest when specifying an IP Address, slower if by the host FQDN, and the slowest if it is left blank (due to additional DNS queries for name resolution). When User’s realm could potentially be different from the web server’s realm, the KDC must be left empty. This is necessary in multi-realm scenarios.</td>
</tr>
<tr>
<td><strong>Account Name</strong></td>
<td>The account name of the Active Directory user account to which logon rights have been delegated</td>
<td>This value must begin with host/, for example, host/bigip_user_acct.mydomain.local.</td>
</tr>
<tr>
<td><strong>Account Password</strong></td>
<td>Type the associated password</td>
<td></td>
</tr>
<tr>
<td><strong>SPN Pattern</strong></td>
<td>Optional: Specify a custom SPN pattern to create the ticket request using the host name from the HTTP request.</td>
<td>This field can be used to modify how Service Principal Name for the servers is constructed. Default value for this field is HTTP/%s@REALM where %s is replaced by the server’s hostname discovered by reverse DNS lookup using the server IP address. When entering the value replace REALM with the actual realm name (as specified in Kerberos Realm field above). Generally, this field may be left blank, unless the user needs a non-standard SPN format.</td>
</tr>
<tr>
<td><strong>Ticket Lifetime</strong></td>
<td>Optional: Type a value in minutes for the lifetime of the kerberos ticket. The default is 600 (10 hours)</td>
<td>This value represents the maximum ticket lifetime; the actual lifetime may be less by up to 1 hour. This is because user’s ticket lifetime is the same as TGT lifetime. The TGT is a Kerberos Ticket Granting Ticket obtained for the delegation account specified in this configuration. The new TGT is fetched every time when current TGT for that account is older than one hour. The new TGT could only be fetched when SSO request is processed. The minimum lifetime that can be specified is 10 minutes. There is no maximum, however most AD domains have this set to 10 hours (600 minutes) and it is not recommended to set ticket lifetime in SSO configuration above what is specified in AD. Active Directory Maximum lifetime for service ticket can modified using the Local Security Policy MMC under Security Settings &gt; Account Policies &gt; Kerberos Policy.</td>
</tr>
<tr>
<td><strong>Send Authorization</strong></td>
<td>Select a value from the list. We recommend the default (Always)</td>
<td>This specifies when to submit Kerberos ticket to the application server(s). The ticket is submitted in a HTTP Authorization header. The header value starts with Negotiate word followed by one space and base64 encoded GSSAPI token containing Kerberos ticket. When Send Authorization is set to On 401 Status Code the BIG-IP will first forward user’s HTTP request to the web server without inserting new Authorization header (but any browser’s Authorization header will be deleted). If server requests authentication by responding with 401 Status Code the BIG-IP will retry the request with the Authorization header. The Kerberos ticket GSSAPI representation will use SPNEGO mechanism type (OID 1.3.6.1.5.5.2). When the Send Authorization Code is to Always, the Authorization header with Kerberos ticket will be inserted into every HTTP request regardless if it requires authentication or not, i.e. it will be inserted pre-emptively. The Kerberos ticket GSSAPI representation will use KRB5 Kerberos 5 mechanism type (OID 1.2.840.113554.1.2.2). Selecting the 401 option will result in an additional BIG-IP/server request round trip in case authentication is required for the request. On the other hand, selecting Always will result in additional overhead of generating Kerberos token for every request (Kerberos tickets are fetched only for first request for the user and then cached for up to configured ticket lifetime, so subsequent requests involve only local processing).</td>
</tr>
</tbody>
</table>
Note: The following configuration items represent a basic APM configuration and are provided as an example. You can alternatively use one of the F5 iApp templates, which configures these objects for you. You may have to disable Strict Updates to enable the Kerberos SSO object you created. Consult the deployment guide for the iApp you are using.

DNS and NTP
See Using the logs for information and troubleshooting on page 13 for specific instructions if you have not yet configured DNS and NTP on your BIG-IP system.

Health Monitors [Local Traffic > Monitors] - Only necessary if creating a pool of Active Directory servers

Configuration
- Select Advanced from the Configuration list (if necessary).
- Name: Type a unique name, such as AD_LDAP_monitor.
- Type: LDAP
- Interval: 10 (recommended)
- Timeout: 31 (recommended)
- User Name: Type a user name with administrative permissions
- Password: Type the associated password
- Base: Specify your LDAP base tree. For example, CN=SharePoint Users,DC=example,DC=com
- Filter: Specify the filter. We type `cn=user1`, using the example above: user1 in OU group “SharePoint Users” and domain “example.com”
- Security: Select a Security option (either None, SSL, or TLS)
- Chase Referrals: Yes
- Alias Address: *All Addresses
- Alias Address Port: 389 (for None or TLS) or 686 (for SSL)

AAA Servers (Access Policy-->AAA Servers)

If you are using a single Active Directory Server
- Name: Type a unique name. We use example-aaa-server.
- Type: Active Directory
- Domain Controller: Type the IP address or FQDN name of an Active Directory Domain Controller
- Domain Name: Type the Active Directory domain name
- Admin Name: Type the AD user name with administrative permissions (optional)
- Admin Password: Type the associated password (optional). Type it again in the Verify Password box

If you are using a pool of Active Directory Servers
- Name: Type a unique name. We use example-aaa-server.
- Type: Active Directory
- Domain Name: Type the FQDN of the Windows Domain name
- Server Connection: Click Use Pool if necessary.
- Domain Controller Pool Name: Type a unique name
- Domain Controllers: IP Address: Type the IP address of the first domain controller
- Domain Name: Type the FQDN of the domain controller
- Admin Name: Type the Administrator name
- Admin Password: Type the associated password

Access Profile (Access Policy > Access Profiles)
- Name: Type a unique name
- Profile Type: LTM-APM
- SSO Configurations: You may want to test without any SSO object for Kerberos configured in the Access Profile. In this case, you should get a 401 for Negotiate. Thus without the SSO, you should get a credentials popup. You should test that credentials will work to access the application. When you have finished testing, reconfigure this Access Profile to select the SSO configuration you created.
- Languages: Move the appropriate language(s) to the Accepted box.

Access Policy
- Edit: Click the Edit link to configure the Access Profile you created using the Visual Policy Editor.

1 Only necessary if using a pool of Active Directory servers
2 Optional; Admin Name and Password are only required if anonymous binding to Active Directory is not allowed in your environment.
Editing the Access Policy

This section provides two examples of ways you can configure the BIG-IP APM Access Policy to use the objects you created. The first is a simple example, the second uses information from a client certificate to configure Kerberos SSO.

Editing the Access Policy - simple example for testing


2. Locate the Access Profile you created, and then in the Access Policy column, click Edit. The VPE opens in a new window.

3. Click the + symbol between Start and Deny. A box opens with options for different actions.

4. Click the Logon tab (if necessary) click the Logon Page option button, and then click Add item.
   a. In the Name field, you can optionally type a new name.
   b. Modify any of the settings as applicable for your configuration. We leave the defaults in our example.
   c. Click Save.

5. Click the + symbol between Logon Page and Deny.

6. Click the SSO Credential Mapping option button, and then click the Add Item button.

7. Click the Save button.

8. Click the Deny link in the box to the right of SSO Credential Mapping.

9. Click Allow and then click Save. Your Access policy should look like the example below.

   ![Simple VPE example](image)

   Figure 5: Simple VPE example

Editing the Access Policy for client certificate authentication example


2. Locate the Access Profile you created, and then in the Access Policy column, click Edit. The VPE opens in a new window.

3. Click the + symbol between Start and Deny. A box opens with options for different actions.

4. Click the Client Cert Inspection option button, and then click Add Item.
   a. Configure the Properties as applicable for your configuration. In our example, we leave the settings at the defaults.
   b. Click the Save button.

5. On the Successful path between Client Cert Inspection and Deny, click the + symbol The options box opens.

6. Click the Variable Assign option button, and then click Add Item. It is important you add the variables in the following order.
   a. Click Add new entry.
   b. Click the Change link on the new entry.
   c. In the Custom Variable box, type: session.logon.last.domain.
   d. In the Custom Expression box, type:

   ```
   session.logon.last.domain = set upn [mcget {session.logon.last.upn}]; if {[string first "@" $upn] >= 0} { return [string range $upn [expr { [string first "@" $upn] + 1 }] end ]; } else { return ""; }
   ```
   e. Click Finished.
   f. Click Add new entry.
g. Click the Change link on the new entry.
h. In the Custom Variable box, type `session.logon.last.username`.
i. In the Custom Expression box, type
   ```
   session.logon.last.username = set upn [mcget {session.logon.last.upn}]; if {[string first "@" $upn] >= 0} {
   return [string range $upn 0 [expr { [string first "@" $upn] - 1 } ] ]; } else { return $upn; }
   ```
j. Click Finished.
k. Click Add new entry.
l. Click the Change link on the new entry.
m. In the Custom Variable box, type `session.logon.last.upn`.

n. In the Custom Expression box, type
   ```
   set e_fields [split [mcget {session.ssl.cert.x509extension}] "\n"]; foreach qq $e_fields { if {[string first "othername:UPN" $qq] >= 0} { return [string range $qq [expr { [string first "<" $qq] + 1 } ] [expr { [string first "]" $qq] - 1 } ] ]; } } return ""
   ```
o. Click Finished.
p. Click Save. When you are finished, your Variable Assign item must look like the following example. Use the arrows on the right to move the variables if necessary.

![Variable assign object](image)

Figure 6: Variable assign object

7. Click the + symbol between Variable Assign and Deny. The options box opens.
8. Click the SSO Credential Mapping option button, and then click Add Item.
9. Click the Save button.
10. On the fallback path between SSO Credential Mapping and Deny, click the Deny box, click Allow, and then click Save.
11. Click the yellow Apply Access Policy link in the upper left part of the window. You must apply an access policy before it takes effect.
12. Click the Close button on the upper right to close the VPE.
Creating the BIG-IP LTM objects

Use the following table for guidance on configuring the load balancing objects on your BIG-IP system. This is just a simple example, you can modify the configuration as appropriate for your environment. Again, if you are using an iApp template to configure your application, these objects are created by the iApp template.

<table>
<thead>
<tr>
<th>Pools (Local Traffic &gt; Pools)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Type a unique name</td>
</tr>
<tr>
<td><strong>Health Monitor</strong></td>
<td>Select the appropriate health monitor, such as http.</td>
</tr>
<tr>
<td><strong>Slow Ramp Time</strong></td>
<td>300 (recommended)</td>
</tr>
<tr>
<td><strong>Load Balancing Method</strong></td>
<td>Choose a load balancing method. We recommend Least Connections (Member)</td>
</tr>
<tr>
<td><strong>Address</strong></td>
<td>Type the IP Address of the nodes</td>
</tr>
<tr>
<td><strong>Service Port</strong></td>
<td>Type the appropriate port (such as 80) or select the service from the list Add to repeat Address and Service Port for all nodes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Profiles (Local Traffic &gt; Profiles)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTTP</strong> (Profiles &gt; Services)</td>
<td></td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Type a unique name</td>
</tr>
<tr>
<td><strong>Parent Profile</strong></td>
<td>http</td>
</tr>
<tr>
<td><strong>Rewrite Redirect</strong></td>
<td>Matching</td>
</tr>
<tr>
<td><strong>Client SSL</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Type a unique name</td>
</tr>
<tr>
<td><strong>Parent Profile</strong></td>
<td>clientssl</td>
</tr>
<tr>
<td><strong>Certificate and Key</strong></td>
<td>Select the Certificate and Key you imported from the associated list</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Virtual Servers (Local Traffic &gt; Virtual Servers)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTTP</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Type a unique name.</td>
</tr>
<tr>
<td><strong>Address</strong></td>
<td>Type the IP Address for the virtual server</td>
</tr>
<tr>
<td><strong>Service Port</strong></td>
<td>80</td>
</tr>
<tr>
<td><strong>HTTP Profile</strong></td>
<td>Select the HTTP profile you created above</td>
</tr>
<tr>
<td><strong>Source Address Translation</strong></td>
<td>Auto Map (optional; see footnote 3)</td>
</tr>
<tr>
<td><strong>Access Policy</strong></td>
<td>Select the Access Policy you created.</td>
</tr>
<tr>
<td><strong>Default Pool</strong></td>
<td>Select the pool you created above</td>
</tr>
<tr>
<td><strong>iRule</strong></td>
<td>If offloading SSL only: Enable the built-in _sys_https_redirect irule</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HTTPS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Type a unique name.</td>
</tr>
<tr>
<td><strong>Address</strong></td>
<td>Type the IP Address for the virtual server</td>
</tr>
<tr>
<td><strong>Service Port</strong></td>
<td>443</td>
</tr>
<tr>
<td><strong>HTTP Profile</strong></td>
<td>Select the HTTP profile you created above</td>
</tr>
<tr>
<td><strong>SSL Profile (Client)</strong></td>
<td>Select the Client SSL profile you created above</td>
</tr>
<tr>
<td><strong>Source Address Translation</strong></td>
<td>Auto Map (optional; see footnote 3)</td>
</tr>
<tr>
<td><strong>Access Policy</strong></td>
<td>Select the Access Policy you created.</td>
</tr>
<tr>
<td><strong>Default Pool</strong></td>
<td>Select the pool you created above</td>
</tr>
</tbody>
</table>

---

1. You must select Advanced from the Configuration list for these options to appear.
2. Do not enable these objects on the HTTP virtual server if offloading SSL. The HTTP virtual server is only used for redirecting users to the HTTPS virtual server.
3. If expecting more than 64,000 simultaneous connections per server, you must configure a SNAT Pool. See the BIG-IP documentation on configuring SNAT Pools.
4. This virtual server is only necessary if offloading SSL.
Using the logs for information and troubleshooting

In order to perform any troubleshooting or familiarizing yourself with the operation of Kerberos Delegation, you can set the SSO Log Level to Debug (rather than leaving it to the default Informational. Don’t leave debug mode on in production, though) and test your Virtual Server.

To set the SSO log to Debug:

- **In BIG-IP v11.6 and earlier**: Click System > Logs > Configuration > Options. From the Access Policy Logging SSO list, select Debug, and then click Update.

- **In BIG-IP v12.0 and later**: Click Access Policy > Event Logs > Log Settings. Check the box next to the log setting you want to modify, and then click Edit. In the left pane, click Access System Logs. From the SSO list, select Debug, and then click OK.

You then need to associate the log settings with your Access Profile. Click Access Policy > Access Profiles > Access Profiles List > name-you-gave-the-access-profile > Logs tab. From the Available box, select the log settings you modified and then click the Add (<>) button to add it to the Selected box. Click Update.

A successful Kerberos ticket request will look similar to the following excerpt from /var/log/apm. Note the entries in bold text.

Feb 10 10:28:23 tmn notice tmm[7337]: 01490500:5: 642ae9bd: New session from client IP 10.10.1.30 (ST=/CC=/C=) at VIP 10.10.2.15 Listener /Common/My_LTM_VS
Feb 10 10:28:33 apmv111 notice apd[4840]: 01490010:5: 642ae9bd: Username 'student3'
Feb 10 10:28:33 apmv111 notice apd[4840]: 01490005:5: 642ae9bd: Following rule 'fallback' from item 'SSO Credential Mapping' to ending 'Allow'
Feb 10 10:28:33 apmv111 notice apd[4840]: 01490102:5: 642ae9bd: Access policy result: LTM+APM Mode
Feb 10 10:28:33 apmv111 info websso.1[7644]: 014d0011:6: 642ae9bd: Websso Kerberos authentication for user 'student3' using config '/Common/sso-kerberos'
Feb 10 10:28:33 apmv111 info websso.1[7644]: 014d0018:7: sid:642ae9bd ctx:0x9b7d6f0 server address = ::ffff:172.16.2.45
Feb 10 10:28:33 apmv111 info websso.1[7644]: 014d0021:7: sid:642ae9bd ctx:0x9b7d6f0 SPN = HTTP/dcone.mydomain.local@MYDOMAIN.LOCAL
Feb 10 10:28:33 apmv111 debug websso.1[7644]: 014d0001:7: Getting UCC:student3@MYDOMAIN.LOCAL@MYDOMAIN.LOCAL, lifetime:36000
Feb 10 10:29:19 apmv111 debug websso.1[7644]: 014d0001:7: fetched new TGT, total active TGTs:1
Feb 10 10:29:19 apmv111 debug websso.1[7644]: 014d0001:7: TGT: client=host/apm.mydomain.local@MYDOMAIN.LOCAL@MYDOMAIN.LOCAL@MYDOMAIN.LOCAL expiration=Fri Feb 10 20:28:33 2012 flags=40600000
Feb 10 10:29:19 apmv111 debug websso.1[7644]: 014d0001:7: TGT: client=host/apm.mydomain.local@MYDOMAIN.LOCAL@MYDOMAIN.LOCAL@MYDOMAIN.LOCAL server=krbtgt/MYDOMAIN.LOCAL@MYDOMAIN.LOCAL lifetime=36000 kcc:0x9afbdf0
Feb 10 10:29:19 apmv111 debug websso.1[7644]: 014d0001:7: Expire thread: TGT expires in  28448 sec, ucc count:     1 princ: host/apm.mydomain.local@MYDOMAIN.LOCAL
Feb 10 10:29:19 apmv111 debug websso.1[7644]: 014d0001:7: Expire thread: TGT expires in  35994 sec, ucc count:     1 princ: host/apm.mydomain.local@MYDOMAIN.LOCAL
Feb 10 10:29:19 apmv111 debug websso.1[7644]: 014d0001:7: fetched new TGT, total active TGTs:1
Feb 10 10:29:19 apmv111 debug websso.1[7644]: 014d0001:7: S4U ======> - NO cached S4U2Proxy ticket for user: student3@MYDOMAIN.LOCAL server: HTTP/dcone.mydomain.local@MYDOMAIN.LOCAL - trying to fetch
Feb 10 10:29:19 apmv111 debug websso.1[7644]: 014d0001:7: S4U ======> - NO cached S4U2Self ticket for user: student3@MYDOMAIN.LOCAL - trying to fetch
Feb 10 10:29:19 apmv111 debug websso.1[7644]: 014d0001:7: S4U ======> OK!
**Configuration Example: Customizing APM Access Policy to support alternative UPN suffixes when using client-side NTLM authentication for Outlook Anywhere**

This section describes the configuration of the Access Policy Manager to support Kerberos Single Sign-On from Microsoft Outlook clients when clients use NTLM authentication and user accounts use an alternative User Principal Name (UPN) format. The access policy must be configured to query Active Directory for the user’s internal domain and assign the correct realm to be used for construction of the Kerberos ticket request.

This configuration requires that:

- The BIG-IP APM has been correctly deployed to support NTLM authentication for Outlook Anywhere clients, and that domain-joined clients that use DOMAIN\user format can successfully connect (F5 strongly recommends using the Microsoft Exchange CAS iApp template to simplify the configuration).
- If you used the Exchange iApp template, the Strict Updates setting must be disabled on the Exchange application service. To disable Strict Updates, click iApp > Application Services > [name you gave the iApp] > Properties (on the Menu bar), and then uncheck Strict Updates (if necessary).

**Important** After disabling Strict Updates and customizing the Access Policy created by the iApp, reconfiguring the iApp will cause all policy modifications to be lost. If you need to reconfigure the iApp after making these changes, F5 recommends manually creating the access policy and assigning to the deployment by selecting the corresponding APM profile in response to the “Would you like to create a new Access Profile, or use an existing Access Profile?” question in the iApp template.

- An LDAP AAA server is configured to process LDAP queries. The credentials of a user account with permission to query Active Directory are required; F5 recommends that this account be set with the Password never expires option.

1. Create an LDAP AAA Server object on APM. Use the following table for guidance. All fields in the table are required, others are optional.

<table>
<thead>
<tr>
<th>AAA Servers (Access Policy--&gt;AAA Servers)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Server Pool Name</td>
</tr>
<tr>
<td>Server Addresses</td>
</tr>
<tr>
<td>Mode</td>
</tr>
<tr>
<td>Service Port</td>
</tr>
<tr>
<td>Admin DN</td>
</tr>
<tr>
<td>Admin Password</td>
</tr>
<tr>
<td>Verify Admin Password</td>
</tr>
<tr>
<td>Group Cache Lifetime</td>
</tr>
</tbody>
</table>

2. Click Access Policy > Access Profiles, and then click the Edit link for your Exchange APM Access Policy. If you used the iApp template, the policy is named exch. It should look like the following when client-side NTLM authentication is selected for Outlook Anywhere.

![Access Policy](image)

3. On the NTLM Auth Result Check path of the policy, click the small X to remove both SSO Credential Mapping items. On the confirmation page, ensure Connecting previous node to Successful branch is selected. After you are finished, the VPE should look like the following.

![VPE Configuration](image)
4. Click the **Add New Macro button** (under the VPE image, shown in the previous example).
   a. In the **Name** field, type **LDAP Custom Query**.
   b. Click **Save**.
   c. Repeat this step twice to add empty queries for **LDAP URN Query** and **LDAP Credentials Variable Assign** objects. Use the bold text in the Name field.

5. Click the expand button to the left of each macro.

6. On the first macro, click the **Edit Terminals** button and then click **Add Terminal**.
   a. In the **Name** field, type **Fail**.
   b. Click the down arrow to move the new terminal below the pre-existing (Out) one. See the example after step d.
   c. Click **Save**.
   d. Repeat this step twice for each of the other macros.

7. In the **LDAP Custom Query** macro item, click the + symbol between **In** and **Out**. A box opens with options for different actions.

8. Click the Authentication tab, click the **LDAP Query** option button, and then click the **Add Item** button.
   a. From the **Server** list, select the LDAP AAA server you configured in step 1.
   b. In the **SearchDN** field, type the DN for your domain to query, for example *dc=trece,dc=local*.
   c. In the **SearchFilter** field, type *(sAMAccountName=%{session.logon.last.username})*.
   d. Click the **Add new entry** button.
      - Type **userPrincipleName**.
      - Type **sAMAccountName**.
      - Type **distinguishedName**.
   e. Click the Branch Rules tab.
      - Click the delete button (x) on the existing Branch rule (User Group Membership).
      - Click **Add Branch Rule**.
      - In the **Name** box, type **LDAP passed**.
      - Click the **change** link.
• Click **Add Expression**.
  • If necessary, from the **Agent Sel** list, select **LDAP Query**.
  • If necessary, from the **Condition** list, select **LDAP Query has passed**.
  • Click **Add Expression**, and then click **Finished**.

f. Click **Save**. This completes the macro.

9. In the **LDAP Credentials Assign** macro item, click the + symbol between **In** and **Out**.

10. Click the Assignment tab, click the **Variable Assign** option button, and then click the **Add Item** button.
  a. Click the **Add new entry** button, and then click the **change** link.
     • In the **Custom Variable** field, type **session.logon.last.username**.
     • In the **Expression** field, type **{session.ldap.last.attr.sAMAccountName}**.
     • Click **Finished**.
  b. Click the **Add new entry** button again, and then click the **change** link.
     • In the **Custom Variable** field, type **session.logon.last.domain**.
     • In the **Expression** field, type or copy paste the following:
       ```expr { [string toupper [string map -nocase {,dc= .} [string range [mcget {session.ldap.last.attr.distinguishedName}] [expr [string first ",,DC=" [mcget {session.ldap.last.attr.distinguishedName}] 0 +4] end ] ] ] ```
     • Click **Finished**.

11. Still in the **LDAP Credentials Assign** macro item, click the + symbol between **Variable Assign** and **Out**.

12. Click the Assignment tab, click the **SSO Credential Mapping** option button, and then click the **Add Item** button.
  a. In the **SSO Token Username** list, ensure **Username from Logon Page** is selected.
  b. In the **SSO Token Password** list, ensure **Password from Logon Page** is selected.
  c. Click **Save**. This completes the macro.

13. In the **LDAP URN Query** macro item, click the + symbol between **In** and **Out**.

14. Click the Authentication tab, click the **LDAP Query** option button, and then click the **Add Item** button.
  a. From the **Server** list, select the LDAP AAA server you configured in step 1.
  b. In the **SearchDN** field, type the DN for your domain to query, for example **dc=trece,dc=local**.
  c. In the **SearchFilter** field, type **(userPrincipalName=%{session.logon.last.logonname})**.
  d. Click the **Add new entry** button.
     • Type **userPrincipalName**.
     • Type **sAMAccountName**.
  e. Click the **Branch Rules** tab.
     • Click the delete button (x) on the existing Branch rule (User Group Membership).
     • Click **Add Branch Rule**.
     • In the **Name** box, type **LDAP passed**.
     • Click the **change** link.
     • Click **Add Expression**.
     • If necessary, from the **Agent Sel** list, select **LDAP Query**.
     • If necessary, from the **Condition** list, select **LDAP Query has passed**.
     • Click **Add Expression**, and then click **Finished**.
  f. Click **Save**. This completes all of the macros.
15. Back on the main VPE, click the + symbol on the Successful path between NTLM Auth result check and Allow.
16. Click the Macrocalls tab, and then click the LDAP Custom Query option button, and then click the Add Item button.
17. Click the + symbol on the Successful path between LDAP Custom Query and Allow.
18. Click the Macrocalls tab, and then click the LDAP Credentials Assign option button, and then click the Add Item button.
19. Click the + symbol on the Successful path between AD Auth and Allow.
20. Click the Macrocalls tab, and then click the LDAP UPN Query option button, and then click the Add Item button.
21. Click the + symbol on the Successful path between LDAP UPN Query and Allow.
22. Click the Macrocalls tab, and then click the LDAP Credentials Assign option button, and then click the Add Item button. Your VPE should now look similar to the example after step 23.
23. Click the yellow Apply Access Policy link found in the top left of the screen next to the F5 logo. You must apply the policy before it takes effect.

This completes the configuration.

**Troubleshooting Kerberos SSO**

If you are having difficulty connecting, you can enable APM debug logging to identify the source of the problem.

1. From the BIG-IP Configuration utility, click System > Logs > Configuration > Options.
2. In the Access Policy Logging section, from the Access Policy and SSL Logging lists, select Debug.
3. Click Update.

To view messages related to APM Access Policy and SSO, log in to the BIG-IP command line and run the command: `tail -f /var/log/apm` while attempting to connect.
Appendix: Configuring additional BIG-IP settings

This section contains information on configuring the BIG-IP system for objects or settings that are required.

Configuring DNS and NTP settings

If you are configuring the iApp to use BIG-IP APM, you must configure DNS and NTP settings on the BIG-IP system before beginning the iApp.

Configuring the DNS settings

In this section, you configure the DNS settings on the BIG-IP system to point to a DNS server that can resolve your Active Directory server or servers. In many cases, this IP address will be that of your Active Directory servers themselves.

Note: DNS lookups go out over one of the interfaces configured on the BIG-IP system, not the management interface. The management interface has its own, separate DNS settings.

Important  The BIG-IP system must have a self IP address in the same local subnet and VLAN as the DNS server, or a route to the DNS server if located on a different subnet. The route configuration is found on the Main tab by expanding Network and then clicking Routes. For specific instructions on configuring a route on the BIG-IP system, see the online help or the product documentation.

To configure DNS settings

1. On the Main tab, expand System, and then click Configuration.
2. On the Menu bar, from the Device menu, click DNS.
3. In the DNS Lookup Server List row, complete the following:
   a. In the Address box, type the IP address of a DNS server that can resolve the Active Directory server.
   b. Click the Add button.
4. Click Update.

Configuring the NTP settings

The next task is to configure the NTP settings on the BIG-IP system for authentication to work properly.

To configure NTP settings

1. On the Main tab, expand System, and then click Configuration.
2. On the Menu bar, from the Device menu, click NTP.
3. In the Address box, type the fully-qualified domain name (or the IP address) of the time server that you want to add to the Address List.
4. Click the Add button.
5. Click Update.

To verify the NTP setting configuration, you can use the ntpq utility. From the command line, run ntpq -np.
## Document Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>New Deployment Guide</td>
<td>09-23-2015</td>
</tr>
<tr>
<td>1.1</td>
<td>Added the section <strong>Configuration Example: Customizing APM Access Policy to support alternative UPN suffixes when using client-side NTLM authentication for Outlook Anywhere on page 14.</strong></td>
<td>01-07-2016</td>
</tr>
</tbody>
</table>