white paper

HP Digital Sending Software 5.01 – Two-Server Authentication

Security Level: Public
Date Written/Updated December 1st, 2013

Document Summary

- Configuring DSS to use two-server authentication

Introduction

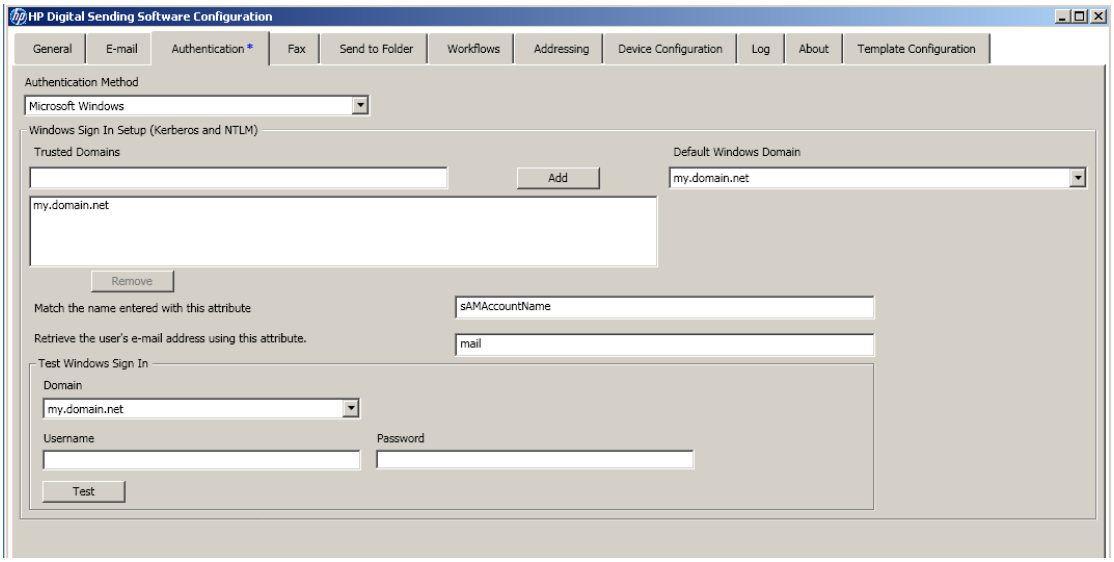
In some network environments DSS may require two different servers to fully authenticate a user at the MFP control panel. A Windows authentication server is employed to verify the user's access, and a second, LDAP, server is used to retrieve the user's full name and email address. The secondary user information query is performed on the LDAP server using bind methods such as "Simple – Non-SSL or SSL" or "Anonymous."

To configure two-server authentication in DSS 5 the Administrator needs to supply parameters for each authentication server separately. First, information for the primary authentication server needs to be entered in the Configuration Utility. Second, an XML document specifying the LDAP query values needs to be edited.

How to Configure DSS

The steps needed to configure DSS are to select a primary authentication method, and then edit the two-server XML document. The following example uses Windows for the primary authentication and LDAP with anonymous bind for the second server.

1. Open the Configuration Utility and select the Authentication tab. This is configured the same as single server authentication and query. When using two-server authentication the "Match the name entered with this attribute" and "Retrieve the user's email address using this attribute" text boxes should remain configured with some non-empty value, but they are not used. These attributes, along with other information about the LDAP server, will be specified in an XML document instead of in the Configuration Utility.



The next several steps involve using a text editor (e.g. Notepad) to edit an XML document.

2. Using a tool such as File Explorer, browse to the DSS installation folder. Within the installation folder, browse to the file
   Hewlett-Packard\HP Digital Sending Software\FileSystems\Product\Dss\Configuration\HP.Dss.App.Utilities.TwoServerAuthentication.xml.

   To open this XML document, right-click on the filename and select "Open with…" and then "Notepad." At the beginning of the document is a comment section that explains all of the values used to enable two-server authentication.

XML documents contain many types of information, but for our purpose we only need to edit certain values. These values are stored in an "attribute" in the format "<attribute>value</attribute>". The attribute is simply a way of identifying the purpose of the value, and it provides a way for other applications to retrieve a specific value from the document. The two-server XML document contains values that DSS uses to connect to the LDAP server and retrieve user information. The following values (in bold) can be set for LDAP queries.

3. Edit the values for the following attributes to match your LDAP server configuration
   <UseConfigFile>
   If you wish to enable two-server authentication you must set this value to true.
   `<UseConfigFile>`**`true`**`</UseConfigFile>`

   To disable two-server authentication set this value to false.
   `<UseConfigFile>`**`false`**`</UseConfigFile>`

   <Server>
   The IP address or host name of the LDAP server.
   `<Server>`**`servername`**`</Server>`

   <Port>
   The port is determined by the LDAP server. DSS needs to use the same port number for communicating as the LDAP server is using. This is typically 389, or if your server uses SSL it is often 636.
   `<Port>`**`389`**`</Port>`

<BindMethod>

The Bind Method is used to indicate if the LDAP server requires credentials (user name and password).

Possible values for the BindMethod attribute:

anonymous	No username and password are required for this server
simple	Username and password are required, and connection is not encrypted
simple-over-SSL	Username and password are required, and connection is encrypted using SSL (recommended)
windows-negotiated	Domain, username, and password are required. Uses the Windows Negotiated protocol (SPNEGO) to authenticate to the LDAP server.

```
<BindMethod>anonymous</BindMethod>
```

<UserName>

The username used to authenticate to the secondary LDAP server. UserName is only required if the BindMethod is not anonymous, and you want to use common LDAP credentials instead of the credentials entered by the user at the device control panel. If a UserName is not supplied in the XML document then the user's credentials are used for LDAP authentication.

If the BindMethod is anonymous then leave the UserName blank.

```
<UserName></UserName>
```

If the BindMethod is not anonymous, and you want to use common credentials then provide an LDAP username.

```
<UserName>ldapuser</UserName>
```

<Password>

The password associated with the UserName used to authenticate to the LDAP server. Password is only required if the BindMethod is not anonymous, and you want to use common LDAP credentials instead of the credentials entered by the user at the device control panel. If a Password is not supplied in the XML document then the user's credentials are used for LDAP authentication.

If the BindMethod is anonymous then leave the Password blank.

```
<Password></Password>
```

If the BindMethod is not anonymous, and you want to use common credentials then provide an LDAP password.

```
<Password>ldappassword</Password>
```

<Domain>

The domain associated with the UserName value. The domain is only needed if BindMethod is windows-negotiated, and you want to use common LDAP credentials instead of the credentials entered by the user at the device control panel. If a Domain is not supplied in the XML document then the user's domain is used for LDAP authentication.

If the BindMethod is not windows-negotiated then leave the Domain blank.

```
<Domain></Domain>
```

If the BindMethod is windows-negotiated then provide the Windows domain.

```
<Domain>ldapdomain</Domain>
```

<BindRoot>

The BindRoot value is the root LDAP directory location to start a search for user information. Multiple search roots are not supported in DSS 5.01. A typical value might look like "o=companyname.com".

```
<BindRoot>o=hp.com</BindRoot>
```

<UserMappingMethod>

UserMappingMethod defines how the user name entered at the device control panel will be formatted to match the LDAP directory.

as-entered	Search for the username as entered at the device
domain-slash-username	Search for Domain\UserName. Only valid for Windows user accounts
domain-colon-username	Search for Domain:UserName. Only valid for Windows user accounts
exchange-sid	Search for Security Identfier (SID) formatted as text (Exchange default). Only valid for Windows user accounts
active-directory-sid	Search for Security Identifier (SID) stored in a binary format (Active Directory default). Only valid for Windows user accounts

```
<UserMappingMethod>as-entered</UserMappingMethod>
```

<UserSearchMatch>

The LDAP attribute used to search for a user's directory entry.

```
<UserSearchMatch>cn</UserSearchMatch>
```

<EmailMatch>

This is the LDAP attribute that contains the user's email address.

```
<EmailMatch>mail</EmailMatch>
```

<DisplayNameMatch>

This is the LDAP attribute that contains the user's display name (or formal name).

```
<DisplayNameMatch>displayName</DisplayNameMatch>
```

4. Save the XML document
   If you are using Notepad, click File, Save.
   Then exit the text editor.
5. Close the DSS Configuration Utility
6. Restart the DSS service

Sample Configuration File

Sample XML document using anonymous LDAP authentication

```
<TwoServerAuthenticationSettings xmlns="TwoServerAuthenticationSettings"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="TwoServerAuthenticationSettings
../../../TwoServerAuthenticationSettings.xsd&gt;">
   <UseConfigFile>true</UseConfigFile>
   <Server>servername</Server>
   <Port>389</Port>
   <BindMethod>anonymous</BindMethod>
   <UserName></UserName>
   <Password></Password>
   <Domain></Domain>
   <BindRoot>bind root</BindRoot>
   <UserMappingMethod>as-entered</UserMappingMethod>
   <UserSearchMatch>cn</UserSearchMatch>
```

```
   <EmailMatch>mail</EmailMatch>
   <DisplayNameMatch>displayName</DisplayNameMatch>
</TwoServerAuthenticationSettings>
```

Sample XML document using Windows Negotiated authentication

```
<TwoServerAuthenticationSettings xmlns="TwoServerAuthenticationSettings"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="TwoServerAuthenticationSettings
../../../TwoServerAuthenticationSettings.xsd&gt;">
   <UseConfigFile>true</UseConfigFile>
   <Server>servername</Server>
   <Port>389</Port>
   <BindMethod>windows-negotiated</BindMethod>
   <UserName>publicname</UserName>
   <Password>Pa$$w0rd</Password>
   <Domain>ldapdomain</Domain>
   <BindRoot>o=hp.com</BindRoot>
   <UserMappingMethod>domain-slash-username</UserMappingMethod>
   <UserSearchMatch>cn</UserSearchMatch>
   <EmailMatch>mail</EmailMatch>
   <DisplayNameMatch>displayName</DisplayNameMatch>
</TwoServerAuthenticationSettings>
```

Summary

There should only be a small percentage of network environments where this two-server authentication process is necessary. Most Windows Active Directory installations contain the necessary user information (email address and display name), and are therefore sufficient to fully authenticate the user at the device control panel. However, this two-server authentication method is being provided in DSS 5.01 for backward compatibility with existing 4.x and 4.25.xx versions.

Document Attributes
Author: David O'Hara, David Lerman HP IPG Technical Marketing
Product Models: HP Digital Sending Software 5.01