SSO Configuration

How-to Guide
The Pulse Secure Access Gateway supports multiple options for single sign on (SSO) to reduce the number of times end-users must login to internal sites. This guide will focus on the following options:

1. Basic authentication
2. NTLM
3. Kerberos
4. Form POST

Pre-requisites shared by all four of these methods:

1. The same username is used for the Pulse Secure Access Gateway (SA) login and the internal application
2. Static password is entered as part of the user login to the SA Gateway

Basic Authentication, NTLM, and Kerberos share a configuration page in which the SA administrator will enable the authentication methods to use for SSO. This page is found at Users > Resource Policies > Web > SSO > General.
The Kerberos option allows definition of the realm, sitename, and pattern list if it is desired to override the value sent by the server. IVE intermediation is the option that will be used to send the credential. The default is “System” and it consists of the primary username and password. This can be overridden to static credentials OR variable credentials. The variable credential option is needed if using secondary username (\<USERNAME[2]\>) and password (\<PASSWORD>[2]\>) values or if other modification is needed to the default values of \<USERNAME\> and \<PASSWORD\>. For example, if the authentication does not include a domain but it is needed, this would need to be considered. For example, the domain is “Pulse Secure” the username could be constructed as Pulse Secure\<USERNAME\>. Constrained delegation is covered in a separate document due to the requirement for backend server modifications that are outside the scope of this document.

The options for NTLM and Basic authentication SSO also have the same default configuration. When a new instance is needed, a label is required as it is used to define the policy. If a specific option is not enabled, it will not be possible to use the defined labels, for example in the screenshots above only NTLM and Kerberos are enabled.

The policy to apply the SSO type and label credentials is configured at Users > Resource Policies > Web > SSO > Kerberos/NTLM/Basic Auth. In order to create a policy, a name is needed; the resource text field will contain the servers/specific paths that should have the credentials applied.