
Sterling External Authentication Server Field Definitions

This document provides screen-by-screen definitions and usage for each field in Sterling External Authentication Server. Use this document to:

- ◆ Look up a field by name using the Find function (Edit>Find or Ctrl+F).
- ◆ Look up a set of fields by screen / functionality using the bookmarks on the left.

For additional information, return to the main page of the [Sterling External Authentication Documentation Library](#).

Login

Following are the field definitions for the login screen. For additional information, refer to Start and Stop EA on UNIX or Start and Stop EA on Window on the [Sterling External Authentication Documentation Library](#).

Basic Login

Following are the field definitions for the basic login screen:

Field Name	Description
Host	Host name or IP address of the EA server.
Port	Port number defined during installation. Default=61365.
User	User name. Default=admin. Change the user name and password after the first login.
Password	Password of user. Default=admin.

Create SSL/TLS Configuration

After you login the first time, you can configure the connection between the GUI and the server to require SSL or TLS. For more information, refer to Create and Manage System Certificates on the [Sterling External Authentication Documentation Library](#).

Complete the following parameters to configure SSL or TLS:

Field Name	Description
SSL/TLS	Available only after you set up certificates on the GUI and server, and configure the secure listener. Click SSL/TLS to enable SSL/TLS between the server and GUI.
Config	After setting up the certificate files, click Config to specify the path for key store and truststore files.
Keystore File	File that contains the private keys and matching key certificates used for SSL and TLS sessions. Each key/certificate pair in the keystore has an associated alias. The secure listener and connection definitions that specify SSL/TLS use the alias to reference the key/certificate.
Keystore Password	Password of the keystore file.
Trust Store File	Location where the system and CA certificates are stored. These certificates verify that a certificate received from a server is signed by a trusted source.
Trust Store Password	Password of the trust store file.

Certificate Validation Definitions

For SSL or TLS authentication, the connection between Sterling External Authentication Server and the client application is authenticated. Then, the client application sends a request with a certificate chain and/or a user ID and password. EA uses the certificate validation to perform the authentication. For more information, refer to Configure a Certificate Validation (CV) definition on the [Sterling External Authentication Documentation Library](#).

From the Certificate Validation Definitions window, click + to create a new certificate validation definition. On the General screen, specify the following parameters:


Parameter	Description
Name	Used by the client application to reference this definition. Can be up to 255 alphanumeric characters, including space, underscore (_), and period (.).
Description	Description to help administrators determine when to use this definition.
Clock tolerance	How much time the EA clock can vary from the certificate clock. Default=0 minutes.
Expiration grace period	How many hours after a certificate expires that Sterling External Authentication Server can accept it. Default is 0 hours. Accepting a certificate after it expires can prevent a shutdown. Note: If you do not continuously monitor logs for expired certificates and have no policies about shutdown based on certificate expiration, consider using the default setting of 0 hours.

Parameter	Description
Expiration warning	When to warn the user about a certificate expiration. Default=14 days.
CRL check required	Enable to require a CRL check.
Verify before certificate date	Enable to verify that the certificate is presented after the date of activation as defined in the certificate. For example, if this certificate can be used beginning November 5, the certificate presented on November 3 fails.
Verify after certificate date	Enable to ensure that a certificate will not be accepted after its expiration date. For example, If a certificate defines an after date of November 5 and this field is enabled, this certificate is rejected if presented on November 6.
Validate to root	Validate the certificate chain to the root certificate. If the request does not include the complete certificate chain, EA searches the trust store for the issuer certificates.
Validate to Trust Anchor	Validate all certificates in the request. At least one of these certificates must also be in the trust store. If not, the issuer of the last certificate in the request must be in the trust store or the request fails.
Validate using custom exits	Enables custom validation by exiting to a Java class, script, or program run from an operating system command. If you implement a custom exit in Java, review the description of the interface and a sample class in standard javadoc at <i>install_dir/doc</i> where <i>install_dir</i> is the installation directory.
Public key minimum key length	Minimum key length required for the certificate public key in order to validate the key.

Subject Verification Query

As part of a CV definition, you can define a subject verification query to define parameters to verify a certificate subject. Sterling External Authentication Server uses the certificate attributes specified in the subject verification query to automatically fill in related parameters.

Define the following parameters to specify how an LDAP query verifies a certificate subject:

Parameter	Description
Define query to verify certificate subject	Enable this option to verify the subject of a certificate using an LDAP attribute query. Define one of the methods below to verify the subject.
Search directory for certificate subject using these attributes	Search for a certificate that matches the defined certificate subject values: <ul style="list-style-type: none"> ◆ CN—Common Name ◆ OU—Organization Unit ◆ O—Organization ◆ L—City/Locality ◆ ST—State/Province ◆ C—Country (2-character abbreviation) ◆ UID—User ID
Certificate subject is a valid DN in directory	Verify that the certificate subject matches a Distinguished Name in a directory. If the subject is appended to the base DN, enable when appended to the following base DN and type the DN value.
Other	None of the previous options match the search criteria needed to verify certificate subjects. For this option, provide query parameters on the Query Parameters dialog.
Use defined connection	Enable user defined connection and specify a connection. Select a system-wide server connection you defined previously or click  to create a new connection definition.
Verify certificate matches certificate in directory	Perform a comparison of the certificate to the certificate stored in the directory entry. Define the name of the directory attribute for the certificate in the Certificate Attribute field. If the attribute listed is not correct, change it.

General Attribute Query

When you create a CV definition, you can define attribute queries and attribute assertions. The certificate validation definitions can include LDAP attribute queries for finding and checking specified data from a request against entries in a directory. Refer to Configure Attribute Queries and Assertions on the [Sterling External Authentication Documentation Library](#).

Click + to create a new attribute query definition and the General screen is displayed. On the General screen, specify the following parameters to define an LDAP attribute query definition:

Parameter	Description
Name	Name of the LDAP attribute query definition.
Description	Description of the definition.
Connection specification	<p>Specify the method to use to connect to the LDAP server:</p> <ul style="list-style-type: none"> ◆ Use globally defined connection—Use a connection definition that exists. Protocol, host, and port to connect to the LDAP server are populated. ◆ Use authenticated user's connection—Only available for attribute queries within LDAP authentication definitions. The query is submitted over the bound session created when the user in the authentication request is authenticated. This prevents the need to perform an additional bind operation to the LDAP server, or to specify login credentials or other parameters required to perform the bind. For the query to succeed, the user must have read permissions over the scope of the search specified by this query definition. ◆ Define connection info with query—Specify protocol, host, and port on the Query Parameters screen that follows.
Query specification	<p>Specify the query specification to use for the definition:</p> <ul style="list-style-type: none"> ◆ Specify query parameters—Manually define the parameters to use in the query. ◆ Specify query as URL—Provide a URL to perform the LDAP attribute query. Use a valid LDAP URL format as illustrated below: ldap://host:port/BaseDN?Attributes?Scope?SearchFilter Paste the URL into the text box and confirm that the URL includes the elements to perform the query.

Query and LDAP Parameters

The LDAP parameters dialog specifies an LDAP search operation to locate directory entries and optionally return attributes from those entries. The search must succeed for certificate validation or CRL checking to succeed. Specify all query parameters in a URL by specifying parameters individually on the Query Parameters screen.

Define the following parameters to specify LDAP parameters:

Parameter	Description
Protocol	Protocol used to connect to the LDAP server: ldap:// (nonsecure) or ldaps://(secure).
Host	Host name of the LDAP server.
Port	Port number to use to connect to the LDAP server.
Base DN	Starting point in the directory to begin the search.

Parameter	Description
Return Attributes	Attribute types to return from the entries that match.
Scope	Starting point when performing the search. Specify one of the following options: <ul style="list-style-type: none"> ◆ Base—Search at the level of the Base DN. This retrieves data from a known entry in the directory. Specify Sterling External Authentication Server variables to represent this element. ◆ One Level—Search only the level immediately below the Base DN. ◆ Sub Tree—Search the entire sub-tree below the Base DN.
Match Attributes	Search filter used to determine which directory entries are a match. The search filter (see RFC 2254) can be very complex, but defines one or two attribute names and their expected values. You can specify Sterling External Authentication Server variables to represent this element.
Query Timeout	How long in minutes and seconds (format MM:SS) before the LDAP attribute query times out and processing ends.

LDAP Connection Definition

Specifying system-wide server connections saves time and reduces errors that could occur when parameters are entered manually. You can create an LDAP connection definition or an HTTP connection definition to define system-wide connections.

Specify the following parameters to connect to the LDAP server:

Parameter	Description
Name	Name of the connection, up to 255 characters to include alphanumeric characters and space, underscore (_), or period (.).
Description	Description of the connection definition.
Protocol	Protocol to use. For a clear text connection, select ldap://. For SSL, select ldaps://.
Host	Host name of the LDAP server.
Port	Port number to connect to the LDAP server.

Parameter	Description
Authentication Method	Select the method to use to authenticate the security principal: <ul style="list-style-type: none"> ◆ None—Not allowed; do not use it. ◆ Simple—Authenticate the password against the password in the directory. ◆ Digest-MD5—Modify the password to Digest-MD5 and then authenticate against the Digest-MD5 encrypted password in the directory. This method transmits message digests over the network instead of a clear text password. ◆ CRAM-MD5—Modify the password to CRAM-MD5 and then authenticate against the CRAM-MD5 encrypted password in the directory. This method transmits message digests over the network instead of a clear text password. ◆ GSSAPI—Use Kerberos V authentication. This is the native authentication used in Active Directory. ◆ External—Not allowed; do not use it.
Principal Name	Security principal to use in the bind operation to the LDAP server. Note: The principal name is displayed as a formula with appropriate details already filled in based on a previous entry or selection for LDAP authentication or an LDAP attribute query parameters.
Principal Password	Password to use for the security principal. It is the password from the authentication request.
Client Key Certificate Alias	The key certificate from the system keystore during SSL or TLS with the LDAP server when client authentication is enabled. Disabled unless the protocol is ldaps://, or the Start TLS option is set to Yes.
LDAP Version	LDAP protocol version. Select one of the following values from the list: <ul style="list-style-type: none"> ◆ 2—Use LDAP version 2. ◆ 3—Use LDAP version 3.
Start TLS	Whether to request TLS encryption using the LDAP v3 extended operation.
Referral Action	Action to take when a request is referred by an LDAP server to another. <ul style="list-style-type: none"> Follow—Follow the referral to the referred directory. Ignore—Ignore the referral. Throw—Ignore the referral and generate an exception.
Advanced option - JNDI Properties	JNDI property names and values if the JNDI service provider bundled with the JRE requires any special properties. Click <input type="button" value="..."/> to specify properties.

Attribute Assertion Definitions

You can create an attribute assertion definition to specify a Boolean statement that must evaluate as true in order for the authentication request or certificate validation request from a client application to succeed. Attribute assertions allow the specification of additional conditions and can compare

details from the request to fixed data or to attributes returned from queries. Refer to [Configure attribute queries and assertions on the Sterling External Authentication Documentation Library](#).

Click + to create a new attribute assertion definition and the General screen is displayed. On the General screen, specify the following parameters to define an attribute assertion definition:

Name	Description
Assertion Name	Name to assign to the attribute, up to 255 alphanumeric characters. Special characters allowed are space, underscore (_), and period (.).
Description	Description of the assertion you are defining.
Assertion	Variables and expressions to create the assertion you want to evaluate. String data must be enclosed in variables. Use the following operators: <ul style="list-style-type: none"> == Equality > Greater than >= Greater than or equal != Inequality < Less than <= Less than or equal && Logical and Logical OR ! Logical NOT () Parenthesis for grouping true Boolean TRUE (case sensitive) false Boolean FALSE (case sensitive)

CRL Definition

Create Certificate Revocation List (CRL) definitions to access information required to download published CRLs. Published CRLs validate certificates and determine if a certificate has been revoked. During certificate validation, Sterling External Authentication Server checks any CRLs referenced in the CV definition to determine whether a certificate has been revoked. To create a CRL definition, click **Manage>CRL Definitions**. Refer to [Configure a certificate revocation list definition on the Sterling External Authentication Documentation Library](#).

General CRL

Specify the following parameters to define a CRL definition:

Parameter	Description
CRL Definition Name	Name assigned to the CRL definition.
Description	Description of the CRL.
Cache CRL	Save the CRL to a local cache and prevent the need to load the CRL for every validation request. Specify the following options: <ul style="list-style-type: none"> ◆ Refresh cache on CRL next update—CRL stored in cache is refreshed on the next CRL publisher update. ◆ Refresh cache at interval—How often to refresh the CRL stored in cache, in minutes.
Refresh CRL on every check	Refresh the CRL on each validation request.
Clock Tolerance	How much difference in seconds between the Sterling External Authentication Server server and the CRL clock.
Reject expired CRL	Reject an expired CRL when a CV definition requires a CLR check. Regardless of this setting, a revoked certificate results in failure of the certificate validation.
Verify Signature	Verify the signature of the CRL. To be verified, the certificate of the CRL issuer must be included in the system trust store or must be one of the certificates in the certificate chain in the validation request.

CRL Query General

On the Query General screen, select one of the following options to identify how to connect to the server where the CRL is published and how to query for the list:

Parameter	Description
Use defined connection	Select a system-wide connection definition from the drop-down list.
Specify query parameters	Define the connection to the server as you specify query parameters.
Specify query as URL	Specify a URL to query where the CRL is stored. Specifying the query as a URL is convenient when you can copy and paste the appropriate URL. Verify that the URL for an LDAP server includes the appropriate parameters.

Supported Extensions for a CV Definition

The KeyUsage, BasicConstraints, and CRLDistributionPoints certificate extensions are supported in Sterling External Authentication Server. These extensions are listed with the corresponding object identifiers (OID) and names on the Supported Extensions dialog. For detailed information on supported extensions, refer to Manage X.509 extensions on the [Sterling External Authentication Documentation Library](#).

Use the parameters on this dialog to define or modify a supported extension:

Parameter	Description
OID	Object identifiers associated with an extension. This cannot be changed
Name	Name of the custom extension. This cannot be changed.
Value	Value associated with the custom extension.
Allowed	Enable Allowed if the extension defined can be present in a certificate. Validation fails if the extension in the certificate does not match the value defined in the extension.
Required	Enable this option if the certificate must include the extension. Validation fails if the extension is not in the certificate. Disable both Allowed and Required to reject an extension.

Custom Extension for a CV Definition

The Custom Extensions dialog displays custom extensions that are defined. When the CV definition is used and custom extensions are defined, the certificate validation searches for the custom extension. Refer to Manage X.509 extensions on the [Sterling External Authentication Documentation Library](#).

Use the parameters on this dialog to define or modify a custom extension:

Parameter	Description
OID	The object identifier associated with a custom extension.
Name	Name of the custom extension.
Value	Value associated with the extension.
Allowed	Enable Allowed if the extension defined can be present in a certificate. Validation fails if the extension in the certificate does not match the value defined in the custom extension.

Parameter	Description
Required	Enable this option if the certificate must include the extension. Validation fails if the extension is not in the certificate.
	Disable both Allowed and Required to reject an extension.

LDAP Authentication Definitions

Authentication definitions configure multi-factor authentication using SSL client certificates, SSH keys, user ID and password, or client IP address as factors. Authentication definitions specify how Sterling External Authentication Server authenticates a security principal when a client application sends a request for authentication. Authentication definitions include parameters for connecting to a server, the authentication principal, and authentication method. An authentication definitions specifies parameters that Sterling External Authentication Server uses when accessing directories, including attribute queries, attribute assertions, and application-specific outputs required to perform authentication. An authentication definition can defined for all of the protocols including LDAP, TAM, SSH, and a generic definition. Refer to [Configure an LDAP authentication definition on the Sterling External Authentication Documentation Library](#).

LDAP Authentication

Define the following parameter for an LDAP authentication definition:

Parameter	Description
Profile name	Name of the definition, up to 255 characters to include alphanumeric characters and space, underscore (_), or period (.), included in the request from a client application.
Description	Description of the authentication definition.
Authentication type	Select LDAP as the authentication type.
Protocol	Protocol to use. For a clear text connection, select ldap://. For SSL, select ldaps://.
Host	Host name of the LDAP server.
Port	Port number to connect to the LDAP server.

Parameter	Description
LDAP principal to bind	<p>Security principal used to bind to the LDAP server. This value is frequently the DN (Distinguished Name) of the user entry with the user ID. The option depends on the LDAP server and authentication used.</p> <ul style="list-style-type: none"> ◆ User ID from request—Bind to the LDAP server using the client user ID from the authentication request. Use this option if the client application presents the user ID in a form that can be used in the bind request. Some Simple Authentication and Security Layer (SASL) implementations may require a user ID rather than a DN. ◆ Search for user DN—Search for the directory entry that contains the user ID in the authentication request. This is usually in the CN or UID attribute of the directory entry, depending on the object class used for user entries by the directory. The DN of this entry is used as the security principal for the bind operation. The default search filter is <code>CN={userId}</code>, where <code>{userId}</code> is a variable representing the user ID from the authentication request. If the directory entry uses an attribute other than CN to store the user ID, use that attribute (for example, UID). ◆ Specify user DN—Bind using the DN specified. This option can only be used if the name of the directory entry contains the user ID to be authenticated. Specifically, the attribute value of the RDN of the user entry must match the user ID received in the authentication request; typically, this is the Common Name (CN) attribute. <p>If you select this option, you specify the DN for the principal in the two fields that follow. Information pre-populated in the fields indicates how to specify the DN. Use the format: <code>cn={userId}, base DN</code>, where: <code>cn</code> is the attribute used to name the entry, <code>userId</code> is the user ID from the authentication request, and <code>base DN</code> is a comma-delimited list of RDNs (Relative Distinguished Names) that represents the parent of the user entry.</p> <ul style="list-style-type: none"> ◆ DN from Certificate Validation—Bind using the DN returned from the subject verification query. Valid when Sterling External Authentication Server authenticates in continuation of certificate validation and the certificate validation includes a subject verification query. ◆ Other principal format—Bind to the LDAP server using the security principal specified by the expression you type in the text field. You can use Sterling External Authentication Server variables.

Define LDAP connections setting. Refer to *LDAP Connection Definition* on page 6.

LDAP Application Output Definition

Create an Application Output definition when you need to perform an query and return login credentials for user authentication to the client application. Lookup `loginCredentials` is an option you select in an Application Output definition. It returns login credentials to the client application.

The following parameters can be defined for an SSH application output definition:

Parameter	Description
Application Feature	Select the output definition to use: <ul style="list-style-type: none"> ◆ To query the Sterling Commerce loginCredentials directory object, select Lookup loginCredentials (Sterling). ◆ To query any other directory object, select Lookup loginCredentials (Custom).
Query	Allows you to create a query that returns attributes mapped to application output. Enable the Use globally defined connection option.

Change Password Settings

Define the following parameters to configure how password settings can be changed:

Parameter	Description
Profile can be used to change password	Enable this option to enable the ability for the user to change his password. Default=disabled.
Warn users when password about to expire	Enable this option to send a warning to the user that the password is close to expiration. This is only available when the Directory server is IBM Tivoli Directory Server or Microsoft Active Directory.
Number of days before warning	Type how many days before the password expires to begin notifying the user.
Use globally defined connection	The globally defined LDAP connection definition to use for the Directory server.

Tivoli Access Manager (TAM) Authentication Definition

Sterling External Authentication Server provides an authentication service to interface with Tivoli Access Manager (TAM). The TAM authentication service provides user ID/password authentication and/or user DN authentication through TAM. DN authentication allows you to authenticate the subject of a certificate received during certificate validation. The TAM authentication service can also provide application-level authorization for accessing a destination service specified in the authentication request and provide credential lookup for logging in to the destination service. Refer to [Configure Tivoli \(TAM\) authentication definitions on the Sterling External Authentication Documentation Library](#).

Tivoli Access Manager Authentication Definition

Complete the following parameters to create a Tivoli Access Manager (TAM) authentication definition:

Parameter	Description
Profile name	Name for the Tivoli Access Manager authentication definition. Profile names can be up to 255 alphanumeric character, including space, underscore (_), and period (.).
Description	Description of the authentication definition.
Authentication type	Select TAM to display the Tivoli Access Manager Authentication dialog.
TAM config file URL	URL to the TAM configuration file. It contains an SSL key and configuration data for secure communications with the authorization server. For example, the file:///home/SeasAdmin/tam/config_file.conf specifies a local configuration file.
Target JRE location	Path to the Java Runtime Environment where the TAM API is installed. For example, specify the location /home/SeasAdmin/java/j2sdk1.4.2_12 for a JRE location. Note: TAM requires JRE version 1.4.2.
TAM user to authenticate	<p>Enable the methods to determine which TAM user to bind for authentication:</p> <ul style="list-style-type: none"> ◆ User ID from request—User ID in the authentication request must be a user in the TAM user registry. ◆ Certificate subject DN—A follow-up authentication request to a previous certificate validation request. The certificate subject DN from the validation request is the security principal passed to the TAM API for authentication. When this option is selected the password and/or user ID are only required if specified by the corresponding options. Doing so provides a form of multi-factor authentication. The user ID and password from the request must match those associated with the user entry corresponding to the certificate subject DN. ◆ Other—Supports specification of the security principal as a reference to an attribute query; for instance, to use the DN returned from an LDAP search for a certificate subject. <p>For example, in the variable expression, {attr[VerifyCertSubject].dn}, VerifyCertSubject is the attribute query name used to locate the subject of the certificate in the directory:</p> <p>The password and/or user ID are only required if specified by the corresponding options. Doing so provides a form of multi-factor authentication. The user ID and password from the request must match those associated with the user entry corresponding to the security principal specified.</p>
User ID required	The authentication request must specify a user ID. Enable this option to require both a certificate and a user ID as a form of multi-factor authentication.
Password required	The authentication request must specify a password. Enable this option to require both a certificate and password as a form of multi-factor authentication.

Parameter	Description
Authorize access to Destination Service	<p>Authorize the user to access the destination service requested. Specify the TAM resource of the destination service and the access permissions to be authorized.</p> <p>The default resource is <code>/SEAS/profileName/{dstsvc}</code>, where <i>profileName</i> is the profile the client application uses to access the TAM authentication definition, and <i>dstsvc</i> is a variable. The default resource suggests the setup of a protected object space, SEAS in the TAM secure domain specified in the TAM configuration file for the API and a protected resource to correspond to each destination service that the client application can request access to.</p> <p>You can specify any valid resource name in the secure domain. The default requested permissions are Traverse and view (Tv). Specify any valid permissions, that reflect the access anticipated by the client application for this resource.</p>

Application Outputs for TAM

The application output for TAM authentication is implemented using TAM GSO resource credentials. Complete the following parameters to create an application output definition for TAM:

Parameter	Description
Return TAM credentials	<p>When Sterling External Authentication Server requests authentication for a security principal, the TAM API returns a credential object that applications may need for additional interaction with TAM.</p> <p>For example, if single sign-on solutions are implemented, a related credential is required for access. Select this option to return this credential to the client application.</p>
Return Destination Service login credentials	<p>Select this option to return the credentials for logging in to a destination service.</p> <ul style="list-style-type: none"> ◆ Look Up GSO resource—Look up the Global Sign On (GSO) resource from the TAM user registry. Specify the resource in the Resource name field. The default value is the variable, <code>{destination service}</code>. The variable <code>{destination service}</code> resolves to the destination service name in the authentication request. ◆ Return user ID and password from request—Return the User ID and Password received in the authentication request. ◆ Return user ID from request and the following password— Return the User ID from the request and the password you specify in the text field. ◆ Other—Return credentials specified in mapped Uid (user ID) and Pwd (password) or in the Mapped SSH Key. This option supports the use of LDAP lookup credentials that are identical to those in the application output wizard of the LDAP authenticator.

SSH Authentication Definition

Create an SSH key authentication definition to identify how to authenticate an SSH user connecting to SSP, using EA. Before creating a definition, define a global connection setting for the LDAP

server. Select the assertion definition to use with the definition. It matches the public key from the request against the keys returned by the SSH public key lookup query. A preconfigured assertion called `VerifySSHPublicKey` is provided with EA. It uses the `openssh` schema to store the public keys. Use this SSH assertion definition or define your own. If you do not use the `openssh` schema, edit the assertion definition and reference the schema used. Refer to [Configure an SSH key authentication and mapping definition on the Sterling External Authentication Documentation Library](#).

SSH Key Authentication Definition

Use this dialog to create an SSH key authentication definition and identify how to authenticate an SSH user connecting to SSP and using EA:

Parameter	Description
Profile name	Profile name to include in the request for the client application, up to 255 alphanumeric characters and spaces, underscores (_), and periods (.).
Description	Description of the authentication definition.
Authentication type	Select SSHKEY as the authentication type.

Define LDAP attribute query definitions and Attribute Assertion definitions. Refer to *General Attribute Query* on page 4 and *Attribute Assertion Definitions* on page 7.

SSH Application Output Definition

Create an SSH Application Output definition when you need to perform an SSH user and key query and return login credentials for user authentication to the client application. Lookup `loginCredentials` is an option you select in an Application Output definition. It returns login credentials to the client application.

The following parameters can be defined for an SSH application output definition:

Parameter	Description
Application Feature	Select the output definition to use: <ul style="list-style-type: none"> ◆ To query the Sterling Commerce <code>loginCredentials</code> directory object, select Lookup loginCredentials (Sterling). ◆ To query any other directory object, select Lookup loginCredentials (Custom).
Query	Allows you to create a query that returns attributes mapped to application output. Enable the Use globally defined connection option.

JAAS Authentication Definition

Select the JAAS authentication definition to create a Java Authentication and Authorization Service (JAAS) as a user authentication method. JAAS extends the Java security model to perform checks based on the identity of the user. EA uses JAAS to authenticate users with RSA SecurID or Active Directory credentials. Refer to Configure JAAS authentication definitions on the [Sterling External Authentication Documentation Library](#).

JAAS Key Authentication Definition

Use this dialog to create a JAAS authentication definition and identify how to authenticate a user connecting to SSP and using EA:

Parameter	Description
Profile name	Name of the RSA authentication definition provided by the client application, up to 255 alphanumeric characters and spaces, underscores (_), and periods (.).
Description	Description of the authentication definition.
Authentication type	Select JAAS as the authentication type.
JAAS Module Name	JAAS Authentication Scheme to use. Option available is: <ul style="list-style-type: none"> ◆ RSA SecurID with LDAP fallback—Use RSA to authenticate the user. If RSA is not available, use LDAP. Use this option if you are migrating to RSA.

RSA Authentication Definition

Select the RSA SecurID authentication definition to create RSA as a user authentication method. Refer to Configure RSA SecurID authentication definitions on the [Sterling External Authentication Documentation Library](#).

Use this dialog to create an RSA SecurID authentication definition and identify how to authenticate a user connecting to SSP and using EA:

Parameter	Description
Profile name	Name of the RSA authentication definition provided by the client application, up to 255 alphanumeric characters and spaces, underscores (_), and periods (.).
Description	Description of the authentication definition.
Authentication type	Select RSA SecurID as the authentication type.

Generic Authentication Definition

Refer to Configure Generic authentication definitions on the [Sterling External Authentication Documentation Library](#).

Generic Authentication




To create a generic authentication definition, specify the following parameters on the Authentication Definitions window:

Parameter	Description
Profile name	Name for the authentication definition, up to 255 alphanumeric characters, space, underscore (_), or period (.). It is included in the request from a client application
Description	Description of the authentication definition.
Authentication type	Select Generic as the authentication type.
User ID required	The authentication request must include a user ID.
Password required	The authentication request must include a password.
Authenticate using custom exits	Perform authentication using a custom exit. Click <input type="button" value="..."/> to specify the Java class or OS command to perform the authentication and other details of the exit.

Custom Exit

Sterling External Authentication Server allows you to use a Java class or operating system command to implement a custom exit from a CV definition or generic authentication definition. The custom exit dialog is displayed if you select **Validate using custom exits** from the General dialog. Using a Java class requires that you implement the Sterling-provided interface called SEASCUSTOMEXITInterface.

Define the parameters on this dialog to specify a Java class or operating system for a custom exit:

Parameter	Description
Java class	<p>Use a Java class to implement a custom exit that implements SEASCustomExitInterface. If you specify this option define the following parameters:</p> <ul style="list-style-type: none"> ◆ Class name—The fully-qualified class name in the format <i>packageName.className</i> when you specify the custom exit class ◆ Properties—Click  on the Properties dialog, specify the name and value for each property required to initialize the custom exit class. Use  and  to add or remove and value pairs.
Native OS command	<p>Enable this option to use a native operating system command as a custom exit. If you specify this option define the following parameter:</p> <ul style="list-style-type: none"> ◆ Command line—The operating system command to use, including all command line arguments. Provide a user ID and password as variables on the command line.
Pass certificate chain to OS command via	<p>Specify how to send the certificate chain to the operating system command. Select one of the following options:</p> <ul style="list-style-type: none"> ◆ Certificate file—Send the certificate chain as a certificate file. Provide the File name and File format as PEM or DER. To remove the certificate file after the custom exit is complete, enable Delete file after exit. ◆ Click Standard input (PEM format) to send the certificate chain through the standard input stream.
Run default validator after exit	Continue processing the authentication validation definition after the custom exit.
Run custom exit synchronously	<p>Enable synchronous use of this custom exit.</p> <p>When a client application sends an authentication request with a custom exit, current exit processing must complete before a subsequent program can run.</p>
Standard error log level	How errors from the custom exit is logged. All error output is logged in SEAS.log. Set the log level to meet your reporting needs.
Standard output log level	How output from the custom exit is logged. Standard output is logged in SEAS.log. Set the log level to meet your reporting needs.

Parameter	Description
Log Level	Set the log level. Log levels include: <ul style="list-style-type: none"> ◆ INFO—Errors, warnings, and informational messages are logged. Default. ◆ WARN—Errors and warnings are logged. ◆ DEBUG—Includes INFO and additional information useful for debugging. ◆ ERROR—Only errors are logged. ◆ TRACE—Details will be captured according to Connect:Direct Trace operation (logging in conjunction with the Trace command). ◆ OFF—Turns off logging so that no server information is captured.
Log output from stderr to response message	Send the error log output to the response message.
Log output from stdout to response message	Send the output log output to the response message.

Generic Application Outputs

Complete the following parameters to create a generic application output definition:

Parameter	Description
Mapped Uid	Return credentials specified in the mapped Uid (user ID). This option supports the use of LDAP lookup of credentials.
Mapped Pwd	Return credentials specified in the mapped Pwd (password).
Mapped SSH Key ID	Return credentials specified in the mapped SSH key ID (key).

To define attribute assertion definitions, refer to *Attribute Assertion Definitions* on page 7.

Check and Confirm Parameters

Because definitions can include a variety of elements, check that all parameters are set correctly before you save the definition. After you create a definition, review the list of parameters displayed on the Confirm screen. If you find a parameter that is not correct on the Confirm screen, click **Back** to navigate through parameters. Access **Help** as needed to make the corrections required. After you make corrections, click **Next** to move forward to the Confirm screen and save. When you edit a definition, review the parameters listed on the **Summary** tab to identify the area that requires a change. Then, click the appropriate tab to make corrections to the parameters that are editable.

Variables for Certificate Validation Requests

This section describes the variables you can use in definitions associated with certificate validation requests. These variables represent data from the certificate validation request as well as the results of various operations performed during the certificate validation process. Refer to Variables for certificate validation requests on the [Sterling External Authentication Documentation Library](#).

The following table lists the variables used in certificate validation requests:

Variable	Description
Attr	Root node representing the results of all attribute queries.
Cert	Raw data of the end entity X.509 certificate received in the certificate validation request and the root node of all certificate variables, such as subject and issuer. This variable can be referenced in an attribute assertion statement to perform a binary compare of the certificate received in a request with the certificate returned from an attribute query.
ClientID	Client ID in the request. This variable depends on the client application. For example, if the client application is Connect:Direct, the client ID is the node name. If the client application is Sterling Secure Proxy, the client ID is the adapter name.
Exit	Root node containing any output variables set by a custom exit.
Ext	The X.509 V3 extensions of the end entity certificate, serving as the parent node of each extension variable. See Using X.509 Extensions, for details.
ipAddress or IP	<p>IP address in the request, formatted in dotted decimal notation, with leading zeros omitted. Include this variable to use the IP address from the client application as an authentication factor.</p> <ul style="list-style-type: none"> ◆ v—Represents the IP version (either 4 or 6 in the request). ◆ x—Hexadecimal representation of the IP address. For example, if IP = 10.20.30.40, then IP.x=0x0a141e28. ◆ 0-3—Indices for individual nodes of the dotted decimal. For example, if IP = 10.20.30.40, then IP[0]=10, IP[1]=20, IP[2]=30, and IP[3]=40.

Variable	Description
Issuer	<p>Certificate issuer field of the end entity certificate, serving as the parent node of the following issuer attribute variables:</p> <ul style="list-style-type: none"> ◆ CN—Common Name ◆ L—Locality Name ◆ ST—State or Province Name ◆ O—Organization Name ◆ OU—Organizational Unit Name ◆ C—Country Name ◆ STREET—Street Address ◆ DC—Domain Component ◆ UID—User ID
Subject	<p>Represents the certificate subject field of the end entity certificate, serving as the parent node of the following subject attribute variables:</p> <ul style="list-style-type: none"> ◆ CN—Common Name ◆ L—Locality Name ◆ ST—State or Province Name ◆ O—Organization Name ◆ OU—Organizational Unit Name ◆ C—Country Name ◆ STREET—Street Address ◆ DC—Domain Component ◆ UID—User ID
ssl	<p>Variables associated with the SSL session the certificate validation request is authenticating. These variables include Server and Client.</p> <ul style="list-style-type: none"> ◆ Server—Indicates whether the certificate belongs to the server in the SSL session. Boolean variable set to true or false. ◆ Client—Indicates whether the certificate belongs to the client in the SSL session. Boolean variable set to true or false.

Variables for Authentication Requests

The variables in this section are valid when a client application sends an authentication request. If the authentication request is a continuation of a certificate validation request, then the variables set during certificate validation are also available to the authentication service. When multiple factors are checked for authentication, this feature allows correlation of the different factors, for instance,

to verify that the certificate subject is the same as the LDAP user. Refer to Variables for authentication requests on the [Sterling External Authentication Documentation Library](#).

The following table describes variables used in authentication requests.

Variable	Description
UserID	User ID received in the authentication request.
Password	Password received in the authentication request.
DestinationService or dstSvc	Destination service name received in the authentication request.
Principal	Authentication principal to be bound to the directory, after it is determined in the LDAP authenticator. Passed directly in the request or as the result of a directory search.
ipAddress or IP	IP address in the request, formatted in dotted decimal notation, with leading zeros omitted. Include this variable to use the IP address from the client application as an authentication factor. <ul style="list-style-type: none"> ◆ v—Represents the IP version (either 4 or 6 in the request). ◆ x—The hexadecimal representation of the IP address. For example, if IP = 10.20.30.40, then IP.x=0x0a141e28. ◆ 0-3—Indices for individual nodes of the dotted decimal. For example, if IP = 10.20.30.40, then IP[0]=10, IP[1]=20, IP[2]=30, and IP[3]=40.
ClientID	Client ID in the request. This variable depends on the client application. For example, if the client application is SSP, the client ID passed is the adapter name.
Exit	Root node containing any output variables set by a custom exit.

Manage System Settings Menu

Following are the field definitions for the settings option on the **Manage> System Settings** screen. Refer to Configure system resources on the [Sterling External Authentication Documentation Library](#).

Listeners Tab

The non-secure listener defines how a client application connects to Sterling External Authentication Server without requiring an SSL or TLS handshake. You must connect on the non-secure listener port the first time you login. After you set up the secure listener port, you can disable the non-secure listener.

Define the following parameters on the Listener screen to define non-secure and secure listeners:

Parameter	Description
Secure Listener	
IP Address	Client IP address to use to connect to EA.
Port	Port that the secure connection listens on. Default is 61366.
Keystore Alias	Alias in the keystore to identify the key certificate file associated with this listener.
Enabled	Enables secure listening on the port or IP address identified.
Non-Secure Listener	
IP Address	Client IP address to use to connect to EA.
Port	Port that the nonsecure connection listens on. Default is 61365.
Enabled	Enables a nonsecure connection on the port and address. After configuring the secure listener, disable this option to disable the non-secure port.

SSL Tab

The SSL keystore file stores the certificate used to connect to secure LDAP servers and to perform TLS/SSL negotiations with connecting client applications.

Define the following parameters on the SSL system settings screen to define how SSL secures LDAP servers:

Parameter	Description
Protocol	Protocol to use for all secure connections. System—Uses the default EA protocol. This is the default. SSLv3—Uses SSL version 3.0 (not valid for Linux). TLS—Uses TLS. JRE—Uses the protocol default of the JRE you are using for EA. Using the protocol default for the JRE is not valid for AIX.
Keystore File	Location of the keystore file on the computer that you are using to initiate a connection with the GUI.
Keystore Password	Password of the keystore file.

Trusted Certificates Tab

The trust store file contains the CA and self-signed certificates that authenticate secure connections to Sterling External Authentication Server from client applications and from EA to LDAP servers that it connects to, as well as to validate signatures on CRLs and certificates.

Define the following parameters on the Trusted Certificates tab to add certificates to the file:

Parameter	Description
Trust Store File	Trust store file on the computer where you initiate a connection with the GUI.
Trust Store Password	Password of the trust store file.

Globals Tab

Use the Globals tab to set the logging level, change the listener connection settings, and set the timeout for accepting an inbound connection or an outbound connection.

Following are the field descriptions for the global tab:

Level	Description
Logging Level	
INFO	Errors, warnings, and informational messages are logged. This is the default.
WARN	Errors and warnings are logged.
DEBUG	Includes INFO and additional information useful for debugging.
ERROR	Only errors are logged.
TRACE	Details are captured according to Connect:Direct Trace operation.
ALL	Logs all available information.
OFF	Turns off logging so that no server performance information is captured.
Listen Backlog	How many client connections are allowed in queue before connections are refused. Valid values are 0 to 2147483.
Accept Timeout	How long to wait after a connection is refused, before a session times out. Default = 30. Valid values are 0 to 2147483 seconds.
SSL Handshake Timeout	How long after a connection starts that SSL is allowed to complete its handshake. This parameter ensures that a connecting client authenticates within a fixed amount of time or the client is disconnected. Default=30 seconds. Valid values are 0 to 2147483.
Session Idle Timeout	Limits the how long a client can stay connected to an EA server without any activity. When the time expires with no activity from the client to the EA server, the server closes the connection. Default=10. To disable the timeout, set the value to 0.
Connect Timeout	How long to timeout after an outbound connection from the server is refused. Valid values are 0 to 2147483 seconds.
Read Timeout	Number of seconds to wait before an unsuccessful read operation times out. Valid values range from 0 to 2147483.

SSO Token Tab

Use the System Settings - SSO Token tab to customize single sign-on attributes in EA. A default configuration is shipped with the product.

Below is an explanation of the fields you can customize:

Field Name	Description
Token Manager	To configure a token manager other than EA, select custom in the Token Manager field. Default is SEAS-SAML and uses EA to manage tokens.
Identity Provider Name	The prefix appended to generated tokens. Select Named Identity Provider and type the prefix to identify the provider. Note: If you change the identity provider name, any outstanding tokens are invalidated.
Token Signing Key	To generate the token signing key using a certificate alias, enable Certificate alias and type the certificate alias. Select Auto generated to automatically generate token signing keys.
Token Expiration Period	Defines how long a token can be used before it expires. Default is 15 minutes.
Additional Properties	This field is reserved for future development.

Kerberos Configuration Tab

EA uses Kerberos to change passwords on Active Directory. Refer to Manage Active Directory on the [Sterling External Authentication Documentation Library](#).

Below is an explanation of the fields you define for a Kerberos configuration:

Parameter	Description
Name	Domain name.
Default Realm	Name of the domain name, used when the realm name cannot be determined. If the user name is in the format <user>@<xyz>, the realm is assumed to be <xyz>. If the user name is an LDAP distinguished name, the realm is assumed to be the concatenation of the DC components of the distinguished name, separated by dots. For example, if user name is CN=testUser,O=People,DC=example,DC=com, the realm is assumed to be example.com.
Description	Description of the realm.
kdc	A list of host names or IP addresses for the Key Distribution Centers. In Active Directory environments, the Key Distribution Centers correspond to the domain controllers.

Users Dialog

User definitions identify users in Sterling External Authentication Server. When you define users, you specify a user name and password and assign the user a role. The admin role is the only role available for assignment initially; it enables all permissions by default. Refer to Manage users and roles on the [Sterling External Authentication Documentation Library](#).

Complete the following fields to create or copy a user definition:

Parameter	Description
Name	Name used to login. Can be up to 255 alphanumeric characters, including space, underscore (_), and period (.).
Password	Password associated with the user name.
Confirm Password	Reenter the password to confirm it.
Role	Role that the user will sign on as. By default, admin role is the only one available.
Description	Description of the user and role.
Properties	This parameter is not used.

Roles

You can create new roles and allow Sterling External Authentication Server users to create, read, update, delete, and execute permissions in the functional areas. Refer to Manage users and roles on the [Sterling External Authentication Documentation Library](#).

Complete the following parameters to define a new role:

Parameter	Description
Role name	Name to use to identify the role. Use this role when you assign create a user.
Description	Description to help administrators determine when to assign the role.
Permissions	Under each permission category, select a check box to allow the permissions as appropriate for the role. Clear a check box to disable a permission for the role.
Select all	Turn on all permissions. Clear the check box to disable all permissions for all categories. Tip: To save time when creating a role that needs several permissions, choose Select All . Customize the role by clearing check boxes for any unnecessary permissions.
Cert validation	Certificate validation permissions allowed for the role:

Parameter	Description
	<ul style="list-style-type: none"> ◆ Create—Allows users to create certificate validation definitions. ◆ Read—Allows users to read certificate validation definitions. ◆ Update—Allows users to update certificate validation definitions. ◆ Delete—Allows users to delete certificate validation definitions. ◆ Execute—Allows users to execute certificate validation definitions.
Cert revocation	<p>Certificate revocation allowed for the role:</p> <ul style="list-style-type: none"> ◆ Create—Allows users to create certificate revocation list definitions. ◆ Read—Allows users to read certificate revocation list definitions. ◆ Update—Allows users to update certificate revocation list definitions. ◆ Delete—Allows users to delete certificate revocation list definitions. ◆ Execute—Allows users to execute certificate revocation list definitions.
Authentication	<p>Authentication permissions allowed for the role:</p> <ul style="list-style-type: none"> ◆ Create— Allows users to create authentication definitions. ◆ Read— Allows users to read authentication definitions. ◆ Update— Allows users to update authentication definitions. ◆ Delete— Allows users to delete authentication definitions. ◆ Execute—Allows users to execute authentication definitions.
Acceptor	<p>Acceptor permissions allowed for the role:</p> <ul style="list-style-type: none"> ◆ Create— Allows users to create accepters. ◆ Read— Allows users to read accepters. ◆ Update— Allows users to update accepters. ◆ Delete— Allows users to delete accepters. ◆ Execute— Allows users to execute accepters.

Parameter	Description
User	<p>User permissions allowed for the role:</p> <ul style="list-style-type: none"> ◆ Create— Allows users to create user definitions. ◆ Read— Allows users to read users definitions. ◆ Update— Allows users to update user definitions. ◆ Delete— Allows users to delete user definitions. ◆ Execute— Allows users to execute user definitions.
Role	<p>Role permissions allowed for the role:</p> <ul style="list-style-type: none"> ◆ Create—Allows users to create role definitions. ◆ Read— Allows users to read role definitions. ◆ Update— Allows users to update role definitions. ◆ Delete— Allows users to delete role definitions. ◆ Execute— Allows users to execute role definitions.
System	<ul style="list-style-type: none"> ◆ Create—Allows users to create system-wide connections and add system settings. ◆ Read— Allows users to read system settings. ◆ Update— Allows users to update system settings. ◆ Delete— Allows users to delete system settings. ◆ Execute— Allows users to execute system settings.

Manage Columns

You can view a variety of information for the definitions displayed. Each definition window has a default view, but you can also customize views by performing the following actions:

- ◆ Display or hide the columns you select
- ◆ Rearrange columns in an order that is important to you
- ◆ Save a view for future use
- ◆ Rename a view
- ◆ Delete a view

