



---

# Discovery and Credentials

SL1 version 8.12.0

---

# Table of Contents

<b>Introduction</b> .....	<b>1</b>
Terminology .....	2
Who Should Read This Manual? .....	2
Requirements .....	2
<b>Credentials</b> .....	<b>3</b>
What Are Credentials? .....	5
Viewing Information about Credentials .....	6
Filtering the List of Credentials .....	7
Defining One or More SNMP Credentials for Initial Discovery .....	8
Defining Credentials .....	9
Defining an SNMP Credential .....	10
Defining a Database Credential .....	12
Monitoring Informix Databases .....	15
Defining a SOAP/XML Host Credential .....	15
Defining an LDAP/AD Credential .....	19
Defining a Basic/Snippet Credential .....	22
Defining an SSH/Key Credential .....	24
Defining a PowerShell Credential .....	26
Testing a Credential .....	29
ScienceLogic Default Credential Tests .....	30
AWS Credential Test .....	30
Azure Credential Test .....	30
Basic/Snippet Credential Test .....	31
Database Credential Test .....	31
PowerShell Credential Test .....	31
SNMP Credential Test .....	32
SOAP/XML Credential Test .....	32
SoftLayer Credential Test .....	32
SSH/Key Credential Test .....	32
VMware Credential Test .....	33
Specifying Credentials During Initial Discovery .....	33
Defining the Primary and Secondary Credentials for a Single Device .....	34
Defining the Credentials for a Specific Device/Dynamic Application Pair .....	37
Specifying Credentials in a Device Template .....	39
How the ScienceLogic Platform Uses Credentials During Discovery .....	39
Aligning One or More Organizations With a Credential .....	39
Default Organizations Aligned with a Credential .....	41
Editing the Organizations Aligned with a Credential .....	42
Restricted Credentials in the Discovery Session Editor Page .....	44
Editing a Credential .....	44
Deleting a Credential .....	45
<b>Discovery</b> .....	<b>46</b>
What Happens During Discovery? .....	48
What Happens During Discovery when the SL 1 agent is Installed? .....	50
What is a Dynamic Application? .....	50
How Does the ScienceLogic Platform Align Dynamic Applications During Discovery? .....	51
Before You Run Discovery .....	52
System Settings that Affect Discovery .....	53
Device Settings that Affect Auto-Discovery and Re-Discovery .....	57
Duplicate IP Addresses and Duplicate MAC Addresses During Discovery .....	58

Duplicate MAC Addresses for Component Devices .....	60
Prerequisites for Discovering Devices on the Devices Page .....	62
Adding Devices Using Universal or Guided Discovery .....	62
Adding Devices Using Guided Discovery .....	67
Working with Discovery Sessions .....	75
Running a Classic Discovery Session .....	75
Creating a New Classic Discovery Session with the Save As Button .....	82
Viewing Information about a Classic Discovery Session .....	83
Editing a Classic Discovery Session .....	86
Scheduling a Classic Discovery Session .....	86
Viewing the Schedule Manager .....	87
Defining a Scheduled or Recurring Discovery Session .....	88
Enabling or Disabling One or More Scheduled Discovery Sessions .....	90
Deleting One or More Scheduled Discovery Sessions .....	91
Manually Re-Running Discovery for a Dynamic Application .....	91
Manually Re-Running Discovery for a Device .....	93
Viewing Information about Classic Discovery .....	94
Managing MAC Vendor Records .....	95
Viewing the List of MAC Vendor Records .....	95
Filtering the List of MAC Vendor Records .....	96
Editing the Virtual Setting for MAC Vendor Records .....	97
Troubleshooting Discovery .....	97
Checking Network Security .....	98
Debugging the Discovery Processes .....	98
Checking Communication between Data Collectors and the Database Server .....	100
How File Systems are Hidden During Discovery .....	101
<b>Collection .....</b>	<b>103</b>
What is Collection? .....	104
Collection Processes .....	104
<b>Managing Credential Tests .....</b>	<b>106</b>
Viewing Information About Credential Tests .....	107
Filtering the List of Credential Tests .....	108
Running a Credential Test from the Credential Test Management Page .....	109
Creating a Credential Test .....	110
Editing a Credential Test .....	112
Deleting Credential Tests .....	112
Available Step Functions .....	112
ping .....	112
nmap_udp .....	113
nmap_tcp .....	113
nslookup_forward .....	114
nslookup .....	114
dynapp_execute .....	115
snmp_getnext .....	115
ssh_request .....	115
db_query .....	116
curl .....	116
aws_connect .....	117
aws_service_scan .....	118
nmap_aws .....	118
nslookup_aws .....	119
ping_aws .....	120

---

# Chapter 1



## Introduction

---

### Overview

This chapter provides an overview of discovery, collection, and credentials in SL1.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ().
- To view a page containing all of the menu options, click the Advanced menu icon (.

This chapter includes the following topics:

<i>Terminology</i> .....	2
<i>Who Should Read This Manual?</i> .....	2
<i>Requirements</i> .....	2

---

## Terminology

The following terms explain the key concepts used with discovery:

- **Discovery** is the tool that automatically discovers devices in your network. You supply the discovery tool with a range or list of IP addresses, and the discovery tool determines if a device exists at each IP address. For each device the discovery tool "discovers", the discovery tool can collect a list of open ports, DNS information, SSL certificates, a list of network interfaces, device classes to align with the device, and basic SNMP information about the device. The discovery tool also determines which (if any) Dynamic Applications to align with the device. If the discovery tool finds Dynamic Applications to align with the device, the discovery tool triggers collection from the device, using each aligned Dynamic Application.

SL1 also uses discovery to update information about an already-discovered device and to add new information about an already-discovered device.

**NOTE:** Discovery collects a very specific set of information for each discovered device. Data that is not retrieved by discovery is retrieved by collection.

- **Collection** is the tool that retrieves policy-based information and Dynamic Application-based information from a device. After a device is discovered, you can define monitoring policies for that device in SL1. For example, if you define a policy to monitor a system process, the collection tool retrieves that information.
- **Credentials** are access profiles (usually username, password, and any additional information required for access) that allow SL1 to retrieve information from devices and from software applications on devices. Discovery uses SNMP credentials to retrieve SNMP information from each discovered device. Dynamic Applications use credentials to retrieve SNMP information, database information, SOAP information, XML information, and LDAP and AD information. SL1 also includes a type of credential called "Basic/Snippet" that is not bound to a specific authentication protocol. You can use this type of credential for Dynamic Applications of type "WMI", of type "snippet", and when defining system backups. Another type of credential allows Dynamic Applications of type "Snippet" to use SSH to communicate with a remote device.

---

## Who Should Read This Manual?

This manual is intended for users who are responsible for provisioning devices in SL1.

---

## Requirements



To perform the troubleshooting steps in this manual, you must be allowed root-level access to SL1 appliances from a shell session.

---

## Overview

This chapter defines credentials and how they are used in SL1.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ().
- To view a page containing all of the menu options, click the Advanced menu icon ().

This chapter includes the following topics:

<i>What Are Credentials?</i> .....	5
<i>Viewing Information about Credentials</i> .....	6
<i>Defining One or More SNMP Credentials for Initial Discovery</i> .....	8
<i>Defining Credentials</i> .....	9
<i>Defining an SNMP Credential</i> .....	10
<i>Defining a Database Credential</i> .....	12
<i>Monitoring Informix Databases</i> .....	15
<i>Defining a SOAP/XML Host Credential</i> .....	15
<i>Defining an LDAP/AD Credential</i> .....	19
<i>Defining a Basic/Snippet Credential</i> .....	22
<i>Defining an SSH/Key Credential</i> .....	24
<i>Defining a PowerShell Credential</i> .....	26
<i>Testing a Credential</i> .....	29

<i>ScienceLogic Default Credential Tests</i> .....	30
<i>Specifying Credentials During Initial Discovery</i> .....	33
<i>Defining the Primary and Secondary Credentials for a Single Device</i> .....	34
<i>Defining the Credentials for a Specific Device/Dynamic Application Pair</i> .....	37
<i>Specifying Credentials in a Device Template</i> .....	39
<i>How the ScienceLogic Platform Uses Credentials During Discovery</i> .....	39
<i>Aligning One or More Organizations With a Credential</i> .....	39
<i>Editing a Credential</i> .....	44
<i>Deleting a Credential</i> .....	45

---

## What Are Credentials?

**Credentials** are access profiles (usually username, password, and any additional information required for access) that allow SL1 to retrieve information from devices and from software applications on devices.

- Discovery uses SNMP credentials to retrieve SNMP information during initial discovery and nightly auto-discovery. If SL1 can connect to a device with an SNMP credential, SL1 deems that device "manageable" in SL1.
- Dynamic Applications use credentials to retrieve SNMP information, database information, SOAP information, XML information, XSLT information, and WMI information.
- Proxied Web Services use SOAP/XML Host credentials to pass authentication information to external web services.
- SL1 includes a type of credential called "Basic/Snippet" that is not bound to a specific authentication protocol. You can use this type of credential for Dynamic Applications of type "WMI", of type "snippet", and when defining system backups. "Basic/Snippet" credentials can also be used for monitoring Windows devices using PowerShell.
- SL1 includes a type of credential that allows SL1 to communicate with an LDAP or Active Directory system. For details on integrating SL1 with LDAP or Active Directory, see the manual **Using Active Directory and LDAP**.
- SL1 includes a type of credential that allows Dynamic Applications of type "Snippet" to use SSH to communicate with a remote device. To use these Dynamic Applications, you must define an SSH credential.
- SL1 includes a type of credential that allows Dynamic Applications to retrieve data from Windows devices. If you align a Dynamic Application for PowerShell with a PowerShell credential, SL1 assumes that you want to use its built-in agentless transport to communicate with Windows devices.

If necessary, a single device can use multiple credentials. If more than one agent or application is running on the device, each agent or application can be associated with its own credential. During discovery, SL1 will use the appropriate credential for each agent.

For example, suppose you want SL1 to discover a device that supports SNMP v2. To retrieve SNMP data from that device, SL1 must use a valid SNMP v2 read-only community string. So we would first go to the device and define the SNMP read-only community string. Then we would return to SL1 and create a credential in the SL1 system, using that community string. This new credential would allow discovery to retrieve SNMP data from the device.

Now suppose this same device also includes a MySQL database. Suppose you want SL1 to use a Dynamic Application to monitor that database. To retrieve data from the database, SL1 must use a valid username and password for that database. So we would first go to the device that hosts the MySQL database and create a database username and database password for SL1 to use. Then we would return to SL1 and create a credential in the SL1 system. The credential would include the database username and database password for the MySQL database. This credential would allow the Dynamic Application to retrieve data about the MySQL database.



# Viewing Information about Credentials

The **Credential Management** page allows you to view a list of all ScienceLogic credentials. From this page, you can also create new credentials and editing existing credentials.

Credential Management | Credentials Found [62]

Profile Name	Organization	RO Use	RW Use	DA Use	Type	Credential User	Host	Port	Timeout (ms)	ID	Last Edited	Edited By
1. Amazon Web Services Credential	System	--	--	--	SOAP/XML Host	[AWS Account Access Key]	example.com	80	2000	1	2015-05-18 17:42:31	em7Admin
2. Azure Credential - SOAP/XML	[all orgs]	--	--	--	SOAP/XML Host	~AD_USER~	login.windows.net	443	80000	60	2015-05-14 11:31:58	em7Admin
3. Azure Credential - SSHKey	[all orgs]	--	--	--	SSHKey	<SUBSCRIPTION_ID_HERE>	N/A	22	180000	59	2015-05-14 11:31:56	em7Admin
4. Cisco SNMPV2 - Example	[all orgs]	--	--	--	SNMP	--	--	161	1500	3	2015-05-14 11:25:09	em7Admin
5. Cisco SNMPV2 - Example	[all orgs]	--	--	--	SNMP	USER_GOES_HERE	--	161	1500	2	2015-05-14 11:25:09	em7Admin
6. Cisco ACI	[all orgs]	--	128	--	Basic/Script	admin	173.30.210.40	443	0	62	2015-05-14 15:05:24	em7Admin
7. Cisco ACI Credential	[all orgs]	--	--	--	Basic/Script	admin	168.18.133.200	443	0	61	2015-05-14 14:32:05	em7Admin
8. Cloudkick - Example	[all orgs]	--	--	--	Basic/Script	[SECURITY KEY GOES HERE]	127.0.0.1	443	5000	9	2015-05-14 11:25:31	em7Admin
9. CUCM PartitionService 9.0 Example	[all orgs]	--	--	--	SOAP/XML Host	--	N/A	8443	2000	4	2015-05-14 11:25:12	em7Admin
10. EMT Central Database	[all orgs]	--	--	--	Database	root	localhost	7706	0	51	2015-05-14 11:26:41	em7Admin
11. EMT Collector Database	[all orgs]	--	--	--	Database	root	7707	0	14	2015-05-14 11:26:43	em7Admin	
12. EMT DB	[all orgs]	--	--	--	Database	root	%D	7706	0	35	2015-05-14 11:26:32	em7Admin
13. EMT DB - DB Info	[all orgs]	--	--	--	SOAP/XML Host	root	%D	80	3000	38	2015-05-14 11:26:32	em7Admin
14. EMT DB - My conf	[all orgs]	--	--	--	SOAP/XML Host	root	%D	80	3000	37	2015-05-14 11:26:32	em7Admin
15. EMT DB - Site Conf	[all orgs]	--	--	--	SOAP/XML Host	root	%D	80	3000	36	2015-05-14 11:26:32	em7Admin
16. EMT Default V2	[all orgs]	--	--	--	SNMP	--	--	161	1500	10	2015-05-14 11:25:42	em7Admin
17. EMT Default V3	[all orgs]	--	--	--	SNMP	em7default3	--	161	500	11	2015-05-14 11:25:42	em7Admin
18. EMC - Example	[all orgs]	--	--	--	Basic/Script	root	%D	443	10000	15	2015-05-14 11:25:47	em7Admin
19. ESXi - Example	[all orgs]	--	--	--	Basic/Script	[SECURITY KEY GOES HERE]	127.0.0.1	443	5000	16	2015-05-14 11:25:51	em7Admin
20. IPSLA Example	[all orgs]	--	--	--	SNMP	--	--	161	1500	5	2015-05-14 11:25:14	em7Admin
21. iSize - Endpoint SNMP	[all orgs]	--	--	--	SNMP	control	--	161	3000	18	2015-05-14 11:25:58	em7Admin
22. iSize - Endpoint SSHCLI	[all orgs]	--	--	--	Basic/Script	admin	N/A	22	3	17	2015-05-14 11:25:58	em7Admin
23. iSize - API	[all orgs]	--	--	--	Basic/Script	em7Admin	10.0.0.100	80	3000	22	2015-05-14 11:26:11	em7Admin
24. NetApp 7-mode	[all orgs]	--	--	--	Basic/Script	root	%D	443	3000	24	2015-05-14 11:26:20	em7Admin
25. NetApp vSSD Option	[all orgs]	--	--	--	SOAP/XML Host	root	%D	443	3000	26	2015-05-14 11:26:20	em7Admin
26. NetApp vSSD Option Off	[all orgs]	--	--	--	SOAP/XML Host	root	%D	443	10000	25	2015-05-14 11:26:20	em7Admin
27. Nexus inconf	[all orgs]	--	--	--	Basic/Script	--	--	22	10000	8	2015-05-14 11:25:16	em7Admin
28. Nexus snmp	[all orgs]	--	--	--	SNMP	--	--	161	10000	7	2015-05-14 11:25:16	em7Admin
29. Polycm - Advanced	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	80	20000	28	2015-05-14 11:26:24	em7Admin
30. Polycm - CDR	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	80	20000	31	2015-05-14 11:26:24	em7Admin
31. Polycm - Interface	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	80	20000	29	2015-05-14 11:26:24	em7Admin
32. Polycm - Network	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	80	20000	30	2015-05-14 11:26:24	em7Admin
33. Polycm - System	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	80	20000	27	2015-05-14 11:26:24	em7Admin
34. Polycm DMA CDR Example	[all orgs]	--	--	--	Basic/Script	username	%D	8443	50	33	2015-05-14 11:26:28	em7Admin
35. Polycm MKA	[all orgs]	--	--	--	SOAP/XML Host	sciencelogic	%D	80	10000	32	2015-05-14 11:26:28	em7Admin
36. Rackspace - Example	[all orgs]	--	--	--	Basic/Script	USERNAME GOES HERE]	127.0.0.1	443	5000	34	2015-05-14 11:26:30	em7Admin
37. SNMP Public V1	[all orgs]	--	--	--	SNMP	--	--	161	1500	12	2015-05-14 11:25:42	em7Admin
38. SNMP Public V2	[all orgs]	--	--	--	SNMP	--	--	161	1500	13	2015-05-14 11:25:42	em7Admin
39. Tandberg Endpoint - Config	[all orgs]	--	--	--	SOAP/XML Host	USERNAME_HERE	%D	80	10000	40	2015-05-14 11:26:36	em7Admin
40. Tandberg Endpoint - History	[all orgs]	--	--	--	SOAP/XML Host	USERNAME_HERE	%D	80	10000	41	2015-05-14 11:26:36	em7Admin
41. Tandberg Endpoint - Status	[all orgs]	--	--	--	SOAP/XML Host	USERNAME_HERE	%D	80	10000	39	2015-05-14 11:26:36	em7Admin
42. Tandberg TCS Cluster Status	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	443	2000	42	2015-05-14 11:26:38	em7Admin
43. Tandberg TCS Configuration	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	443	2000	40	2015-05-14 11:26:38	em7Admin

**TIP:** To sort the list of credentials, click on a column heading. The list will be sorted by the column value, in ascending order. To sort by descending order, click the column heading again. The **Last Edited** column sorts by descending order on the first click; to sort by ascending order, click the column heading again.

For each credential, the page displays:

- **Profile Name.** Name of the credential.
- **Organization.** If you have an account of type "User" and are a member of only one ScienceLogic organization, this field will not appear in the **Credential Management** page. The **Credential Management** page will display only credentials that are aligned with your organization. For all other users, this column specifies the organization(s) aligned with the credential. Possible values are all orgs, multiple orgs, a single organization name, or none. For details, see the section [Aligning One or More Organizations with a Credential](#).
- **RO Use.** Specifies the number of devices that SL1 can retrieve read-only information from, using the credential.
- **RW Use.** Specifies the number of devices that SL1 can both read from and write to, using the credential.
- **DA Use.** Specifies the number of Dynamic Applications aligned with this credential.

- **Type**. Type of credential. Possible types are SNMP, Database, SOAP/XML, LDAP/AD, Basic/Snippet, SSH/Key, and PowerShell.
- **Credential User**. Username associated with the credential.
- **Host**. Hostname or IP address that SL1 will use the credential to communicate with.
- **Port**. Port used by the credential to communicate with the external device or application.
- **Timeout**. Time, in milliseconds, after which SL1 will stop trying to communicate with the external device or application.
- **ID**. Unique numeric ID, automatically assigned by SL1 to each credential.
- **Last Edited**. Date and time the credential was created or last edited.
- **Edited By**. ScienceLogic user who created or last edited the credential.

## Filtering the List of Credentials

To filter the list of credentials in the **Credential Management** page, use the search fields at the top of each column. The search fields are find-as-you-type filters; as you type, the page is filtered to match the text in the search field, including partial matches. Text matches are not case-sensitive. Additionally, you can use the following special characters in each filter:

- , (comma). Specifies an "or" operation. For example:  
"dell, micro" would match all values that contain the string "dell" OR the string "micro".
- & (ampersand). Specifies an "and" operation. For example:  
"dell & micro" would match all values that contain the string "dell" AND the string "micro".
- ! (exclamation mark). Specifies a "not" operation. For example:  
"!dell" would match all values that do not contain the string "dell".
- ^ (caret mark). Specifies "starts with." For example:  
"^ micro" would match all strings that start with "micro", like "microsoft".  
"^" will include all rows that have a value in the column.  
"!^" will include all rows that have no value in the column.

- \$ (dollar sign). Specifies "ends with." For example:
  - "\$ware" would match all strings that end with "ware", like "VMware".
  - "\$" will include all rows that have a value in the column.
  - "!\$" will include all rows that have no value in the column.
- min-max. Matches numeric values only. Specifies any value between the minimum value and the maximum value, including the minimum and the maximum. For example:
  - "1-5" would match 1, 2, 3, 4, and 5.
- - (dash). Matches numeric values only. A "half open" range. Specifies values including the minimum and greater or including the maximum and lesser. For example:
  - "1-" matches 1 and greater, so it would match 1, 2, 6, 345, etc.
  - "-5" matches 5 and less, so it would match 5, 3, 1, 0, etc.
- > (greater than). Matches numeric values only. Specifies any value "greater than." For example:
  - ">7" would match all values greater than 7.
- < (less than). Matches numeric values only. Specifies any value "less than." For example:
  - "<12" would match all values less than 12.
- >= (greater than or equal to). Matches numeric values only. Specifies any value "greater than or equal to." For example:
  - ">=7" would match all values 7 and greater.
- <= (less than or equal to). Matches numeric values only. Specifies any value "less than or equal to." For example:
  - "<=12" would match all values 12 and less.
- = (equal). Matches numeric values only. For numeric values, allows you to match a negative value. For example:
  - "=-5" would match "-5" instead of being evaluated as the "half open range" as described above.

---

## Defining One or More SNMP Credentials for Initial Discovery

Before running discovery, you must first define credentials for the devices and applications in the network to be managed. You must either define or note the credentials on the device to be managed, and then you must define matching credentials in SL1.

To create credentials for initial discovery, you must first:

1. Determine which devices or IP ranges you want to discover.
2. Determine which of these devices support SNMP.
3. Determine the SNMP community string or SNMP credentials for each device that supports SNMP.

**NOTE:** If you do not know which devices in your network support SNMP, consult your system administrator. In some cases, you might also need to consult your system administrator about enabling SNMP, and defining SNMP community strings or SNMP credentials on these devices. For advice and details on configuring SNMP on your devices, see the manuals *Monitoring Cisco Unified Communications*, *Monitoring Video Endpoints*, *Monitoring VMWare*, *Monitoring Windows Devices*, and *Monitoring Linux and Solaris Devices*.

4. In SL1, define one or more SNMP credentials to use during discovery. These credentials should match those SNMP community strings and SNMP credentials that already exist in your network.
5. Initially, discovery uses only SNMP credentials. However, when SL1 collects data specified in Dynamic Applications, SL1 can use other types of credentials.

If necessary, a single device can use multiple credentials. If more than one agent or application is running on the device, each agent or application can be associated with its own credential. During discovery, SL1 will use the appropriate credential for each agent.

---

## Defining Credentials

To define a credential in SL1:

1. Collect the information you need to create each credential (usually username and password).
2. Go to the **Credential Management** page (System > Manage > Credentials).
3. In the **Credential Management** page, click the **[Create]** menu. Select the type of credential you want to create. Your choices are:
  - [SNMP Credential](#)
  - [Database Credential](#)
  - [SOAP/XML Host Credential](#)
  - [LDAP/AD Credential](#)
  - [Basic/Snippet Credential](#)
  - [SSH/Key Credential](#)
  - [PowerShell Credential](#)
4. The **Credential Editor** modal page appears. In this page, you can define the new credential. The following sections explain how to create each type of credential.
5. Click the **[Save]** button to save the new credential.

# Defining an SNMP Credential

SNMP Credentials (called "community strings" in earlier versions of SNMP) allow SL1 to access SNMP data on a managed device. SL1 uses SNMP credentials to perform discovery, run auto-discovery, and gather information from SNMP Dynamic Applications.

To create an SNMP credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).

Profile Name	Organization	RO Use	RW Use	DA Use	Type	Credential User	Host	Port	Timeout (ms)	ID	Last	Actions
1. Amazon Web Services Credential	System	--	--	--	SOAP/XML Host	[AWS Account Access]	example.com	80	2000	1	2015-05-16	Create SNMP Credential
2. Azure Credential - SOAP/XML	[all orgs]	--	--	--	SOAP/XML Host	<<AD_USER>>	login.windows.net	443	60000	60	2015-05-14	Create Database Credential
3. Azure Credential - SSH/Key	[all orgs]	--	--	--	SSH/Key	<<SUBSCRIPTION_ID_H>>		22	180000	59	2015-05-14	Create SOAP/XML Host Credential
4. Cisco SNMPv2 - Example	[all orgs]	--	--	--	SNMP			161	1500	3	2015-05-14	Create LDAP/AD Credential
5. Cisco SNMPv3 - Example	[all orgs]	--	--	--	SNMP	[USER_GOES_HERE]		161	1500	2	2015-05-14	Create Basic/Snippet Credential
6. Cisco ACI	[all orgs]	--	--	126	Basic/Snippet	admin	173.36.219.46	443	0	62	2015-05-14 15:05:24	Create SSH/Key Credential
7. Cisco ACI Credential	[all orgs]	--	--	--	Basic/Snippet	admin	168.16.133.200	443	0	81	2015-05-14 14:32:20	Create PowerShell Credential
8. Cloudtek - Example	[all orgs]	--	--	--	Basic/Snippet	{SECURITY KEY GOES}	127.0.0.1	443	5000	9	2015-05-14 11:25:31	
9. CUCM PartitionService 8.0 Example	[all orgs]	--	--	--	SOAP/XML Host			8443	2000	4	2015-05-14 11:28:12	
10. EM7 Central Database	[all orgs]	--	--	--	Database	root	localhost	7706	0	51	2015-05-14 11:28:41	
11. EM7 Collector Database	[all orgs]	--	--	--	Database	root	%D	7707	0	14	2015-05-14 11:25:43	
12. EM7 DB	[all orgs]	--	--	--	Database	root	%D	7706	0	35	2015-05-14 11:28:32	
13. EM7 DB - DB Info	[all orgs]	--	--	--	SOAP/XML Host	root	%D	80	3000	38	2015-05-14 11:28:32	
14. EM7 DB - My.cnf	[all orgs]	--	--	--	SOAP/XML Host	root	%D	80	3000	37	2015-05-14 11:28:32	
15. EM7 DB - Ssl.conf	[all orgs]	--	--	--	SOAP/XML Host	root	%D	80	3000	36	2015-05-14 11:28:32	
16. EM7 Default V2	[all orgs]	--	--	--	SNMP			161	1500	10	2015-05-14 11:25:42	
17. EM7 Default V3	[all orgs]	--	--	--	SNMP	em7default3		161	500	11	2015-05-14 11:25:42	
18. EMC - Example	[all orgs]	--	--	--	Basic/Snippet	root	%D	443	10000	15	2015-05-14 11:25:47	
19. ESGrid - Example	[all orgs]	--	--	--	Basic/Snippet	{SECURITY KEY GOES}	127.0.0.1	443	5000	16	2015-05-14 11:25:51	
20. IPSLA Example	[all orgs]	--	--	--	SNMP			161	1500	5	2015-05-14 11:25:14	
21. LifeSize - Endpoint SNMP	[all orgs]	--	--	--	SNMP	control		161	3000	18	2015-05-14 11:25:58	
22. LifeSize - Endpoint SSH/CLI	[all orgs]	--	--	--	Basic/Snippet	auto	%D	22	3	17	2015-05-14 11:25:58	
23. Local API	[all orgs]	--	--	--	Basic/Snippet	em7admin	10.0.0.190	80	5000	22	2015-05-14 11:28:11	
24. NetApp 7-mode	[all orgs]	--	--	--	Basic/Snippet	root	%D	443	3000	24	2015-05-14 11:28:20	
25. NetApp w/SSL Option	[all orgs]	--	--	--	SOAP/XML Host	root	%D	443	3000	26	2015-05-14 11:28:20	
26. NetApp w/SSL Option Off	[all orgs]	--	--	--	SOAP/XML Host	root	%D	443	10000	25	2015-05-14 11:28:20	
27. Nexus netconf	[all orgs]	--	--	--	Basic/Snippet			22	10000	6	2015-05-14 11:25:16	
28. Nexus snmp	[all orgs]	--	--	--	SNMP			161	10000	7	2015-05-14 11:25:16	
29. Polcom - Advanced	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	80	20000	28	2015-05-14 11:28:24	
30. Polcom - CDR	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	80	20000	31	2015-05-14 11:28:24	
31. Polcom - Interface	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	80	20000	29	2015-05-14 11:28:24	

2. Click the **[Actions]** button and select **Create SNMP Credential**. The **Credential Editor** page appears.

**Credential Editor** X

**Create New SNMP Credential** Reset

---

**Basic Settings**

Profile Name:  SNMP Version:

Port:  Timeout(ms):  Retries:

---

**SNMP V1/V2 Settings**

SNMP Community (Read-Only):  SNMP Community (Read/Write):

---

**SNMP V3 Settings**

Security Name:  Security Passphrase:

Authentication Protocol:  Security Level:  SNMP v3 Engine ID:

Context Name:  Privacy Protocol:  Privacy Protocol Pass Phrase:

**Save**

3. Supply values in the following fields:

- **Profile Name.** Name of the credential. Can be any combination of alphanumeric characters. This field is required.
- **SNMP Version.** SNMP version. Choices are *SNMP V1*, *SNMP V2*, and *SNMP V3*. The default value is *SNMP V2*. This field is required.
- **Port.** The port SL1 will use to communicate with the external device or application. The default value is *161*. This field is required.
- **Timeout (ms).** Time, in milliseconds, after which SL1 will stop trying to communicate with the SNMP device. The default value is *1500*. This field is required.
- **Retries.** Number of times SL1 will try to authenticate and communicate with the external device. The default value is *1*. This field is required.

### SNMP V1/V2 Settings

These fields appear if you selected *SNMP V1* or *SNMP V2* in the **SNMP Version** field. Otherwise, these fields are grayed out.

- **SNMP Community (Read Only).** The SNMP community string (password) required for read-only access of SNMP data on the remote device or application. For *SNMP V1* and *SNMP V2* credentials, you must supply a community string, either in this field or in the **SNMP Community (Read/Write)** field.
- **SNMP Community (Read/Write).** The SNMP community string (password) required for read and write access of SNMP data on the remote device or application. For *SNMP V1* and *SNMP V2* credentials, you must supply a community string, either in this field or in the **SNMP Community (Read Only)** field.

### SNMP V3 Settings

These fields appear if you selected *SNMP V3* in the **SNMP Version** field. Otherwise, these fields are grayed out.

- **Security Name.** Name for SNMP authentication. This field is required.
- **Security Passphrase.** Password to authenticate the credential. This value must contain at least 8 characters. This value is required if you use a **Security Level** that includes authentication.
- **Authentication Protocol.** Select an authentication algorithm for the credential. Choices are *MD5* or *SHA*. The default value is *MD5*. This field is required.
- **Security Level.** Specifies the combination of security features for the credentials. This field is required. Choices are:
  - *No Authentication / No Encryption.*
  - *Authentication Only.* This is the default value.
  - *Authentication and Encryption.*
- **SNMP v3 Engine ID.** The unique engine ID for the SNMP agent you want to communicate with. (SNMPv3 authentication and encryption keys are generated based on the associated passwords and

the engine ID.) This field is optional.

- **Context Name.** A context is a mechanism within SNMPv3 (and AgentX) that allows you to use parallel versions of the same MIB objects. For example, one version of a MIB might be associated with SNMP Version 2 and another version of the same MIB might be associated with SNMP Version 3. For SNMP Version 3, specify the context name in this field. This field is optional.
- **Privacy Protocol.** The privacy service encryption and decryption algorithm. Choices are *DES* or *AES*. The default value is *DES*. This field is required.
- **Privacy Protocol Passphrase.** Privacy password for the credential. This field is optional.

4. Click the **[Save]** button to save the new SNMP credential.
5. Repeat steps 1-4 for each SNMP-enabled device in your network that you want to monitor with SL1.

**NOTE:** When you define a SNMP Credential, SL1 automatically aligns the credential with all organizations of which you are a member.

## Defining a Database Credential

Database Credentials allow SL1 to access data on a database on a managed device. SL1 uses database credentials when collecting data for Database Dynamic Applications.

To define a database credential:

1. Collect the information you need to create each credential (usually username and password).
2. Go to the **Credential Management** page (System > Manage > Credentials).

Credential Management | Credentials Found [62]

Profile Name	Organization	RD Use	RDV Use	DB Use	Type	Credential User	Host	Port	Timeout (ms)	ID	Last	Actions	Reset	Guide
1. Amazon Web Services Credential	System	--	--	--	SOAP/XML Host	[AWS Account Access]	example.com	80	2000	1	2015-05-14	Create SNMP Credential		
2. Azure Credential - SOAP/XML	[All Orgs]	--	--	--	SOAP/XML Host	<AD_USERS>	login.windows.net	443	60000	60	2015-05-14	Create Database Credential		
3. Azure Credential - SSHKey	[All Orgs]	--	--	--	SSHKey	<SUBSCRIPTION_ID_M_H_ND		22	180000	59	2015-05-14	Create SOAP/XML Host Credential		
4. Cisco SNMPv2 - Example	[All Orgs]	--	--	--	SNMP			161	1500	3	2015-05-14	Create Basic/Snmpet Credential		
5. Cisco SNMPv3 - Example	[All Orgs]	--	--	--	SNMP			161	1500	2	2015-05-14	Create SSH/Key Credential		
6. Cisco ACI	[All Orgs]	--	--	--	Basic/Snmpet	admin	173.36.210.46	443	0	62	2015-05-14 15:05:24	Create PowerShell Credential		
7. Cisco ACI Credential	[All Orgs]	--	--	--	Basic/Snmpet	admin	108.18.133.200	443	0	61	2015-05-14 14:32:20			
8. Cloudkick - Example	[All Orgs]	--	--	--	Basic/Snmpet	[SECURITY KEY GOES]	127.0.0.1	443	5000	9	2015-05-14 11:25:31	em7admin		
9. CUCM PerfmonService 0.0 Example	[All Orgs]	--	--	--	SOAP/XML Host		ND	8443	2000	4	2015-05-14 11:25:32	em7admin		
10. EMT Central Database	[All Orgs]	--	--	--	Database	root	localhost	7706	0	51	2015-05-14 11:25:41	em7admin		
11. EMT Collector Database	[All Orgs]	--	--	--	Database	root	ND	7707	0	14	2015-05-14 11:25:43	em7admin		
12. EMT DB	[All Orgs]	--	--	--	Database	root	ND	7706	0	35	2015-05-14 11:26:32	em7admin		
13. EMT DB - DB Info	[All Orgs]	--	--	--	SOAP/XML Host	root	ND	80	3000	38	2015-05-14 11:26:32	em7admin		
14. EMT DB - My conf	[All Orgs]	--	--	--	SOAP/XML Host	root	ND	80	3000	37	2015-05-14 11:26:32	em7admin		
15. EMT DB - Sdk conf	[All Orgs]	--	--	--	SOAP/XML Host	root	ND	80	3000	36	2015-05-14 11:26:32	em7admin		
16. EMT Default V2	[All Orgs]	--	--	--	SNMP			161	1500	10	2015-05-14 11:25:42	em7admin		
17. EMT Default V3	[All Orgs]	--	--	--	SNMP	em7defaultv3		161	500	11	2015-05-14 11:25:42	em7admin		
18. EMC - Example	[All Orgs]	--	--	--	Basic/Snmpet	root	ND	443	10000	15	2015-05-14 11:25:47	em7admin		
19. GIGGL - Example	[All Orgs]	--	--	--	Basic/Snmpet	[SECURITY KEY GOES]	127.0.0.1	443	5000	16	2015-05-14 11:25:51	em7admin		
20. IPSLA Example	[All Orgs]	--	--	--	SNMP			161	1500	5	2015-05-14 11:25:14	em7admin		
21. LifeSize Endpoint SNMP	[All Orgs]	--	--	--	SNMP	control		161	3000	18	2015-05-14 11:25:58	em7admin		
22. LifeSize Endpoint SSH/CLI	[All Orgs]	--	--	--	Basic/Snmpet	auto	ND	22	3	17	2015-05-14 11:25:58	em7admin		
23. Local API	[All Orgs]	--	--	--	Basic/Snmpet	em7admin	10.0.0.180	80	5000	22	2015-05-14 11:26:11	em7admin		
24. NetApp 7-mode	[All Orgs]	--	--	--	Basic/Snmpet	root	ND	443	3000	24	2015-05-14 11:26:20	em7admin		
25. NetApp w/SSL Option	[All Orgs]	--	--	--	SOAP/XML Host	root	ND	443	3000	26	2015-05-14 11:26:20	em7admin		
26. NetApp w/SSL Option OP	[All Orgs]	--	--	--	SOAP/XML Host	root	ND	443	10000	25	2015-05-14 11:26:20	em7admin		
27. Nexus netconf	[All Orgs]	--	--	--	Basic/Snmpet		ND	22	10000	6	2015-05-14 11:25:16	em7admin		
28. Nexus snmp	[All Orgs]	--	--	--	SNMP			161	10000	7	2015-05-14 11:25:16	em7admin		
29. Polycom - Advanced	[All Orgs]	--	--	--	SOAP/XML Host	admin	ND	80	20000	28	2015-05-14 11:26:24	em7admin		
30. Polycom - CDR	[All Orgs]	--	--	--	SOAP/XML Host	admin	ND	80	20000	31	2015-05-14 11:26:24	em7admin		
31. Polycom - Interleave	[All Orgs]	--	--	--	SOAP/XML Host	admin	ND	80	20000	29	2015-05-14 11:26:24	em7admin		

- In the **Credential Management** page, click the **[Actions]** menu. Select **Create Database Credential**.

The screenshot shows a 'Credential Editor' window titled 'Create New Database Credential'. It has a 'Reset' button in the top right. The form is organized into two main sections: 'Basic Settings' and 'Oracle Settings'.  
**Basic Settings:**  
 - Profile Name: Text input field.  
 - DB Type: Dropdown menu with '[ Oracle & \*SQLNet ]' selected.  
 - DB Name: Text input field.  
 - DB User: Text input field.  
 - Password: Text input field.  
 - Hostname/IP: Text input field.  
 - Port: Text input field with '1521' entered.  
**Oracle Settings:**  
 - Oracle Connect Type: Dropdown menu with '[ Oracle System Identifier (SID) ]' selected.  
 - SID (if required): Text input field.  
 A 'Save' button is located at the bottom center of the form.

- The **Credential Editor** modal page appears. In this page, you can define the new database credential. To define the new credential, supply values in the following fields:

**Basic Settings**

- **Profile Name.** Name of the credential. Can be any combination of alphanumeric characters. This field is required.
- **DB Type.** Type of database that will be accessed with the credential. Select from a list of databases supported by SL1. This field is required.

**NOTE:** For information about monitoring Informix databases, see the [Monitoring Informix Databases](#) section.

- **DB Name.** Name of the database that will be accessed with the credential.
- **DB User.** Username associated with a valid account on the database.
- **Password.** Password associated with a valid account on the database.
- **Hostname/IP.** Hostname or IP address where the database resides. This field is required.
  - You can include the variable **%D** in this field. SL1 will replace the variable with the IP address of the current device (device that is currently using the credential).
  - You can include the variable **%N** in this field. SL1 will replace the variable with the hostname of the current device (device that is currently using the credential). If SL1 cannot determine the hostname, SL1 will replace the variable with the primary management IP address for the current device.



**NOTE:** To use the localhost, in the **Hostname/IP** field, enter the IP address *127.0.0.1*. The credential will not work if you enter the string *localhost* in the **Hostname/IP** field.

- **Port.** Port number associated with the database you want to access with this credential. This field is required.
  - For **DB Type** of MySQL, the default value is 3306.
  - For **DB Type** of MS SQL Server, the default value is 1433.
  - For **DB Type** of Oracle and SQLNet, the default value is 1521.
  - For **DB Type** of PostgreSQL, the default value is 5432.
  - For **DB Type** of IBM DB2, the default value is 523.
  - For **DB Type** of Sybase ASE, the default value is 4100.
  - For **DB Type** of Informix, see the 9088 section.
  - For **DB Type** of Ingress, the default value is 1572.

**NOTE:** SL1's Database Servers include a MySQL database running on port 7706. Data Collectors and Message Collectors include a MySQL database running on port 7707.

### Oracle Settings

These fields appear if you selected *Oracle* & *\*SQLNet* in the **DB Type** field. Otherwise, these fields are grayed out.

- **Oracle Connect Type.** Specifies the method SL1 should use to connect to the Oracle database. The choices are:
  - *Oracle System Identifier (SID)*
  - *Oracle Real Application Clusters (SERVICE)*
  - *Oracle Server Direct Connection (SERVER)*

**NOTE:** In Oracle 11g, the "Oracle Server Direct Connection" option is deprecated. If you select this Oracle Connect Type for an Oracle 11g database, you must edit the file listener.ora and add the line "DEFAULT\_SERVICE\_LISTENER= <SID>", where <SID> is the SID value.

- **SID (if required).** Enter the value for the Oracle Connect Type (either Oracle SID, Oracle RAC, or Oracle Server) selected in the **Oracle Connect Type** field.

5. Click the **[Save]** button to save the new database credential.
6. Repeat steps 1-5 for each database credential in your network.

**NOTE:** When you define a Database Credential, the credential will automatically be aligned with the organization(s) you are a member of. To learn more about credentials and organizations, see the section [Aligning Organizations With a Credential](#) in this chapter.

---

## Monitoring Informix Databases

For SL1 to connect to an Informix database:

- The Informix database server must have a DRDA listener configured on a separate port than the current listener(s).
- The DRDA listener must be configured to share data with other listeners using a DBSERVERALIASES entry in the server's onconfig file.
- For servers that host multiple databases, multiple DRDA listeners are required with different port assignments.

For example Informix configuration files, please contact ScienceLogic Support.

---

## Defining a SOAP/XML Host Credential

SOAP/XML credentials allow SL1 to access a web server on a managed device. SOAP/XML credentials are used in several places in SL1, including:

- *With Dynamic Applications of type "SOAP".*
- *With Dynamic Applications of type "XML".*
- *With Dynamic Applications of type "XSLT".*
- *With Dynamic Applications of type "snippet".* The snippet code must define the authentication protocol. Dynamic Applications of type "snippet" can use any type of credential.
- *When defining a proxied web service.*

**NOTE:** For instructions on how to create a SOAP/XML credential for a proxied web service, see the [Web Proxies](#) manual.

To define a SOAP/XML credential:

1. Collect the information you need to create each credential (usually username and password).

- Go to the **Credential Management** page (System > Manage > Credentials).

Profile Name	Organization	BO Use	DA Use	Type	Credential User	Host	Port	Timeout (ms)	ID	Last	Actions
1. Amazon Web Services Credential	[Org]	--	--	SOAP/XML Host	[AWS Account Access] example.com		80	2000	1	2015-05-14 11:25:14	em7admin
2. Azure Credential - SOAP/XML	[Org]	--	--	SOAP/XML Host	<AD_USER>	login.windows.net	443	60000	80	2015-05-14 11:25:14	em7admin
3. Azure Credential - SSHKey	[Org]	--	--	SSHKey	<SUBSCRIPTION_ID_H ID		22	180000	59	2015-05-14 11:25:14	em7admin
4. Cisco SNMPV2 - Example	[Org]	--	--	SNMP			161	1500	3	2015-05-14 11:25:14	em7admin
5. Cisco SNMPV3 - Example	[Org]	--	--	SNMP	[USER_GOES_HERE]		161	1500	2	2015-05-14 11:25:14	em7admin
6. Cisco ACI	[Org]	--	--	126 Basic/Snippet	admin	173.36.219.46	443	0	62	2015-05-14 15:05:24	em7admin
7. Cisco ACI Credential	[Org]	--	--	Basic/Snippet	admin	198.16.133.200	443	0	61	2015-05-14 14:32:20	em7admin
8. Cloudkick - Example	[Org]	--	--	Basic/Snippet	[SECURITY KEY GOES]	127.0.0.1	443	5000	9	2015-05-14 11:25:31	em7admin
9. CUCM Performance Service 9.9 Example	[Org]	--	--	SOAP/XML Host			8443	2000	4	2015-05-14 11:25:12	em7admin
10. EMC Central Database	[Org]	--	--	Database	root	localhost	7706	0	51	2015-05-14 11:26:41	em7admin
11. EMC Collector Database	[Org]	--	--	Database	root	ND	7707	0	14	2015-05-14 11:25:43	em7admin
12. EM7 DB	[Org]	--	--	Database	root	ND	7706	0	35	2015-05-14 11:26:32	em7admin
13. EM7 DB - DB Info	[Org]	--	--	SOAP/XML Host	root	ND	80	3000	36	2015-05-14 11:26:32	em7admin
14. EM7 DB - My conf	[Org]	--	--	SOAP/XML Host	root	ND	80	3000	37	2015-05-14 11:26:32	em7admin
15. EM7 DB - Sdk conf	[Org]	--	--	SOAP/XML Host	root	ND	80	3000	36	2015-05-14 11:26:32	em7admin
16. EM7 Default V2	[Org]	--	--	SNMP			161	1500	10	2015-05-14 11:25:42	em7admin
17. EM7 Default V3	[Org]	--	--	SNMP	em7admin3		161	500	11	2015-05-14 11:25:42	em7admin
18. EMC - Example	[Org]	--	--	Basic/Snippet	root	ND	443	10000	15	2015-05-14 11:25:47	em7admin
19. GIGWI - Example	[Org]	--	--	Basic/Snippet	[SECURITY KEY GOES]	127.0.0.1	443	5000	16	2015-05-14 11:25:51	em7admin
20. IPSLA Example	[Org]	--	--	SNMP			161	1500	5	2015-05-14 11:25:14	em7admin
21. iService Endpoint SNMP	[Org]	--	--	SNMP	control	ND	161	3000	18	2015-05-14 11:25:58	em7admin
22. iService Endpoint SSH/CLI	[Org]	--	--	Basic/Snippet	auto	ND	22	3	17	2015-05-14 11:25:58	em7admin
23. Local API	[Org]	--	--	Basic/Snippet	em7admin	10.0.0.160	80	5000	22	2015-05-14 11:26:11	em7admin
24. NetApp 7-mode	[Org]	--	--	Basic/Snippet	root	ND	443	3000	24	2015-05-14 11:26:20	em7admin
25. NetApp iSSM Option	[Org]	--	--	SOAP/XML Host	root	ND	443	3000	26	2015-05-14 11:26:20	em7admin
26. NetApp iSSM Option CRT	[Org]	--	--	SOAP/XML Host	root	ND	443	10000	25	2015-05-14 11:26:20	em7admin
27. Nexus netconf	[Org]	--	--	Basic/Snippet		ND	22	10000	6	2015-05-14 11:25:16	em7admin
28. Nexus snmp	[Org]	--	--	SNMP		ND	161	10000	7	2015-05-14 11:25:16	em7admin
29. Polycom - Advanced	[Org]	--	--	SOAP/XML Host	admin	ND	80	20000	28	2015-05-14 11:26:24	em7admin
30. Polycom - CDR	[Org]	--	--	SOAP/XML Host	admin	ND	80	20000	31	2015-05-14 11:26:24	em7admin
31. Polycom - Interface	[Org]	--	--	SOAP/XML Host	admin	ND	80	20000	29	2015-05-14 11:26:24	em7admin

- In the **Credential Management** page, click the **[Actions]** menu. Select **Create SOAP/XML Host Credential**.

- The **Credential Editor** modal page appears. In this page, you can define the new SOAP/XML credential. To define the new credential, supply values in the following fields:

### **Basic Settings**

- Profile Name.** Name of the credential. Can be any combination of alphanumeric characters.

- **Content Encoding.** Tells the SOAP server or XML data-store how the content is encoded, so the SOAP server or XML data-store knows how to decode the message. Select the encoding that is appropriate for your request and response. If you are creating a credential to use with a proxied web service, you can accept the default value in this field; the proxied web service does not use this value.
- **Method.** HTTP method to use to exchange credential data from the managed device. Choices are *GET* or *POST*. If you are creating a credential to use with a proxied web service, you can accept the default value in this field; the proxied web service does not use this value.

**NOTE:** Typically, Dynamic Applications of type "XML" use GET methods. Dynamic Applications of type "SOAP" and of type "XSLT" use POST methods.

- **HTTP Version.** Version of HTTP to use. Choices are *1.0* or *1.1*. If you are creating a credential to use with a proxied web service, you can accept the default value in this field; the proxied web service does not use this value.
- **URL.** Address of the SOAP server, HTML document, or XML document. Should be of the format:  

https://IP address:port/full path to desired SOAP, HTML, or XML document

  - You can include the variable **%D** in this field. SL1 will replace the variable with the IP address of the current device (device that is currently using the credential).

**NOTE:** For component devices, SL1 will replace %D with the IP address of the root device.

- You can include the variable **%N** in this field. SL1 will replace the variable with the hostname of the current device (device that is currently using the credential). If SL1 cannot determine the hostname, SL1 will replace the variable with the primary management IP address for the current device.
- If you are creating a credential to use with a proxied web service, you can enter any valid URL in this field. The proxied web service does not use this value, but the **Credential Editor** page requires a value in this field.
- **HTTP Auth User.** Username with which to log in to the web server. If you will use this credential with a proxied web service, you can include one or more of the following variables in this field:
  - **%u.** The username of the user currently logged in to the Administration Portal or All-In-One Appliance.
  - **%e.** Email address of the user currently logged in to the Administration Portal or All-In-One Appliance.
- **HTTP Auth Password.** Password with which to access the web server. If you use this credential with a proxied web service, you can include the following variable in this field:
  - **%p.** The password of the user currently logged in to the Administration Portal or All-In-One Appliance.

**NOTE:** You can use the %e, %p, and %u substitution variables only in credentials that will be aligned with a proxied web service. You cannot use these substitution variables in credentials that will be aligned with a Dynamic Application.

- **Timeout (seconds).** Time, in seconds, after which SL1 will stop trying to communicate with the web server. If you are creating a credential to use with a proxied web service, you can accept the default value in this field; the proxied web service does not use this value.

### Proxy Settings

This pane displays optional fields. If you use a proxy server in front of the SOAP server(s) or XML data-store (s) you want to communicate with, enter values in these fields.

- **Hostname/IP.** The host name or IP address of the proxy server.
- **Port.** Port on the proxy server to which you will connect.
- **User.** Username to use to access the proxy server.
- **Password.** Password to use to access the proxy server.

### cURL Options

- You can include the cURL command and various options in your credential. The list of cURL options lists all the options you can include in your credential. To include a cURL option in the credential, select it and then select the right-arrow icon. You can then supply arguments in the field to the left of the option.
- For more information on cURL commands, see the cURL manpage at <http://curl.haxx.se/docs/manpage.html>.

### SOAP Options

These fields are optional. When a SOAP/XML credential is aligned with a SOAP or XSLT Dynamic Application, the requests defined in the Dynamic Application can use the values defined in these fields. To use a value defined in one of these fields, the request must include the substitution character associated with that value. For example, suppose a Dynamic Application request includes the XML tag <high\_value=%1 >. Suppose you specified "100" in the **Embed Value [%1]** field in the credential aligned with that Dynamic Application. The request will be sent with the XML tag <high\_value=100>.

- **Embedded Password [%P].** Specifies a password value to include in a request. The value defined in this field is substituted in to the %P substitution character. The value will be encrypted in the request, will be masked in the **Credential Editor**, and will be stored in an encrypted form in the database.
- **Embed Value %1.** The value defined in this field is substituted in to the %1 substitution character.
- **Embed Value %2.** The value defined in this field is substituted in to the %2 substitution character.
- **Embed Value %3.** The value defined in this field is substituted in to the %3 substitution character.
- **Embed Value %4.** The value defined in this field is substituted in to the %4 substitution character.

## HTTP Headers

- If you require custom HTTP headers to communicate with the SOAP server, you can build the custom header here.
- If you are using this credential with a proxied web service, you can include one or more of the following variables in your custom HTTP headers:
  - %u. The username of the user currently logged in to the Administration Portal or All-In-One Appliance.
  - %e. Email address of the user currently logged in to the Administration Portal or All-In-One Appliance.
  - %p. The password of the user currently logged in to the Administration Portal or All-In-One Appliance.

**NOTE:** You can use the %e, %p, and %u substitution variables only in credentials that will be aligned with a proxied web service. You cannot use these substitution variables in credentials that will be aligned with a Dynamic Application.

5. Click the **[Save]** button to save the new SOAP/XML credential.
6. Repeat steps 1-5 for each SOAP/XML credential in your network.

**NOTE:** When you define a SOAP/XML Credential, the credential will automatically be aligned with the organization(s) you are a member of. To learn more about credentials and organizations, see the section [Aligning Organizations With a Credential](#) in this chapter.

---

## Defining an LDAP/AD Credential

LDAP or Active Directory credentials allow SL1 to access data on an LDAP server or an Active Directory server.

**Authentication** is the method by which SL1 determines if a user can access the SL1 system. For user accounts that are to be authenticated with LDAP or Active Directory, SL1 uses the LDAP or Active Directory credential to establish communication with the LDAP or Active Directory server. SL1 will then query the Active Directory or the LDAP server to determine if the username and password are legitimate and accurate.

Additionally, SL1 can automatically create accounts for one or more LDAP or Active Directory users. SL1 uses the LDAP or Active Directory credential to communicate with Active Directory or the LDAP server and:

- Determine if the username and password are legitimate and accurate.
- Gather information to populate fields in the user's automatically-created account.

For details on using Active Directory or LDAP for authentication, see the manual *Using Active Directory and LDAP*.

To define an LDAP/AD credential:

1. Collect the information you need to create each credential (usually username and password).
2. Go to the **Credential Management** page (System > Manage > Credentials).

Credential Management | Credentials Found [62]

Profile Name	Organization	BO Use	EV Use	DA Use	Type	Credential User	Host	Port	Timeout(ms)	ID	Law	Actions	
1. Amazon Web Services Credential		--	--	--	SOAP/XML Host	[AWS Account Access]	example.com	80	2000	1	2015-05-14	Create SNMP Credential	
2. Azure Credential - SOAP/XML	[AD orgs]	--	--	--	SOAP/XML Host	<AD_USER>	login.windows.net	443	60000	60	2015-05-14	Create Database Credential	
3. Azure Credential - SSHKey	[AD orgs]	--	--	--	SSHKey	<SUBSCRIPTION_ID_H_ND		22	180000	59	2015-05-14	Create SOAP/XML Host Credential	
4. Cisco SNMPV2 - Example	[AD orgs]	--	--	--	SNMP			161	1500	3	2015-05-14	Create LDAP/AD Credential	
5. Cisco SNMPV3 - Example	[AD orgs]	--	--	--	SNMP	[USER_GOES_HERE]		161	1500	2	2015-05-14	Create SSH/Key Credential	
6. Cisco ACI	[AD orgs]	--	--	--	126	Basic/Snippet	admin	173.38.219.46	443	0	62	2015-05-14 15:05:24	Create PowerShell Credential
7. Cisco ACI Credential	[AD orgs]	--	--	--	Basic/Snippet	admin	198.18.133.200	443	0	61	2015-05-14 14:32:20		
8. Cloudkick - Example	[AD orgs]	--	--	--	Basic/Snippet	[SECURITY KEY GOES]	127.0.0.1	443	5000	9	2015-05-14 11:25:31		
9. EMC ProtectionService 6.9 Example	[AD orgs]	--	--	--	SOAP/XML Host			8443	2000	4	2015-05-14 11:26:12		
10. EMAT Central Database	[AD orgs]	--	--	--	Database	root	localhost	7706	0	51	2015-05-14 11:26:41		
11. EMAT Collector Database	[AD orgs]	--	--	--	Database	root	ND	7707	0	14	2015-05-14 11:25:43		
12. EMAT DB	[AD orgs]	--	--	--	Database	root	ND	7706	0	35	2015-05-14 11:26:32		
13. EMAT DB - DB Info	[AD orgs]	--	--	--	SOAP/XML Host	root	ND	80	3000	38	2015-05-14 11:26:32		
14. EMAT DB - My conf	[AD orgs]	--	--	--	SOAP/XML Host	root	ND	80	3000	37	2015-05-14 11:26:32		
15. EMAT DB - Sdk conf	[AD orgs]	--	--	--	SOAP/XML Host	root	ND	80	3000	36	2015-05-14 11:26:32		
16. EMAT Default V2	[AD orgs]	--	--	--	SNMP			161	1500	10	2015-05-14 11:26:42		
17. EMAT Default V3	[AD orgs]	--	--	--	SNMP	em7Default3		161	500	11	2015-05-14 11:26:42		
18. EMC - Example	[AD orgs]	--	--	--	Basic/Snippet	root	ND	443	10000	15	2015-05-14 11:25:47		
19. GIGWI - Example	[AD orgs]	--	--	--	Basic/Snippet	[SECURITY KEY GOES]	127.0.0.1	443	5000	16	2015-05-14 11:25:51		
20. IPSLA Example	[AD orgs]	--	--	--	SNMP			161	1500	5	2015-05-14 11:25:14		
21. LIFESize Endpoint SNMP	[AD orgs]	--	--	--	SNMP	control		161	3000	18	2015-05-14 11:25:58		
22. LIFESize Endpoint SSH/CLI	[AD orgs]	--	--	--	Basic/Snippet	auto	ND	22	3	17	2015-05-14 11:25:58		
23. Local API	[AD orgs]	--	--	--	Basic/Snippet	em7Admin	10.0.0.180	80	5000	22	2015-05-14 11:26:11		
24. NetApp 7-mode	[AD orgs]	--	--	--	Basic/Snippet	root	ND	443	3000	24	2015-05-14 11:26:20		
25. NetApp iSSSL Option	[AD orgs]	--	--	--	SOAP/XML Host	root	ND	443	3000	26	2015-05-14 11:26:20		
26. NetApp iSSSL Option Off	[AD orgs]	--	--	--	SOAP/XML Host	root	ND	443	10000	25	2015-05-14 11:26:20		
27. Nexus netconf	[AD orgs]	--	--	--	Basic/Snippet		ND	22	10000	6	2015-05-14 11:25:16		
28. Nexus snmp	[AD orgs]	--	--	--	SNMP			161	10000	7	2015-05-14 11:25:16		
29. Polycom - Advanced	[AD orgs]	--	--	--	SOAP/XML Host	admin	ND	80	20000	28	2015-05-14 11:26:24		
30. Polycom - CDR	[AD orgs]	--	--	--	SOAP/XML Host	admin	ND	80	20000	31	2015-05-14 11:26:24		
31. Polycom - Interface	[AD orgs]	--	--	--	SOAP/XML Host	admin	ND	80	20000	29	2015-05-14 11:26:24		

3. In the **Credential Management** page, click the **[Actions]** menu. Select **Create LDAP/AD Credential**.

Credential Editor

Create New LDAP/AD Credential

Basic Settings

Profile Name:  LDAP Type:

Hostname/IP:  Secure:  Port:  Timeout(ms):

RDN (Bind DN / bind user):  LDAP Domain:  Bind Password:

User Search Base:  User Search Scope:

Save

4. The **Credential Editor** modal page appears. In this page, you can define the new LDAP/AD Credential. To define the new credential, supply values in the following fields:

**Basic Settings**

- **Profile Name.** Name of the credential. Can be any combination of alphanumeric characters.
- **LDAP Type.** Specifies the "flavor" or LDAP running on the directory server. Choices are LDAP or Active Directory.
- **Hostname/IP.** Hostname or IP address of the LDAP or Active Directory server.
- **Port.** Port number on the LDAP or Active Directory server to which SL1 will send requests.
- **Secure.** Specifies whether you are using LDAP over SSL.

- **RDN (Bind DN / bind user)**. Bind DN. The bind DN is a user on the LDAP or Active Directory server who is permitted to search the directory within the specified search base.
  - In many LDAP or AD configurations, each user has read-access to his/her own account. Therefore, you might find it most useful to include the %u variable in this field. When an LDAP or AD user logs in to SL1, SL1 stores the username in the %u variable. SL1 then uses the %u variable to build the bind DN, uses the bind DN to communicate with the LDAP or AD server, and then authenticates the current user.
  - An example entry in the RDN field might be:

```
uid=%u, ou=People, dc=sciencelogic, dc=com
```

This creates a DN using the current login name as the uid.

- You can also include the %d variable in this field. The %d variable represents the name of the LDAP domain, as specified in the **LDAP Domain** field.

**NOTE:** If you have configured SL1 to automatically create accounts when a user logs in with an LDAP/AD username, you must include the %u variable in the RDN field.

- **LDAP Domain**. If your LDAP or Active Directory configuration includes multiple domains, specify the domain components to bind to in this field. For example, you could specify:

```
dc=reston, dc=sciencelogic, dc=com.
```

This would bind to the sub-domain "reston", in the domain "sciencelogic", in the domain "com".

- **Bind Password**. Password that allows access to the LDAP or Active Directory server. In most cases, when you specify a bind password in a credential, you are creating a "write" credential (that is, a credential that allows SL1 to make changes to the LDAP or AD server).



- **User Search Base.** In this field, you specify the area in the directory where users to be authenticated reside, using RDN notation. For example, if you want to authenticate five users from the ou called "people", you could specify the RDN that includes that ou.

```
ou=People, dc=sciencelogic, dc=com.
```

This would allow SL1 to authenticate users in the ou called "people." In the **User Search Scope** field, you can specify whether SL1 should also authenticate all users in any ou underneath "people".

- **User Search Scope.** In this field, you specify whether SL1 should search only the directory specified in **User Search Base** or whether SL1 should search the directory specified in **User Search Base** and all its child branches. Choice are:
  - *Subtree.* SL1 should search the directory specified in **User Search Base** and also search all its child branches.
  - *One Level.* SL1 should search only the directory specified in **User Search Base**.

5. Click the **[Save]** button to save the new LDAP/AD credential.

6. Repeat steps 1-5 for each LDAP/AD credential in your network.

**NOTE:** When you define an LDAP/AD Credential, the credential will automatically be aligned with the organization(s) you are a member of. To learn more about credentials and organizations, see the section [Aligning Organizations With a Credential](#).

---

## Defining a Basic/Snippet Credential

**NOTE:** Dynamic Applications of type "snippet" are not required to use only the Basic/Snippet Credential. In Dynamic Applications of type "snippet", the snippet code must define the authentication protocol. Therefore, Dynamic Applications of type "snippet" can use any type of credential.

Basic/Snippet credentials define standard authentication parameters, but are not tied to a specific authentication protocol. Basic/Snippet credentials are used in several places in SL1, including:

- **With Dynamic Applications of type "snippet".** The snippet code must define the authentication protocol.
- **With Dynamic Applications of type "WMI".** The authentication protocol is specific to WMI and is specified by SL1 when the Dynamic Application is executed. To access WMI information on a Windows server, ensure that the **Username** you specify is allowed access to the server and to the WMI namespace.
- **With Dynamic Applications of type "PowerShell".** For information about configuring your environment for PowerShell collection, see the **Monitoring Windows Systems** manual.
- **When defining external backups.** The authentication protocol is defined in the **Backup Management** page (System > Settings > Backup).

To define a Basic/Snippet credential:

1. Collect the information you need to create each credential (usually username and password).
2. Go to the **Credential Management** page (System > Manage > Credentials).

Profile Name	Organization	EO Use	EW Use	DA Use	Type	Credential User	Host	Port	Timeout (ms)	ID	Law	Actions
1 Amazon Web Services Credential		--	--	--	SOAP/XML Host	[AWS Account Access]	example.com	80	2000	1	2015-05-14	Create SNMP Credential
2 Azure Credential - SOAP/XML	[AI orgs]	--	--	--	SOAP/XML Host	<AD_USER>	login.windows.net	443	60000	60	2015-05-14	Create Database Credential
3 Azure Credential - SSHKey	[AI orgs]	--	--	--	SSHKey	<SUBSCRIPTION_ID_H	N/D	22	180000	59	2015-05-14	Create SOAP/XML Host Credential
4 Cisco SNMPV2 - Example	[AI orgs]	--	--	--	SNMP			161	1500	3	2015-05-14	Create LDAP/AD Credential
5 Cisco SNMPV3 - Example	[AI orgs]	--	--	--	SNMP	[USER_GOES_HERE]		161	1500	2	2015-05-14	Create SSH/Key Credential
6 Cisco ACI	[AI orgs]	--	--	--	Basic/Snippet	admin	173.38.219.46	443	0	62	2015-05-14 15:05:24	Create PowerShell Credential
7 Cisco ACI Credential	[AI orgs]	--	--	--	Basic/Snippet	admin	198.18.133.200	443	0	61	2015-05-14 14:32:20	
8 Cloudkick - Example	[AI orgs]	--	--	--	Basic/Snippet	[SECURITY KEY GOES]	127.0.0.1	443	5000	9	2015-05-14 11:25:31	
9 CUCM PerformanceService 9.1 Example	[AI orgs]	--	--	--	SOAP/XML Host			8443	2000	4	2015-05-14 11:25:12	
10 EMAT Central Database	[AI orgs]	--	--	--	Database	root	localhost	7706	0	51	2015-05-14 11:26:41	
11 EMAT Collector Database	[AI orgs]	--	--	--	Database	root	N/D	7707	0	14	2015-05-14 11:25:43	
12 EMAT DB	[AI orgs]	--	--	--	Database	root	N/D	7706	0	35	2015-05-14 11:26:32	
13 EMAT DB - DB Info	[AI orgs]	--	--	--	SOAP/XML Host	root	N/D	80	3000	38	2015-05-14 11:26:32	
14 EMAT DB - My conf	[AI orgs]	--	--	--	SOAP/XML Host	root	N/D	80	3000	37	2015-05-14 11:26:32	
15 EMAT DB - Sdk conf	[AI orgs]	--	--	--	SOAP/XML Host	root	N/D	80	3000	36	2015-05-14 11:26:32	
16 EMAT Default V2	[AI orgs]	--	--	--	SNMP			161	1500	10	2015-05-14 11:25:42	
17 EMAT Default V3	[AI orgs]	--	--	--	SNMP	em7DefaultV3		161	500	11	2015-05-14 11:25:42	
18 EMC - Example	[AI orgs]	--	--	--	Basic/Snippet	root	N/D	443	10000	15	2015-05-14 11:25:47	
19 GIGWI - Example	[AI orgs]	--	--	--	Basic/Snippet	[SECURITY KEY GOES]	127.0.0.1	443	5000	16	2015-05-14 11:25:51	
20 IPSLA Example	[AI orgs]	--	--	--	SNMP			161	1500	5	2015-05-14 11:25:14	
21 iService Endpoint SNMP	[AI orgs]	--	--	--	SNMP	control	N/D	161	3000	18	2015-05-14 11:25:58	
22 iService Endpoint SSH/CLI	[AI orgs]	--	--	--	Basic/Snippet	admin	N/D	22	3	17	2015-05-14 11:25:58	
23 Local API	[AI orgs]	--	--	--	Basic/Snippet	em7Admin	10.0.0.180	80	5000	22	2015-05-14 11:26:11	
24 NetApp 7-mode	[AI orgs]	--	--	--	Basic/Snippet	root	N/D	443	3000	24	2015-05-14 11:26:20	
25 NetApp iWSSL Option	[AI orgs]	--	--	--	SOAP/XML Host	root	N/D	443	3000	26	2015-05-14 11:26:20	
26 NetApp iWSSL Option CRT	[AI orgs]	--	--	--	SOAP/XML Host	root	N/D	443	10000	25	2015-05-14 11:26:20	
27 Nexus netconf	[AI orgs]	--	--	--	Basic/Snippet		N/D	22	10000	6	2015-05-14 11:25:16	
28 Nexus snmp	[AI orgs]	--	--	--	SNMP			161	10000	7	2015-05-14 11:25:16	
29 Polycom - Advanced	[AI orgs]	--	--	--	SOAP/XML Host	admin	N/D	80	20000	28	2015-05-14 11:26:24	
30 Polycom - CDR	[AI orgs]	--	--	--	SOAP/XML Host	admin	N/D	80	20000	31	2015-05-14 11:26:24	
31 Polycom - Interface	[AI orgs]	--	--	--	SOAP/XML Host	admin	N/D	80	20000	29	2015-05-14 11:26:24	

3. In the **Credential Management** page, click the **[Actions]** menu. Select **Create Basic/Snippet Credential**.

**Credential Editor** X

Create New Basic/Snippet Credential Reset

---

**Basic Settings**

Credential Name

Hostname/IP  Port  Timeout(ms)

Username  Password

**Save**

4. The **Credential Editor** modal page appears. In this page, you can define the new Basic/Snippet credential. To define the new credential, supply values in the following fields:

- **Credential Name.** Name of the credential. Can be any combination of alphanumeric characters. This field is required.
- **Hostname/IP.** Hostname or IP address of the device from which you want to retrieve data. This field is required.
  - You can include the variable **%D** in this field. SL1 will replace the variable with the IP address of the current device (device that is currently using the credential).
  - You can include the variable **%N** in this field. SL1 will replace the variable with the hostname of the current device (device that is currently using the credential). If SL1 cannot determine the hostname, SL1 will replace the variable with the primary management IP address for the current device.

- **Port**. Port number associated with the data you want to retrieve. This field is required.
- **Timeout (ms)**. Time, in milliseconds, after which SL1 will stop trying to communicate with the authenticating server.
- **Username**. Username for a user account on the device.
- **Password**. Password for a user account on the device.

5. Click the **[Save]** button to save the new Basic/Snippet credential.
6. Repeat steps 1-5 for each Basic/Snippet credential in your network.

**NOTE:** When you define a Basic/Snippet credential, the credential will automatically be aligned with the organization(s) you are a member of. To learn more about credentials and organizations, see the section [Aligning Organizations With a Credential](#).

---

## Defining an SSH/Key Credential

Secure Shell (SSH) is a network protocol that enables users to securely access a command-line shell on a remote computer or server over an unsecured network. SSH provides strong encryption and authentication capabilities, making it an ideal method for securely administering commands or transferring data between a client and server.

To make SSH even more secure, you can use SSH keys instead of a simple password to log into a server. SSH keys consist of two long strings of characters, called a public/private key pair, that are much less susceptible than passwords are to brute force attacks. The public key is placed on the server you want to access, while the private key resides on the client. When you use SSH to log into the server from the client, the key pair is used to authenticate the session.

In SL1, some Dynamic Applications of type "Snippet" use SSH to communicate with a remote device. To use these Dynamic Applications, you must define an SSH credential. This credential specifies the hostname or IP address of the system you want to monitor, the port number used to access that system, and the private key used for authentication.

**NOTE:** Consult the documentation associated with the PowerPack that contains the Dynamic Application of type "Snippet" to find detailed directions on configuring the remote device and generating a private key for SL1 to use.

To define an SSH/Key credential:

1. Collect the information you need to create each credential (usually username and password).

2. Go to the **Credential Management** page (System > Manage > Credentials).

Profile Name	Organization	BU Use	DA Use	Type	Credential User	Host	Port	Timeout (ms)	ID	Last
1 Amazon Web Services Credential	[All Orgs]	--	--	SOAP/XML Host	[AWS Account Access]	example.com	80	2000	1	2015-05-14 11:25:14
2 Azure Credential - SOAP/XML	[All Orgs]	--	--	SOAP/XML Host	<AD_USER>	login.windows.net	443	60000	60	2015-05-14 11:25:14
3 Azure Credential - SSH/Key	[All Orgs]	--	--	SSH/Key	<SUBSCRIPTION_ID_H	ND	22	180000	59	2015-05-14 11:25:14
4 Cisco SNMPv2 - Example	[All Orgs]	--	--	SNMP	--	--	161	1500	3	2015-05-14 11:25:14
5 Cisco SNMPv3 - Example	[All Orgs]	--	--	SNMP	[USER_GOES_HERE]	--	161	1500	2	2015-05-14 11:25:14
6 Cisco - ACI	[All Orgs]	--	--	126	Basic/Snippet	admin	173.30.219.46	443	0	2015-05-14 15:05:24
7 Cisco - ACI Credential	[All Orgs]	--	--	Basic/Snippet	admin	198.16.133.200	443	0	61	2015-05-14 14:32:20
8 Cloudkick - Example	[All Orgs]	--	--	Basic/Snippet	[SECURITY KEY GOES]	127.0.0.1	443	5000	9	2015-05-14 11:25:31
9 Cloud Managed Network Service 0 0 Example	[All Orgs]	--	--	SOAP/XML Host	--	ND	8443	2000	4	2015-05-14 11:25:12
10 EMC Centri Database	[All Orgs]	--	--	Database	root	localhost	7706	0	51	2015-05-14 11:26:41
11 EMC Collector Database	[All Orgs]	--	--	Database	root	ND	7707	0	14	2015-05-14 11:25:43
12 EMC DB	[All Orgs]	--	--	Database	root	ND	7706	0	35	2015-05-14 11:26:32
13 EMC DB - DB Info	[All Orgs]	--	--	SOAP/XML Host	root	ND	80	3000	38	2015-05-14 11:26:32
14 EMC DB - My conf	[All Orgs]	--	--	SOAP/XML Host	root	ND	80	3000	37	2015-05-14 11:26:32
15 EMC DB - Siko.conf	[All Orgs]	--	--	SOAP/XML Host	root	ND	80	3000	36	2015-05-14 11:26:32
16 EMC Default V2	[All Orgs]	--	--	SNMP	--	--	161	1500	10	2015-05-14 11:25:42
17 EMC Default V3	[All Orgs]	--	--	SNMP	em7DefaultV3	--	161	500	11	2015-05-14 11:25:42
18 EMC - Example	[All Orgs]	--	--	Basic/Snippet	root	ND	443	10000	15	2015-05-14 11:25:47
19 GIGWI - Example	[All Orgs]	--	--	Basic/Snippet	[SECURITY KEY GOES]	127.0.0.1	443	5000	16	2015-05-14 11:25:51
20 IPSLA Example	[All Orgs]	--	--	SNMP	--	--	161	1500	5	2015-05-14 11:25:14
21 iPractice - Endpoint SNMP	[All Orgs]	--	--	SNMP	control	ND	161	3000	18	2015-05-14 11:25:58
22 iPractice - Endpoint SSH/CLI	[All Orgs]	--	--	Basic/Snippet	auto	ND	22	3	17	2015-05-14 11:25:58
23 Local API	[All Orgs]	--	--	Basic/Snippet	em7admin	10.0.0.160	80	5000	22	2015-05-14 11:26:11
24 NetApp 7-mode	[All Orgs]	--	--	Basic/Snippet	root	ND	443	3000	24	2015-05-14 11:26:20
25 NetApp w/SSL Option	[All Orgs]	--	--	SOAP/XML Host	root	ND	443	3000	26	2015-05-14 11:26:20
26 NetApp w/SSL Option CRT	[All Orgs]	--	--	SOAP/XML Host	root	ND	443	10000	25	2015-05-14 11:26:20
27 Nexus netconf	[All Orgs]	--	--	Basic/Snippet	--	ND	22	10000	6	2015-05-14 11:25:16
28 Nexus snmp	[All Orgs]	--	--	SNMP	--	--	161	10000	7	2015-05-14 11:25:16
29 Polycom - Advanced	[All Orgs]	--	--	SOAP/XML Host	admin	ND	80	20000	28	2015-05-14 11:26:24
30 Polycom - CDR	[All Orgs]	--	--	SOAP/XML Host	admin	ND	80	20000	31	2015-05-14 11:26:24
31 Polycom - Interface	[All Orgs]	--	--	SOAP/XML Host	admin	ND	80	20000	29	2015-05-14 11:26:24



3. In the **Credential Management** page, click the **[Actions]** menu. Select **Create SSH/Key Credential**.

4. The **Credential Editor** modal page appears. In this page, you can define the new SSH/Key credential. To define the new credential, supply values in the following fields:

- **Credential Name.** Name of the credential. Can be any combination of alphanumeric characters.
- **Hostname/IP.** Hostname or IP address of the device from which you want to retrieve data.
  - You can include the variable %D in this field. SL1 will replace the variable with the IP address of the current device (device that is currently using the credential).
  - You can include the variable %N in this field. SL1 will replace the variable with hostname of the current device (device that is currently using the credential). If SL1 cannot determine the hostname, SL1 will replace the variable with the primary, management IP address for the current device.

- **Port**. Port number associated with the data you want to retrieve.

**NOTE:** The default TCP port for SSH servers is 22.

- **Timeout (ms)**. Time, in milliseconds, after which SL1 will stop trying to communicate with the authenticating server.
  - **Username**. Username for an SSH or user account on the device to be monitored.
  - **Password**. Password for an SSH user account on the device to be monitored.
  - **Private Key (PEM Format)**. Enter the SSH private key that you want SL1 to use, in PEM format.
5. Click the **[Save]** button to save the new SSH/Key credential.
  6. Repeat steps 1-5 for each SSH/Key credential in your network.

**NOTE:** When you define a SSH/Key credential, the credential will automatically be aligned with the organization(s) you are a member of. To learn more about credentials and organizations, see the section [Aligning Organizations With a Credential](#).

---

## Defining a PowerShell Credential

Dynamic Applications can include PowerShell commands that collect data from Windows devices. If you want to use SL1's built-in transport agent (that is, run "agentless" on the Windows device), you can align a PowerShell credential with those Dynamic Applications.

**NOTE:** Consult the *Monitoring Windows* and *WMI and PowerShell Dynamic Application Development* manuals to find detailed directions on configuring the Windows devices for agentless communication and on configuring a proxy server.

To define a PowerShell credential in SL1:

1. Collect the information you need to create the credential:
  - The username and password for a user on the Windows device.
  - If the user is an Active Directory account, the hostname or IP address of the Active Directory server and the domain.
  - Whether an encrypted connection should be used.
  - If you are using a Windows Management Proxy, the hostname or IP address of the proxy server.
2. Go to the **Credential Management** page (System > Manage > Credentials).

- In the **Credential Management** page, click the **[Actions]** menu. Select **Create PowerShell Credential**.

Credential Management | Credentials Found [62]

Profile Name	Organization	RO Use	RW Use	DA Use	Type	Credential User	Host	Port	Timeout (ms)	ID	Last	Actions
1. Amazon Web Services Credential					SOAP/XML Host	[AWS Account Access]	example.com	80	2000	1	2015-05-14	Create SNMP Credential
2. Azure Credential - SOAP/XML	[All Orgs]				SOAP/XML Host	<AD_USER>	login.windows.net	443	60000	60	2015-05-14	Create Database Credential
3. Azure Credential - SSHKey	[All Orgs]				SSHKey	<SUBSCRIPTION_ID_H	%D	22	180000	59	2015-05-14	Create LDAP/AD Host Credential
4. Cisco SNMPv2 - Example	[All Orgs]				SNMP			161	1500	3	2015-05-14	Create Basic/Snippet Credential
5. Cisco SNMPv3 - Example	[All Orgs]				SNMP	[USER_GOES_HERE]		161	1500	2	2015-05-14	Create SSH/Key Credential
6. Cisco - ACI	[All Orgs]				Basic/Snippet	admin	173.36.210.46	443	0	62	2015-05-14 15:05:24	Create PowerShell Credential
7. Cisco - ACI Credential	[All Orgs]				Basic/Snippet	admin	198.18.133.200	443	0	61	2015-05-14 14:32:20	
8. Cloudkick - Example	[All Orgs]				Basic/Snippet	[SECURITY KEY GOES]	127.0.0.1	443	5000	9	2015-05-14 11:25:31	
9. CUCM PerformanceService 8.0 Example	[All Orgs]				SOAP/XML Host			8443	2000	4	2015-05-14 11:26:12	
10. EM7 Central Database	[All Orgs]				Database	root	localhost	7706	0	51	2015-05-14 11:26:41	
11. EM7 Collector Database	[All Orgs]				Database	root	%D	7707	0	14	2015-05-14 11:25:43	
12. EM7 DB	[All Orgs]				Database	root	%D	7706	0	35	2015-05-14 11:26:32	
13. EM7 DB - DR Info	[All Orgs]				SOAP/XML Host	root	%D	80	3000	36	2015-05-14 11:26:32	
14. EM7 DB - My conf	[All Orgs]				SOAP/XML Host	root	%D	80	3000	37	2015-05-14 11:26:32	
15. EM7 DB - Slic conf	[All Orgs]				SOAP/XML Host	root	%D	80	3000	36	2015-05-14 11:26:32	
16. EM7 Default V2	[All Orgs]				SNMP			161	1500	10	2015-05-14 11:25:42	
17. EM7 Default V3	[All Orgs]				SNMP	em7defaultv3	%D	161	500	11	2015-05-14 11:25:42	
18. EMC - Example	[All Orgs]				Basic/Snippet	root	%D	443	10000	15	2015-05-14 11:25:47	
19. GuGrid - Example	[All Orgs]				Basic/Snippet	[SECURITY KEY GOES]	127.0.0.1	443	5000	16	2015-05-14 11:25:51	
20. IPSLA Example	[All Orgs]				SNMP			161	1500	5	2015-05-14 11:25:14	
21. iReSize - Endpoint SNMP	[All Orgs]				SNMP	control		161	3000	18	2015-05-14 11:25:58	
22. iReSize - Endpoint SNMPCLI	[All Orgs]				Basic/Snippet	auto	%D	22	3	17	2015-05-14 11:25:58	
23. Local API	[All Orgs]				Basic/Snippet	em7admin	10.0.0.180	80	5000	22	2015-05-14 11:26:11	
24. NetApp 7-mode	[All Orgs]				Basic/Snippet	root	%D	443	3000	24	2015-05-14 11:26:20	
25. NetApp w/SSL Option	[All Orgs]				SOAP/XML Host	root	%D	443	3000	26	2015-05-14 11:26:20	
26. NetApp w/SSL Option Off	[All Orgs]				SOAP/XML Host	root	%D	443	10000	25	2015-05-14 11:26:20	
27. Nexus netconf	[All Orgs]				Basic/Snippet		%D	22	10000	6	2015-05-14 11:25:16	
28. Nexus snmp	[All Orgs]				SNMP			161	10000	7	2015-05-14 11:25:16	
29. Polycom - Advanced	[All Orgs]				SOAP/XML Host	admin	%D	80	20000	28	2015-05-14 11:26:24	
30. Polycom - CDR	[All Orgs]				SOAP/XML Host	admin	%D	80	20000	31	2015-05-14 11:26:24	
31. Polycom - Interface	[All Orgs]				SOAP/XML Host	admin	%D	80	20000	28	2015-05-14 11:26:24	

2

- The **Credential Editor** page appears, where you can define the following fields:

**Credential Editor**

Create New PowerShell Credential [Reset]

**Basic Settings**

Profile Name:

Account Type: [Active Directory] ▼

Hostname/IP:

Timeout (ms):

Username:

Password:

Encrypted: [yes] ▼

Port:

PowerShell Proxy Hostname/IP:

**Active Directory Settings**

Active Directory Hostname/IP:

Domain:

[Save]

- Profile Name.** Name of the credential. Can be any combination of alphanumeric characters.

- **Hostname/IP.** Hostname or IP address of the device from which you want to retrieve data.
  - You can include the variable **%D** in this field. SL1 will replace the variable with the IP address of the device that is currently using the credential.
  - You can include the variable **%N** in this field. SL1 will replace the variable with the hostname of the device that is currently using the credential. If SL1 cannot determine the hostname, SL1 will replace the variable with the primary, management IP address for the current device.
  - You can include the prefix **HOST** or **WSMAN** before the variable **%D** in this field if the device you want to monitor uses a service principal name (for example, "HOST://%D" or "WSMAN://%D"). SL1 will use the WinRM service **HOST** or **WSMan** instead of **HTTP** and replace the variable with the IP address of the device that is currently using the credential.
- **Username.** Username for an account on the Windows device to be monitored or on the proxy server.

**NOTE:** The user should not include the domain name prefix in the username for Active Directory accounts. For example, use "em7admin" instead of "MSDOMAIN\em7admin".

- **Encrypted.** Select whether SL1 will communicate with the device using an encrypted connection. Choices are:
  - *yes.* When communicating with the Windows server, SL1 will use a local user account with authentication of type "Basic Auth". You must then use HTTPS and can use a Microsoft Certificate or a self-signed certificate.
  - *no.* When communicating with the Windows server, SL1 will not encrypt the connection.
- **Port.** The port number used by the WinRM service on the Windows device. This field is automatically populated with the default port based on the value you selected in the **Encrypted** field.
- **Account Type.** Type of authentication for the username and password in this credential. Choices are:
  - *Active Directory.* On the Windows device, Active Directory will authenticate the username and password in this credential.
  - *Local.* Local security on the Windows device will authenticate the username and password in this credential.
- **Timeout (ms).** Time, in milliseconds, after which SL1 will stop trying to collect data from the authenticating server. For collection to be successful, SL1 must connect to the authenticating server, execute the PowerShell command, and receive a response within the amount of time specified in this field.
- **Password.** Password for the account on the Windows device to be monitored or on the proxy server.
- **PowerShell Proxy Hostname/IP.** If you use a proxy server in front of the Windows devices you want to communicate with, enter the fully-qualified domain name or the IP address of the proxy server in this field.
- **Active Directory Hostname/IP.** If you selected Active Directory in the **Account Type** field, specify the hostname or IP address of the Active Directory server that will authenticate the credential.

- **Domain**. If you selected Active Directory in the **Account Type** field, specify the domain where the monitored Windows device resides.

5. To save the credential, click the **[Save]** button. To clear the values you set, click the **[Reset]** button.

## Testing a Credential

You can test a credential from the **Credential Management** page using a predefined credential test. For more information about creating and managing credential tests, see the [Managing Credential Tests](#) chapter.

To run a credential test from the **Credential Management** page:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the **[Actions]** menu, and then select **Test Credential**. The **Credential Tester** modal page appears:

The screenshot shows a modal window titled "Credential Tester [BETA]". It has a close button (X) in the top right corner. The form contains the following fields:

- Test Type:** A dropdown menu with "SNMP Credential Test" selected.
- Credential:** A dropdown menu with "EM7 Default V2" selected.
- Hostname/IP:** An empty text input field.
- Collector:** A dropdown menu with "em7ao" selected.

At the bottom center of the modal is a button labeled "Run Test".

3. Supply values in the following fields:
  - **Test Type**. Select a credential test to run. This list includes the [ScienceLogic Default Credential Tests](#), credential tests included in any PowerPacks that have been optionally installed on your system, and credential tests that users have created on your system.
  - **Credential**. Select the credential to test. This drop-down list includes only credentials that you have access to that can be tested using the selected credential test.
  - **Hostname/IP**. Enter a hostname or IP address that will be used during the test. For example, if you are testing an SNMP credential, the hostname/IP address you supply will be used to perform a test SNMP request.
  - **Collector**. Select the All-In-One Appliance or Data Collector that will run the test.
4. Click the **[Run Test]** button to run the credential test. The **Test Credential** window appears:

Step	Description	Log Message	Status
1 Test Reachability	Check to see if the device is reachable using ICMP	The device is reachable using ICMP. The average response time is 0.397ms	Passed
2 Test Port Availability	Check to see if the SNMP port is open	Port 161 is open	Passed
3 Test SNMP Availability	Check to see if a walk of SNMP will return results	The SNMP SysName is ScienceLogic EM7 G3 - All-In-One	Passed

The **Test Credential** window displays a log entry for each step in the credential test. The steps performed are different for each credential test. The log entry for each step includes the following information:



- **Step**. The name of the step.
- **Description**. A description of the action performed during the step.
- **Log Message**. The result of the step for this execution of the credential test.
- **Status**. Whether the result of this step indicates the credential and/or the network environment is configured correctly (Passed) or incorrectly (Failed).
- **Step Tip**. Mouse over the question mark icon (❓) to display the tip text. The tip text recommends what to do to change the credential and/or the network environment if the step has a status of "Failed".

5. Optionally, you can click the **[Execute Discovery Session]** button to run a discovery session using the **Credential**, **Hostname/IP**, and **Collector** you selected in the **Credential Tester** modal page.

---

## ScienceLogic Default Credential Tests

This section describes the credential tests supplied by ScienceLogic in the default installation.

### AWS Credential Test

The AWS Credential Test can be used to test a SOAP/XML credential for monitoring AWS using the Dynamic Applications in the *Amazon Web Services* PowerPack. The AWS Credential Test performs the following steps:

- **Test Reachability**. Performs an ICMP ping request to the URL for the EC2 service in the region specified in the credential. If a region is not specified in the credential, the us-east-1 region is used.
- **Test Port Availability**. Performs an NMAP request to TCP port 443 on the URL for the EC2 service in the region specified in the credential. If a region is not specified in the credential, the us-east-1 region is used.
- **Test Name Resolution**. Performs an nslookup request on the URL for the EC2 service in the region specified in the credential. If a region is not specified in the credential, the us-east-1 region is used.
- **Make connection to AWS account**. Attempts to connect to the AWS service using the account specified in the credential.
- **Scan AWS services**. Verifies that the account specified in the credential has access to the services.

### Azure Credential Test

The Azure Credential Test can be used to test a SOAP/XML credential for monitoring Microsoft Azure using the Dynamic Applications in the *Microsoft: Azure* PowerPack. The Azure Credential Test performs the following steps:

- **Test Port Availability**. Performs an NMAP request to TCP port 443 on management.azure.com.
- **Test Name Resolution**. Performs an nslookup request on management.azure.com.
- **Make connection to Azure account**. Attempts to connect to the Azure service using the account specified in the credential.
- **Make Azure Active Directory Request**. Verifies that the account specified in the credential has the permissions required to discover the Azure account.

## Basic/Snippet Credential Test

The Basic/Snippet Credential Test can be used to test a Basic/Snippet credential for connectivity. The Basic/Snippet Credential Test performs the following steps:

- **Test Reachability.** Performs an ICMP ping request to the host specified in the credential.
- **Test Port Availability.** Performs an NMAP request to the TCP port specified in the credential on the host specified in the credential.
- **Test Name Resolution.** Performs an nslookup request on the host specified in the credential.

## Database Credential Test

The Database Credential Test can be used to test a Database credential for connectivity. The Database Credential Test performs the following steps:

- **Test Reachability.** Performs an ICMP ping request to the host specified in the credential.
- **Test Port Availability.** Performs an NMAP request to the TCP port specified in the credential on the host specified in the credential.
- **Test Name Resolution.** Performs an nslookup request on the host specified in the credential.
- **Make DB Connection.** Attempts to make a database connection using the credential and executes the query "SELECT 1;".
- **Verify Table Existence.** Attempts to make a database connection using the credential and executes the query "SELECT \* FROM master.system\_settings\_core;".

## PowerShell Credential Test

The PowerShell Credential Test can be used to test a PowerShell credential for connectivity. The PowerShell Credential Test performs the following steps:

- **Test Reachability.** Performs an ICMP ping request to the host specified in the credential.
- **Test Port Availability.** Performs an NMAP request to the TCP port specified in the credential on the host specified in the credential.
- **Test Name Resolution.** Performs an nslookup request on the host specified in the credential.
- **Test Kerberos.** If the credential does not specify local authentication, attempts to acquire a kerberos ticket using the credential.
- **Test WinRM Connection.** Attempts a WinRM connection using the credential.
- **Execute PowerShell Cmdlet.** Attempts to execute the 'Get-WmiObject Win32\_Process | Select Name' PowerShell Cmdlet using the credential.

## SNMP Credential Test

The SNMP Credential Test can be used to test an SNMP credential for connectivity. The SNMP Credential Test performs the following steps:

- **Test Reachability.** Performs an ICMP ping request to the host specified in the credential.
- **Test Port Availability.** Performs an NMAP request to the UDP port specified in the credential on the host specified in the credential.
- **Test SNMP Availability.** Attempts an SNMP getnext request to .1.3.6.1 using the credential.

## SOAP/XML Credential Test

The SOAP/XML Credential Test can be used to test a SOAP/XML credential for connectivity. The SOAP/XML Credential Test performs the following steps:

- **Test Reachability.** Performs an ICMP ping request to the host specified in the credential.
- **Test Port Availability.** Performs an NMAP request to the TCP port specified in the credential on the host specified in the credential.
- **Test Name Resolution.** Performs an nslookup request on the host specified in the credential.
- **Make cURL Request.** Attempts to make a cURL request connection using the credential.
- **Verify Content.** Attempts to make a cURL request connection using the credential and verifies whether "discovery\_session" appears in the response.

## SoftLayer Credential Test

The SoftLayer Credential Test can be used to test a SOAP/XML credential for monitoring SoftLayer using the Dynamic Applications in the *SoftLayer: Cloud PowerPack*. The SoftLayer Credential Test performs the following steps:

- **Test Reachability.** Performs an ICMP ping request to api.softlayer.com.
- **Test Port Availability.** Performs an NMAP request to TCP port 443 on api.softlayer.com.
- **Test Name Resolution.** Performs an nslookup request on api.softlayer.com.
- **Make connection to SoftLayer account.** Attempts to connect to the Softlayer Account endpoint using the account specified in the credential.
- **Query SoftLayer Resource.** Performs a getDatacenters request to the Softlayer Location endpoint using the account specified in the credential.

## SSH/Key Credential Test

The SSH/Key Credential Test can be used to test a SSH/Key credential for connectivity. The SSH/Key Credential Test performs the following steps:

- **Test Reachability.** Performs an ICMP ping request to the host specified in the credential.
- **Test Port Availability.** Performs an NMAP request to the TCP port specified in the credential on the host specified in the credential. If no port is specified in the credential, port 22 is used.
- **Test Name Resolution.** Performs an nslookup request on the host specified in the credential.
- **Make SSH Connection.** Attempts to make an SSH connection using the credential.
- **Execute Command via SSH.** Attempts to make an SSH connection using the credential and executes the command "ping localhost -c1".

## VMware Credential Test

The VMware Credential Test can be used to test a SOAP/XML credential for monitoring VMware using the Dynamic Applications in the *VMware: vSphere Base Pack PowerPack*. The VMware Credential Test performs the following steps:

- **Test Reachability.** Attempts to reach the vCenter server using ICMP.
- **Attempt VMware Connection.** Attempts to connect to the VMware service using the account specified in the credential.

---

## Specifying Credentials During Initial Discovery

**Discovery** is the process by which SL1 discovers what types of hardware and applications exist on the network and then retrieves data from the discovered hardware and applications.

Before running discovery, you must:

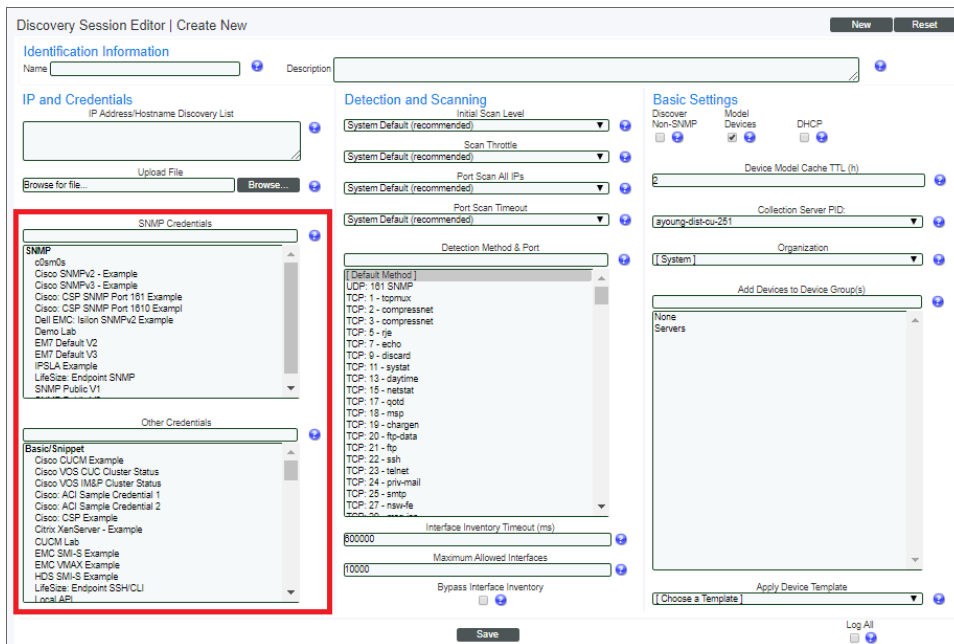
- Determine the SNMP credentials for the devices and applications in your network. Define correlating credentials in SL1, to allow discovery to retrieve as much information as possible.
- If you want SL1 to immediately start collecting data from devices using Dynamic Applications, you should also define any additional credentials required for those Dynamic Applications. For example, if you want SL1 to immediately start monitoring all MySQL databases in your network, you should define credentials that allow SL1 to communicate with each MySQL database in your network. During discovery, SL1 will determine which devices can be monitored with a Dynamic Application for MySQL. After discovery, SL1 will use the database credential to collect data about each MySQL database in your network.

Use the previous sections to define credentials for your network.

When you run discovery, you must specify one or more of these credentials to use. The more credentials you align with a discovery session, the more access SL1 will have to devices and their data during discovery.

To specify credentials during initial discovery:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
2. In the **Discovery Control Panel** page, click the **[Create]** button.
3. In the **Discovery Session Editor** page, supply values in each field.



4. In the **SNMP Credentials** field and in the **Other Credentials** field, you can select one or more credentials to use during discovery. In these fields, you should see a list of all credentials in SL1.
5. When trying to communicate with discovered hardware and applications, SL1 will look at the list of selected credentials and use the appropriate credential to get permission to access data on the external system.

**NOTE:** During discovery, SL1 tries each SNMP credential specified in the discovery session on each discovered device, to determine if SL1 can collect SNMP details from the device. Later in the discovery session, during alignment of Dynamic Applications, discovery again tries each SNMP credential specified in the discovery session. If one of the SNMP credentials times out three times **without any response**, discovery will stop trying to use that SNMP credential to align SNMP Dynamic Applications. Note that "no response" means that a device did not respond at all. Note that if a device reports that "no OID was found" or "the end of the OID tree was reached", these are considered a legitimate response and would not cause SL1 to abandon the credential.

## Defining the Primary and Secondary Credentials for a Single Device

You can define multiple credentials for a single device. This allows SL1 to align multiple agents and applications for a single device. For example, SL1 might use an SNMP credential to discover hardware information about a device and a database credential to retrieve information about the database on the same device.

To define primary and secondary credentials for a single device:

**NOTE:** When defining primary and secondary credentials for a device, you will see only the credentials aligned to organizations you are a member of. If a primary or secondary credential has already been defined on the device, and is aligned to an organization you are not a member of, the credential will be restricted.

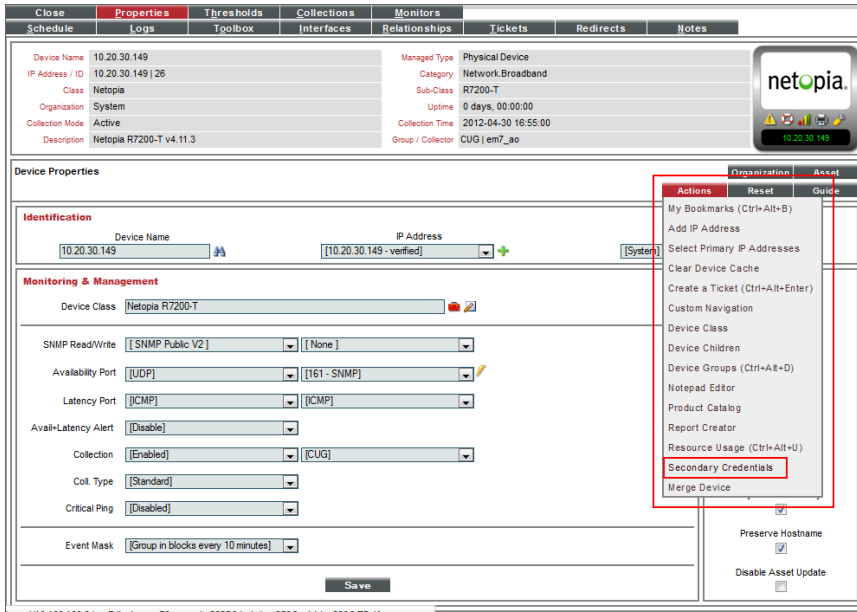
1. Go to the **Device Manager** page (Devices > Device Manager).
2. In the **Device Manager** page, find the device you want to edit. Click its wrench icon (🔧).
3. The **Device Properties** page is displayed.

The screenshot shows the Netopia Device Properties page for device 10.20.30.149. The page is divided into several sections:

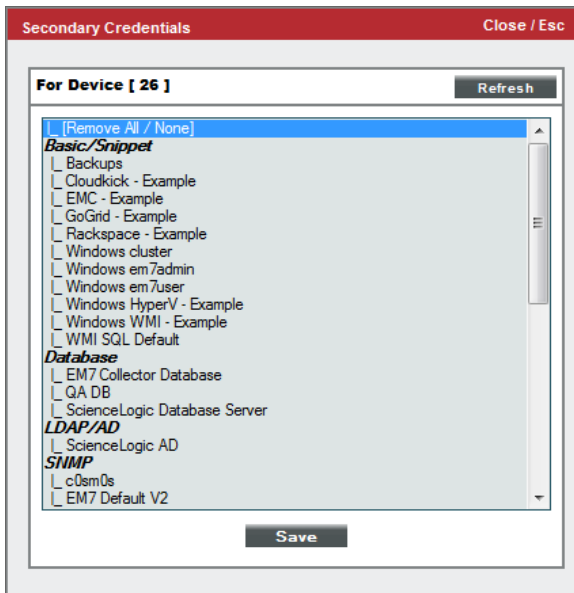
- Identification:** Device Name (10.20.30.149), IP Address (10.20.30.149 - verified), Organization (System).
- Monitoring & Management:** Device Class (Netopia R7200-T), Availability Port (LUDP), Latency Port (ICMP), Avail-Latency Alert (Disable), Collection (Enabled), Col. Type (Standard), Critical Ping (Disable), Event Mask (Group in blocks every 10 minutes).
- SNMP Read/Write:** Two dropdown menus are highlighted with a red box. The first is set to "[SNMP Public V2]" and the second is set to "[None]".
- Preferences:** A list of checkboxes for various settings: Auto-Clear Events (checked), Accept All Logs (checked), Daily Port Scans (checked), Auto-Update (unchecked), Scan All IPs (unchecked), Dynamic Discovery (checked), Preserve Hostname (checked), Disable Asset Update (unchecked).

4. In the **Device Properties** page, you can select two SNMP credentials in the fields **SNMP Read** and **SNMP Write**.

- To select a second credential (either of type SNMP or of another type), click the **[Actions]** menu. Select **Secondary Credentials**.



- The **Secondary Credentials** modal page appears. In the **Secondary Credentials** modal page, you can select one or more credentials to associate with the device. To add a secondary credential to a device, highlight an entry in the list of credentials. To select multiple credentials, hold down the **<CTRL>** key and select the entries by left-clicking with your mouse.



7. During discovery (either nightly, manual, or associated with device policies), SL1 will first try the primary credentials for the device and then will try the secondary credentials.
8. Click the **[Save]** button to save the change to the device.


---

## Defining the Credentials for a Specific Device/Dynamic Application Pair

After a device has been discovered by SL1 and one or more Dynamic Applications have been aligned with the device, you can manually assign the credential to use for each Dynamic Application.

The manually assigned credential will be used by SL1 only for this specific Dynamic Application associated with this specific device. For all other devices, SL1 will use the default credential associated with each device, or will use the credential defined in the **Dynamic Application Collections** page for each device.

To manually associate a credential with a Dynamic Application aligned to a device:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. In the **Device Manager** page, find the device for which you want to define a credential. Click its wrench icon ()
3. In the Device Administration panel, click the **[Collections]** tab.
4. In the **Dynamic Application Collections** page, find the Dynamic Application you want to define a credential for. Select its checkbox (). To apply a credential to multiple Dynamic Applications, select the checkbox for each Dynamic Application.



The screenshot shows a network management interface with the following sections:

- Device Properties:**
  - Device Name: 10.100.100.28
  - IP Address / ID: 10.100.100.28 | 1
  - Class: Microsoft
  - Organization: Acme Corporation
  - Collection Mode: Unavailable
  - Description:
- Managed Type:** Physical Device
- Category:** Pingable
- Sub-Class:** ICMP
- Uptime:** 0 days, 00:00:00
- Collection Time:** 2012-03-30 12:12:00
- Group / Collector:** CUG | em7\_ao

**Dynamic Application™ Collections Table:**

Dynamic Application	ID	Poll Frequency	Type	Credential	Action
Windows CPU	304	1 mins - override	WMI Performance	Windows cluster	[Select Action]
Windows Disk	305	1 mins - override	WMI Performance	Windows em7user	[Select Action]
Windows Interface	307	1 mins - override	WMI Performance	Windows em7user	[Select Action]
Windows Memory	306	1 mins - override	WMI Performance	Windows em7user	[Select Action]
Windows Asset	303	1 mins - override	WMI Config	Windows em7user	[Select Action]
Windows Process List	309	1 mins - override	WMI Config	Windows em7user	[Select Action]
Windows Service List	310	1 mins - override	WMI Config	Windows em7admin	[Select Action]
Windows SMART Status	308	1 mins - override	WMI Config	Windows em7admin	[Select Action]

**Open Credential Selection Menu:**

- Assign Default Credential:
  - L\_Default SNMP Credential
- Assign SNMP Credential:
  - L\_c0sm0s
  - L\_EM7 Default V2
  - L\_EM7 Default V3
  - L\_SNMP Public V1
  - L\_SNMP Public V2
- Assign Database Credential:
  - L\_EM7 Collector Database
  - L\_QA DB
  - L\_ScienceLogic Database Server
- Assign SOAP/XML Host Credential:
  - L\_CUCM PerfmonService 8.0 Example
  - L\_Polycom - Advanced
  - L\_Polycom - Interface
  - L\_Polycom - Network
  - L\_Polycom - System
  - L\_Polycom CDR
  - L\_Proxy IS

[Go] button is visible at the bottom right of the menu.

- From the **Select Action** drop-down list, select the credential from the list of all credentials that you are allowed to use, and then click the **[Go]** button.

**NOTE:** Your organization membership(s) might affect the list of credentials you can see in the **Select Action** drop-down list.

**NOTE:** If this Dynamic Application has already been aligned with a credential to which you do not have access, the **Credential** column will display the value *Restricted Credential*. If you align the Dynamic Application with a different credential, you will not be able to re-align the device with the *Restricted Credential*.

- The selected Dynamic Applications will now use the manually selected credential when collecting data from this device. You should see your change reflected in the **Credential** column in the **Dynamic Application Collections** page.

---

## Specifying Credentials in a Device Template

You can specify the primary SNMP credentials in a device template. Then, when you use the device template to create a new device or when you apply the device template to a device group, the primary credentials are automatically applied to each device and appear in the **Device Properties** page, in the [SNMP Read](#) field.

If you include a device template during discovery or re-discovery, SL1 will discover devices first and then apply the device template to each discovered device. During discovery, SL1 automatically assigns a default SNMP credential to each discovered device (that is not a **pingable** device) and then applies the device template.

**CAUTION:** If you include a primary SNMP credential in a device template and then apply that device template during discovery, you might overwrite the default SNMP credential assigned by SL1. In some cases, this could prevent SL1 from communicating further with the device.

For more details on device templates and device groups, see the manual [Device Groups and Device Templates](#).

---

## How the ScienceLogic Platform Uses Credentials During Discovery

During initial discovery, nightly discovery, discovery associated with device policies, and any manually triggered discovery, SL1 uses credentials in the following order:

1. For devices that have not yet been discovered, SL1 uses the credentials supplied in the [Discovery Session Editor](#) page to collect both SNMP data and Dynamic Application data.
2. For devices that have already been discovered at least once, SL1 uses the [SNMP credentials](#) specified in the **Device Properties** page.
3. For devices that have already been discovered at least once, SL1 uses [the secondary credentials](#) defined in the **Device Properties** page if the primary credentials don't work.
4. For devices that have already been discovered at least once, SL1 will use the [credentials defined in the Dynamic Application Collections page](#) for specific Dynamic Applications.

---

## Aligning One or More Organizations With a Credential

To support multi-tenancy, SL1 allows you to align each credential with one, multiple or all organizations in SL1. You can also align a credential with no organizations.

When you align an organization with a credential, you control who can view details about the credential, who can view the name of the credential, and who can apply the credential in SL1.

**NOTE:** When you align an organization with a credential, you are restricting only the users who can view and assign the credential. You are not restricting the devices and actions that can be associated with the credential. For example, you can align a credential only with the organization "Operations" but assign the credential to a device in the "Finance" organization.

If you have an account of type "User" and are a member of only one organization, the **Organization** column will not appear in the **Credential Management** page. The **Credential Management** page will display only credentials that are aligned with your organization.

Profile Name	Organization	ID	R/W	DA	Type	Credential User	Host	Port	Timeout (ms)	ID	Last Edited	Edited By
1. Amazon Web Services Credential	[all orgs]	...	...	...	SOAP/XML Host	[AWS Account Access Key]	example.com	80	2000	1	2015-05-18 17:42:31	em7Admin
2. Azure Credential - SOAP/XML	[all orgs]	...	...	...	SOAP/XML Host	<AD_USER>	login.windows.net	443	60000	60	2015-05-14 11:31:56	em7Admin
3. Azure Credential - SSHKey	[all orgs]	...	...	...	SSHKey	<SUBSCRIPTION_ID_HERE>	%D	22	180000	59	2015-05-14 11:31:56	em7Admin
4. Cisco SNMPv2 - Example	[all orgs]	...	...	...	SNMP	[USER_GOES_HERE]	...	161	1500	3	2015-05-14 11:25:09	em7Admin
5. Cisco SNMPv3 - Example	[all orgs]	...	...	...	SNMP	[USER_GOES_HERE]	...	161	1500	2	2015-05-14 11:25:09	em7Admin
6. Cisco ACI	[all orgs]	...	...	...	Basic/Snippet	admin	173.36.219.46	443	0	62	2015-05-14 15:05:24	em7Admin
7. Cisco ACI Credential	[all orgs]	...	...	...	Basic/Snippet	admin	198.18.133.200	443	0	61	2015-05-14 14:32:20	em7Admin
8. CloudKit - Example	[all orgs]	...	...	...	Basic/Snippet	[SECURITY KEY GOES HERE]	127.0.0.1	443	5000	9	2015-05-14 11:25:31	em7Admin
9. COCOM Performance B B Example	[all orgs]	...	...	...	SOAP/XML Host	%D	...	8443	2000	4	2015-05-14 11:25:32	em7Admin
10. EM7 Central Database	[all orgs]	...	...	...	Database	root	localhost	7706	0	51	2015-05-14 11:26:41	em7Admin
11. EM7 Collector Database	[all orgs]	...	...	...	Database	root	%D	7707	0	14	2015-05-14 11:25:43	em7Admin
12. EM7 DB	[all orgs]	...	...	...	Database	root	%D	7706	0	35	2015-05-14 11:26:32	em7Admin
13. EM7 DB - Info	[all orgs]	...	...	...	SOAP/XML Host	root	%D	80	3000	38	2015-05-14 11:26:32	em7Admin
14. EM7 DB - My.conf	[all orgs]	...	...	...	SOAP/XML Host	root	%D	80	3000	37	2015-05-14 11:26:32	em7Admin
15. EM7 DB - Sys.conf	[all orgs]	...	...	...	SOAP/XML Host	root	%D	80	3000	36	2015-05-14 11:26:32	em7Admin
16. EM7 Default V2	[all orgs]	...	...	...	SNMP	...	...	161	1500	10	2015-05-14 11:25:42	em7Admin
17. EM7 Default V3	[all orgs]	...	...	...	SNMP	em7Default3	...	161	500	15	2015-05-14 11:25:42	em7Admin
18. EMC - Example	[all orgs]	...	...	...	Basic/Snippet	root	%D	443	10000	15	2015-05-14 11:25:47	em7Admin
19. GoGrid - Example	[all orgs]	...	...	...	Basic/Snippet	[SECURITY KEY GOES HERE]	127.0.0.1	443	5000	16	2015-05-14 11:25:51	em7Admin
20. HPDLA Example	[all orgs]	...	...	...	SNMP	...	...	161	1500	5	2015-05-14 11:25:14	em7Admin
21. iKube Endpoint SNMP	[all orgs]	...	...	...	SNMP	control	...	161	2000	18	2015-05-14 11:25:42	em7Admin
22. iLifeSize Endpoint SSHCLI	[all orgs]	...	...	...	Basic/Snippet	auto	%D	22	3	17	2015-05-14 11:25:58	em7Admin
23. Local API	[all orgs]	...	...	...	Basic/Snippet	em7Admin	19.0.0.180	80	5000	22	2015-05-14 11:26:11	em7Admin
24. NetApp T-mode	[all orgs]	...	...	...	Basic/Snippet	root	%D	443	5000	24	2015-05-14 11:26:20	em7Admin
25. NetApp wSSL Option	[all orgs]	...	...	...	SOAP/XML Host	root	%D	443	20000	26	2015-05-14 11:26:20	em7Admin
26. NetApp wSSL Option Off	[all orgs]	...	...	...	SOAP/XML Host	root	%D	443	10000	25	2015-05-14 11:26:20	em7Admin
27. Nexus netconf	[all orgs]	...	...	...	Basic/Snippet	netconf	%D	22	10000	6	2015-05-14 11:25:16	em7Admin
28. Nexus snmp	[all orgs]	...	...	...	SNMP	...	...	161	10000	7	2015-05-14 11:25:16	em7Admin
29. Polcom - Advanced	[all orgs]	...	...	...	SOAP/XML Host	admin	%D	80	20000	28	2015-05-14 11:26:24	em7Admin
30. Polcom - CDR	[all orgs]	...	...	...	SOAP/XML Host	admin	%D	80	20000	31	2015-05-14 11:26:24	em7Admin
31. Polcom - Interface	[all orgs]	...	...	...	SOAP/XML Host	admin	%D	80	20000	29	2015-05-14 11:26:24	em7Admin
32. Polcom - Network	[all orgs]	...	...	...	SOAP/XML Host	admin	%D	80	20000	30	2015-05-14 11:26:24	em7Admin
33. Polcom - System	[all orgs]	...	...	...	SOAP/XML Host	admin	%D	80	20000	27	2015-05-14 11:26:24	em7Admin
34. Polcom DMA CDR Example	[all orgs]	...	...	...	Basic/Snippet	username	%D	8443	30	33	2015-05-14 11:26:28	em7Admin
35. Polcom RMX	[all orgs]	...	...	...	SOAP/XML Host	sciencelogic	%D	80	10000	32	2015-05-14 11:26:28	em7Admin
36. Rackspace - Example	[all orgs]	...	...	...	Basic/Snippet	[USERNAME GOES HERE]	127.0.0.1	443	5000	34	2015-05-14 11:26:30	em7Admin
37. SNMP Public V1	[all orgs]	...	...	...	SNMP	...	...	161	1500	12	2015-05-14 11:25:42	em7Admin
38. SNMP Public V2	[all orgs]	...	...	...	SNMP	...	...	161	1500	13	2015-05-14 11:25:42	em7Admin
39. Tandberg Endpoint - Config	[all orgs]	...	...	...	SOAP/XML Host	USERNAME_HERE	%D	80	10000	40	2015-05-14 11:26:36	em7Admin
40. Tandberg Endpoint - History	[all orgs]	...	...	...	SOAP/XML Host	USERNAME_HERE	%D	80	10000	41	2015-05-14 11:26:36	em7Admin
41. Tandberg Endpoint - Status	[all orgs]	...	...	...	SOAP/XML Host	USERNAME_HERE	%D	80	10000	39	2015-05-14 11:26:36	em7Admin
42. Tandberg TCS Cluster Status	[all orgs]	...	...	...	SOAP/XML Host	admin	%D	443	2000	42	2015-05-14 11:26:38	em7Admin
43. Tandberg TCS Configuration	[all orgs]	...	...	...	SOAP/XML Host	admin	%D	443	2000	46	2015-05-14 11:26:38	em7Admin

Credentials that are aligned with an organization have the following behavior:

- For each credential that is aligned with an organization, only administrators and users who are members of the aligned organization will be able to see the credential in the **Credential Management** page.
- In SL1, in any field or column that displays the name of the credential, users who are not members of the aligned organization will not see the credential name. Instead, these users will see either a dash character (-) or the text "Restricted Credential".
- In SL1, in any list from which users can select a credential, users who are not members of the aligned organization will not see the credential as an entry in the list.
- In SL1, in any page where the credential has already been assigned, users who are not members of the aligned organization will see only the name "Restricted Credential".
- In SL1, in any page where the credential has already been assigned, users who are not members of the aligned organization can save the page and maintain the credential. The credential will still appear to that user as "Restricted Credential".

- In SL1, in any page where the credential has already been assigned, users who are not members of the aligned organization can change the credential to a credential aligned with their organization(s). However, those users cannot change the credential again and re-assign the "Restricted Credential". The entry for "Restricted Credential" is removed from the list of possible credentials.

To understand the behavior of a credential aligned with an organization, consider the following example:

- Suppose you have a user account of type "Administrator". Suppose you create an SNMP credential called "ops\_cred". Suppose you align that credential with the organization "Operations".
- In the **Credential Management** page, only administrators and users who are members of the organization "Operations" will be able to see the credential "ops\_cred" in SL1.
- In SL1, in any field or column that displays the name of the credential (for example, in the **SNMP Credential** column in the **Device Manager** page), users who are not members of the organization "Operations" will not see the "ops\_cred" name displayed. Instead, these users will see either a dash character (-) or the text "Restricted Credential".
- In SL1, in any list from which users can select a credential (for example, in the **SNMP Read** field, in the **Device Properties** page), users who are not members of the organization "Operations" will not see the "ops\_cred" credential as an entry in the field.
- In SL1, in any page where the credential "ops\_cred" has already been assigned, users who are not members of the organization "Operations" will see only the name "Restricted Credential".
- In SL1, in any page where the credential "ops\_cred" has already been assigned (for example, in the **SNMP Read** field, in the **Device Properties** page), users who are not members of the organization "Operations" can save the page and maintain the "ops\_cred" credential. The credential will still appear to that user as "Restricted Credential".
- In SL1, in any page where the credential "ops\_cred" has already been assigned, (for example, in the **SNMP Read** field, in the **Device Properties** page), users who are not members of the organization "Operations" can change the credential to a credential aligned with their organization. However, that user cannot change the credential again and re-assign the "Restricted Credential". The entry for "Restricted Credential" is removed from the list of possible credentials.

## Default Organizations Aligned with a Credential

When you create a new credential, SL1 automatically aligns the credential with all your organizations. For example:


Account Type	Organization(s) Aligned with the ScienceLogic Account	Default Organizations Aligned with Credential
Administrator	All	All
User	<i>Primary Organization = NOC</i> <i>Additional Organization Memberships = All organizations</i>	All

Account Type	Organization(s) Aligned with the ScienceLogic Account	Default Organizations Aligned with Credential
User	<i>Primary Organization = NOC</i> <i>Additional Organization Memberships = Sales</i>	NOC, Sales
User	<i>Primary Organization = NOC</i> <i>Additional Organization Memberships = None</i>	NOC

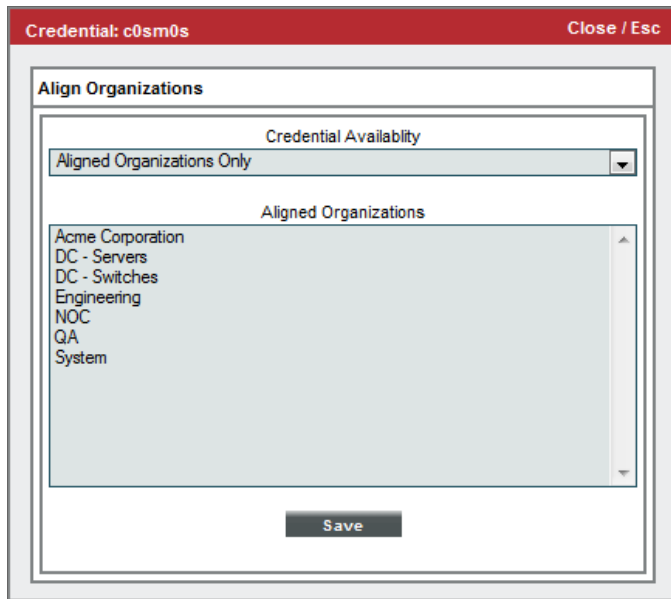
After you save the credential, you can edit the organization(s) aligned with the credential.

## Editing the Organizations Aligned with a Credential

After a credential has been created, you change the default organizations aligned with a credential. To edit the organization alignment on a credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. In the **Credential Management** page, find the credential for which you want to edit the organization. In the **Organization** column, click its org icon ().

3. The **Align Organizations** modal page appears. In this page, provide values in the following fields:



- **Credential Availability.** Specifies whether you want to align all organizations with the credentials or manually select one, multiple, or no organizations to align with the credential. Choices are:
  - *Aligned Organizations Only.* Selecting this option will make the *Aligned Organizations* pane available. You can select one or multiple organizations to be aligned with the credential.
  - *System (All Organizations).* This option is only available if you are a system administrator or a member of all organizations in SL1. All organizations will be aligned with the credential. If another organization is created, it will be aligned to the credential, by default.

**NOTE:** The **Credential Availability** field appears only for users who are Administrators and users who are members of all organizations.

- **Aligned Organizations.** Displays a list of all organizations to which you belong. Select one, multiple, or no organizations to align with the credential.
  - To select a single organization, highlight it and left-click.
  - To unselect a single organization, highlight it and left-click.
  - To select multiple organizations, hold down the CTRL key and select the entries by left-clicking.
  - To unselect multiple organizations, hold down the CTRL key and select the entries by left-clicking.

**NOTE:** Only users who are Administrators and users who are members of all organizations can unselect all organizations in the **Aligned Organizations** list.

4. To save the new organization alignment, click the **[Save]** button.

## Restricted Credentials in the Discovery Session Editor Page

The **Discovery Session Editor** page allows you to select multiple credentials to align with a discovery session.

In the **SNMP Credentials** field and the **Other Credentials** field, the **Discovery Session Editor** page might include credentials that have been aligned with one or more organizations. If one of these credentials has been previously selected, users who are not members of the aligned organization(s) will see "Restricted Credential" appear in the **SNMP Credentials** field or the **Other Credentials** field.

If multiple aligned credentials have been previously selected for a discovery session, users who are not members of the aligned organization(s) will see only a single "Restricted Credential" entry appear in the **SNMP Credentials** field or the **Other Credentials** field. This single entry of Restricted Credential represents all restricted credentials. If a user who is not a member of the aligned organization(s) removes the entry Restricted Credential from the discovery session, all restricted credentials are removed. That user cannot change the credential again and re-assign Restricted Credential. The entry for Restricted Credential is removed from the list of possible credentials.

---

## Editing a Credential

The **Credential Management** page allows you to edit credentials from SL 1. To do so:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. In the **Credential Management** page, click the wrench icon (🔧) for the credential you want to edit.
3. The **Credential Editor** modal page will appear.

The screenshot shows the 'Credential Editor [28]' modal window. It has a red title bar with 'Close / Esc' on the right. Below the title bar, it says 'Edit SNMP Credential #28' and has 'New' and 'Reset' buttons. The form is divided into three sections: 'Basic Settings', 'SNMP V1/V2 Settings', and 'SNMP V3 Settings'. 'Basic Settings' includes fields for Profile Name (c0sm0s), SNMP Version ([SNMP V2]), Port (161), Timeout(ms) (1500), and Retries (1). 'SNMP V1/V2 Settings' includes fields for SNMP Community (Read-Only) (c0sm0s) and SNMP Community (Read/Write). 'SNMP V3 Settings' includes fields for Security Name, Security Passphrase, Authentication Protocol (MD5), Security Level (No Authentication / No Encryption), SNMP v3 Engine ID, Context Name, Privacy Protocol (DES), and Privacy Protocol Pass Phrase. At the bottom, there are 'Save' and 'Save As' buttons.

- After editing the fields in the **Credential Editor**, click the **[Save]** button. If you want to save your changes as a new credential, click the **[Save As]** button.

## Deleting a Credential

The **Credential Management** page allows you to delete one or more credentials from SL1. To do so:

**NOTE:** You cannot delete a credential until all aligned devices, Dynamic Applications, proxied web services, backup settings, LDAP/AD settings, and discovery sessions that use the credential are aligned with another credential.

- Go to the **Credential Management** page (System > Manage > Credentials).
- In the **Credential Management** page, select the checkbox for each credential you want to delete.
- Go to the **Select Actions** menu (in the lower right). Select **DELETE Credential Policy**. Click the **[Go]** button.

Id	Profile Name	Organization	OS	OS ID	Type	Custom User	Host	Port	Timeout (sec)	ID	Last Edited	Edited By
1	IPNetwork		Linux	...	BasicSnmp		hostname				2015-03-26 15:25:18	entAdmin
2	IPNetwork		Linux	...	BasicSnmp		hostname				2015-03-26 15:25:18	entAdmin
3	IPNetwork		Linux	...	BasicSnmp	SECURITY KEY DOES NOT EXIST	hostname				2015-03-26 15:25:18	entAdmin
4	IPNetwork		Linux	...	SCARDNet		hostname				2015-03-22 15:25:26	entAdmin
5	IPNetwork		Linux	...	Database		hostname				2015-03-22 15:25:19	entAdmin
6	IPNetwork		Linux	...	SNMP		hostname				2015-03-22 15:25:26	entAdmin
7	IPNetwork		Linux	...	SNMP	entAdmin	hostname				2015-03-22 15:25:26	entAdmin
8	IPNetwork		Linux	...	BasicSnmp		hostname				2015-03-22 15:25:26	entAdmin
9	IPNetwork		Linux	...	BasicSnmp	SECURITY KEY DOES NOT EXIST	hostname				2015-03-22 15:25:26	entAdmin
10	IPNetwork		Linux	...	SCARDNet		hostname				2015-03-22 15:25:37	entAdmin
11	IPNetwork		Linux	...	SCARDNet	admin	hostname				2015-03-22 15:25:37	entAdmin
12	IPNetwork		Linux	...	SCARDNet	admin	hostname				2015-03-22 15:25:37	entAdmin
13	IPNetwork		Linux	...	SCARDNet	admin	hostname				2015-03-22 15:25:37	entAdmin
14	IPNetwork		Linux	...	SCARDNet	admin	hostname				2015-03-22 15:25:37	entAdmin
15	IPNetwork		Linux	...	SCARDNet	admin	hostname				2015-03-22 15:25:37	entAdmin
16	IPNetwork		Linux	...	Database		hostname				2015-03-22 15:25:25	entAdmin
17	IPNetwork		Linux	...	BasicSnmp	SECURITY KEY DOES NOT EXIST	hostname				2015-03-22 15:25:26	entAdmin
18	IPNetwork		Linux	...	LDAPAD	%s%4d	hostname				2015-03-14 12:21:52	entAdmin
19	IPNetwork		Linux	...	Database		hostname				2015-04-09 15:25:50	entAdmin
20	IPNetwork		Linux	...	SCARDNet		hostname				2015-04-09 15:26:43	entAdmin
21	IPNetwork		Linux	...	SNMP		hostname				2015-03-22 15:25:26	entAdmin
22	IPNetwork		Linux	...	SNMP		hostname				2015-03-22 15:25:26	entAdmin
23	IPNetwork		Linux	...	SCARDNet		hostname				2015-03-12 18:07:34	entAdmin
24	IPNetwork		Linux	...	SCARDNet	USERNAME	hostname				2015-03-22 15:25:29	entAdmin
25	IPNetwork		Linux	...	SCARDNet	USERNAME	hostname				2015-03-22 15:25:29	entAdmin
26	IPNetwork		Linux	...	SCARDNet	USERNAME	hostname				2015-03-22 15:25:29	entAdmin
27	IPNetwork		Linux	...	SCARDNet	MANAGER ACCOUNT OF	hostname				2015-03-22 15:25:49	entAdmin
28	IPNetwork		Linux	...	SCARDNet		hostname				2015-03-22 15:25:31	entAdmin
29	IPNetwork		Linux	...	SCARDNet		hostname				2015-04-25 09:36:47	entAdmin
30	IPNetwork		Linux	...	SCARDNet		hostname				2015-04-13 13:24:43	entAdmin
31	IPNetwork		Linux	...	BasicSnmp	ADMINISTRATOR	hostname				2015-03-14 15:28:13	entAdmin
32	IPNetwork		Linux	...	BasicSnmp	admin	hostname				2015-03-10 10:42:43	entAdmin
33	IPNetwork		Linux	...	BasicSnmp	entUser	hostname				2015-03-22 19:48:07	entAdmin
34	IPNetwork		Linux	...	BasicSnmp	administrator	hostname				2015-03-22 22:41:23	entAdmin
35	IPNetwork		Linux	...	BasicSnmp	administrator	hostname				2015-03-22 15:25:26	entAdmin
36	IPNetwork		Linux	...	BasicSnmp	administrator	hostname				2015-03-14 15:28:13	entAdmin
37	IPNetwork		Linux	...	SCARDNet		hostname				2015-03-22 15:25:26	entAdmin

- The selected credentials will be deleted.





---

# Chapter

# 3



## Discovery

---

### Overview

This chapter describes how to use discovery in SL1 to find devices on your network. You can use the **[Add Devices]** button on the **Devices** page to start a discovery process, or you can run a "Classic Discovery" from the **Discovery Control Panel** page (System > Customize > Classic Discovery).

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ().
- To view a page containing all of the menu options, click the Advanced menu icon (.

This chapter includes the following topics:

<i>What Happens During Discovery?</i> .....	48
<i>What is a Dynamic Application?</i> .....	50
<i>Before You Run Discovery</i> .....	52
<i>System Settings that Affect Discovery</i> .....	53
<i>Device Settings that Affect Auto-Discovery and Re-Discovery</i> .....	57
<i>Duplicate IP Addresses and Duplicate MAC Addresses During Discovery</i> .....	58
<i>Duplicate MAC Addresses for Component Devices</i> .....	60
<i>Prerequisites for Discovering Devices on the Devices Page</i> .....	62
<i>Adding Devices Using Universal or Guided Discovery</i> .....	62
<i>Adding Devices Using Guided Discovery</i> .....	67
<i>Working with Discovery Sessions</i> .....	75
<i>Running a Classic Discovery Session</i> .....	75

<i>Creating a New Classic Discovery Session with the Save As Button</i> .....	82
<i>Viewing Information about a Classic Discovery Session</i> .....	83
<i>Editing a Classic Discovery Session</i> .....	86
<i>Scheduling a Classic Discovery Session</i> .....	86
<i>Manually Re-Running Discovery for a Dynamic Application</i> .....	91
<i>Manually Re-Running Discovery for a Device</i> .....	93
<i>Viewing Information about Classic Discovery</i> .....	94
<i>Managing MAC Vendor Records</i> .....	95
<i>Troubleshooting Discovery</i> .....	97
<i>How File Systems are Hidden During Discovery</i> .....	101

---

## What is Discovery?

**Discovery** is the tool that automatically finds all the hardware-based devices, hardware components, and software applications in your network. You must provide the discovery tool with a range or list of IP addresses and/or a list of fully-qualified domain names (hostnames), and the discovery tool determines if a device, hardware component, or software application exists at each IP address. For each device, hardware component, or software application the discovery tool "discovers", the discovery tool can collect a list of open ports, DNS information, SSL certificates, list of network interfaces, device classes to align with the device, topology information, and basic SNMP information about the device.

The discovery tool also determines which (if any) Dynamic Applications to align with the device. If the discovery tool finds Dynamic Applications to align with the device, the discovery tool triggers collection for each aligned Dynamic Application.

SL1 also uses discovery to update existing information about a device and to add to existing information about a device. This type of discovery is called auto-discovery. For each existing device, SL1 automatically runs auto-discovery every night, to keep device data up-to-date.

You can manually trigger discovery at any time and update the data for one device or multiple devices.

---

## What Happens During Discovery?

Discovery is executed:

- During the initial discovery of network devices and applications. This is called **initial discovery**.
- Automatically runs once a day to update the data on each discovered device. This is called **auto-discovery**.
- On demand, when a user manually asks SL1 to rediscover a group of IP addresses or a list of fully-qualified domain names, rediscover a single device, or rediscover all devices to find those that should align with a selected Dynamic Application. This is called **re-discovery**.

Discovery uses the following processes:

- **Discovery: Auto (*discover\_iprange.py*)**. This process examines one or more IP addresses or fully-qualified domain names and determines which IP addresses or fully-qualified domain names are aligned with a device. For each device, this process retrieves basic information about the device.
- **Discovery: Detail (*discover\_detail.py*)**. This process is triggered by the **Discovery: Auto** process and retrieves details about each discovered device.
- **Discovery: Dynamic App (*discover\_app.py*)**. This process is triggered manually from the **Dynamic Applications Manager** page and checks all existing devices against the selected Dynamic Application.
- **Discovery: Nightly Update (*discover\_update.py*)**. SL1 runs this process each night for already discovered devices. This process updates the information collected during initial discovery.

During discovery of an IP address range (the Discovery: Auto process), SL1 does the following:

1. Performs a DNS lookup to determine the IP address for each fully-qualified domain name supplied in the discovery session. These IP addresses are added to the list of IP addresses supplied in the discovery session.
2. Pings each IP address to determine which are in use.
3. Based on the settings in the discovery session, runs nmap on each IP address to determine which are in use and which ports are open.
4. Searches DNS records to determine the fully qualified domain name at each IP address in range.
5. Tries each selected credential on each IP address to determine if each device is manageable (supports SNMP) or will be a device of type "pingable".
6. For devices that support SNMP, retrieves a system description, SysObject ID, system uptime, system contact, system name, and system location.
7. Assigns a device class to each device.
8. For devices that can be managed (supports SNMP or if non-SNMP discovery is enabled), assigns a device ID, device name, a primary IP address for use in SL1, and a primary credential.

For each device discovered by the Discovery: Auto process, the Discovery: Detail process does the following:

1. If interface discovery is enabled, finds all network interfaces for devices that support SNMP.
2. If the discovery scan level is set to *Initial Population of Apps* or higher, SL1 checks each discovered device (both those that support SNMP and those that don't) against the list of already-defined Dynamic Applications. SL1 searches each discovered device to find "discovery objects" and aligns devices with the appropriate Dynamic Application(s). For details about Dynamic Applications and discovery objects, see the section in this chapter on [How Does the ScienceLogic Platform Align Dynamic Applications During Discovery?](#).
3. If the discovery scan level is set to *Discover SSL Certificates* or higher, checks for SSL certificates on port 443 (HTTPS).
4. If the discovery scan level is set to *Discover Open Ports*, *Advanced Port Discovery*, or *Deep Discovery*, SL1 performs a port scan using the settings appropriate for the scan level to determine the open ports for the device.

Immediately after the initial discovery session is completed, SL1 will use the aligned Dynamic Applications to collect additional data from devices. (For more information about this process, see the chapter on **Collection** in this manual.)

## What Happens During Discovery when the SL1 agent is Installed?

If a device is monitored using the agent and is discovered as a SNMP or pingable device using the Discovery tool, the following default data collection methods, data display settings, and monitoring policies are applied during discovery:

- The method SL1 uses to monitor availability of the device is determined by the first method of discovery:
  - If the agent is installed and creates a device record before the device is discovered as an SNMP or pingable device, availability is based on whether the agent is reporting data to SL1.
  - If the device is discovered as an SNMP or pingable device before the agent is installed, availability is based on the method used to discover the device (SNMP, ICMP, or TCP).
- For Linux devices, the **[TCP/UDP Ports]** tab in the **Device Reports** panel will display open ports detected by the agent and open ports detected by the discovery process (using the NMAP command).
- The **[Processes]** tab in the **Device Reports** panel will display running processes detected by the agent and processes collected using SNMP.
- Port monitoring policies specify whether the policy will be executed using the agent or by a Data Collector using NMAP.
- Process monitoring policies are always executed using the agent.
- Data precedence settings specify whether Dynamic Applications that use data collected by the agent or Dynamic Applications that poll devices for data are used to represent CPU and memory utilization for devices.

For more information about configuring data precedence settings on the agent, or about monitoring ports, processes, and device availability with the agent, see the *Monitoring with the SL1 agent* manual.

---

## What is a Dynamic Application?

**Dynamic Applications** are the customizable policies that tell SL1 what data to collect from devices and applications. For example, suppose you want to monitor a MySQL database running on a device in your network. Suppose you want to know how many insert operations are performed on the MySQL database. You can create or edit a Dynamic Application that monitors inserts. Every five minutes (for example), SL1 could check the number of insert operations performed on the MySQL database. SL1 can use the retrieved data to trigger events and/or to create performance reports.

SL1 includes Dynamic Applications for the most common hardware and software. You can customize these default Dynamic Applications to suit your environment. You can also create custom Dynamic Applications.

Dynamic Applications in SL1 support a variety of protocols to ensure that SL1 can always communicate with the devices and applications in your network and retrieve information from them. Dynamic Applications can use the following protocols to communicate with devices:

- SNMP

- SQL
- XML
- SOAP
- XSLT (uses SOAP and XSLT to convert XML data to a new format)
- WMI (Windows Management Instrumentation), including WMI and WBEM
- Windows PowerShell
- Custom Python applications (called "snippets") for proprietary or more complex data retrieval

## How Does the ScienceLogic Platform Align Dynamic Applications During Discovery?

Most Dynamic Applications include a discovery object. A discovery object enables SL1 to determine which devices to align with a Dynamic Application.

During discovery, SL1:

1. Searches the list of Dynamic Applications.
2. If a Dynamic Application includes a discovery object, SL1 adds that Dynamic Application to the list of Dynamic Applications to try to align during discovery.
3. For each Dynamic Application that includes a discovery object, SL1 checks the current discovery session for an appropriate credential. For example, for each database Dynamic Application, SL1 would look for one or more database credentials that have been selected for the discovery session.
4. For each discovered device, both those that support SNMP and those that don't, discovery tries to determine which Dynamic Applications to align. For each discovered device, SL1 tries to align each Dynamic Application in the list of Dynamic Applications to try during discovery. For each Dynamic Application in the list, SL1 tries to connect to each device with each of the appropriate credentials (until SL1 finds a working credential) and then tries to find the discovery object. If SL1 is able to connect to a device with one of the credentials and can then retrieve the discovery object, SL1 will align the Dynamic Application with the device.

**NOTE:** SL1 also includes more sophisticated logic that allows you to define multiple discovery objects, validate the value of the discovery object, and to align the Dynamic Application if a discovery object is not available. However, the most common use of a discovery object is as described above (discovery object exists).

5. If discovery aligns a Dynamic Application with a device, immediately after discovery completes SL1 will start the first collection from that device using the aligned Dynamic Application. This step is not performed for Dynamic Applications that meet all of the following three criteria:
  - Has a collection frequency of 1 minute, 2 minutes, 3 minutes or 5 minutes.
  - Does not have component mapping enabled (does not discover component devices).
  - Is aligned with a component device.

**NOTE:** During discovery, SL1 tries each SNMP credential specified in the discovery session on each discovered device, to determine if SL1 can collect SNMP details from the device. Later in the discovery session, during alignment of Dynamic Applications, discovery again tries each SNMP credential specified in the discovery session. If one of the SNMP credentials times out three times **without any response**, discovery will stop trying to use that SNMP credential to align SNMP Dynamic Applications. Note that "no response" means that a device did not respond at all. Note that if a device reports that "no OID was found" or "the end of the OID tree was reached", these are considered a legitimate response and would not cause SL1 to abandon the credential.

For details on Dynamic Applications, see the appropriate manual for each type of Dynamic Application.

---

## Before You Run Discovery

To make your initial discovery session as productive as possible, you might want to perform these configuration tasks before running discovery:

- Determine the SNMP credentials for the devices and applications in your network. Define correlating credentials in SL1, to allow discovery to retrieve as much information as possible.
- If you want SL1 to immediately start collecting data from devices using Dynamic Applications, you should make sure that each of those Dynamic Applications includes a discovery object.
- If you want SL1 to immediately start collecting data from devices using Dynamic Applications, you should also define any additional credentials required for those Dynamic Applications. For example, if you want SL1 to immediately start monitoring all MySQL databases in your network, you should define credentials that allow SL1 to communicate with each MySQL database in your network. During discovery, SL1 will determine which devices can be monitored with a Dynamic Application for MySQL. After discovery, SL1 will use the database credential to collect data about each MySQL database in your network.
- Defining the global Behavior Settings that affect discovery and auto-discovery. For a description of the Behavior Settings that affect discovery, see the section [Behavior Settings that Affect Discovery](#). For a detailed description of all the Behavior Settings, see the manual [System Administration](#).
- Define one or more organizations. During discovery, all discovered devices will be placed into a single organization. If you do not define an organization, SL1 will place all devices in the **System** organization. However, you can later assign one or more devices to another organization after discovery.
- If you want to perform bulk configuration of discovered devices by using device groups, device templates, or both, you should define device groups and device templates before performing discovery. However, you can apply device groups, device templates or both to one or more devices after initial discovery. For details on device groups and device templates, see the manual [Device Groups and Device Templates](#).

## System Settings that Affect Discovery

Some of the parameters in the **Behavior Settings** page affect discovery functionality (discovery, auto-discovery, and re-discovery) in SL1.

**NOTE:** You can define global parameters for auto-discovery in this page, but you can always override those parameters on a per-device basis by editing the device settings in a device's **Device Properties** page. For details on configuring a device, see the manual *Device Management*.

To define or edit the settings that affect discovery in the **Behavior Settings** page:

1. Go to the **Behavior Settings** page (System > Settings > Behavior).

2. In the **Behavior Settings** page, edit the values in one or more of the following fields:

- **Ping & Poll Timeout (Msec.)**. This field specifies the number of milliseconds the discovery tool will wait for a response after pinging a device. After the specified number of milliseconds have elapsed without a response, the poll will timeout. The choices are from 100 to 5000 milliseconds.



- **SNMP Poll Timeout (Msec.)**. This field specifies the number of milliseconds the discovery tool will wait for a response after sending an SNMP query to a device. After the specified number of milliseconds have elapsed without a response, the SNMP poll will timeout. The choices are from 100 to 5000 milliseconds.
- **SNMP Failure Retries**. This field specifies the number of times the discovery tool will try to communicate with a device after a timeout or failure. After that number of times has been met, the discovery tool will not retry unless the user manually restarts the discovery process. The choices are 0–6.
- **DHCP Community Strings**. SNMP "read only" community string, to use during discovery. This is required only if DHCP servers and devices use a different SNMP community string than other devices in the network. If the community string specified in the **Discovery Control Panel** (System > Manage > Classic Discovery) page does not work for DHCP devices, SL1 will automatically use the community string specified in this field.
- **NFS Detection Disable**. If selected, this checkbox prevents SL1 from monitoring and reporting on NFS "shared" hard drives. SL1 will monitor and report only on local hard drives.
- **Port Polling Type**. Specifies how SL1 should poll devices to discover open ports. The choices are:
  - *Half Open*. Uses a faster TCP/IP connection method and does not appear on device's logs.
  - *Full Connect*. Uses the standard TCP/IP connection to detect open ports.
- **Initial Discovery Scan Level**. Specifies the data to be gathered during the initial discovery session. The options are:

**NOTE:** You can override this setting for a single discovery session in the **Discovery Session Editor** modal page.

- *0. Model Device Only*. Discovery tool will discover if device is up and running and if so, collect the make and model of the device. SL1 will then generate a device ID for the device, so it can be managed by SL1.
- *1. Initial Population of Apps*. Discovery tool will search for Dynamic Applications to associate with the device. Discovery tool will attempt to collect data for the aligned Dynamic Applications. Discovery will also perform *0. Model Device Only* discovery.
- *2. Discover SSL Certificates*. Discovery tool will search for SSL certificates and retrieve SSL data. Discovery tool will also perform *1. Initial Population of Apps* and *0. Model Device Only*.
- *3. Discover Open Ports*. Discovery tool will search for open ports. Discovery tool will also perform *2. Discover SSL Certificates*, *1. Initial Population of Apps*, and *0. Model Device Only*.

**NOTE:** If your system includes a firewall and you select *3. Discover Open Ports*, discovery might be blocked and/or might be taxing to your network.

- *4. Advanced Port Discovery*. Discovery tool will search for open ports, using a faster TCP/IP connection method. Discovery tool will also perform *2. Discover SSL Certificates*, *1. Initial Population of Apps*, and *0. Model Device Only*.

**NOTE:** If your system includes a firewall and you select *4. Advanced Port Discovery*, some auto-discovered devices might remain in a pending state (purple icon) for some time after discovery. These devices will achieve a healthy status, but this might take several hours.

- *5. Deep Discovery*. Discovery tool will use nmap to retrieve operating system name and version. Discovery will also scan for services running on each open port and can use this information to match devices to device classes. Discovery tool will search for open ports, using a faster TCP/IP connection method. Discovery tool will also perform *2. Discover SSL Certificates*, *1. Initial Population of Apps*, and *0. Model Device Only*.

**NOTE:** For devices that don't support SNMP, option *5. Deep Discovery* allows you to discover devices that don't support SNMP and then align those devices with a device class other than "pingable".

**CAUTION:** Option *5. Deep Discovery* is compute-intensive and might significantly tax your network if used as the default setting. ScienceLogic recommends that you use this option on a per-discovery basis by selecting it in the **Discovery Session Editor** page.

- **Rediscovery Scan Level (Nightly)**. Specifies the data to be gathered/updated each night during auto-discovery. The auto-discovery process will find any changes to previously discovered devices and will also find any new devices added to the network. The options are the same as for **Initial Discovery Scan Level**.
- **Discovery Scan Throttle**. Specifies the amount of time a discovery process should pause between each IP address or hostname in a discovery session. (You specify the list of IP addresses or hostnames for a discovery session in the **IP Address/Hostname Discovery List** field in the **Discovery Session Editor** page.) Pausing discovery processes between IP addresses or hostnames spreads the amount of network traffic generated by discovery over a longer period of time. The choices are:
  - *Disabled*. Discovery processes will not pause.
  - *1000 Msec to 10000 Msec*. A discovery process will pause for a random amount of time between half the selected value and the selected value.

- **Port Scan All IPs.** Specifies whether SL1 should scan all IP addresses on a device for open ports. The choices are:

**NOTE:** You can override this setting for a single discovery session in the **Discovery Session Editor** modal page.

- *0. Disabled.* SL1 will scan only the primary IP address (the one used to communicate with SL1) for open ports.
  - *1. Enabled.* SL1 will scan all discovered IP addresses for open ports.
- **Port Scan Timeout.** Length of time, in milliseconds, after which SL1 should stop trying to scan an IP address for open ports and begin scanning the next IP address (if applicable). Choices are between 60,000 and 1,800,000 milliseconds.

**NOTE:** You can override this setting for a single discovery session in the **Discovery Session Editor** modal page.

- **Hostname Precedence.** Specifies which name SL1 will use for each discovered device. Choices are:
  - *0. SNMP System Name.* Use the device name specified in the device's MIB.
  - *1. DNS Reverse Lookup.* Use the device name specified in the device's reverse-lookup record.
- **DNS Hostnames.** Specifies which DNS name SL1 will use for each discovered device. Choices are:
  - *0. Strip Device Name.* SL1 will use the DNS hostname as the device name for each device.
  - *1. Use Full Domain Name (FQD).* SL1 will use the fully-qualified domain name as the device name for each device.

3. Click the **[Save]** button to save changes in this page.

## Device Settings that Affect Auto-Discovery and Re-Discovery

For each discovered device, the following settings in the **Device Properties** page affect how auto-discovery and rediscovery behaves for that device. These settings override any global settings defined in the **Behavior Settings** page (System > Settings > Behavior).

Close	Properties	Thresholds	Collections	Monitors			
Schedule	Logs	Toolbox	Interfaces	Relationships	Tickets	Redirects	Notes
Device Name	10.100.100.8	Managed Type	Physical Device				
IP Address / ID	10.100.100.8   46	Category	Pingable				
Class	Apache	Sub-Class	Apache Web Server				
Organization	Acme Corporation	Uptime	0 days, 00:00:00				
Collection Mode	Active	Collection Time	2012-05-01 10:32:00				
Description		Group / Collector	CUG   em7_a0				

Device Properties		Organization	Asset	
		Actions	Reset	Guide
<b>Identification</b>				
Device Name	IP Address	Organization		
10.100.100.8	[10.100.100.8 - verified]	[Acme Corporation]		
<b>Monitoring &amp; Management</b>				
Device Class	Apache Apache Web Server			
SNMP Read/Write	c0sm0s	[None]		
Availability Port	[ICMP]	[ICMP]		
Latency Port	[ICMP]	[ICMP]		
Avail-Latency Alert	[Disable]			
Collection	[Enabled]	[CUG]		
Coll. Type	[Standard]			
Critical Ping	[Disable]			
Event Mask	[Group in blocks every 10 minutes]			
<b>Save</b>				
<b>Preferences</b>				
Auto-Clear Events <input checked="" type="checkbox"/>				
Accept All Logs <input checked="" type="checkbox"/>				
Daily Port Scans <input checked="" type="checkbox"/>				
Auto-Update <input checked="" type="checkbox"/>				
Scan All IPs <input type="checkbox"/>				
Dynamic Discovery <input checked="" type="checkbox"/>				
Preserve Hostname <input checked="" type="checkbox"/>				
Disable Asset Update <input type="checkbox"/>				

- **SNMP Read Only.** The community string for read-only access to SNMP information on the device. The community string is a password that allows SL1 to gather information from the device.
- **SNMP Write.** The community string for read-and-write access to SNMP information on the device. The community string is a password that allows SL1 to gather information from the device and send information to the device.
- **Availability Port.** Specifies the protocol and specific port SL1 should monitor to determine if the device is available. The list of ports will contain all the ports discovered by SL1. The data collected from this port will be used in device availability reports.
- **Latency Port.** Specifies the protocol and specific port SL1 should monitor to determine latency for the device. The list of ports will contain all the ports discovered by SL1. The data collected from this port will be used in device latency reports.

- **Collection State.** Specifies (among other things) if the device will be automatically updated each night with SL1's auto-discovery tool. To edit this field, select one of the following from the drop-down list:
  - *Enabled.* Device will be polled by the auto-discovery tool.
  - *Disabled.* Device will not be polled by the auto-discovery tool.
  - *Maintenance.* Manually turn off polling for the device. Until you unselect this checkbox and select the **Enabled** checkbox, the device will not be polled by the auto-discovery tool. Note that Service Action and System Action (part of service policies) will not be executed while the device is in *Maintenance* state.
- **Collector Group.** Specifies which collector group will gather data from the device. You can select from a list of available collector groups.
- **Coll. Type.** Specifies how SL1 should perform auto-discovery. The choices are:
  - *Standard.* SL1 will perform auto-discovery of each device based on the device's IP address. This method is appropriate for devices using standard DNS.
  - *DHCP.* SL1 will perform auto-discovery of each device based on the device's MAC address. This method is appropriate for devices using DHCP.
- **Daily Port Scans.** This checkbox specifies whether or not you want SL1 to perform a daily scan of the device for open ports.
- **Auto-Update.** This checkbox specifies whether or not you want SL1 to perform auto-discovery of the device and update records with changes to the device. If this field is unchecked, SL1 will not perform auto-discovery. Changes to the device, including newly opened ports, will not be recorded by SL1.
- **Scan All IPs.** If the device uses multiple IP Addresses, SL1 will scan for open ports on all IPs during auto-discovery.
- **Dynamic Discovery.** If selected, SL1 will automatically assign the appropriate Dynamic Applications to the device during auto-discovery.
- **Preserve Hostname.** If selected, the name of the device in SL1 will remain the same, even if the name of the actual device is changed. If unselected, the name for the device will be updated if the name of the actual device is changed.
- **Disable Asset Update.** If selected, during nightly auto-discovery, SL1 will not update the asset record associated with the device. For the single device, this checkbox overrides any settings defined in the **Asset Automation** page (System > Settings > Assets).

---

## Duplicate IP Addresses and Duplicate MAC Addresses During Discovery

**NOTE:** Component devices are discovered using Dynamic Applications instead of using a discovery session. The description in this section does not apply to component devices. For details on how SL1 handles duplicate MAC addresses for component devices, see the section [Duplicate MAC Addresses for Component Devices](#).

During discovery, SL1 compares the IP addresses and MAC addresses of a newly discovered device with the IP addresses and MAC addresses of devices that have already been discovered to ensure that devices are not duplicated and IP conflicts do not occur. There are three possible outcomes of this comparison:

- The newly discovered device is considered a duplicate of an existing device and the information collected during discovery is used to update that existing device record.
- The newly discovered device is not a duplicate of an existing device and the information collected during discovery is used to create a new device record.
- The newly discovered device could be considered a duplicate of an existing device. SL1 does not automatically use the information collected during discovery to either create or update a device record. **The Discovery Session Logs** page includes an option for a user to manually create a new device record using the information collected during discovery.

**NOTE:** If SL1 discovers an existing MAC address that is not part of a range of MAC addresses that are marked as "virtual", it will be considered a duplicate of an existing device, regardless of its collector group.

Each managed device in SL1 can have three types of IP addresses:

- **Admin Primary.** This is the IP address that SL1 uses to communicate with a device. This IP address is always a primary address and cannot be demoted to a secondary address. Within a single Collector Group, devices cannot have duplicate **Admin Primary** IP addresses.
- **Primary.** One or more IP addresses that SL1 uses to match incoming log messages (traps and syslog messages) with a device. You can define a primary IP address in the **Device Properties** page for a device.
- **Secondary.** SL1 gathers information about this IP address, but does not use this IP address to match incoming messages (traps and syslog messages) with a device. You can define a secondary IP address in the **Device Properties** page for a device.

If any of the following conditions are true, the newly discovered device is considered a duplicate of an existing device and the information collected during discovery is used to update that existing device record:

- The primary IP address of the newly discovered device is not unique to the Collector Group that discovered the device.
- The primary IP address of the newly discovered device is not unique within the system and the primary IP address is in a public address space.
- A secondary IP address of the newly discovered device is not unique within the system and that secondary IP address is in a public address space.

If any of the following conditions are true, the newly discovered device could be considered a duplicate of an existing device. SL1 does not automatically use the information collected during discovery to either create or update a device record. **The Discovery Session Logs** page includes an option for a user to manually create a new device record using the information collected during discovery:

- The primary IP address of the newly discovered device is unique within the system; the secondary IP addresses associated with the newly discovered device are either unique within the system or are in a private

address space; and the MAC addresses associated with the device match the MAC addresses associated with an existing device.

- The primary IP address of the newly discovered device is not unique within the system; the primary IP address is in a private address space; the secondary IP addresses associated with the newly discovered device are either unique within the system or are in a private address space; and the MAC addresses associated with the device match the MAC addresses associated with an existing device.
- The primary IP address of the newly discovered device is not unique within the system; the primary IP address is in a private address space; and no secondary IP address information has been discovered for the device.
- The primary IP address of the newly discovered device is not unique within the system; the primary IP address is in a private address space; the secondary IP addresses associated with the newly discovered device are either unique within the system or are in a private address space; and no MAC address information has been discovered for the device.

**NOTE:** For more information about configuring virtual MAC addresses, see the section [Managing MAC Vendor Records](#).

## Duplicate MAC Addresses for Component Devices

SL1 handles duplicate MACs for component devices differently than duplicate MACs for physical devices. When a component device is assigned a MAC address, SL1 does not enforce uniqueness and will allow a component device to be created with the same MAC address as existing physical devices and/or existing component devices.

Unlike how SL1 discovers physical devices, SL1 uses Dynamic Applications to retrieve data from a management device and "discover" each entity managed by that management device as a component device. SL1 then uses that retrieved data to create a device for each managed entity. In some cases, the managed entities are nested. In SL1, physical devices are identified by IP address and MAC address. In SL1, component devices are identified by a device name, a unique identifier, and a device class. A Dynamic Application that creates component devices can assign a MAC address to each component device, but is not required to.

- In SL1, a managed entity is called a **component device**. A component device is an entity that runs under the control of a physical management device.
- In SL1, the **root device** is the physical device that manages one or more component devices.
- In SL1, a **parent device** is a device that has associated entities modeled as component devices. A parent device can be either a root device or another component device.

For example, in a Cisco UCS system, SL1 might discover a physical server that hosts the UCS manager. This physical server is the **root device**. SL1 might discover a chassis on the root device. The chassis is a **component device**. The chassis is a child device to the physical server. SL1 might also discover a blade as a component device that is part of the chassis. The blade is a child device to the chassis. The chassis is the **parent device**.

SL1 does not automatically combine new component devices with any existing device record using the MAC address of the new component device. A component device can be combined with an existing device record under the following conditions:

- Dynamic Applications that create component devices can assign a globally unique identifier (GUID) to each component device. When SL1 performs collection for a Dynamic Application, and the Dynamic Application includes a collection object with a GUID component identifier, SL1 compares the collected values for that collection object with all GUID values for all component devices discovered in the system. If a newly collected value matches a GUID value for an existing component device, the device from which SL1 collected the new value will become the parent of the existing component device. The existing component device will no longer be associated with its previous parent device. No new component device will be created.
- You can merge a physical device and a component device. You can do this in the **[Actions]** menu in the **Device Properties** page (Devices > Device Manager > wrench icon) for either the physical device or the component device. When you merge a physical device and a component device, the device record for the component device is no longer displayed in the user interface; the device record for the physical device is displayed in user interface pages that previously displayed the component device. For example, the physical device is displayed in lieu of the component device in the **Device Components** page and the **Component Map** page. All existing and future data for both devices will be associated with the physical device. You can unmerge a component device from a physical device in the **[Actions]** menu in the **Device Properties** page for the physical device (Devices > Device Manager > wrench icon).



---

## Prerequisites for Discovering Devices on the Devices Page

To discover all of the devices on your network:

1. Make a note of the range of IP addresses used on your network. If your device does not have an IP address, make a note of the name of the root device. If you need help, ask your network administrator.
2. An Organization must exist in SL1 for the new devices. If you need to create an Organization go to the **Organizations** page (Registry > Accounts > Organizations).
3. A Collector Group must exist in SL1 that can reach the target device using a valid network path for the needed protocol. For example, UDP 161 for SNMP and general ICMP traffic for Ping. If you don't know what Collector Group to use, consult an SL1 Architecture diagram or ask your SL1 System Administrator. You can access collector information on the **Collector Group Management** page (System > Settings > Collector Groups).
4. You must create or use an existing credential in the classic user interface. You can access credential information on the **Credential Management** page (System > Manage > Credentials). Because credential problems are the most common cause for discovery failure, you can test any credential that you create on the **Credential Tests** page (System > Customize > Credential Tests).
5. Similarly, if you want to use a device template with a discovery session, you must use an existing template in SL1. You can access device templates on the **Configuration Templates** page (Devices > Templates).
6. The Grant All user needs to be used to access new discovery workflow, as the SYS\_SETTINGS\_LICENSES\_PAGE and SYS\_SETTINGS\_CUGS\_PAGE access keys are needed to get collector or collector group information. For more information, see the **Access Keys** page (System > Manage > Access Keys).

---

## Adding Devices Using Universal or Guided Discovery

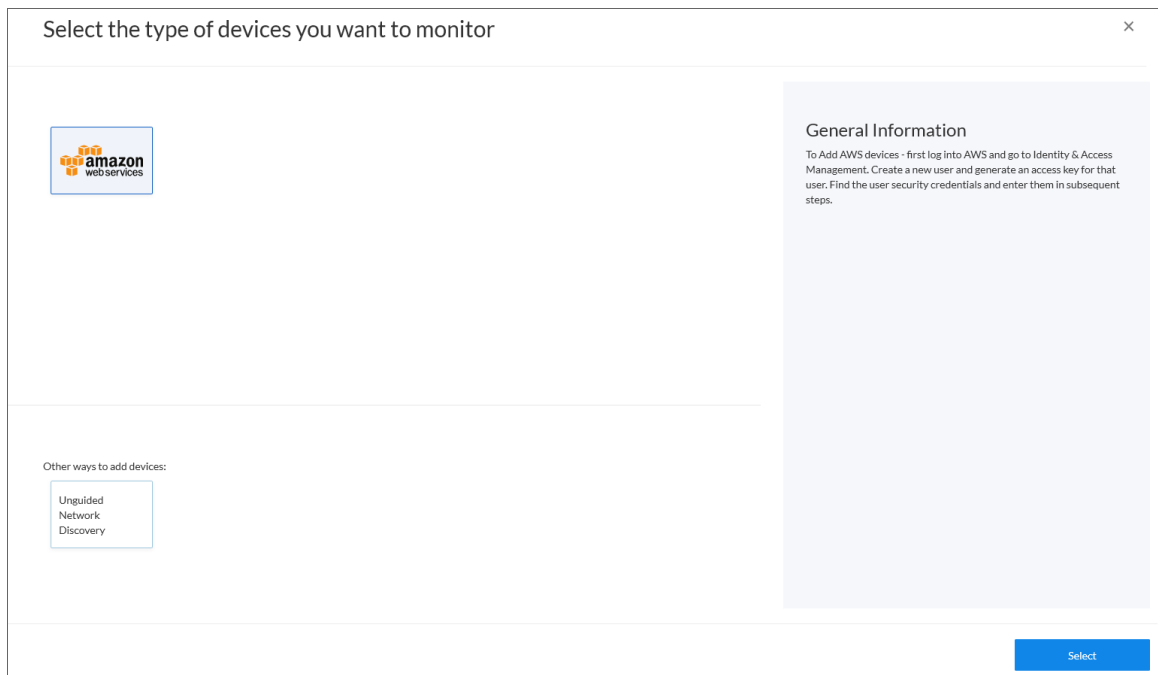
On the **Devices** page, you can add or "discover" new devices for monitoring in SL1. You add devices by creating a **discovery session**, which searches for devices on the network you specify.

You can use the Universal Discovery Framework process in SL1 that guides you through a variety of existing discovery types in addition to traditional SNMP discovery. This process lets you pick a discovery type based on the type of devices you want to monitor.

**NOTE:** The following procedure uses Amazon Web Services as an example of the discovery type. Some steps and fields might vary depending on the discovery type.

To run a guided or Universal Discovery:

1. On the **Devices** page, click the **[Add Devices]** button. The **Select** page appears:



2. Select a discovery type for the devices you want to discover, such as **Amazon Web Services**. Additional information about the requirements for device discovery appears in the **General Information** pane to the right.

**NOTE:** If you want to do a more general discovery, you can select one of the options in the **Other ways to add devices** pane, such as **Unguided Network Discovery**. For more information, see [Adding Devices Using Unguided Discovery](#).

3. Click **[Select]**. The first **Create Guided Discovery Session** page displays the following list of requirements for Discovery (in this example, the requirements are for Amazon Web Services):
  - The name of the root device
  - The credentials you need to access the API
4. Click **[Next]**. The second **Create Guided Discovery Session** page appears.
5. Complete the following fields:
  - **Name**. Type a unique name for this discovery session. This name is displayed in the list of discovery sessions on the **Discovery Sessions** page (Devices > Discovery Sessions).
  - **Description**. Type a short description of the discovery session. You can use the text in this description to search for the discovery session on the **Discovery Sessions** page. Optional.
  - **Select the organization to add discovered devices to**. Select the name of the organization to which you want to add the discovered devices.

6. Click [Next]. The **Credentials** page of the **Create Guided Discovery Session** page appears:

The screenshot shows a web interface titled "Create Guided Discovery Session" with a close button (ESC) in the top right corner. Below the title is a header "Choose credentials that connect your devices" and a "Create New" button. A table lists various credentials with columns for NAME, TYPE, and LAST EDIT. The "AWS\_GOV" credential is selected with a checked checkbox. At the bottom, there are "Back" and "Next" buttons.

NAME	TYPE	LAST EDIT
<input type="checkbox"/> AppDynamics Example	SOAP/XML	Tue Feb 19 2019 19:08:49 GMT+0000 (UTC)
<input type="checkbox"/> AppDynamics Example export	SOAP/XML	Thu Mar 14 2019 16:43:44 GMT+0000 (UTC)
<input type="checkbox"/> AWS Credential	SOAP/XML	Wed Jan 30 2019 18:15:13 GMT+0000 (UTC)
<input type="checkbox"/> AWS Credential - Proxy	SOAP/XML	Wed Jan 30 2019 18:15:13 GMT+0000 (UTC)
<input type="checkbox"/> AWS Credential - Specific Region	SOAP/XML	Wed Jan 30 2019 18:15:13 GMT+0000 (UTC)
<input type="checkbox"/> AWS_COM_04	SOAP/XML	Tue Feb 12 2019 18:15:43 GMT+0000 (UTC)
<input type="checkbox"/> AWS_COM_04-RO	SOAP/XML	Tue Feb 12 2019 18:15:43 GMT+0000 (UTC)
<input checked="" type="checkbox"/> AWS_GOV	SOAP/XML	Tue Feb 12 2019 18:15:43 GMT+0000 (UTC)
<input type="checkbox"/> AWS_GOV Export	SOAP/XML	Thu Mar 14 2019 16:43:45 GMT+0000 (UTC)
<input type="checkbox"/> Azure Classic Credential SOAP	SOAP/XML	Wed Jan 30 2019 18:15:07 GMT+0000 (UTC)
<input type="checkbox"/> Azure Credential - Germany	SOAP/XML	Wed Jan 30 2019 18:15:34 GMT+0000 (UTC)

7. If the credential you need is not in the list, click **[Create New]** to open the **Create Credential** window, where you can specify the name and organization for the credential, the third-party username and password, and other data such as Cloud Type and Proxy information. Click **[Save]** to save the credential and return to the **Credentials** page of the **Create Guided Discovery Session** page.

**NOTE:** You can also edit an existing credential on the **Credentials** page by clicking the **[Actions]** button (⋮) for the credential, selecting *Edit*, and editing that credential as needed.

8. Select a credential to allow SL1 to access a device and click **[Next]**. The **Root Device Details** page appears:

The screenshot shows a web interface titled "Create Guided Discovery Session" with a sub-header "Root Device Details". The form contains the following fields:

- Root Device Name:** AWSRootDevice
- Collector Group Name:** CUG1 | fh-sl1-ranch-cu-37:10.2.18.37

Below the "Collector Group Name" field is a search bar labeled "Q Search Collectors". At the bottom of the form, there is a "← Back" button on the left and a "Create Discovery Session" button on the right.

9. Complete the following fields:

- **Root Device Name.** Type the name of the root device for the application you want to monitor (in this case, an Amazon Web Services root device).
- **Collector Group Name.** Select an existing collector group to communicate with the discovered devices. Required.

**NOTE:** The contents of this page might vary depending on the discovery type you selected at the start of the Guided Discovery.

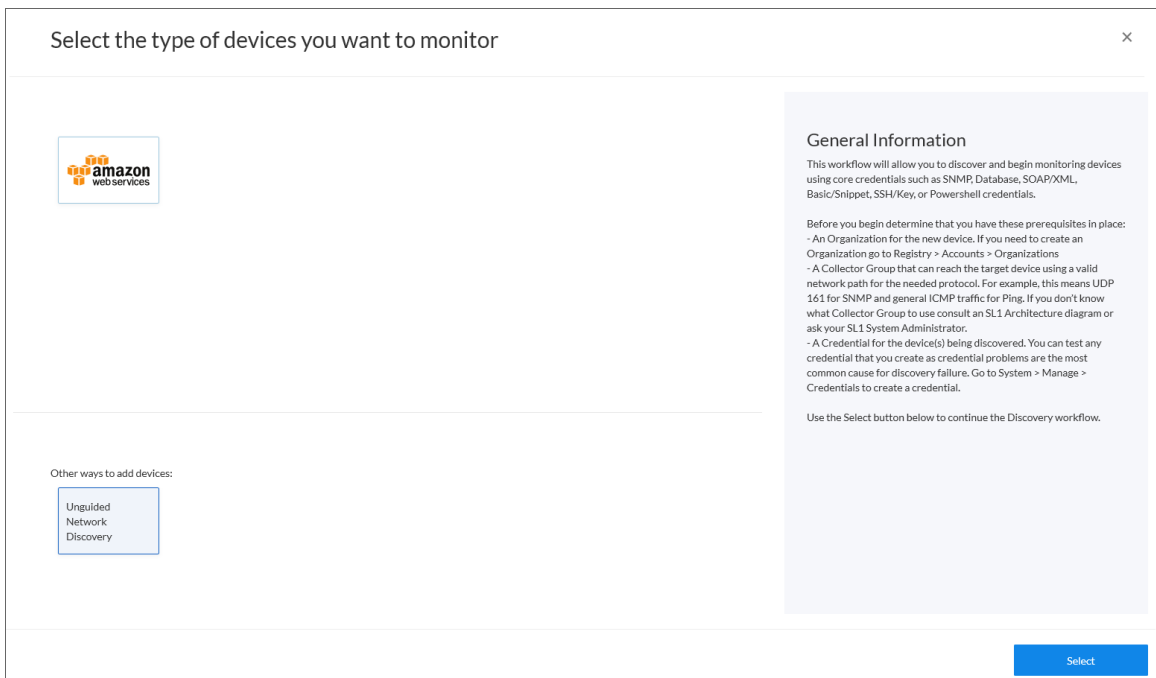
10. Click the **[Create Discovery Session]** button. A summary of the new discovery session appears on this page.
11. Click **[Close]**. The **Discovery Sessions** page (Devices > Discovery Sessions) displays the new discovery session.

## Adding Devices Using Guided Discovery

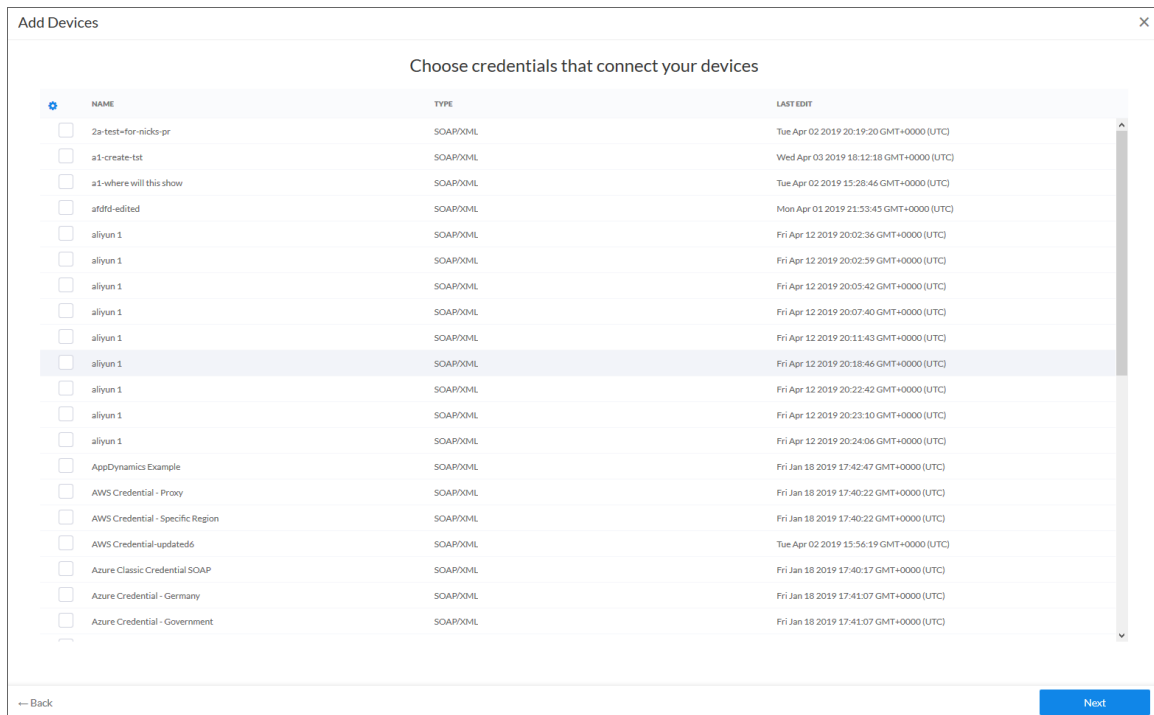
Instead of running a Universal Discovery for a specific discovery type, you can run an "unguided" discovery to find a range of devices using core credentials such as SNMP, Database, SOAP/XML, Basic/Snippet, SSH/Key, or PowerShell credentials.

To run an unguided discovery:

1. On the **Devices** page, click the **[Add Devices]** button. The **Select** page appears:



2. Click the **[Unguided Network Discovery]** button. Additional information about the requirements for discovery appears in the **General Information** pane to the right.
3. Click **[Select]**. The **Add Devices** page appears:
4. Complete the following fields:
  - **Name**. Type a unique name for this discovery session. This name is displayed in the list of discovery sessions on the **[Discovery Sessions]** tab.
  - **Description**. Type a short description of the discovery session. You can use the text in this description to search for the discovery session on the **[Discovery Sessions]** tab. Optional.
  - **Select the organization to add discovered devices to**. Select the name of the organization to which you want to add the discovered devices.
3. Click **[Next]**. The Credentials page of the **Add Devices** wizard appears:




4. Select one or more SNMP credentials to allow SL1 to access a device's SNMP data and click **[Next]**. The Discovery Session Details page of the **Add Devices** wizard appears:

The screenshot shows the 'Add Devices' wizard interface. It includes a text area for 'List of IPs/Hostnames' with an 'Upload File' button. Below this is a dropdown menu for 'Which collector will monitor these devices?'. There is a 'Run after save' toggle switch which is turned on. Under 'Advanced options ^', there are four dropdown menus: 'Initial Scan Level', 'Scan Throttle', 'Port Scan All IPs', and 'Port Scan Timeout', all set to '[ System Default (recommended) ]'. At the bottom left is a 'Back' button and at the bottom right is a 'Save and Close' button.

5. Complete the following fields:

- **List of IPs/Hostnames.** Provide a list of IP addresses, hostnames, or fully-qualified domain names for SL1 to scan during discovery. You can also click the **[Upload File]** button to upload a comma-separated list of IPs. This field is required. In this field, you can enter a combination of one or more of the following:
  - One or more *single IPv4 addresses* separated by commas and a new line. Each IP address must be in standard IP notation and cannot exceed 15 characters. For example, "10.20.30.1, 10.20.30.2, 10.20."
  - One or more *ranges of IPv4 addresses* with "-" (dash) characters between the beginning of the range and the end of the range. Separate each range with a comma. For example, "10.20.30.1 – 10.20.30.254".
  - One or more IP address ranges in *IPv4 CIDR notation*. Separate each item in the list with a comma. For example, "192.168.168.0/24".
  - One or more *ranges of IPv6 addresses* with "-" (dash) characters between the beginning of the range and the end of the range. Separate each range with a comma. For example, "2001:DB8:0:0:0:0:0-2001:DB8:0:0:0:0:0:0003".
  - One or more IP address ranges in *IPv6 CIDR notation*. Separate each item in the list with a comma. For example, "2001:DB8:0:0:0:0:0/117".
  - One or more hostnames (fully-qualified domain names). Separate each item in the list with a comma.



- **Which collector will monitor these devices?** Select an existing collector to monitor the discovered devices. Required.
- **Run after save.** Select this option to run this discovery session as soon as you click **[Save and Close]**.
- **Advanced options.** Click the down arrow icon (  ) to access additional discovery options.

In the **Advanced options** section, complete the following fields as needed:

- **Initial Scan Level.** For this discovery session only, specifies the data to be gathered during the initial discovery session. The options are:
  - *System Default (recommended).* Use the value defined in the **Behavior Settings** page (System > Settings > Behavior) in the classic user interface of SL1.
  - *1. Model Device Only.* Discovery will discover if the device is up and running and if so, collect the make and model of the device. SL1 will then generate a device ID for the device so it can be managed by SL1.
  - *2. Initial Population of Apps.* Discovery will search for Dynamic Applications to associate with the device. The discovery tool will attempt to collect data for the aligned Dynamic Applications. Discovery will later retrieve full sets of data from each Dynamic Application. Discovery will also perform *1. Model Device Only* discovery.
  - *3. Discover SSL Certificates.* Discovery will search for SSL certificates and retrieve SSL data. Discovery will also perform *2. Initial Population of Apps* and *1. Model Device Only*.
  - *4. Discover Open Ports.* Discovery will search for open ports. Discovery will also perform *3. Discover SSL Certificates*, *2. Initial Population of Apps*, and *1. Model Device Only*.

**NOTE:** If your system includes a firewall and you select *4. Discover Open Ports*, discovery might be blocked and/or might be taxing to your network.

- *5. Advanced Port Discovery.* Discovery will search for open ports, using a faster TCP/IP connection method. Discovery will also perform *3. Discover SSL Certificates*, *2. Initial Population of Apps*, and *1. Model Device Only*.

**NOTE:** If your system includes a firewall and you select *5. Advanced Port Discovery*, some devices might remain in a pending state (purple icon) for some time after discovery. These devices will achieve a healthy status, but this might take several hours.

- *6. Deep Discovery.* Discovery will use nmap to retrieve the operating system name and version. Discovery will also scan for services running on each open port and can use this information to match devices to device classes. Discovery will search for open ports, using a faster TCP/IP connection method. Discovery will also perform *3. Discover SSL Certificates*, *2. Initial Population of Apps*, and *1. Model Device Only*.

**NOTE:** For devices that don't support SNMP, option 6. *Deep Discovery* allows you to discover devices that don't support SNMP and then align those devices with a device class other than "pingable". Note that option 6. *Deep Discovery* is compute-intensive.

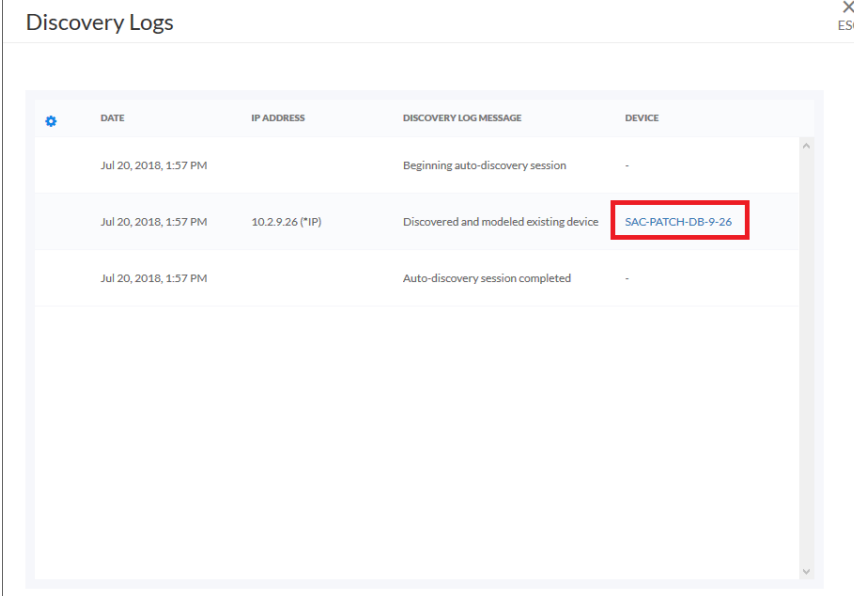
- **Scan Throttle.** Specifies the amount of time a discovery process should pause between each specified IP address (specified in the **IP Address/Hostname Discovery List** field). Pausing discovery processes between IP addresses spreads the amount of network traffic generated by discovery over a longer period of time. The choices are:
  - *System Default (recommended).* Use the value defined in the **Behavior Settings** page (System > Settings > Behavior) in the classic user interface for SL1.
  - *Disabled.* Discovery processes will not pause.
  - *1000 Msec to 10000 Msec.* A discovery process will pause for a random amount of time between half the selected value and the selected value.
- **Port Scan All IPs.** For the initial discovery session only, specifies whether SL1 should scan all IP addresses on a device for open ports. The choices are:
  - *System Default (recommended).* Use the value defined in the **Behavior Settings** page (System > Settings > Behavior) in the classic user interface for SL1.
  - *Enabled.* SL1 will scan all discovered IP addresses for open ports.
  - *Disabled.* SL1 will scan only the primary IP address (the one used to communicate with SL1) for open ports.
- **Port Scan Timeout.** For the initial discovery session only, specifies the length of time, in milliseconds, after which SL1 should stop trying to scan an IP address for open ports and begin scanning the next IP address (if applicable). Choices are:
  - *System Default (recommended).* Use the value defined in the **Behavior Settings** page (System > Settings > Behavior).
  - Choices between 60 to 1,800 seconds.
- **Scan Ports.** Specify a list of ports to scan, separated by colons (:). The default is 21:22:25:80:136.
- **Interface Inventory Timeout (ms).** Specifies the maximum amount of time that the discovery processes will spend polling a device for the list of interfaces. After the specified time, SL1 will stop polling the device, will not model the device, and will continue with discovery. The default value is 600,000 ms (10 minutes).
  - During the execution of this discovery session, SL1 uses the value in this field first. If you delete the default values and do not specify another value in this field, SL1 uses the value in the **Global Threshold Settings** page (System > Settings > Thresholds).

- If you specify a value in this field and do not apply a device template to this discovery session, the **Interface Inventory Timeout** setting in the **Device Thresholds** page (Registry > Devices > Device Manager > wrench icon > Thresholds) is set to this value for each discovered device. If there is no device template applied to the discovery session and no value is supplied in this field, SL1 uses the value in the **Global Threshold Settings** page (System > Settings > Thresholds).
- **Maximum Allowed Interfaces**. Specifies the maximum number of interfaces per devices. If a device exceeds this number of interfaces, SL1 will stop scanning the device, will not model the device, and will continue with discovery. The default value is 10,000.
  - During the execution of this discovery session, SL1 uses the value in this field first. If you delete the default values and do not specify another value in this field, SL1 uses the value in the **Global Threshold Settings** page.
  - If you specify a value in this field and do not apply a device template to this discovery session, the **Maximum Allowed Interfaces** setting in the **Device Thresholds** page is set to this value for each discovered device. If there is no device template applied to the discovery session and no value is supplied in this field, SL1 uses the value in the **Global Threshold Settings** page.
- **Bypass Interface Inventory**. Specifies whether or not the discovery session should discover network interfaces.
  - *Selected*. SL1 will not attempt to discover interfaces for each device in the discovery session. For each discovered device, the **Bypass Interface Inventory** checkbox on the **Device Investigator [Settings]** tab will be selected.
  - *Not Selected*. SL1 will attempt to discover network interfaces, using the **Interface Inventory Timeout** value and **Maximum Allowed Interfaces** value.
- **Discover Non-SNMP**. Specifies whether or not SL1 should discover devices that don't respond to SNMP requests.
  - *Selected*. SL1 will discover devices that don't respond to the SNMP credentials selected in the **SNMP Credentials** field. These devices will be discovered as "pingable" devices.
  - *Not Selected*. SL1 will not discover devices that don't respond to the SNMP credentials selected in the **SNMP Credentials** fields.
- **Model Devices**. Determines whether or not the devices that are discovered with this discovery session can be managed through SL1. Choices are:
  - *Enabled*. When a device is modeled, SL1 creates a device ID for the device; you can then access the device through the **Device Manager** page and manage the device in SL1.
  - *Disabled*. If a device is not modeled, you cannot access the device through the **Device Manager** page, and you cannot manage the device in SL1. However, each discovered device will still appear in the Discovery Session logs. For each discovered device, the discovery logs will display the IP address and device class for the device. This option is useful when performing an initial discovery of your network, to determine which devices you want to monitor

and manage with SL1. For the amount of time specified in the **Device Model Cache TTL (h)** field, a user can manually model the device from the **Discovery Session** window.

- **Enable DHCP.** Specifies whether or not the specified range of IPs and hostnames use DHCP.
  - *Selected.* SL1 will perform a DNS lookup for the device during discovery and each time SL1 retrieves information from the device.
  - *Not Selected.* SL1 will perform normal discovery.
- **Device Model Cache TTL (h).** Amount of time, in hours, that SL1 stores information about devices that are discovered but not modeled, either because the **Model Devices** option is not enabled or because SL1 cannot determine whether a duplicate device already exists. The cached data can be used to manually model the device from the **Discovery Session** window.
- **Log All.** Specifies whether or not the discovery session should use verbose logging. When you select verbose logging, SL1 logs details about each IP address or hostname specified in the **IP Address/Hostname Discovery List** field, even if the results are "No device found at this address."
  - *Selected.* This discovery session will use verbose logging.
  - *Not Selected.* This discovery session will not use verbose logging.
- **Apply Device Template.** As SL1 discovers a device in the IP discovery list, that device is configured with the selected device template. You can select from a list of all device templates in SL1. For more information on device templates, see the manual on **Device Groups and Device Templates**.

6. Click **[Save and Close]** to save the discovery session. The **Discovery Sessions** page (Devices > Discovery Sessions) displays the new discovery session.
7. If you selected the **Run after save** option on this page, the discovery session runs, and the **Discovery Logs** page displays any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page includes a link to the **Device Investigator** page for the discovered device:

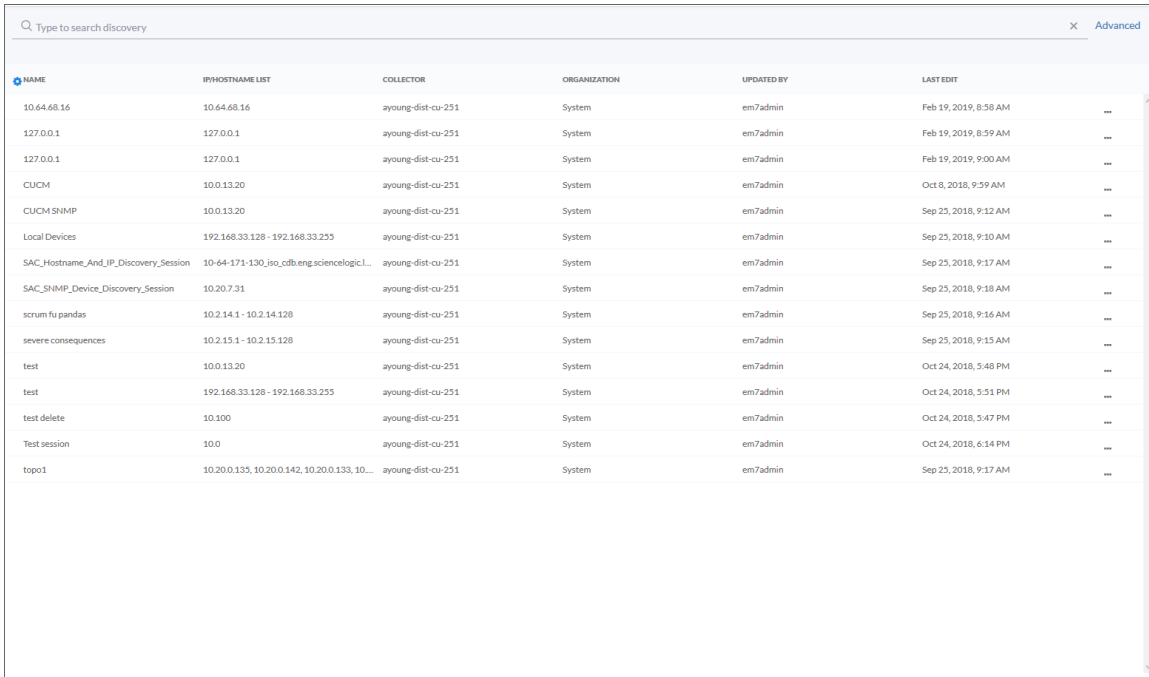


DATE	IP ADDRESS	DISCOVERY LOG MESSAGE	DEVICE
Jul 20, 2018, 1:57 PM		Beginning auto-discovery session	-
Jul 20, 2018, 1:57 PM	10.2.9.26 (*IP)	Discovered and modeled existing device	<a href="#">SAC-PATCH-DB-9-26</a>
Jul 20, 2018, 1:57 PM		Auto-discovery session completed	-

---

## Working with Discovery Sessions

The **Discovery Sessions** page (Devices > Discovery Sessions) displays a list of all the existing **discovery sessions**, which are previous attempts to add devices using discovery:



NAME	IP/HOSTNAME LIST	COLLECTOR	ORGANIZATION	UPDATED BY	LAST EDIT	
10.64.68.16	10.64.68.16	ayoung-dist-cu-251	System	em7admin	Feb 19, 2019, 8:58 AM	...
127.0.0.1	127.0.0.1	ayoung-dist-cu-251	System	em7admin	Feb 19, 2019, 8:59 AM	...
127.0.0.1	127.0.0.1	ayoung-dist-cu-251	System	em7admin	Feb 19, 2019, 9:00 AM	...
CUCM	10.0.13.20	ayoung-dist-cu-251	System	em7admin	Oct 6, 2018, 9:59 AM	...
CUCM SHMP	10.0.13.20	ayoung-dist-cu-251	System	em7admin	Sep 25, 2018, 9:12 AM	...
Local Devices	192.168.33.128 - 192.168.33.255	ayoung-dist-cu-251	System	em7admin	Sep 25, 2018, 9:10 AM	...
SAC_Hostname_And_IP_Discovery_Session	10-64-171-130_ipo_cdb.eng.sciencelogic.L...	ayoung-dist-cu-251	System	em7admin	Sep 25, 2018, 9:17 AM	...
SAC_SHMP_Device_Discovery_Session	10.20.7.31	ayoung-dist-cu-251	System	em7admin	Sep 25, 2018, 9:18 AM	...
scrum fu pandas	10.2.14.1 - 10.2.14.128	ayoung-dist-cu-251	System	em7admin	Sep 25, 2018, 9:16 AM	...
severe consequences	10.2.15.1 - 10.2.15.128	ayoung-dist-cu-251	System	em7admin	Sep 25, 2018, 9:15 AM	...
test	10.0.13.20	ayoung-dist-cu-251	System	em7admin	Oct 24, 2018, 5:48 PM	...
test	192.168.33.128 - 192.168.33.255	ayoung-dist-cu-251	System	em7admin	Oct 24, 2018, 5:51 PM	...
test delete	10.100	ayoung-dist-cu-251	System	em7admin	Oct 24, 2018, 5:47 PM	...
Test session	10.0	ayoung-dist-cu-251	System	em7admin	Oct 24, 2018, 6:14 PM	...
topo1	10.20.0.135, 10.20.0.142, 10.20.0.133, 10...	ayoung-dist-cu-251	System	em7admin	Sep 25, 2018, 9:17 AM	...

On this page you can click the **[Actions]** button (⋮) for a session and select one of the following actions:

- *Edit*. Run the **Add Device** wizard again so you can make changes to the selected discovery session.
- *Delete*. Delete the selected discovery session. You do not get a confirmation window after you click *Delete*; the session is immediately deleted.
- *Start*. Run the selected discovery session again. The **Discovery Logs** page appears when discovery completes.
- *Show Logs*. The **Discovery Logs** page for the selected discovery session displays data about the most recent run of a discovery session.

---

## Running a Classic Discovery Session

To perform a discovery session for one IP address, multiple IP addresses, or a range of IP addresses on the **Classic Discovery** page:

**NOTE:** To discover all the devices in your network, you must first know the range of IP addresses used in your network. If you need help, ask your network administrator.

1. Go to the **Discovery Control Panel** page (System > Customize > Classic Discovery).
2. In the **Discovery Control Panel**, click the **[Actions]** button. The **Discovery Session Editor** page appears:

Discovery Session Editor | Create New

New Reset

Identification Information

Name Description

IP and Credentials

IP Address/Hostname Discovery List

Upload File

Browse for file... Browse...

SNMP Credentials

SNMP

- c0sm0s
- Cisco SNMPv2 - Example
- Cisco SNMPv3 - Example
- Cisco: CSP SNMP Port 161 Example
- Cisco: CSP SNMP Port 1610 Examp
- Dell EMC: Isilon SNMPv2 Example
- Demo Lab
- EM7 Default V2
- EM7 Default V3
- IPSLA Example

Other Credentials

Basic/Snippet

- Cisco CUCM Example
- Cisco VOS CUC Cluster Status
- Cisco VOS IM&P Cluster Status
- Cisco: ACI Sample Credential 1
- Cisco: ACI Sample Credential 2
- Cisco: CSP Example
- Citrix XenServer - Example
- CUCM Lab
- EMC SMI-S Example
- EMC VMAX Example

Detection and Scanning

Initial Scan Level

System Default (recommended)

Scan Throttle

System Default (recommended)

Port Scan All IPs

System Default (recommended)

Port Scan Timeout

System Default (recommended)

Detection Method & Port

[Default Method]

- UDP: 161 SNMP
- TCP: 1 - tcpmux
- TCP: 2 - compressnet
- TCP: 3 - compressnet
- TCP: 5 - rje
- TCP: 7 - echo
- TCP: 9 - discard
- TCP: 11 - systat
- TCP: 13 - daytime
- TCP: 15 - netstat
- TCP: 17 - qotd
- TCP: 18 - msp
- TCP: 19 - chargen
- TCP: 20 - ftp-data

Interface Inventory Timeout (ms)

600000

Maximum Allowed Interfaces

10000

Bypass Interface Inventory

Basic Settings

Discover Non-SNMP

Model Devices

DHCP

Device Model Cache TTL (h)

2

Collection Server PID:

ayoung-dist-cu-251

Organization

[System]

Add Devices to Device Group(s)

None

Servers

Apply Device Template

[Choose a Template]

Save

Log All

3. Supply values in the following fields:

- **Name.** Type a name for the discovery session. This name is displayed in the list of discovery sessions in the **Discovery Control Panel** page.
- **Description.** Optionally, type a description of the discovery session.

- **IP Address/Hostname Discovery List.** Provide a list of IP addresses or fully-qualified domain names for SL1 to scan during discovery. In this field, you can enter a combination of one or more of the following:

**NOTE:** Instead of manually entering a list of IP addresses and hostnames, you can upload a file that contains the list of IP addresses and hostnames. See the description of the **Upload File** field.

- One or more *single IPv4 addresses* separated by commas. Each IP address must be in standard IP notation and cannot exceed 15 characters. For example, "10.20.30.1, 10.20.30.2, 10.20.30.3".
- One or more *ranges of IPv4 addresses* with "-" (dash) characters between the beginning of the range and the end of the range. Separate each range with a comma. For example, "10.20.30.1 – 10.20.30.254".
- One or more IP address ranges in *IPv4 CIDR notation*. Separate each item in the list with a comma. For example, "192.168.168.0/24".
- One or more *ranges of IPv6 addresses* with "-" (dash) characters between the beginning of the range and the end of the range. Separate each range with a comma. For example, "2001:DB8:0:0:0:0:0:0-2001:DB8:0:0:0:0:0:0:0003".
- One or more IP address ranges in *IPv6 CIDR notation*. Separate each item in the list with a comma. For example, "2001:DB8:0:0:0:0:0:0/117".
- One or more hostnames (fully-qualified domain names). Separate each item in the list with a comma.

**NOTE:** The following types of notation are **not supported**: IPv4 netmask with comma notation (e.g., 192.168.168.0,24); a list of single IPv6 addresses, separated by comma.

**NOTE:** SL1 will display an error if your discovery session exceeds the maximum size for optimum performance. SL1 will display a warning message if your discovery session includes 100 or more IP addresses. The warning message will tell you that discovery with more than 100 IP addresses might "take a long time to discover".

- **Upload File.** Instead of manually entering a list of IP addresses and hostnames in the **IP Address/Hostname Discovery List** field, you can upload a file that contains a list of IP addresses and hostnames. The IP addresses and hostnames in the file must be in a format that is allowed for the **IP Address/Hostname Discovery List** field. Each address or range of addresses in the file must be separated by a newline character instead of a comma. You can browse to the file and then select it. After uploading the file, the **IP Address/Hostname Discovery List** field will display the IP addresses and hostnames from the file.
- **SNMP Credentials.** A community string that allows SL1 to access a device's SNMP data. SNMP credentials are defined in the **Credential Management** page (System > Manage > Credentials). If



you want to retrieve SNMP data from one or more devices, you must select one or more working SNMP credentials in this field. You can select multiple credentials from this field. SL1 will try each selected credential when discovering devices and retrieving device data.

- **Other Credentials.** A username and password pair (among other fields) that allows SL1 to access a device's database data, SOAP data, XML data, WMI data, WBEM data, or data that is monitored with a Snippet Dynamic Application. These credentials are defined in the **Credential Management** page (System > Manage > Credentials). You can select multiple credentials from this field. SL1 will try each selected credential when searching for Dynamic Applications to align with each discovered device.

**NOTE:** You can use the field at the top of the **SNMP Credentials** field and the **Other Credentials** field to filter the list of credentials. If you enter an alpha-numeric string in the field, the **SNMP Credentials** field or the **Other Credentials** field will include only credentials that match the string.

**NOTE:** Your organization membership(s) might affect the list of credentials you can see in the **SNMP Credentials** field and the **Other Credentials** field.

- **Initial Scan Level.** For this discovery session only, specifies the data to be gathered during the initial discovery session. The options are:
  - *System Default (recommended).* Use the value defined in the **Behavior Settings** page (System > Settings > Behavior).
  - *0. Model Device Only.* Discovery will discover if the device is up and running and if so, collect the make and model of the device. SL1 will then generate a device ID for the device so it can be managed by SL1.
  - *1. Initial Population of Apps.* Discovery will search for Dynamic Applications to associate with the device. The discovery tool will attempt to collect data for the aligned Dynamic Applications. Discovery will later retrieve full sets of data from each Dynamic Application. Discovery will also perform *0. Model Device Only* discovery.
  - *2. Discover SSL Certificates.* Discovery will search for SSL certificates and retrieve SSL data. Discovery will also perform *1. Initial Population of Apps* and *0. Model Device Only*.
  - *3. Discover Open Ports.* Discovery will search for open ports. Discovery will also perform *2. Discover SSL Certificates*, *1. Initial Population of Apps*, and *0. Model Device Only*.

**NOTE:** If your system includes a firewall and you select *3. Discover Open Ports*, discovery might be blocked and/or might be taxing to your network.

- *4. Advanced Port Discovery.* Discovery will search for open ports, using a faster TCP/IP connection method. Discovery will also perform *2. Discover SSL Certificates*, *1. Initial Population of Apps*, and *0. Model Device Only*.

**NOTE:** If your system includes a firewall and you select 4. *Advanced Port Discovery*, some devices might remain in a pending state (purple icon) for some time after discovery. These devices will achieve a healthy status, but this might take several hours.

- 5. *Deep Discovery*. Discovery will use nmap to retrieve the operating system name and version. Discovery will also scan for services running on each open port and can use this information to match devices to device classes. Discovery will search for open ports, using a faster TCP/IP connection method. Discovery will also perform 2. *Discover SSL Certificates*, 1. *Initial Population of Apps*, and 0. *Model Device Only*.

**NOTE:** For devices that don't support SNMP, option 5. *Deep Discovery* allows you to discover devices that don't support SNMP and then align those devices with a device class other than "pingable". Note that option 5. *Deep Discovery* is compute-intensive.

- **Scan Throttle**. Specifies the amount of time a discovery process should pause between each specified IP address (specified in the **IP Address/Hostname Discovery List** field). Pausing discovery processes between IP addresses spreads the amount of network traffic generated by discovery over a longer period of time. The choices are:
  - *System Default (recommended)*. Use the value defined in the **Behavior Settings** page (System > Settings > Behavior).
  - *Disabled*. Discovery processes will not pause.
  - *1000 Msec to 10000 Msec*. A discovery process will pause for a random amount of time between half the selected value and the selected value.
- **Port Scan All IPs**. For the initial discovery session only, specifies whether SL1 should scan all IP addresses on a device for open ports. The choices are:
  - *System Default (recommended)*. Use the value defined in the **Behavior Settings** page (System > Settings > Behavior).
  - *0. Disabled*. SL1 will scan only the primary IP address (the one used to communicate with SL1) for open ports.
  - *1. Enabled*. SL1 will scan all discovered IP addresses for open ports.
- **Port Scan Timeout**. For the initial discovery session only, specifies the length of time, in milliseconds, after which SL1 should stop trying to scan an IP address for open ports and begin scanning the next IP address (if applicable). Choices are:
  - *System Default (recommended)*. Use the value defined in the **Behavior Settings** page (System > Settings > Behavior).
  - Choices between 60,000 to 1,800,000 milliseconds.

- **Detection Method & Port.** During discovery, SL1 will scan the list of ports selected in this field to determine if the range of devices is up and running and which ports are open on each discovered device. If a device does not respond to SNMP or ICMP, SL1 uses an open port to collect availability data for that device. If you are not sure which ports are used by the range of devices, select the entry *Default Method*. SL1 will check ICMP (ping), FTP, SSH, Telnet, SMTP, and HTTP ports.

**NOTE:** You can use the field at the top of the **Detection Method & Port** field to filter the list of ports. If you enter an alpha-numeric string in the field, the **Detection Method & Port** field will include only ports that match the string.

- **Interface Inventory Timeout (ms).** Specifies the maximum amount of time that the discovery processes will spend polling a device for the list of interfaces. After the specified time, SL1 will stop polling the device, will not model the device, and will continue with discovery. The default value is 600,000 ms (10 minutes).
  - During the execution of this discovery session, SL1 uses the value in this field first. If you delete the default values and do not specify another value in this field, SL1 uses the value in the **Global Threshold Settings** page (System > Settings > Thresholds).
  - If you specify a value in this field and do not apply a device template to this discovery session, the **Interface Inventory Timeout** setting in the **Device Thresholds** page (Registry > Devices > Device Manager > wrench icon > Thresholds) is set to this value for each discovered device. If there is no device template applied to the discovery session and no value is supplied in this field, SL1 uses the value in the **Global Threshold Settings** page (System > Settings > Thresholds).
- **Maximum Allowed Interfaces.** Specifies the maximum number of interfaces per devices. If a device exceeds this number of interfaces, SL1 will stop scanning the device, will not model the device, and will continue with discovery. The default value is 10,000.
  - During the execution of this discovery session, SL1 uses the value in this field first. If you delete the default values and do not specify another value in this field, SL1 uses the value in the **Global Threshold Settings** page.
  - If you specify a value in this field and do not apply a device template to this discovery session, the **Maximum Allowed Interfaces** setting in the **Device Thresholds** page is set to this value for each discovered device. If there is no device template applied to the discovery session and no value is supplied in this field, SL1 uses the value in the **Global Threshold Settings** page.
- **Bypass Interface Inventory.** Specifies whether or not the discovery session should discover network interfaces.
  - *Selected.* SL1 will not attempt to discover interfaces for each device in the discovery session. For each discovered device, the **Bypass Interface Inventory** checkbox in the **Device Properties** page will be selected.
  - *Not Selected.* SL1 will attempt to discover network interfaces, using the **Interface Inventory Timeout** value and **Maximum Allowed Interfaces** value.

**NOTE:** If a device has already been discovered and then is rediscovered through the **Discovery Session Editor** page, the **Bypass Interface Inventory** checkbox in the **Device Properties** page will retain its previous value, regardless of what is selected in the **Discovery Session Editor** page.

- **Discover Non-SNMP Devices.** Specifies whether or not SL1 should discover devices that don't respond to SNMP requests.
  - *Selected.* SL1 will discover devices that don't respond to the SNMP credentials selected in the **SNMP Credentials** field. These devices will be discovered as "pingable" devices.
  - *Not Selected.* SL1 will not discover devices that don't respond to the SNMP credentials selected in the **SNMP Credentials** fields.
- **Model Devices.** Determines whether or not the devices that are discovered with this discovery session can be managed through SL1. Choices are:
  - *Enabled.* When a device is modeled, SL1 creates a device ID for the device; you can then access the device through the **Device Manager** page and manage the device in SL1.
  - *Disabled.* If a device is not modeled, you cannot access the device through the **Device Manager** page, and you cannot manage the device in SL1. However, each discovered device will still appear in the Discovery Session logs. For each discovered device, the discovery logs will display the IP address and device class for the device. This option is useful when performing an initial discovery of your network, to determine which devices you want to monitor and manage with SL1. For the amount of time specified in the **Device Model Cache TTL (h)** field, a user can manually model the device from the **Discovery Session** window.
- **DHCP.** Specifies whether or not the specified range of IPs and hostnames use DHCP.
  - *Selected.* SL1 will perform a DNS lookup for the device during discovery and each time SL1 retrieves information from the device.
  - *Not Selected.* SL1 will perform normal discovery.
- **Device Model Cache TTL (h).** Amount of time, in hours, that SL1 stores information about devices that are discovered but not modeled, either because the **Model Devices** option is not enabled or because SL1 cannot determine whether a duplicate device already exists. The cached data can be used to manually model the device from the **Discovery Session** window.
- **Collection Server PID.** This field contains a list of all Data Collectors on the network. Select the Data Collector that is local or closest to the devices to be discovered.
  - For SL1 appliances, only the name of the appliance will appear in this field.


**NOTE:** After initial discovery, each device will use the collector group that contains this Data Collector for collection and rediscovery.

- **Organization**. This field contains a list of all organizations defined in SL1. Devices discovered during the discovery session will be assigned to the selected organization.

**NOTE:** Make sure you have the desired organization created and selected before running the discovery process. This field assigns all devices and networks in the specified IP range to a single organization. However, you can later assign individual devices and networks to different organizations.

- **Add Devices to Device Group(s)**. When SL1 discovers a device in the IP discovery list, that device is added to each selected device group. You can select one or more device groups from a list of device groups in SL1 that have "Discovery" selected in the **Visibility** field. For more information on device groups, see the manual on **Device Groups and Device Templates**.

**NOTE:** You can use the field at the top of the **Add Devices to Device Group(s)** field to filter the list of device groups. If you enter an alpha-numeric string in the field, the **Add Devices to Device Group(s)** field will include only device groups that match the string.

- **Apply Device Template**. As SL1 discovers a device in the IP discovery list, that device is configured with the selected device template. You can select from a list of all device templates in SL1. For more information on device templates, see the manual on **Device Groups and Device Templates**.
  - **Log All**. Specifies whether or not the discovery session should use verbose logging. When you select verbose logging, SL1 logs details about each IP address or hostname specified in the **IP Address/Hostname Discovery List** field, even if the results are "No device found at this address."
    - *Selected*. This discovery session will use verbose logging.
    - *Not Selected*. This discovery session will not use verbose logging.
4. Click the **[Save]** button to save the discovery session. Close the **Discovery Session Editor** page.
  5. In the **Discovery Control Panel** page, click the **[Reset]** button. The new discovery session will appear in the **Session Register** pane.
  6. To launch the new discovery session, click its **Queue this Session** icon (.
  7. If no other discovery sessions are currently running, the session will be executed immediately. If another discovery session is currently running, your discovery session will be queued for execution.

---

## Creating a New Classic Discovery Session with the Save As Button

You can edit an existing discovery session, make one or more changes, and then save the edited discovery session as a new session. The previous session still exists, unedited. To do this:

1. In the **Discovery Control Panel** page (System > Manage > Classic Discovery), in the **Session Registry** pane, find the discovery session you want to edit. Click its wrench icon (.

2. The **Discovery Session Editor** page appears.
3. In the **Discovery Session Editor** page, you can edit one or more values listed in the [Running a Discovery Session](#) section.
4. Click the **[Save As]** button to save the discovery session as a new session. The new session appears in the **Discovery Control Panel** page (System > Manage > Classic Discovery).

## Viewing Information about a Classic Discovery Session

The **Session Register** pane in the **Discovery Control Panel** (System > Manage > Classic Discovery) page displays information about all discovery sessions defined in SL1.

Session Name	IP/hostname List	Collector	Organization	Pin	Rediscovery	User Edit	Last Edit
1. --	10.100.100.7	em7_ao	System	No	Disabled	em7admin	2015-05-14 10:35:34
2. --	173.38.219.46	em7_ao	System	Yes	Disabled	em7admin	2015-05-14 13:35:29
3. --	10.100.100.48	em7_ao	System	No	Disabled	em7admin	2015-05-18 12:30:57
4. --	10.100.100.35	em7_ao	System	Yes	Disabled	em7admin	2015-05-18 12:31:48
5. --	10.100.100.72	em7_ao	System	No	Disabled	em7admin	2015-05-18 12:32:12
6. --	10.100.100.29	em7_ao	System	No	Disabled	em7admin	2015-05-18 12:32:39

**TIP:** To sort the list of discovery sessions, click on a column heading. The list will be sorted by the column value, in ascending order. To sort by descending order, click the column heading again. The **Last Edit** column sorts by descending order on the first click; to sort by ascending order, click the column heading again.

For each session, the **Session Register** displays:

- **Session Name.** Name of the discovery session. This field is optional.
- **IP/Hostname List.** The range of IP addresses and/or hostnames for SL1 to scan during discovery. This field can contain a combination of one or more of the following:
  - One or more *single IPv4 addresses* separated by commas. Each IP address must be in standard IP notation and cannot exceed 15 characters. For example, "10.20.30.1, 10.20.30.2, 10.20.30.3".

- One or more *ranges of IPv4 addresses* with "-" (dash) characters between the beginning of the range and the end of the range. Separate each range with a comma. For example, "10.20.30.1 – 10.20.30.254".
- One or more IP address ranges in *IPv4 CIDR notation*. Separate each item in the list with a comma. For example, "192.168.168.0/24".
- One or more *ranges of IPv6 addresses* with "-" (dash) characters between the beginning of the range and the end of the range. Separate each range with a comma. For example, "2001:DB8:0:0:0:0:0:0-2001:DB8:0:0:0:0:0:0003".
- One or more IP address ranges in *IPv6 CIDR notation*. Separate each item in the list with a comma. For example, "2001:DB8:0:0:0:0:0:0/117".
- One or more fully-qualified domain names or hostnames.

**NOTE:** The following types of notation are **not supported**: IPv4 netmask with comma notation (192.168.168.0,24); a list of single IPv6 addresses, separated by comma.

- **Collector.** Data Collector used for the discovery session.
- **Organization.** The organization to which devices discovered during the discovery session will be assigned.
- **Pings.** This field specifies whether or not SL1 should discover devices that don't respond to the selected SNMP credentials. The possible values are:
  - Yes. SL1 will discover devices that don't respond to the SNMP credentials selected in the **SNMP Credentials** field for the discovery session. These devices will be discovered as "pingable" devices.
  - No. SL1 will not discover devices that don't respond to the SNMP credentials selected in the **SNMP Credentials** field for this discovery session.
- **Rediscovery.** Specifies whether or not SL1 is scheduled to run this discovery session, and if so, the frequency and time specified in the schedule.
- **User Edit.** Name of user who created or last edited the discovery session.
- **Last Edit.** Date and time discovery session was created or last edited.

To filter the list of discovery sessions in the **Session Register**, use the search fields at the top of each column. The search fields are find-as-you-type filters; as you type, the page is filtered to match the text in the search field, including partial matches. Text matches are not case-sensitive. Additionally, you can use the following special characters in each filter:

- , (comma). Specifies an "or" operation. For example:
 

"dell, micro" would match all values that contain the string "dell" OR the string "micro".
- & (ampersand). Specifies an "and" operation. For example:
 

"dell & micro" would match all values that contain the string "dell" AND the string "micro".
- ! (exclamation mark). Specifies a "not" operation. For example:

"!dell" would match all values that do not contain the string "dell".

- ^ (caret mark). Specifies "starts with." For example:

"^micro" would match all strings that start with "micro", like "microsoft".

"^" will include all rows that have a value in the column.

"!^" will include all rows that have no value in the column.

- \$ (dollar sign). Specifies "ends with." For example:

"\$ware" would match all strings that end with "ware", like "VMware".

"\$" will include all rows that have a value in the column.

"!\$" will include all rows that have no value in the column.

- min-max. Matches numeric values only. Specifies any value between the minimum value and the maximum value, including the minimum and the maximum. For example:

"1-5" would match 1, 2, 3, 4, and 5.

- - (dash). Matches numeric values only. A "half open" range. Specifies values including the minimum and greater or including the maximum and lesser. For example:

"1-" matches 1 and greater, so it would match 1, 2, 6, 345, etc.

"-5" matches 5 and less, so it would match 5, 3, 1, 0, etc.

- > (greater than). Matches numeric values only. Specifies any value "greater than." For example:

">7" would match all values greater than 7.

- < (less than). Matches numeric values only. Specifies any value "less than." For example:

"<12" would match all values less than 12.

- >= (greater than or equal to). Matches numeric values only. Specifies any value "greater than or equal to." For example:

">=7" would match all values 7 and greater.

- <= (less than or equal to). Matches numeric values only. Specifies any value "less than or equal to." For example:

"<=12" would match all values 12 and less.

- = (equal). Matches numeric values only. For numeric values, allows you to match a negative value. For example:



"=-5" would match "-5" instead of being evaluated as the "half open range" as described above.



---

## Editing a Classic Discovery Session

You can edit the parameters of a discovery session in the **Discovery Control Panel** page. To do this:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
2. Find the discovery session you want to edit. Click its wrench icon (.
3. The **Discovery Session Editor** page appears with the values from the previous discovery session. You can edit any of the fields described in the section [Running a Discovery Session](#).
4. Click the **[Save]** button to save your changes. To save the edited discovery session **as a new session** (the previous session will still exist), click the **[Save As]** button. Close the **Discovery Session Editor** page.
5. To manually run discovery using the edited session, find the edited session in the **Session Register** pane and click its **Queue this Session** icon (). If no other discovery sessions are currently running, the session will be executed immediately. If another discovery session is currently running, your discovery session will be queued for execution.

3

---

## Scheduling a Classic Discovery Session

You can schedule one-time and recurring re-execution of a selected discovery session. You can use the **Schedule Manager** page (System > Manage > Classic Discovery > calendar icon) to:

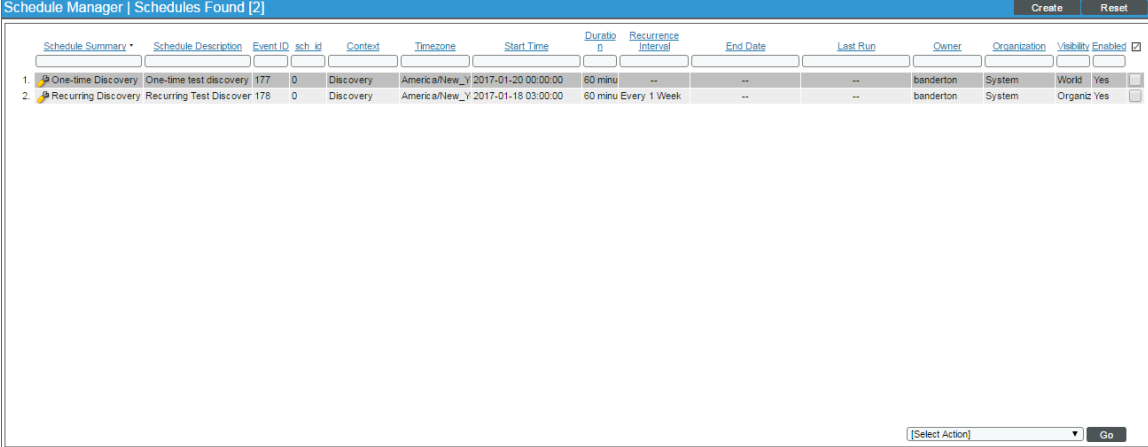
- Specify regularly recurring discovery of a specific IP range. This is helpful when you want to monitor an IP range where new devices are frequently added.
- Specify one-time re-discovery of a specific IP range. This is helpful when you are aware of hardware or software changes within that IP range that you want SL1 to monitor.

**NOTE:** Scheduled re-execution of a discovery session is slightly different than SL1's automatic, nightly rediscovery. Nightly rediscovery is applied only to already discovered devices and uses the policies and configuration applied to each device. Re-execution of a discovery session can discover new devices within an IP range and uses only the settings specified in the **Discovery Control Panel** page.

**NOTE:** You can also view and manage all scheduled processes from the **Schedule Manager** page (Registry > Schedules > Schedule Manager). For more information, see the **System Administration** manual.

## Viewing the Schedule Manager

The **Schedule Manager** page (System > Manage > Classic Discovery > calendar icon) displays the following information about each scheduled or recurring discovery session:



The screenshot shows the 'Schedule Manager' interface with a table of scheduled discovery sessions. The table has the following columns: Schedule Summary, Schedule Description, Event ID, sch. id, Context, Timezone, Start Time, Duration, Recurrence Interval, End Date, Last Run, Owner, Organization, Visibility, and Enabled. There are two rows of data:

	Schedule Summary	Schedule Description	Event ID	sch. id	Context	Timezone	Start Time	Duration	Recurrence Interval	End Date	Last Run	Owner	Organization	Visibility	Enabled
1.	One-time Discovery	One-time test discovery	177	0	Discovery	America/New_Y	2017-01-20 00:00:00	60 minu	--	--	--	banderton	System	World	Yes
2.	Recurring Discovery	Recurring Test Discover	178	0	Discovery	America/New_Y	2017-01-18 03:00:00	60 minu	Every 1 Week	--	--	banderton	System	Organiz	Yes

- **Schedule Summary.** Displays the name assigned to the scheduled process.
- **Schedule Description.** Displays a description of the scheduled process.
- **Event ID.** Displays a unique, numeric ID for the scheduled process. SL1 automatically created this ID for each scheduled process.
- **sch. id.** Displays a unique, numeric ID for the schedule. SL1 automatically created this ID for each schedule.
- **Context.** Displays the area of SL1 upon which the schedule works.
- **Timezone.** Displays the time zone associated with the scheduled process.
- **Start Time.** Displays the date and time at which the scheduled process will begin.
- **Duration.** Displays the duration, in minutes, which the scheduled process occurs.
- **Recurrence Interval.** If applicable, displays the interval at which the scheduled process recurs.
- **End Date.** If applicable, displays the date and time on which the scheduled process will recur.
- **Last Run.** If applicable, displays the date and time the scheduled process most recently ran.
- **Owner.** Displays the username of the owner of the scheduled process.
- **Organization.** Displays the organization to which the scheduled process is assigned.
- **Visibility.** Displays the visibility level for the scheduled process. Possible values are "Private", "Organization", or "World".
- **Enabled.** Specifies if the scheduled process is enabled. Possible values are "Yes" or "No".

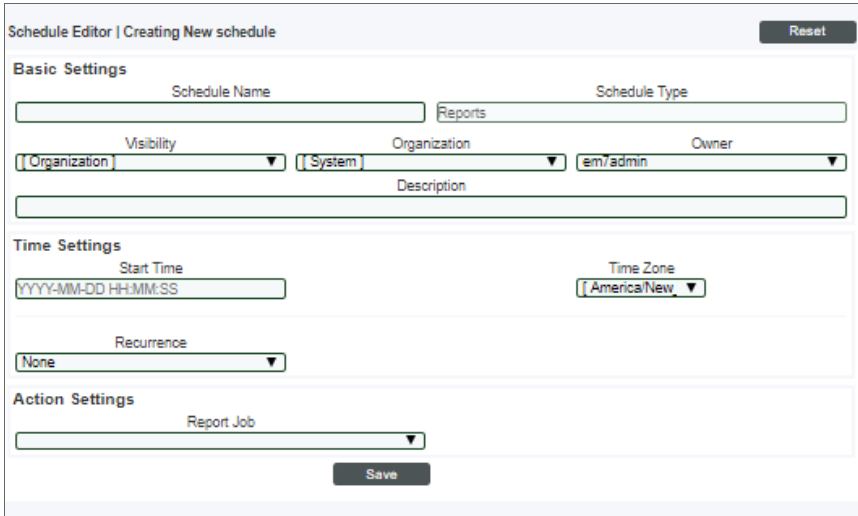
To edit a scheduled or recurring discovery session, click its wrench icon (🔧) and update the discovery session as needed on the **Schedule Editor** modal page. (For more information, see the section [Defining a Scheduled or Recurring Discovery Session](#).)

## Defining a Scheduled or Recurring Discovery Session

You can schedule a discovery session in SL1 from the **Schedule Manager** page. SL1 will automatically run the discovery session at the scheduled time.

To define a scheduled or recurring discovery session:

1. Go to the **Schedule Manager** page (System > Manage > Classic Discovery > calendar icon).
2. Click **[Create]**. The **Schedule Editor** modal page appears.
3. On the **Schedule Editor** modal page, make entries in the following fields:



The screenshot shows the 'Schedule Editor | Creating New schedule' modal window. It is divided into three main sections: 'Basic Settings', 'Time Settings', and 'Action Settings'.  
- **Basic Settings:** Includes 'Schedule Name' (text input), 'Schedule Type' (text input with 'Reports' selected), 'Visibility' (dropdown menu with 'Organization' selected), 'Organization' (dropdown menu with 'System' selected), 'Owner' (dropdown menu with 'em/admin' selected), and 'Description' (text input).  
- **Time Settings:** Includes 'Start Time' (text input with a YYYY-MM-DD HH:MM:SS mask), 'Time Zone' (dropdown menu with 'America/New' selected), and 'Recurrence' (dropdown menu with 'None' selected).  
- **Action Settings:** Includes 'Report Job' (dropdown menu).  
Buttons for 'Reset' (top right), 'Save' (bottom center), and 'Save' (bottom right) are visible.

### **Basic Settings**

- **Schedule Name.** Type a name for the scheduled process.
- **Schedule Type.** Indicates the scheduled process type (such as Tickets, Reports, or Devices).
- **Visibility.** Select the visibility for the scheduled process. You can select one of the following:
  - *Private.* The scheduled process is visible only to the owner selected in the **Owner** field.
  - *Organization.* The scheduled process is visible only to the organization selected in the **Organization** field.
  - *World.* The scheduled process is visible to all users.
- **Organization.** Select the organization to which you want to assign the scheduled process.
- **Owner.** Select the owner of the scheduled process. The default value is the username of the user who created the scheduled process.
- **Description.** Type a description of the scheduled process.

## **Time Settings**

- **Start Time.** Click in the field and select the date and time you want the scheduled process to start.
- **Time Zone.** Select the region or time zone for the scheduled start time.

**NOTE:** If you want SL1 to automatically adjust for daylight savings time (if applicable), then you must select a named region (such as *America/New York*) in the **Time Zone** field. If you select a specific time zone (such as *EST*) or a specific time offset (such as *GMT-5*), then SL1 will not automatically adjust for daylight savings time.

- **Recurrence.** Select whether you want the scheduled process to occur once or on a recurring basis. You can select one of the following:
  - *None.* The scheduled process occurs only once.
  - *By Interval.* The scheduled process recurs at a specific interval.

If you select *By Interval*, the following additional fields appear:

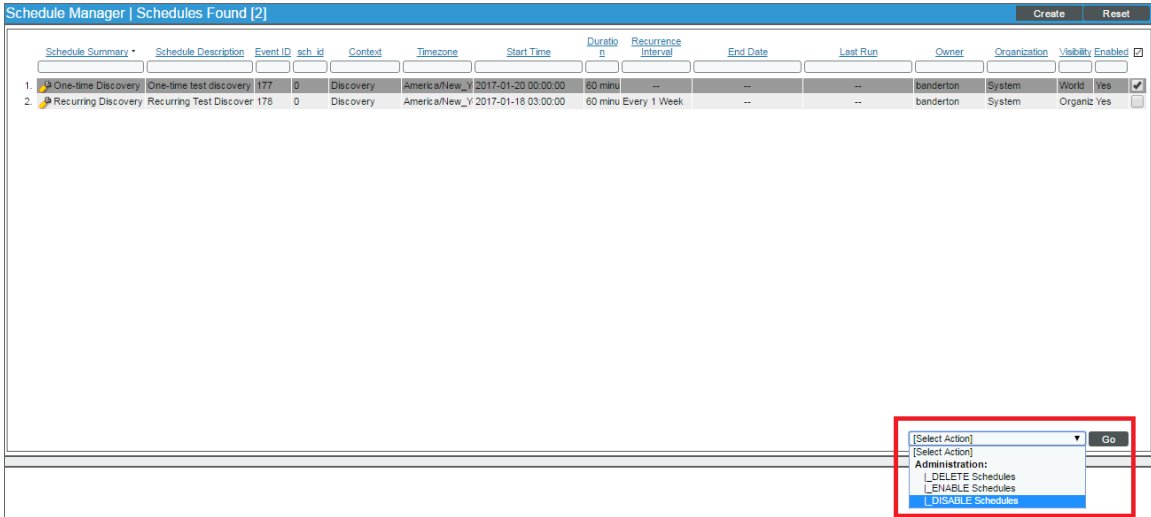
- **Interval.** In the first field, enter a number representing the frequency of the scheduled process, then select the time interval in the second field. Choices are *Minutes, Hours, Days, Weeks, or Months*. For example:
  - If you specify "6 Hours", then the scheduled process recurs every six hours from the time listed in the **Start Date** field.
  - If you specify "10 Days", then the scheduled process recurs every 10 days from the date listed in the **Start Date** field.
  - If you specify "2 Weeks", then the scheduled process recurs every two weeks, on the same day of the week as the **Start Date**.
  - If you specify "3 Months" the ticket recurs every three months, on the same day of the month as the **Start Date**.
- **Recur Until.** Specifies when the scheduled process stops recurring. You can select one of the following:
  - *No Limit.* The scheduled process recurs indefinitely until it is disabled.
  - *Specified Date.* The scheduled process recurs until a specific date and time. If you select *Specified Date*, you must enter a date and time in the **Last Recurrence** field.
- **Last Recurrence.** Click in the field and select the date and time you want the scheduled process to stop recurring.

4. Click **[Save]**.

## Enabling or Disabling One or More Scheduled Discovery Sessions

You can enable or disable one or more scheduled or recurring discovery sessions from the **Schedule Manager** page (System > Manage > Classic Discovery > calendar icon). To do this:

1. Go to the **Schedule Manager** page (System > Manage > Classic Discovery > calendar icon).



The screenshot shows the 'Schedule Manager' interface with a table of scheduled discovery sessions. The table has columns for Schedule Summary, Schedule Description, Event ID, sch. id, Context, Timezone, Start Time, Duration, Recurrence Interval, End Date, Last Run, Owner, Organization, Visibility, and Enabled. Two rows are visible: a one-time discovery session and a recurring discovery session. A dropdown menu is open over the 'Enabled' column, showing options: [Select Action], [Select Action], Administrations, DELETE Schedules, ENABLE Schedules, and DISABLE Schedules. The 'DISABLE Schedules' option is highlighted. A 'Go' button is also visible next to the dropdown.

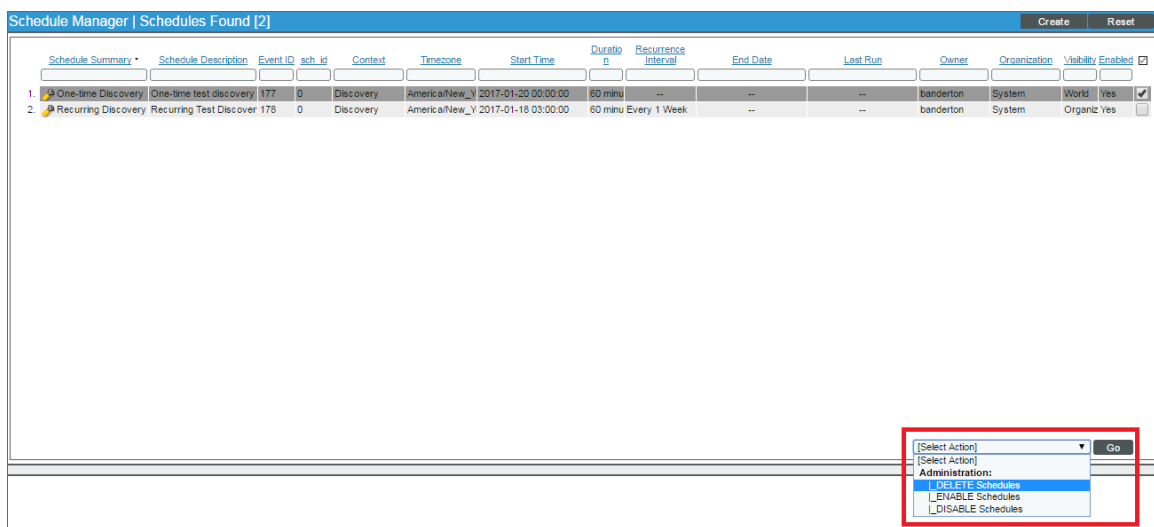
Schedule Summary	Schedule Description	Event ID	sch. id	Context	Timezone	Start Time	Duration	Recurrence Interval	End Date	Last Run	Owner	Organization	Visibility	Enabled
One-time Discovery	One-time test discovery	177	0	Discovery	America/New_Y	2017-01-20 00:00:00	60 min	--	--	--	banderton	System	World	Yes
Recurring Discovery	Recurring Test Discover	178	0	Discovery	America/New_Y	2017-01-18 03:00:00	60 min	Every 1 Week	--	--	banderton	System	Organiz	Yes

2. Select the checkbox icon for each scheduled process you want to enable or disable.
3. Click the **Select Action** menu and choose *Enable Schedules* or *Disable Schedules*.
4. Click the **[Go]** button.

## Deleting One or More Scheduled Discovery Sessions

You can delete one or more scheduled or recurring discovery sessions from the **Schedule Manager** page (System > Manage > Discovery > calendar icon). To do this:

1. Go to the **Schedule Manager** page (System > Manage > Classic Discovery > calendar icon).



2. Select the checkbox icon for each scheduled process you want to delete.
3. Click the **Select Action** menu and choose *Delete Schedules*.
4. Click the **[Go]** button.

---

## Manually Re-Running Discovery for a Dynamic Application

From the **Dynamic Applications Manager** page, you can manually run the Dynamic Application alignment portion of discovery for all existing devices in the system. That is, you can ask SL1 to check each Dynamic Application and each existing device and align each device with each appropriate Dynamic Application.

For each Dynamic Application you select for re-discovery, SL1 tries to connect to each existing device using the credentials already aligned with each device. If SL1 is able to connect to a device with one of the credentials and can then retrieve the discovery object associated with the Dynamic Application, SL1 will align the Dynamic Application with the device.

To manually run discovery for a *single Dynamic Application*:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Dynamic Applications).



- If no other discovery tasks are currently running, SL1 will immediately perform discovery of the entire network, using the selected Dynamic Application.
- If other discovery tasks are currently running, SL1 will add the request to the discovery queue.

## Manually Re-Running Discovery for a Device

You can manually re-discover a device, using the settings and configuration in the **Device Properties** page for the device.

Remember that the credentials and settings defined in the **Device Properties** page override:

- Settings in the **Behavior Settings** page (System > Settings > Behavior).
- Credentials and settings in the **Discovery Control Panel** page () from the initial discovery of the device.

SL1 will update the device with the data from the discovery session. The discovery session does not change, overwrite, or affect the existing, historical data associated with the device.

To re-discover a device:

- Go to the **Device Manager** page (Devices > Device Manager).
- In the **Device Manager** page, find the device you want to re-discover. Click its wrench icon (🔧).
- In the **Device Properties** page, click the **Rediscover** icon (🔄).

The screenshot shows the 'Device Properties' page for a device with IP 10.168.44.205. The page is divided into several sections:

- Identification:** Contains fields for Device Name (10.168.44.205), IP Address ([10.168.44.205 - verified]), and Organization ([Acme Corporation]). A red box highlights the Rediscover icon (🔄) next to the Device Name field.
- Monitoring & Management:** Contains various configuration options such as Device Class (Microsoft Windows Cluster Point), SNMP Read/Write (c0em0s), Availability Port ([ICMP]), Latency Port ([ICMP]), Avail-Latency Alert ([Disable]), Collection ([Enabled]), Coll. Type ([Standard]), Critical Ping ([Disabled]), and Event Mask ([Group in blocks every 10 minutes]).
- Preferences:** Contains a list of checkboxes for settings like Auto-Clear Events, Accept All Logs, Daily Port Scans, Auto-Update, Scan All IPs, Dynamic Discovery, Preserve Hostname, and Disable Asset Update.

A 'Save' button is located at the bottom of the page.

- If no other discovery tasks are currently running, SL1 will immediately perform discovery of the selected device.

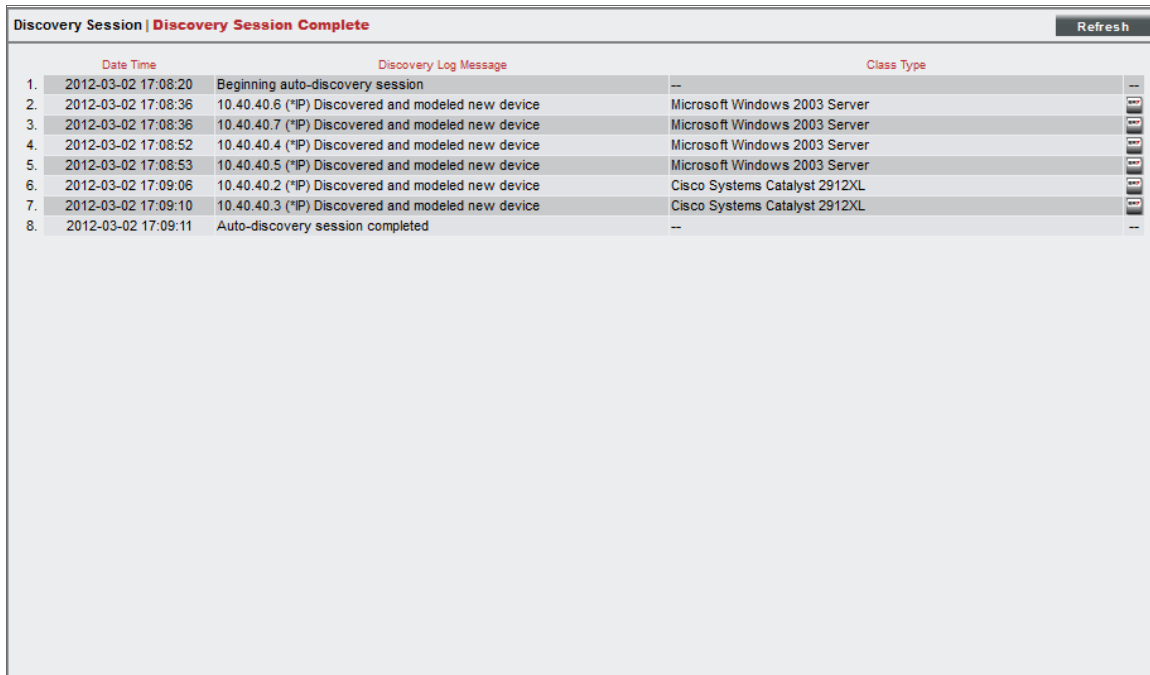


5. If other discovery tasks are currently running, SL1 will add the request to the discovery queue.

## Viewing Information about Classic Discovery

To view information about a discovery session that has already run:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
2. In the **Discovery Control Panel** page, in the Session Register, find the discovery session you are interested in. Click its magnifying glass icon (🔍).
3. The **Discovery Session** modal page appears. This page provides details on the discovery session.



The screenshot shows a modal window titled "Discovery Session | Discovery Session Complete" with a "Refresh" button in the top right corner. The main content is a table with three columns: "Date Time", "Discovery Log Message", and "Class Type". The table contains eight rows of log entries, each with a small magnifying glass icon in the right margin.

	Date Time	Discovery Log Message	Class Type
1.	2012-03-02 17:08:20	Beginning auto-discovery session	--
2.	2012-03-02 17:08:36	10.40.40.6 (*IP) Discovered and modeled new device	Microsoft Windows 2003 Server
3.	2012-03-02 17:08:36	10.40.40.7 (*IP) Discovered and modeled new device	Microsoft Windows 2003 Server
4.	2012-03-02 17:08:52	10.40.40.4 (*IP) Discovered and modeled new device	Microsoft Windows 2003 Server
5.	2012-03-02 17:08:53	10.40.40.5 (*IP) Discovered and modeled new device	Microsoft Windows 2003 Server
6.	2012-03-02 17:09:06	10.40.40.2 (*IP) Discovered and modeled new device	Cisco Systems Catalyst 2912XL
7.	2012-03-02 17:09:10	10.40.40.3 (*IP) Discovered and modeled new device	Cisco Systems Catalyst 2912XL
8.	2012-03-02 17:09:11	Auto-discovery session completed	--

4. The **Discovery Session** page includes an entry for each action performed during the discovery session. Each entry in the **Discovery Session** page contains:
  - **Date Time.** Date and time the action was executed.
  - **Discovery Log Message.** When applicable, starts with the IP address of the discovered device. Also includes a description of the action that was executed by the discovery session.

**NOTE:** If you did not select [Auto-Update](#) in the **Device Properties** page for one or more devices, when the discovery process tries to discover one of those devices, the log will display the message "Auto-Update is disabled and prevents discovery from updating any device properties."

- **Class Type.** The device class for each discovered device. SL1 will determine the device class for each device, even if a device will not be modeled by SL1.

- **Checkbox.** If a device was discovered but not modeled, you can select this checkbox and click the **[Model]** button to model the device. If this device is a potential duplicate, the **Discovery Session** page displays the message "Not modeled, potential duplicate device". If you are certain that the device is not a duplicate, you can choose to model the device.

5. To save the log to the local computer, go to the **Discovery Control Panel** page (System > Manage > Classic Discovery), and click the **Export** icon (📄) for the session.

## Managing MAC Vendor Records

The **MAC Vendor Records** page (System > Customize > MAC Vendors) allows you to view and edit the list of MAC Vendor Records in SL1. MAC Vendor Records include vendor information about each MAC address prefix. A MAC address prefix is the first three groups of hexadecimal digits in a MAC address. The MAC Address prefix uniquely identifies the vendor of the network interface. Some vendors use multiple MAC Address prefixes, but each vendor's MAC Address prefixes are unique to that vendor and are not used by other vendors.

### Viewing the List of MAC Vendor Records

The **MAC Vendor Records** page (System > Customize > MAC Vendors) displays information about each MAC Vendor Record in SL1. The **MAC Vendor Records** page displays the following for each MAC Vendor Record:

MAC Hex	Vendor	Vendor Notes	Visual
1. 08:00:24	10netCommu	10NET COMMUNICATIONS DCA	no
2. 00:0B:10	11waveTech	11wave Technology Co. Ltd	no
3. 00:50:29	1394Printe	1394 PRINTER WORKING GROUP	no
4. 00:A0:2D	1394TradeA	1394 Trade Association	no
5. 00:36:70	1net	1Net Corporation	no
6. 00:11:82	2001Techno	2001 Technology Inc.	no
7. 00:13:87	27mTechnol	27M Technologies AS	no
8. 00:16:A9	2ei	--	no
9. 00:19:29	2m2bMontad	2M2B Montadora de Maquinas Bahia Brasil LTDA	no
10. 00:1B:8A	2mElectron	2M Electronic A S	no
11. 00:11:99	2wicom	2wicom GmbH	no
12. 00:12:88	2wire	2Wire Inc.	no
13. 00:1B:5B	2wire	2Wire Inc.	no
14. 00:1A:C4	2wire	2Wire Inc.	no
15. 00:19:E4	2wire	2Wire Inc.	no
16. 00:D6:9E	2wire	2WIRE INC.	no
17. 00:14:95	2wire	2Wire Inc.	no
18. 00:18:3F	2wire	2Wire Inc.	no
19. 00:0D:72	2wire	2Wire Inc.	no
20. 00:05:56	360	360 Systems	no
21. 00:0E:80	360sunDigi	360SUN Digital Broadband Corporation	no
22. 00:0F:05	38System	38 SYSTEM INC.	no
23. 00:10:5A	3com	3COM CORPORATION	no
24. 00:10:4B	3com	3COM CORPORATION	no
25. 00:0A:5E	3com	3COM CORPORATION	no
26. 00:20:AF	3com	3COM CORPORATION	no
27. 00:20:85	3com	--	no
28. 00:26:54	3com	3com Corporation	no
29. 00:01:03	3com	3COM CORPORATION	no
30. 00:01:02	3com	3COM CORPORATION	no
31. 00:02:9C	3com	--	no
32. 00:04:75	3Com	3 Com Corporation	no
33. 00:04:76	3com	3 Com Corporation	no
34. 00:60:08	3com	3COM CORPORATION	no
35. 00:50:DA	3com	3COM CORPORATION	no

- **MAC Hex.** The MAC address prefix for the vendor record.
- **Vendor.** The name of the vendor of the network interfaces that use the MAC address prefix.
- **Vendor Notes.** Additional information about the vendor.

- **Virtual.** Indicates whether the vendor associated with this MAC address prefix allows the same MAC address to be re-used on multiple devices:
  - Yes. The vendor allows the same MAC address to be re-used on multiple devices. If a new interface is discovered during nightly discovery and that interface has a MAC address with this prefix that is already associated with an interface record in the system, SL1 will create a new interface record for the newly discovered interface.
  - No. The vendor does not allow the same MAC address to be re-used on multiple devices. If a new interface is discovered during nightly discovery and that interface has a MAC address with this prefix that is already associated with an interface record in the system, SL1 will NOT create a new interface record for the newly discovered interface.

## Filtering the List of MAC Vendor Records

The **MAC Vendor Records** page includes four filters, in the top row in the list of MAC Vendor Records. You can specify one or more parameters to filter the display of MAC Vendor Records. Only MAC Vendor Records that meet all the filter criteria will be displayed in the **MAC Vendor Records** page.

You can filter by one or more of the following parameters. The list of MAC Vendor Records is dynamically updated as you select each filter.

- For each filter, you must enter text to match against. SL1 will search for MAC Vendor Records that match the text, including partial matches. Text matches are not case sensitive. You can use the following special characters in each filter:
  - , (comma). Specifies an "or" operation. For example:
 

"dell, micro" would match all values that contain the string "dell" OR the string "micro".
  - ! (exclamation mark). Specifies a "not" operation. For example:
 

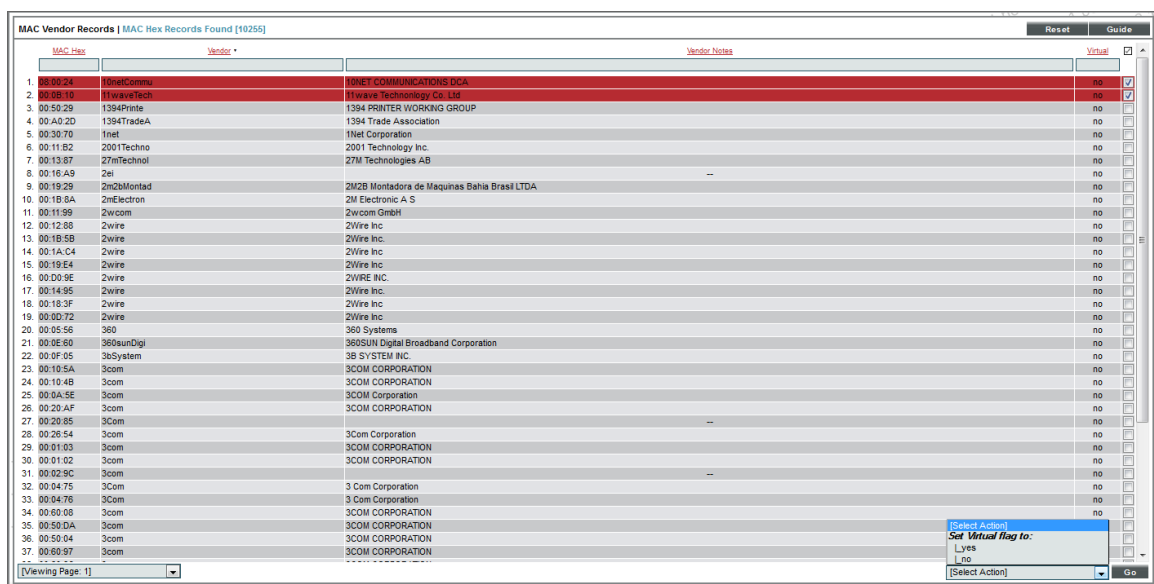
"!dell" would match all values that do not contain the string "dell".
- **MAC Hex.** You can enter text to match, including special characters, and the **MAC Vendor Records** page will display only MAC Vendor Records that have a matching prefix.
- **Vendor.** You can enter text to match, including special characters, and the **MAC Vendor Records** page will display only MAC Vendor Records that have a matching vendor name.
- **Vendor Notes.** You can enter text to match, including special characters, and the **MAC Vendor Records** page will display only MAC Vendor Records that have a matching vendor note.
- **Virtual.** You can enter text to match, including special characters, and the **MAC Vendor Records** page will display only MAC Vendor Records that have a matching virtual setting.

## Editing the Virtual Setting for MAC Vendor Records

The **MAC Vendor Records** page contains a drop-down field in the lower right called **Select Action**. This field allows you to apply an action to multiple MAC Vendor Records simultaneously.

To apply an action to multiple MAC Vendor Records:

1. Go to the **MAC Vendor Records** page (System > Customize > MAC Vendors).
2. In the **MAC Vendor Records** page, select the checkbox for each MAC Vendor Record you want to apply the action to. To select all checkboxes for all MAC Vendor Records, select the red checkbox (☑) at the top of the page.
3. In the **Select Action** drop-down list, select one of the following actions:
  - **Set Virtual Flag To: Yes**. Sets the virtual setting for the Mac Vendor Record to "yes".
  - **Set Virtual Flag To: No**. Sets the virtual setting for the Mac Vendor Record to "no".
4. Click the **[Go]** button to apply the selected action to the selected MAC Vendor Records.



## Troubleshooting Discovery

If discovery is not working as you expected, you can try these troubleshooting steps to try to fix any problems. If problems persist, please contact ScienceLogic Customer Care.

## Checking Network Security

Your network security and network configuration can prevent SL1 from communicating with each device in your network. To ensure that discovery can access each device in your network, check the following:

- To discover a device as a "pingable" device, SL1 must be able to either:
  - Ping the device (access through ICMP).
  - Access at least one of the ports selected in the **Discovery Control Panel** page.
- To discover a device as "manageable" (that is, the device supports SNMP), SL1 must be able to access the UDP port defined in the working SNMP credential for that device.
- On each DNS server(s) for your network, SL1 must access UDP port 53.
- If there are firewalls between the Data Collectors and devices to be monitored, make sure that the firewalls are configured to allow SL1 access to those devices.

## Debugging the Discovery Processes

When you debug a process, you tell SL1 to use verbose logging for that process. You can then view the log file to view detailed log files. If discovery is not performing as you would expect, you might find it helpful to debug one or more of the discovery processes.

In general:

- If SL1 is not discovering one or more devices that you know exist, debug the process **Discovery: Auto**.
- If SL1 is discovering devices but not retrieving the appropriate information, debug the process **Discovery: Detail**.
- If SL1 is not aligning Dynamic Applications with devices during discovery, debug the process **Discovery: Dynamic App**.

**WARNING:** ScienceLogic recommends that you enable the debug option only while troubleshooting a problem and that you immediately turn off debugging when you have completed troubleshooting. Don't leave the debug option enabled during normal operation of SL1. When you turn on debugging, SL1 will run significantly more slowly.

To enable the debug option for a discovery process:

1. Go to the **Process Manager** page (System > Settings > Admin Processes).

- In the **Process Manager** page, find the process you want to debug and click its wrench icon (🔧).

Process Name	Process File	Frequency	Runtime	Alerts	Batch	Time	Run	Status	Debug	ID	Edited By	Exit Date
Application & Report Server: Remote diagnostic	em7_httpd_admin	0	--	--	--	--	15	Enabled	Disabled	54	em7admin	2009-05-29 14:06:59
Application & Report Server: Scheduled Report Runner	scheduled_report_run.py	-1	--	25	--	15	15	Enabled	Disabled	58	em7admin	2009-07-14 12:20:00
Application & Report Server: Secure	em7_httpsd	0	--	--	--	--	--	Enabled	Disabled	53	em7admin	2009-05-29 14:06:59
Application & Report Server: Standard	em7_httpd	0	--	--	--	--	--	Enabled	Disabled	52	em7admin	2009-05-29 14:06:59
Data Collection: Async Dynamic App Collection	async_dynamic_collect.py	-1	--	2	--	15	15	Enabled	Disabled	129	em7admin	2010-03-04 11:53:41
Data Collection: Availability	availability_collect.py	5	2	--	30	5	30	Enabled	Disabled	10	em7admin	2009-05-29 14:06:59
Data Collection: COP Collection	cop_collect.py	120	0	--	30	0	120	Enabled	Disabled	53	em7admin	2010-03-08 10:37:39
Data Collection: Critical Availability	em7_cavald	0	--	--	--	--	--	Enabled	Disabled	47	em7admin	2009-05-29 14:06:59
Data Collection: Critical Port	em7_portc	0	--	--	--	--	--	Enabled	Disabled	48	em7admin	2009-05-29 14:06:59
Data Collection: DNS Policy Monitoring	dns_collect.py	5	2	--	30	5	30	Enabled	Disabled	29	em7admin	2009-05-29 14:06:59
Data Collection: Dynamic App	dynamic_collect.py	1	0	--	20	15	16	Enabled	Enabled	11	em7admin	2012-04-09 17:19:55
Data Collection: Dynamic Refresh	dynamic_check.py	1440	200	--	30	0	1440	Enabled	Disabled	28	em7admin	2009-05-29 14:06:59
Data Collection: Email RoundTrip	email_collect.py	5	0	--	30	0	5	Enabled	Disabled	30	em7admin	2009-05-29 14:06:59
Data Collection: Filesystem statistics	filesystem_stats_collect.py	5	0	--	30	0	5	Enabled	Disabled	32	em7admin	2009-05-29 14:06:59
Data Collection: Host Filesystem Inventory	filesystem_inventory_collect.py	120	44	--	30	0	120	Enabled	Disabled	31	em7admin	2009-05-29 14:06:59
Data Collection: Interface Bandwidth	if_collect.py	1	0	--	10	11	11	Enabled	Disabled	12	em7admin	2009-05-29 14:06:59
Data Collection: L3 Topology Collection	l3_topology_collect.py	120	90	--	30	1	240	Enabled	Disabled	34	em7admin	2010-03-26 10:37:39
Data Collection: OS Process	process_collect.py	120	0	--	20	0	120	Enabled	Disabled	14	em7admin	2009-05-29 14:06:59
Data Collection: OS Process Check	process_check.py	5	4	--	20	2	15	Enabled	Disabled	16	em7admin	2009-05-29 14:06:59
Data Collection: OS Service	service_collect.py	120	20	--	20	0	120	Enabled	Disabled	16	em7admin	2009-05-29 14:06:59
Data Collection: OS Service Check	service_check.py	5	0	--	20	2	15	Enabled	Disabled	17	em7admin	2009-05-29 14:06:59
Data Collection: RSS Event Feed	rss_collect.py	10	0	--	30	0	10	Enabled	Disabled	23	em7admin	2009-05-29 14:06:59
Data Collection: SNMP Detail	snmp_detail_collect.py	5	0	--	30	0	5	Enabled	Disabled	24	em7admin	2009-05-29 14:06:59
Data Collection: TCP Port Monitor	port_collect.py	5	0	--	30	0	5	Enabled	Disabled	20	em7admin	2009-05-29 14:06:59
Data Collection: Topology	topology_collect.py	60	12	--	30	0	60	Enabled	Disabled	25	em7admin	2009-05-29 14:06:59
Data Collection: Virtual Topology	vm_topology_collect.py	60	42	--	30	0	60	Enabled	Disabled	26	em7admin	2009-05-29 14:06:59
Data Collection: Web Content Verifier	content_verification_collect.py	5	1	--	30	0	5	Enabled	Disabled	18	em7admin	2009-05-29 14:06:59
Data Collection: Web Transaction Verifier	transaction_verification_collect.py	5	0	--	30	0	5	Enabled	Disabled	19	em7admin	2009-05-29 14:06:59
Discovery: Auto	discover_brainage.py	-1	--	2	--	360	360	Enabled	Disabled	133	em7admin	2009-05-29 14:06:59
Discovery: Detail	discover_detail.py	-1	--	5	--	60	60	Enabled	Disabled	130	em7admin	2009-05-29 14:06:59
Discovery: Dynamic App	discover_app.py	-1	--	2	--	360	360	Enabled	Disabled	131	em7admin	2009-05-29 14:06:59
Discovery: Nightly Update	discover_update.py	1440	0	--	30	0	1440	Enabled	Enabled	90	em7admin	2012-03-05 12:46:28
PEM7 Core: Async Device Deletion	maint_delete_device.py	-1	--	2	--	5	5	Enabled	Disabled	135	em7admin	2009-05-29 14:06:59
PEM7 Core: Async Maintenance	async_maint.py	-1	--	2	--	10	10	Enabled	Disabled	140	em7admin	2010-10-14 13:32:54

- The **Process Editor** modal page appears.

- Edit the following field:
  - Debug Mode**. Enables or disables debugging information for a process. Select *Enabled*.

**Process Editor | Editing Process [54]** Reset Guide

Process Name: Application & Report Server: Remote diagnostic

Program File: em7\_httpd\_admin

Operating State: [Enabled]

Frequency: [Always]

Appliance Types:

- All-In-One Server [1]
- Database [2]
- Administration Portal [3]
- Customer Portal [4]
- Data Collection Unit [5]
- Message Collection Unit [6]
- Integration Server [7]

Debug Mode: [Disabled] (selected), [Disabled], Enabled

Save

- Click the **[Reset]** button.
- Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery) and **run the discovery session again**.
- Log in to the console of the SL1 appliance where the process is running. Alternately, you can use SSH to open a shell session on the SL1 appliance. In most cases, you will log in as "root".
  - If you are using a SL1 system, log in to the current SL1 appliance.
  - If you are using a distributed SL1 system, log in to the Data Collector associated with the discovery session.

**NOTE:** For details on enabling and using SSH with SL1, information about root access, and instructions on making root access secure, see the manual **Security**.

**TIP:** To view a list of IP addresses for all SL1 appliances in your network, go to the **Appliance Manager** page (System > Settings > Appliances).

8. Navigate to the directory `/data/logs`. View the file `silosilo.log`. The most recent entries will be posted at the end of the file.
9. After you have finished troubleshooting the process, remember to disable debugging.

## Checking Communication between Data Collectors and the Database Server

For distributed SL1 systems, discovery can fail if the Data Collectors and the Database Server cannot communicate with each other.

To check communication between the Database Server and a Data Collector:

1. Log in to the console of the SL1 appliance where the process is running. Alternately, you can use SSH to open a shell session on the SL1 appliance. Log in as **em7admin**.
  - If you are using a SL1 system, log in to the current SL1 appliance.
  - If you are using a distributed SL1 system, log in to the Database Server.

**TIP:** To view a list of IP addresses for all SL1 appliances in your network, go to the **Appliance Manager** page (System > Settings > Appliances).

**NOTE:** For details on enabling and using SSH, see the manual **Security**.

2. From the command line, enter the following:

```
silosilo_mysql -P 7707 -h <IP address of the Data Collection Server associated with  
the discovery session> -u root -p
```

You will be prompted to enter the MySQL root password.

3. If you can successfully execute this command from the Database Server, this means that the Database Server is successfully communicating with the Data Collector.

4. If you cannot successfully execute this command from the Database Server:

- Go to the **Appliance Manager** page (System > Settings > Appliances) and ensure that the settings for the Database Server and the Data Collector server are correct.
- Ensure that a network firewall is not preventing the Database Server and the Data Collector from communicating with each other.
- Log in to the console of the Data Collector. Alternately, you can use SSH to open a shell session on the Data Collector. Log in as **em7admin**. To ensure that MySQL is running on the Data Collector, enter the following at the command line:

```
siilo_mysqladmin -u root -p status
```

You will be prompted for the password.

- If the database is running, the command will return statistics about the database.
- If the database is not running, the command will return an error message. To restart the database, enter the following at the command line:

```
sudo service em7_db_start
```

---

## How File Systems are Hidden During Discovery

When you hide a file system, SL1 stops collecting information about the file system. When you hide a file system:

- SL1 does not generate events about the file system.
- SL1 does not monitor the file system for thresholds (defined in the **Device Thresholds** and **Global Threshold Settings** pages).
- SL1 does not include the file system in the **Device Summary** page.
- SL1 does not include the file system in file system reports in the **Device Performance** page.

The following rules are applied during discovery to automatically hide file systems:

- If the **NFS Detection Disable** checkbox is selected in the **Behavior Settings** page (System > Settings > Behavior), NFS file systems are automatically hidden during discovery.
- File systems of type "iso9660" are automatically hidden during discovery.
- File systems for which the storage size is not reported or the storage size is less than 1024 KB are automatically hidden during discovery.
- File systems of type "Other" are automatically hidden during discovery.



**NOTE:** If the type of a discovered file system changes, the auto-hide rules are re-applied to that file system. For example, suppose a Windows drive letter is initially discovered as a removable disk and auto-hidden. If that drive-letter is later re-used for a fixed drive, this change will cause the file system to be automatically un-hidden.

To manually hide one or more file systems:

1. Go to the **Device Hardware** page (Devices > Hardware).
2. Filter the list to display only **Comp Type** of "file system".
3. Select the checkbox for one or more file systems you would like to hide.
4. From the **Select Actions** field (in the lower right), select *Hide File Systems*.
5. Click the **[Go]** button.
6. Each selected file system will be hidden in SL1.

To manually unhide one or more file systems:

1. Go to the **Device Hardware** page (Devices > Hardware).
2. Filter the list to display only **Comp Type** of "file system".
3. Select the checkbox for one or more file systems you would like to unhide.
4. From the **Select Actions** field (in the lower right), select *Unhide File Systems*.
5. Click the **[Go]** button.
6. SL1 will resume collection for each selected file system and will include each selected file system in the **Device Summary** and **Device Performance** pages.

---

# Chapter

# 4



# Collection

---

## Overview

This chapter describes collection and collection processes in SL1.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ().
- To view a page containing all of the menu options, click the Advanced menu icon (.

This chapter includes the following topics:

<i>What is Collection?</i> .....	104
<i>Collection Processes</i> .....	104

---

## What is Collection?

**Collection** is the tool that retrieves policy-based information and Dynamic Application-based information from a device. After a device is discovered, you can define monitoring policies for that device in SL1. For example, if you define a policy to monitor a system process, the collection tool retrieves that information.

- Dynamic Applications use collection processes to collect data.
- Monitoring Policies for devices also trigger collection. These policies include:
  - Domain Name Policies
  - Email Round-Trip policies
  - SOAP/XML Transaction policies
  - System Process Policies
  - TCP/IP Port Policies
  - Web Content Policies
  - Windows Services Policies
- SL1 automatically collects the following about each managed device:
  - Device availability and device latency
  - Network topology
  - File system information, if available
  - A list of open ports
  - Bandwidth usage
- The SL1 agent automatically collects the following about each device on which it is installed:
  - Device availability
  - Device performance and configuration metrics
  - A list of open ports
  - Log information
  - System processes

---

## Collection Processes

Unlike discovery, collection tasks run at scheduled intervals throughout the day. Collection tasks collect the types of data described below. The interval specified is the default interval and can be modified.

- Device availability and device latency (based on the port through which SL1 communicates), every five minutes.

- CDP relationships between devices, every two hours.
- LLDP relationships between devices, every two hours.
- Critical device availability (if enabled, based on ping to specified port), every 5 seconds, 30 seconds, 60 seconds or 120 seconds (defined by user).
- Critical port availability (if enabled, based on ping to specified port), every 5 seconds, 30 seconds, 60 seconds or 120 seconds (defined by user).
- DNS availability based on DNS-monitoring policies, every five minutes.
- Data specified in Dynamic Applications. Collection tasks retrieve data from each aligned device, at the frequency specified in the Dynamic Application.
- Email round-trip statistics based on Email-monitoring policies, every five minutes.
- File system information, every five minutes.
- File system inventory, every two hours.
- Bandwidth usage on managed interfaces, every minute, 5 minutes, 10 minutes, 15 minutes, 30 minutes, 60 minutes, or 120 minutes (defined by user).
- Layer-3 relationships between devices, every two hours.
- List of all discovered system processes on all discovered devices, every two hours.
- Availability of system processes based on process-monitoring policies, every five minutes.
- List of all discovered Windows services on all discovered devices, every two hours.
- Availability of Windows services based on service-monitoring policies, every five minutes.
- Events for inclusion in RSS feed, every 10 minutes.
- SNMP details for each discovered device, every five minutes.
- Availability of ports based on port-monitoring policies, every five minutes.
- Layer-2 relationships between devices, every hour.
- Virtual machine relationships between devices, every hour.
- Availability of web content based on web content-monitoring policies, every five minutes.
- Web-transaction statistics based on a SOAP/XML-monitoring policy, every five minutes.
- If the SL1 agent is installed, SL1 collects a list of all processes running on a device, every five minutes.

For details on collection processes, go to the **Process Manager** page (System > Settings > Admin Processes) and look for processes with names that start with "Data Collection".

## Managing Credential Tests



---

### Overview

Credential Tests define a series of steps that SL1 can execute on-demand to validate whether a credential works as expected. This chapter describes how to manage existing credential tests and create new credential tests. For information about executing a credential test, see the [Credentials](#) chapter.

Credential Tests can be included in PowerPacks. For information about including a credential test in a PowerPack, see the [PowerPacks](#) manual.

Use the following menu options to navigate the SL1 user interface:

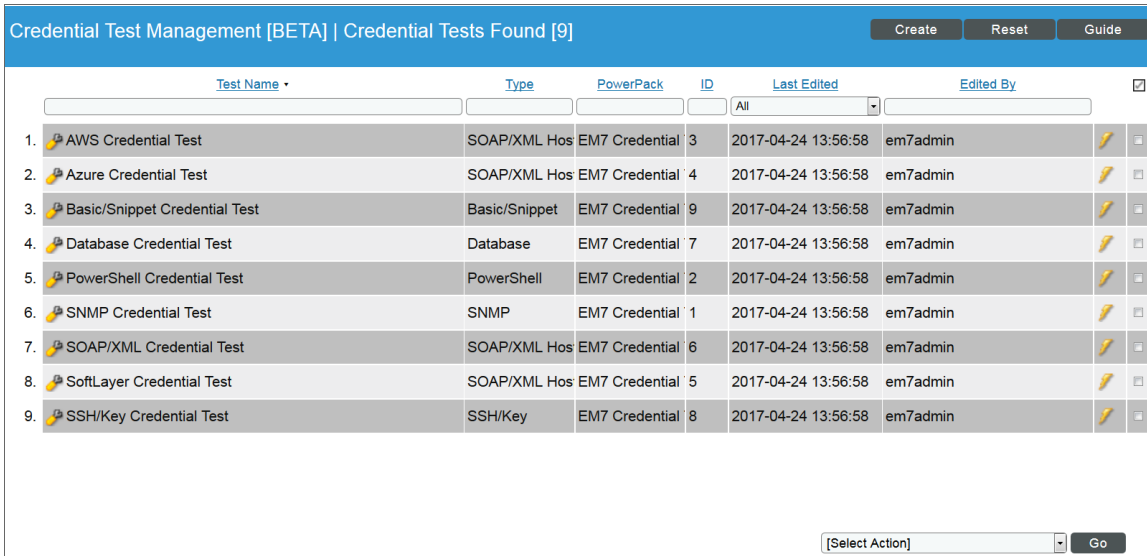
- To view a pop-out list of menu options, click the menu icon (.
- To view a page containing all of the menu options, click the Advanced menu icon (.

This chapter includes the following topics:

<a href="#">Viewing Information About Credential Tests</a> .....	107
<a href="#">Running a Credential Test from the Credential Test Management Page</a> .....	109
<a href="#">Creating a Credential Test</a> .....	110
<a href="#">Editing a Credential Test</a> .....	112
<a href="#">Deleting Credential Tests</a> .....	112
<a href="#">Available Step Functions</a> .....	112



















## Viewing Information About Credential Tests

The **Credential Test Management** page allows you to view a list of all credential tests. From this page, you can also create, edit, run, and delete credential tests.



Credential Test Management [BETA] | Credentials Tests Found [9]

Create Reset Guide

Test Name	Type	PowerPack	ID	Last Edited	Edited By	
1. AWS Credential Test	SOAP/XML Hos	EM7 Credential	3	2017-04-24 13:56:58	em7admin	 
2. Azure Credential Test	SOAP/XML Hos	EM7 Credential	4	2017-04-24 13:56:58	em7admin	 
3. Basic/Snippet Credential Test	Basic/Snippet	EM7 Credential	9	2017-04-24 13:56:58	em7admin	 
4. Database Credential Test	Database	EM7 Credential	7	2017-04-24 13:56:58	em7admin	 
5. PowerShell Credential Test	PowerShell	EM7 Credential	2	2017-04-24 13:56:58	em7admin	 
6. SNMP Credential Test	SNMP	EM7 Credential	1	2017-04-24 13:56:58	em7admin	 
7. SOAP/XML Credential Test	SOAP/XML Hos	EM7 Credential	6	2017-04-24 13:56:58	em7admin	 
8. SoftLayer Credential Test	SOAP/XML Hos	EM7 Credential	5	2017-04-24 13:56:58	em7admin	 
9. SSH/Key Credential Test	SSH/Key	EM7 Credential	8	2017-04-24 13:56:58	em7admin	 

[Select Action] Go

**TIP:** To sort the list of credential tests, click on a column heading. The list will be sorted by the column value, in ascending order. To sort by descending order, click the column heading again. The **Last Edited** column sorts by descending order on the first click; to sort by ascending order, click the column heading again.

For each credential test, the page displays:

- **Test Name.** Name of the credential test.
- **Type.** The type of credential that can be tested using this credential test. Possible types are SNMP, Database, SOAP/XML, LDAP/AD, Basic/Snippet, SSH/Key, and Powershell.
- **PowerPack.** The PowerPack that contains the credential test.
- **ID.** Unique numeric ID, automatically assigned by SL1 to each credential test.
- **Last Edited.** Date and time the credential test was created or last edited.
- **Edited By.** The username of the user who created or last edited the credential test.

## Filtering the List of Credential Tests

To filter the list of credentials in the **Credential Test Management** page, use the search fields at the top of each column. The search fields are find-as-you-type filters; as you type, the page is filtered to match the text in the search field, including partial matches. Text matches are not case-sensitive. Additionally, you can use the following special characters in each filter:

- , (comma). Specifies an "or" operation. For example:  
"dell, micro" would match all values that contain the string "dell" OR the string "micro".
- & (ampersand). Specifies an "and" operation. For example:  
"dell & micro" would match all values that contain the string "dell" AND the string "micro".
- ! (exclamation mark). Specifies a "not" operation. For example:  
"!dell" would match all values that do not contain the string "dell".
- ^ (caret mark). Specifies "starts with." For example:  
"^ micro" would match all strings that start with "micro", like "microsoft".  
"^" will include all rows that have a value in the column.  
"!^" will include all rows that have no value in the column.
- \$ (dollar sign). Specifies "ends with." For example:  
"\$ware" would match all strings that end with "ware", like "VMware".  
"\$" will include all rows that have a value in the column.  
"!\$" will include all rows that have no value in the column.
- min-max. Matches numeric values only. Specifies any value between the minimum value and the maximum value, including the minimum and the maximum. For example:  
"1-5" would match 1, 2, 3, 4, and 5.
- - (dash). Matches numeric values only. A "half open" range. Specifies values including the minimum and greater or including the maximum and lesser. For example:  
"1-" matches 1 and greater, so it would match 1, 2, 6, 345, etc.  
"-5" matches 5 and less, so it would match 5, 3, 1, 0, etc.
- > (greater than). Matches numeric values only. Specifies any value "greater than." For example:  
">7" would match all values greater than 7.

- < (less than). Matches numeric values only. Specifies any value "less than." For example:  
" < 12 " would match all values less than 12.
- >= (greater than or equal to). Matches numeric values only. Specifies any value "greater than or equal to." For example:  
" = > 7 " would match all values 7 and greater.
- <= (less than or equal to). Matches numeric values only. Specifies any value "less than or equal to." For example:  
" = < 12 " would match all values 12 and less.
- = (equal). Matches numeric values only. For numeric values, allows you to match a negative value. For example:  
" = -5 " would match "-5" instead of being evaluated as the "half open range" as described above.

---

## Running a Credential Test from the Credential Test Management Page

The **Credential Test Management** page allows you to run a credential test to validate that a credential works as expected. To do so:

1. Go to the **Credential Test Management** page (System > Customize > Credential Tests).
2. Find the credential test that you want to run and click its lightning bolt icon (⚡). The **Credential Tester** modal page appears:

3. Supply values in the following fields:
  - **Test Type**. This field is pre-populated with the credential test you selected.
  - **Credential**. Select the credential to test. This drop-down list includes only credentials that you have access to that can be tested using the selected credential test.
  - **Hostname/IP**. Enter a hostname or IP address that will be used during the test. For example, if you are testing an SNMP credential, the hostname/IP address you supply will be used to perform a test SNMP request.



- **Collector**. Select which All-In-One Appliance or Data Collector will run the test from the drop-down list.
4. Click the **[Run Test]** button to run the credential test. The **Test Credential** window appears:

Step	Description	Log Message	Status
1 Test Reachability	Check to see if the device is reachable using ICMP	The device is reachable using ICMP. The average response time is 0.397ms	Passed
2 Test Port Availability	Check to see if the SNMP port is open	Port 161 is open	Passed
3 Test SNMP Availability	Check to see if a walk of SNMP will return results	The SNMP SysName is ScienceLogic EM7 G3 - All-In-One	Passed

The **Test Credential** window displays a log entry for each step in the credential test. The steps performed are different for each credential test. The log entry for each step includes the following information:

- **Step**. The name of the step.
  - **Description**. A description of the action performed during the step.
  - **Log Message**. The result of the step for this execution of the credential test.
  - **Status**. Whether the result of this step indicates the credential and/or the network environment is configured correctly (Passed) or incorrectly (Failed).
  - **Step Tip**. Mouse over the question mark icon (?) to display the tip text. The tip text recommends what to do to change the credential and/or the network environment if the step has a status of "Failed".
5. Optionally, you can click the **[Execute Discovery Session]** button to run a discovery session using the **Credential**, **Hostname/IP**, and **Collector** you selected in the **Credential Tester** modal page.

## Creating a Credential Test

The **Credential Test Management** page allows you to create a new credential test. To do so:

1. Go to the **Credential Test Management** page (System > Customize > Credential Tests).
2. Click the **[Create]** button. The **Add Credential Test** modal page appears:

3. Supply values in the following fields:

- **Test Name.** Enter a name for the credential test.
- **Credential Type.** Select the type of credential that can be used with this test. Possible types are *SNMP, Database, SOAP/XML, LDAP/AD, Basic/Snippet, SSH/Key, and PowerShell.*
- **Execution Environment.** Select the execution environment to which you want to align the credential test. An execution environment contains the supporting modules, code, scripts, directories, and files (packaged in ScienceLogic Libraries) for the credential test. An execution environment includes its own installation directories, doesn't share libraries with other environments, and allows granular control of dependencies, versions, and permissions. The default execution environment is "EM7 Credential Tests". For more information, see the **ScienceLogic Libraries** manual.
- **Steps.** Enter the JSON structure that defines how each step in the credential test will be executed. The JSON structure must specify an array (square-bracket notation) of objects (curly-braces notation). Each object in the list defines a step to be executed by the credential test. The object for a step must include the following keys:
  - *name.* The name of the step. This text will be displayed in the **Step** column in the credential test results.
  - *description.* A description of the step. This text will be displayed in the **Description** column in the credential test results.
  - *pass\_message.* The log message to display when the success criteria of the specified *function* are met. To use the output from a function in the log message, you can include substitutions in this field.
  - *fail\_message.* The log message to display when the success criteria of the specified *function* are not met. To use the output from a function in the log message, you can include substitutions in this field.
  - *step\_tip.* Information for the user to troubleshoot their credential if this step fails. This text will be displayed if the user hovers over the information icon (📘) in the credential test results.
  - *function.* The name of the function that will be called by SL1 to execute the step. For a list of available functions, see the [Available Step Functions](#) section.

For step functions that accept additional arguments, add an additional key/value pair in the object for that step to specify additional arguments.

The *pass\_message* and *fail\_message* can include substitutions. Substitutions are specified using the following format:

```
%( [Return Value Name] )s
```

Where *[Return Value Name]* is the name of the return value you want to substitute in to the *pass\_message* and *fail\_message*. For example, the ping function returns the latency in milliseconds in the variable "result". Suppose your step uses the ping function with the following *pass\_message*:

```
Latency is %(result)s ms
```

Suppose that when a user runs the credential test, the ping function returns "10" in the variable "result". The following log message is displayed to the user:


```
Latency is 10 ms
```

4. Click the **[Save]** button to save your changes to the credential test.

---

## Editing a Credential Test

The **Credential Test Management** page allows you to edit an existing credential test. To do so:

1. Go to the **Credential Test Management** page (System > Customize > Credential Tests).
2. Find the credential test that you want to edit and click its wrench icon (). The **Edit\_Credential\_Test** modal page appears.
3. Edit one or more parameters for the credential test. For a description of each field, see the [Creating a Credential Test](#) section.
4. Click the **[Save]** button to save your changes to the credential test.

---

## Deleting Credential Tests

The **Credential Test Management** page allows you to delete one or more credential tests from SL1. To do so:

1. Go to the **Credential Test Management** page (System > Customize > Credential Tests).
2. Select the checkbox for each credential test you want to delete.
3. Click the **Select Actions** menu (in the lower right) and select *DELETE Credential Test*, then click the **[Go]** button.
4. In the pop-up window that appears, click **[OK]**. The selected credential tests will be deleted.

5

---

## Available Step Functions

### ping

This function executes the following ping command using the provided IP address or hostname:

```
sudo /bin/ping -c1 [IP address/Hostname]
```

- **Success/Failure Criteria.** Successful if a response is received.
- **Arguments.** None.
- **Return values on success:**

- *success*. Returns True.
- *result*. Returns the response time, in ms.

- **Return values on failure:**

- *success*. Returns False.

## nmap\_udp

This function executes the following nmap command using the provided IP address or hostname and the port in the provided credential:

```
sudo /usr/bin/nmap -sU -p [port] [IP address/Hostname]
```

- **Success/Failure Criteria**. Successful if the NMAP command returns "open" or "open | filtered" as the state of the port.
- **Arguments**. None.
- **Return values on success:**
  - *port*. Returns the port number from the credential.
  - *success*. Returns True.
  - *result*. Returns the state of the port from the NMAP output.
- **Return values on failure:**
  - *port*. Returns the port number from the credential or "Undefined" if no port is specified in the credential.
  - *success*. Returns False.
  - *result*. Returns the state of the port from the NMAP output.

## nmap\_tcp

This function executes the following nmap command using the provided IP address or hostname and the port in the provided credential:

```
sudo /usr/bin/nmap -P0 -p [port] [IP address/Hostname]
```

- **Success/Failure Criteria**. Successful if the NMAP command returns "open" or "open | filtered" as the state of the port.
- **Arguments**. None.
- **Return values on success:**
  - *port*. Returns the port number from the credential.
  - *success*. Returns True.
  - *result*. Returns the state of the port from the NMAP output.
- **Return values on failure:**

- *port*. Returns the port number from the credential or "Undefined" if no port is specified in the credential.
- *success*. Returns False.
- *result*. Returns the state of the port from the NMAP output.

## nslookup\_forward

This function executes the nslookup command-line utility using the provided hostname.

- **Success/Failure Criteria**. Successful if the forward lookup returns one or more results.
- **Arguments**. None.
- **Return values on success**:
  - *success*. Returns True.
  - *result*. Returns a string in the following format: Forward returned *[number]* result[s]
- **Return values on failure**:
  - *success*. Returns False.
  - *result*. Returns "Forward Failed".

## nslookup

If the user provides a hostname, this function:

1. Executes the nslookup command-line utility using the provided hostname.
2. Executes the nslookup command-line utility using the IP address returned by the first nslookup command.

If the user provides an IP address, this function:

1. Executes the nslookup command-line utility using the provided IP address.
2. Executes the nslookup command-line utility using the hostname returned by the first nslookup command.

- **Success/Failure Criteria**. Successful if both the forward and reverse lookups return one or more results.
- **Arguments**. None.
- **Return values on success**:
  - *success*. Returns True.
  - *result*. Returns a string in the following format: *[direction]* returned *[number]* result[s], *[direction]* returned *[number]* result[s]
- **Return values on failure**:
  - *success*. Returns False.
  - *result*. Returns a string in one of the following formats:

- *[direction]* failed, *[direction]* returned *[number]* result[s]
- *[direction]* returned *[number]* result[s], *[direction]* failed
- *[direction]* failed, *[direction]* failed

## dynapp\_execute

This function performs collection of a specified Dynamic Application using the credential and IP/hostname provided by the user.

- **Success/Failure Criteria.** Successful if Dynamic Application collection is successful.
- **Arguments.** One of the following arguments is required. If both are specified, only `app_id` is used:
  - `app_id`. Integer. The ID of the Dynamic Application to execute.
  - `app_guid`. String. The GUID of the Dynamic Application to execute.
- **Return values on success:**
  - `success`. Returns True.
- **Return values on failure:**
  - `success`. Returns False.

## snmp\_getnext

This function executes an SNMP getnext request on .1.3.6.1 using the credential and IP/hostname provided by the user. This function works only with SNMP credentials.

- **Success/Failure Criteria.** Successful if a value is returned by the getnext request.
- **Arguments.** None.
- **Return values on success:**
  - `success`. Returns True.
  - `result`. Returns the value returned by the request (typically the System Name).
- **Return values on failure:**
  - `success`. Returns False.

## ssh\_request

This function attempts to make an SSH connection using the following values:

- **The IP address/hostname from the provided Credential.** The host to use for the SSH connection.
- **The SSH Key from the provided SSH/Key Credential.** The private key to use for the SSH connection.
- **The Username from the provided Credential.** The username for the SSH connection.
- **The Password from the provided Credential.** The password for the SSH connection.

- **The Port from the provided Credential.** The port for the SSH connection. If no port is supplied, port 22 is used.
- **The command argument supplied to the function.** The command that is executed using the SSH connection. If the command argument is not supplied, no command is executed.

If the connection is successful and the command argument is supplied to the function, the function executes the command specified in the command argument.

- **Success/Failure Criteria.** If a command is not specified in the arguments, successful if an SSH connection is established. If a command is specified in the arguments, successful if the an SSH connection is established and the command returns an exit code of 0.
- **Arguments.** The following argument is optional:
  - *command.* String. SSH command to execute.
- **Return values on success:**
  - *success.* Returns True.
- **Return values on failure:**
  - *success.* Returns False.
  - *result.* Returns an error message.

## db\_query

This function attempts to make a database connection and execute a query using the credential and IP/hostname provided by the user. This function works only with Database credentials.

- **Success/Failure Criteria.** Successful if the database query returns rows.
- **Arguments.** The following argument is optional:
  - *query.* String. Database query to execute. If no query is supplied, "SELECT 1;" is executed.
- **Return values on success:**
  - *success.* Returns True.
- **Return values on failure:**
  - *success.* Returns False.
  - *result.* Returns an error message.

## curl

This function executes a cURL request using the credential and IP/hostname provided by the user. Optionally, this function can perform an expression match on the returned content. This function works only with SOAP/XML credentials.

- **Success/Failure Criteria.** If match text is not specified in the arguments, successful if the cURL request returns an HTTP status code that does not begin with a 4 or 5. If match text is specified in the arguments, successful if the cURL request returns an HTTP status code that does not begin with a 4 or 5 and the supplied expression match is included in the response.
- **Arguments.** The following argument is optional:
  - *match\_text*. String. Text to match to the response.
- **Return values on success:**
  - *success*. Returns True.
  - *result*. Returns one of the following:
    - If no match text is specified, the string "HTTP [*Status Code*]" is returned.
    - If match text is specified, the string "Match text found" is returned.
- **Return values on failure:**
  - *success*. Returns False.
  - *result*. Returns one of the following:
    - If no match text is specified and the HTTP request returned a 400-series or 500-series status code, the string "HTTP [*Status Code*]" is returned.
    - If match text is specified and the HTTP request was successful, the string "Match text not found" is returned.
    - If an error is encountered executing the cURL request, an error message is returned.

## aws\_connect

Using the boto3 library, this function creates an IAM client object using the following values:

- **Username from the provided credential.** Used as the AWS Access Key ID.
- **Password from the provided credential.** Used as the AWS Secret Access Key.
- **%1 value from the provided SOAP/XML Credential.** Used as the AWS region. If the region is not supplied in the credential, "us-east-1" is used.

After creating the object, the function calls the `get_user()` request using the object.

- **Success/Failure Criteria.** Successful if the `get_user()` request is successful.
- **Arguments.** None
- **Return values on success:**
  - *success*. Returns True.
- **Return values on failure:**
  - *success*. Returns False.
  - *result*. Returns an error message.



## aws\_service\_scan

Using the boto3 library, this function creates an AWS session object using the following values:

- **Username from the provided credential.** Used as the AWS Access Key ID.
- **Password from the provided credential.** Used as the AWS Secret Access Key.
- **%1 value from the provided SOAP/XML Credential.** Used as the AWS region. If the region is not supplied in the credential, "us-east-1" is used.

After creating the object, the function iterates through the list of services specified in the `expected_services` argument. For each `expected_services` argument, the function attempts to connect to the service using the AWS session object.

- **Success/Failure Criteria.** Successful if the connection to every service in the `expected_services` argument was successful.
- **Arguments.** The following argument is required:
  - `expected_services`. Specify a list of service names. The service names must match the possible service names returned by the `get_available_resources()` function for an AWS session object.
- **Return values on success:**
  - `success`. Returns True.
- **Return values on failure:**
  - `success`. Returns False.
  - `result`. Returns one of the following:
    - If a client error occurs creating the AWS session object, returns an error message.
    - If the AWS session object was created successfully, returns the following string: "cannot access the following services: [comma-separated list of failed services]"

## nmap\_aws

This function performs a port scan of port 443 on the URL of a specific AWS service and region. The function uses the following values to build the URL:

- **%1 value from the provided SOAP/XML Credential.** Used as the AWS region. If the region is not supplied in the credential, "us-east-1" is used.
- **The service argument supplied to the function.** Used as the AWS service. If the service argument is not supplied, "ec2" is used.

For services that do not use regions, this function executes the following nmap command:

```
sudo /usr/bin/nmap -P0 -p 443 [service].[region].amazonaws.com
```

For services that use regions, this function executes the following nmap command:

```
sudo /usr/bin/nmap -P0 -p 443 [service].amazonaws.com
```

- **Success/Failure Criteria**. Successful if the NMAP command returns "open" or "open | filtered" as the state of the port.
- **Arguments**. The following argument is optional:
  - *service*. The service to use in the URL. If the service argument is not supplied, "ec2" is used.
- **Return values on success:**
  - *port*. Returns "443".
  - *success*. Returns True.
  - *result*. Returns the state of the port from the NMAP output.
- **Return values on failure:**
  - *port*. Returns "443".
  - *success*. Returns False.
  - *result*. Returns the state of the port from the NMAP output.

## nslookup\_aws

This function executes the nslookup command-line utility URL of a specific AWS service and region. The function uses the following values to build the URL:

- **%1 value form the provided SOAP/XML Credential**. Used as the AWS region. If the region is not supplied in the credential, "us-east-1" is used.
- **The service argument supplied to the function**. Used as the AWS service. If the service argument is not supplied, "ec2" is used.

For services that do not use regions, the URL is in the following format:

```
[service].[region].amazonaws.com
```

For services that use regions, the URL is in the following format:

```
[service].amazonaws.com
```

- **Success/Failure Criteria**. Successful if the forward lookup returns one or more results.
- **Arguments**. The following argument is optional:
  - *service*. The service to use in the URL. If the service argument is not supplied, "ec2" is used.
- **Return values on success:**
  - *success*. Returns True.
  - *result*. Returns a string in the following format: Forward returned *[number]* result[s]
- **Return values on failure:**

- *success*. Returns False.
- *result*. Returns "Forward Failed".

## ping\_aws

This function executes a ping command to the URL of a specific AWS service and region. The function uses the following values to build the URL:

- **%1 value form the provided SOAP/XML Credential**. Used as the AWS region. If the region is not supplied in the credential, "us-east-1" is used.
- **The service argument supplied to the function**. Used as the AWS service. If the service argument is not supplied, "ec2" is used.

For services that do not use regions, the ping command is in the following format:

```
sudo /bin/ping -c1 [service].[region].amazonaws.com
```

For services that use regions, the ping command is in the following format:

```
sudo /bin/ping -c1 [service].amazonaws.com
```

- **Success/Failure Criteria**. Successful if a response is received.
- **Arguments**. The following argument is optional:
  - *service*. The service to use in the URL. If the service argument is not supplied, "ec2" is used.
- **Return values on success:**
  - *success*. Returns True.
  - *result*. Returns the response time, in ms.
- **Return values on failure:**
  - *success*. Returns False.

© 2003 - 2019, ScienceLogic, Inc.

All rights reserved.

#### LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

#### Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

#### Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: [legal@sciencelogic.com](mailto:legal@sciencelogic.com)



800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010