User Management

Dynatrace Training Module

dynatrace

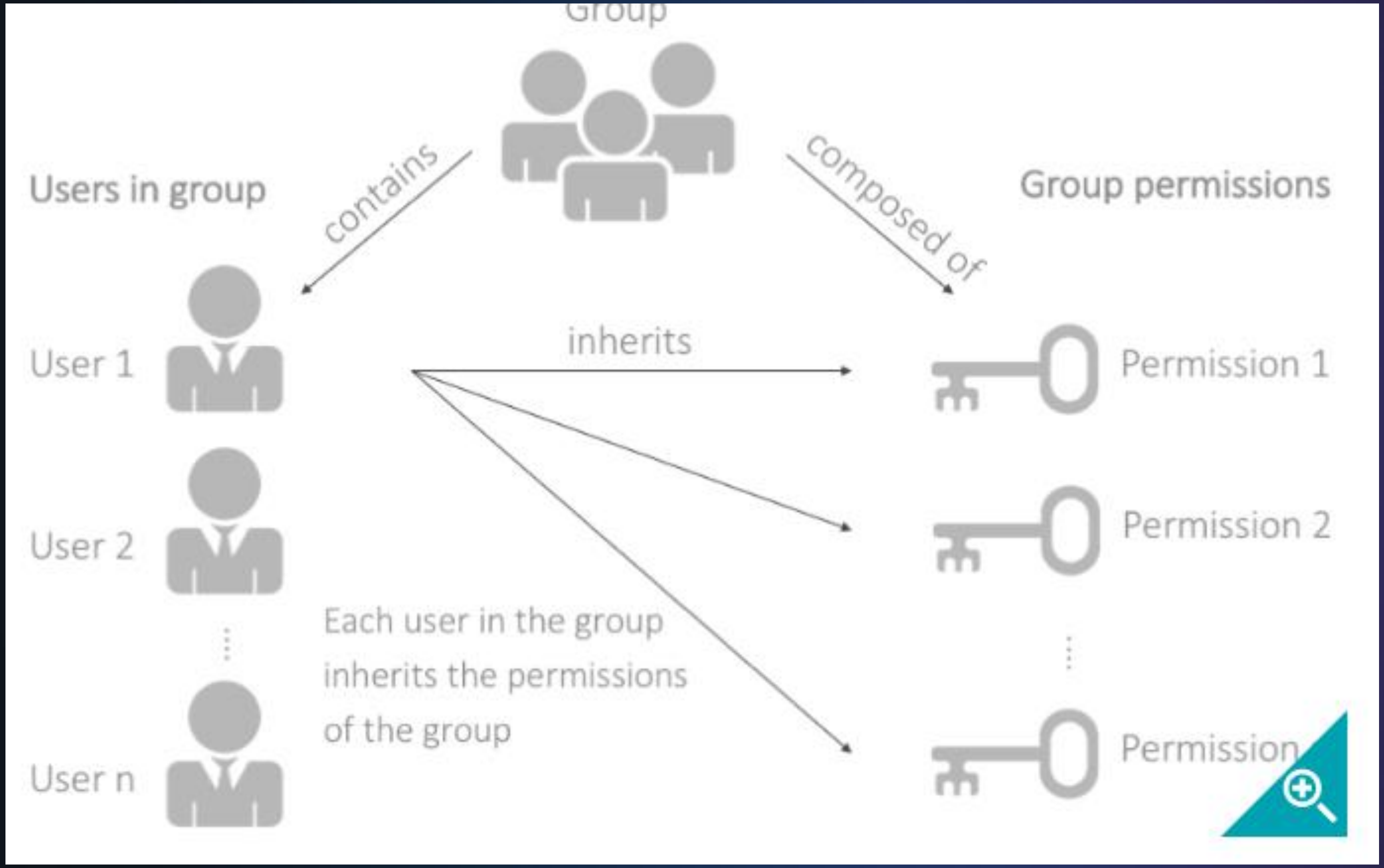
Agenda

- Overview
- Permissions
  - SaaS Specific
  - Managed Specific
  - Environment (SaaS & Managed)
  - Management Zones (SaaS & Managed)
- Managing Groups and Users
  - SaaS
  - Managed

Overview

Overview

- The permission management system is based on groups
  - Reflecting Unix- and Windows-based permissions
- It enables you to create groups that have pre-defined (fully customizable) permissions sets
  - Users added to a group inherit the permissions of that group



Permissions

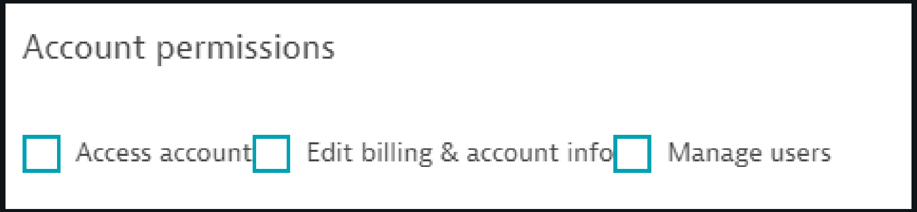
Permissions

- Each user group is assigned a set of permissions.
- Each user account is assigned to one or more user groups.
- Each user assigned to a group inherits the permissions of that group.
- When you change the permissions of a group, the permissions of each user in that group change accordingly.
- When you assign a user to multiple groups, the user inherits the combined permissions of all those groups. Groups are fully customizable and can be modified to contain any permission you require for a specific group
- Even the default groups can be modified to meet your needs

https://www.dynatrace.com/support/help/shortlink/users-sso-hub

SaaS Account Permissions

Account Permissions



Account permissions

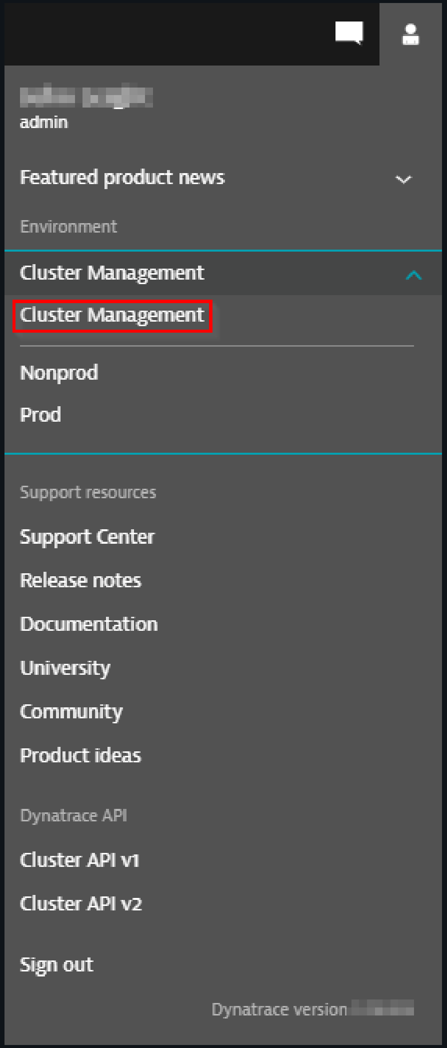
□ Access account □ Edit billing & account info □ Manage users

- Access account
  - Allows access to the account to view environment data (host hours, sessions, synthetic monitors) and Dynatrace Documentation (documentation) links. Also allows access to Dynatrace ONE (to view and create support tickets) and the Dynatrace Community user forum. There is no access to billing or user/group management.
- Edit billing & account info
  - Allows access to payment data (credit card details), billing data (invoices), and contact information (company contact data).
- Manage users
  - Allows access to user management (add, edit, remove users to groups) and group management (create, edit, delete groups)
  - Allows access to identity management to setup SSO (Single Sign-On)

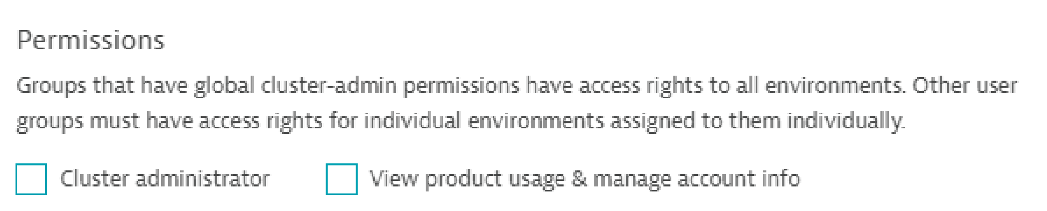
Managed Cluster Permissions

Admin account

- Default administrator account
  - A default administrator account is created during Dynatrace Managed installation.
  - This account exists regardless of the authentication type you select (internal or LDAP).
  - The default administrator account has cluster permissions.



Group Permissions



Permissions

Groups that have global cluster-admin permissions have access rights to all environments. Other user groups must have access rights for individual environments assigned to them individually.

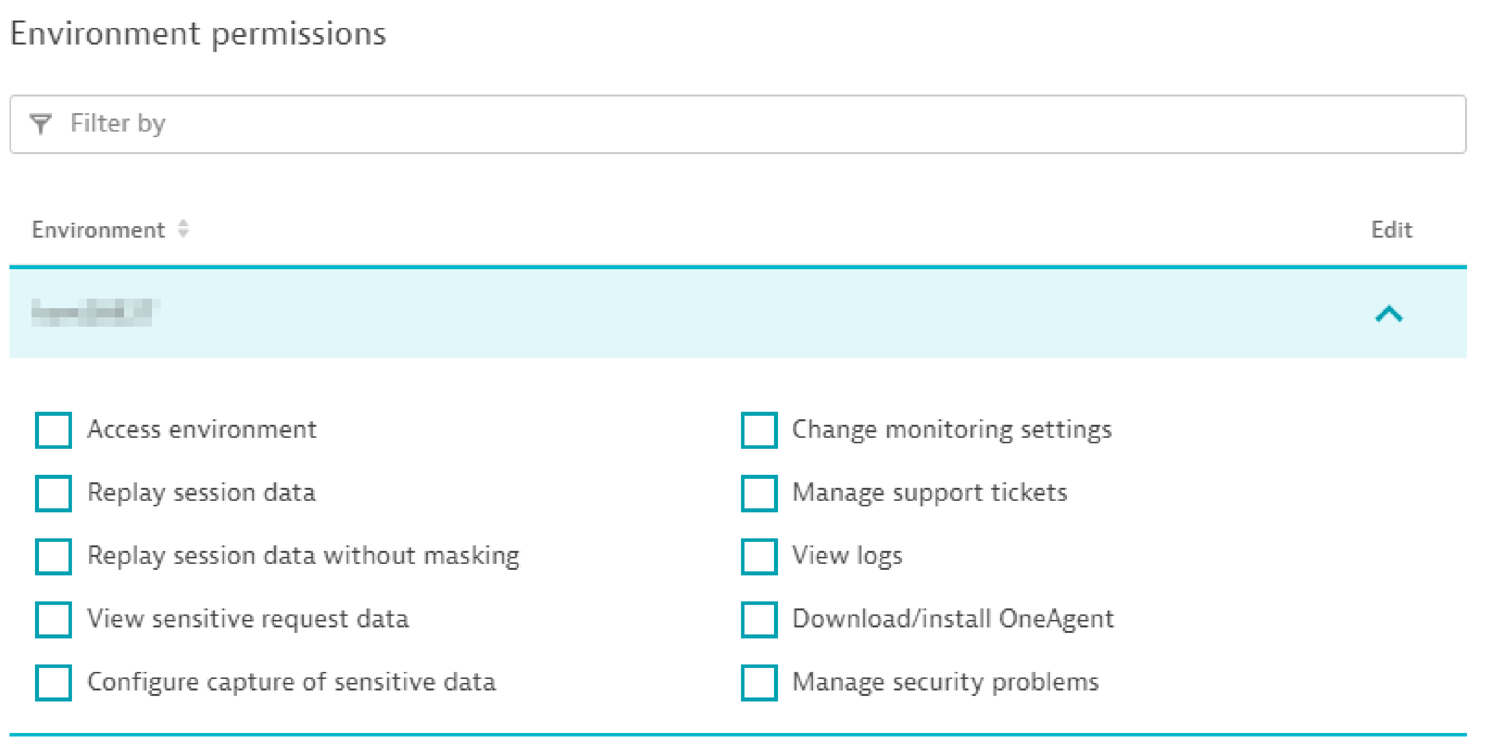
□ Cluster administrator □ View product usage & manage account info

- Cluster administrator
  - Users assigned to groups with this permission are automatically given administrator access rights for all environments. They have access to Cluster Management Console and can manage your monitoring environments and Dynatrace Server
  - Users assigned to groups with this permission can also:
    - Add new Dynatrace Server nodes
    - Upgrade Dynatrace Server
    - Manage Dynatrace Managed users and user groups
    - Install Dynatrace OneAgent into any monitoring environment
    - Configure monitoring settings for any monitoring environment
  - When users that have the **Cluster admin** permission log into Dynatrace Managed, they arrive on the **Cluster Management** Console (CMC) page.
- View Product usage and manage account info
  - Users assigned to groups with this permission can access usage and adoption information (new feature coming - as of 6/22/2021)

Environment Permissions

Environment Permissions

- Environment Permissions
  - https://www.dynatrace.com/support/help/shortlink/user-groups-setup#environment-permissions-



Environment permissions

Filter by

Environment	Edit
[redacted]	

□ Access environment

□ Replay session data

□ Replay session data without masking

□ View sensitive request data

□ Configure capture of sensitive data

□ Change monitoring settings

□ Manage support tickets

□ View logs

□ Download/install OneAgent

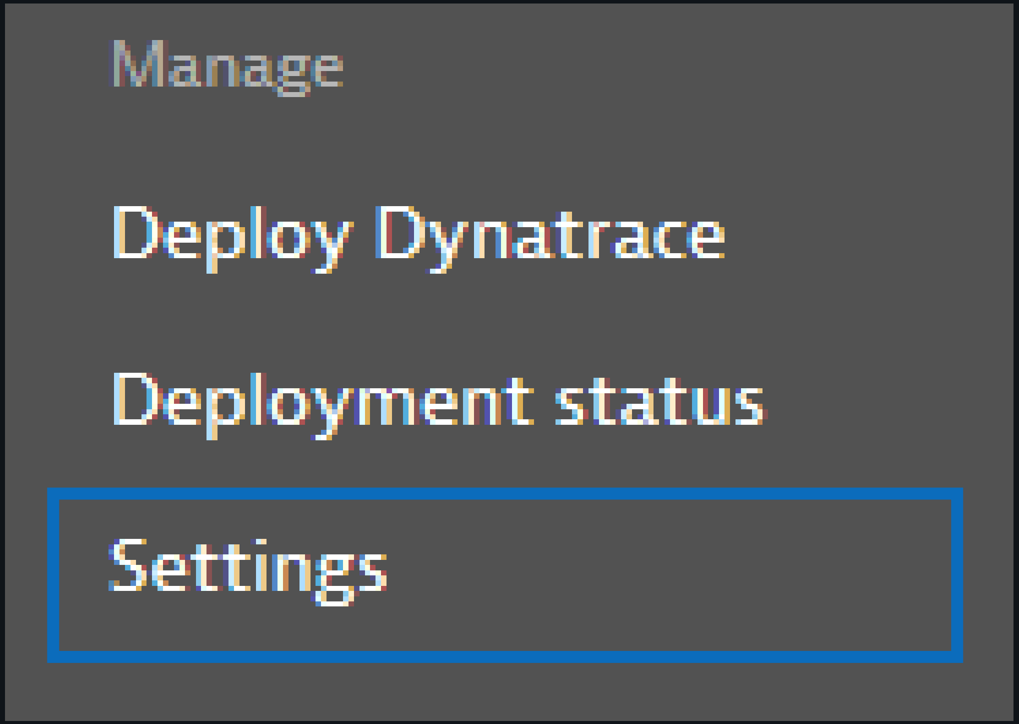
□ Manage security problems

Environment Permissions

- Access Environment
  - Allows read-only access to the environment. Can’t change settings. Can’t install OneAgent
  - The Access Environment Permissions allow the users to do the following:
    - View the monitored data
    - View Dynatrace reports
    - Build, clone, & share dashboards
    - Create custom charts
    - Add/Remove key user actions

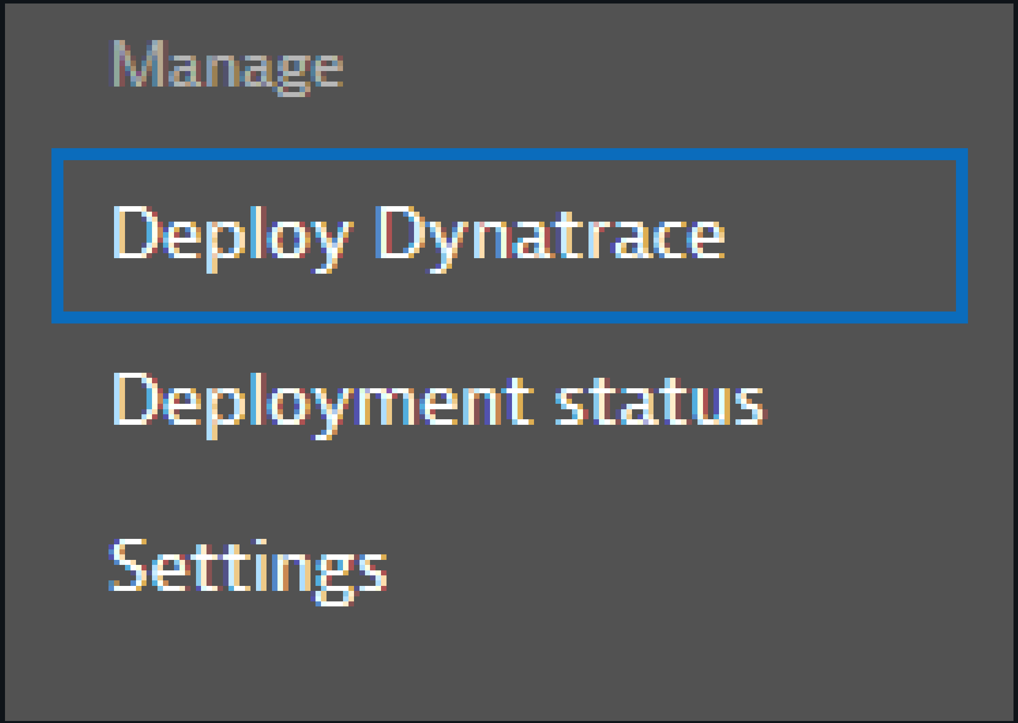
Environment Permissions

- Change monitoring settings
  - Can change all Dynatrace monitoring settings. Can't install OneAgent



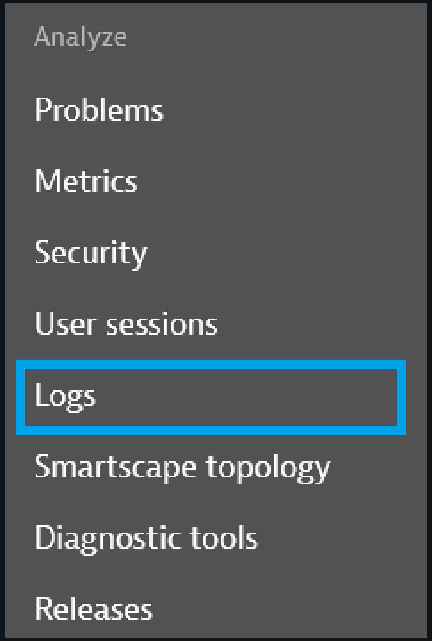
Environment Permissions

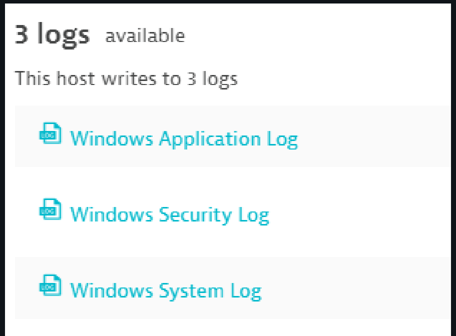
- Download & install OneAgent
  - Allows download and installation of OneAgent on hosts. Can't change Dynatrace monitoring settings



Environment Permissions

- View logs
  - Allows access to log file content, which may contain sensitive information
- Log file data can be masked by the OneAgent prior to being seen in the UI or stored on the Dynatrace Server
  - https://www.dynatrace.com/support/help/shortlink/log-analytics-mask-info#mask-personal-data

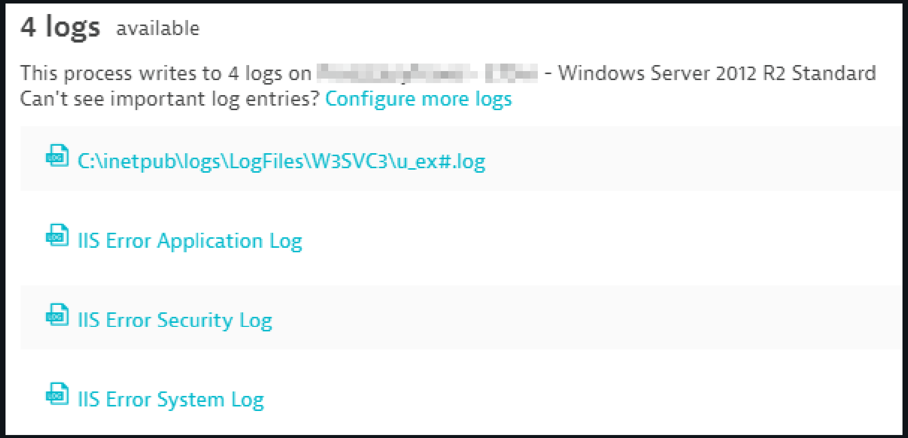




3 logs available

This host writes to 3 logs

- Windows Application Log
- Windows Security Log
- Windows System Log



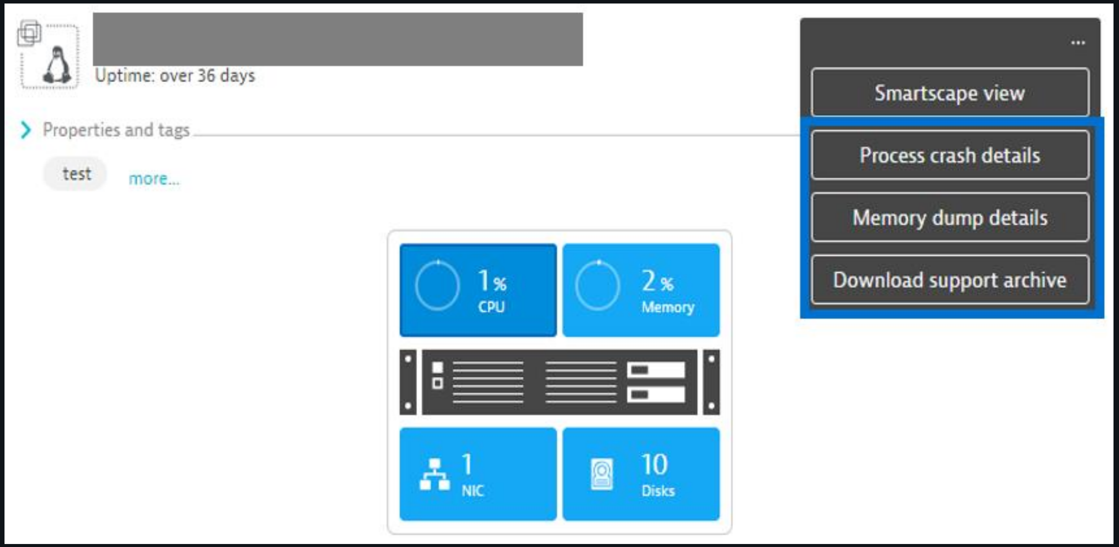
4 logs available

This process writes to 4 logs on [redacted] [redacted] - Windows Server 2012 R2 Standard
Can't see important log entries? Configure more logs

- C:\inetpub\logs\LogFiles\W3SVC3\u_ex#.log
- IIS Error Application Log
- IIS Error Security Log
- IIS Error System Log

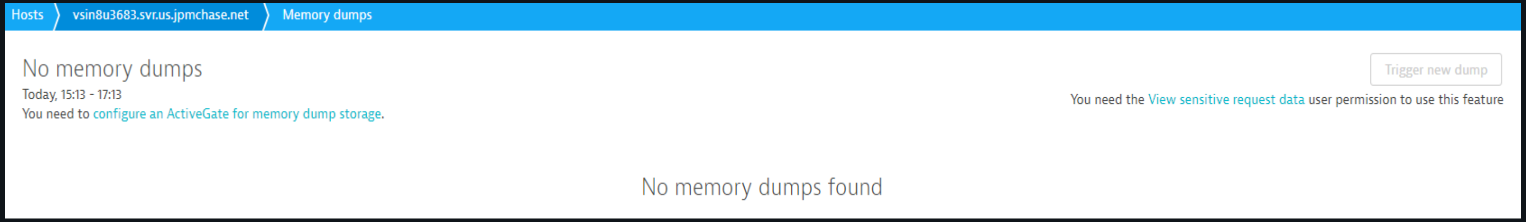
Environment Permissions

- View sensitive request data
  - Allows viewing of potentially sensitive data
  - Users who do not have this permission see that the data point exists, but the personal data is masked by asterisks (*****)
  - See details of what is considered sensitive on next slide



[redacted]

Uptime: over 36 days



No memory dumps

Today, 15:13 - 17:13

You need to configure an ActiveGate for memory dump storage.

You need the View sensitive request data user permission to use this feature

No memory dumps found

Sensitive Data

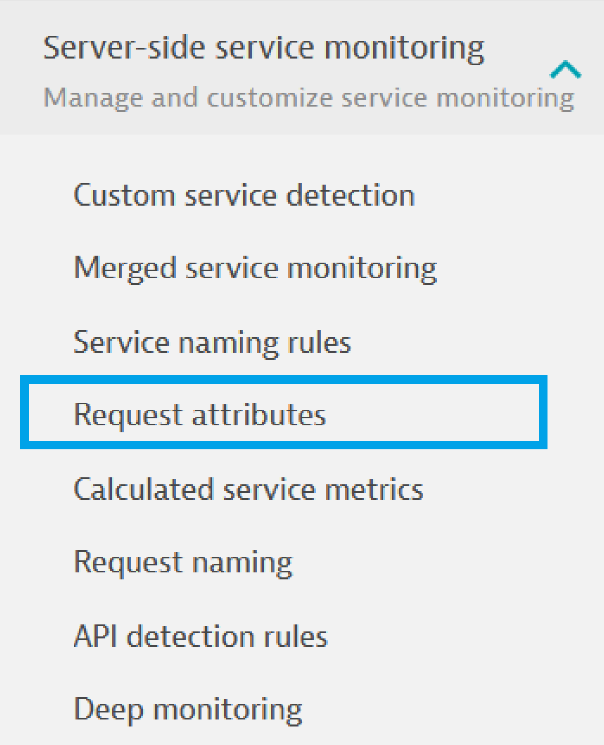
- Dynatrace will automatically classify certain data items as sensitive
- This includes things like client IP addresses, Exception messages, URL query parameters, HTTP Headers/post parameters and extends to certain patterns in exception messages like GUIDs
- Support archives and memory dumps are considered sensitive data
- Users can configure the capture of additional data, which will require the user to have the permission to do so (Configure capture of sensitive data)
  - The User will be able to explicitly designate these newly captured data points as sensitive or non sensitive
- OneAgent diagnostics and memory dumps are also considered sensitive data

  https://www.dynatrace.com/support/help/shortlink/sensitive-data

  https://www.dynatrace.com/support/help/shortlink/section-data-privacy-and-security

Environment Permissions

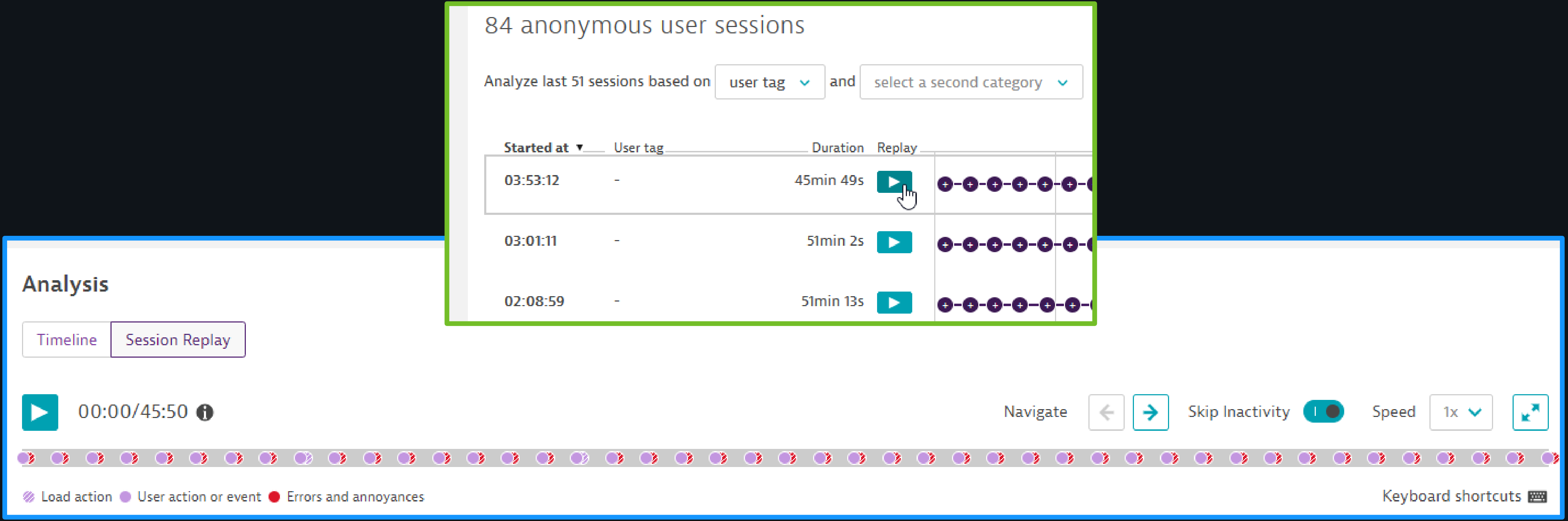
- Configure capture of sensitive data
  - Allows configuration of request-attribute capture rules. These can be used to capture elements such as HTTP headers or Post parameters for storage, filtering, and search.
  - Also allows manually triggering memory dumps. Captured request data can be stored, filtered, and searched



Server-side service monitoring
Manage and customize service monitoring
Custom service detection
Merged service monitoring
Service naming rules
Request attributes
Calculated service metrics
Request naming
API detection rules
Deep monitoring

Environment Permissions

- Replay session data
  - Allows replaying recorded user sessions with playback masking rules applied at the time of *playback*.
    - Note: Any data masked at time of *recording* is never captured, therefore, always masked during play.



84 anonymous user sessions

Analyze last 51 sessions based on user tag and select a second category

Started at ▼	User tag	Duration	Replay
03:53:12	-	45min 49s	▶
03:01:11	-	51min 2s	▶
02:08:59	-	51min 13s	▶

Analysis

Timeline | Session Replay

▶ 00:00/45:50

Navigate

Skip Inactivity

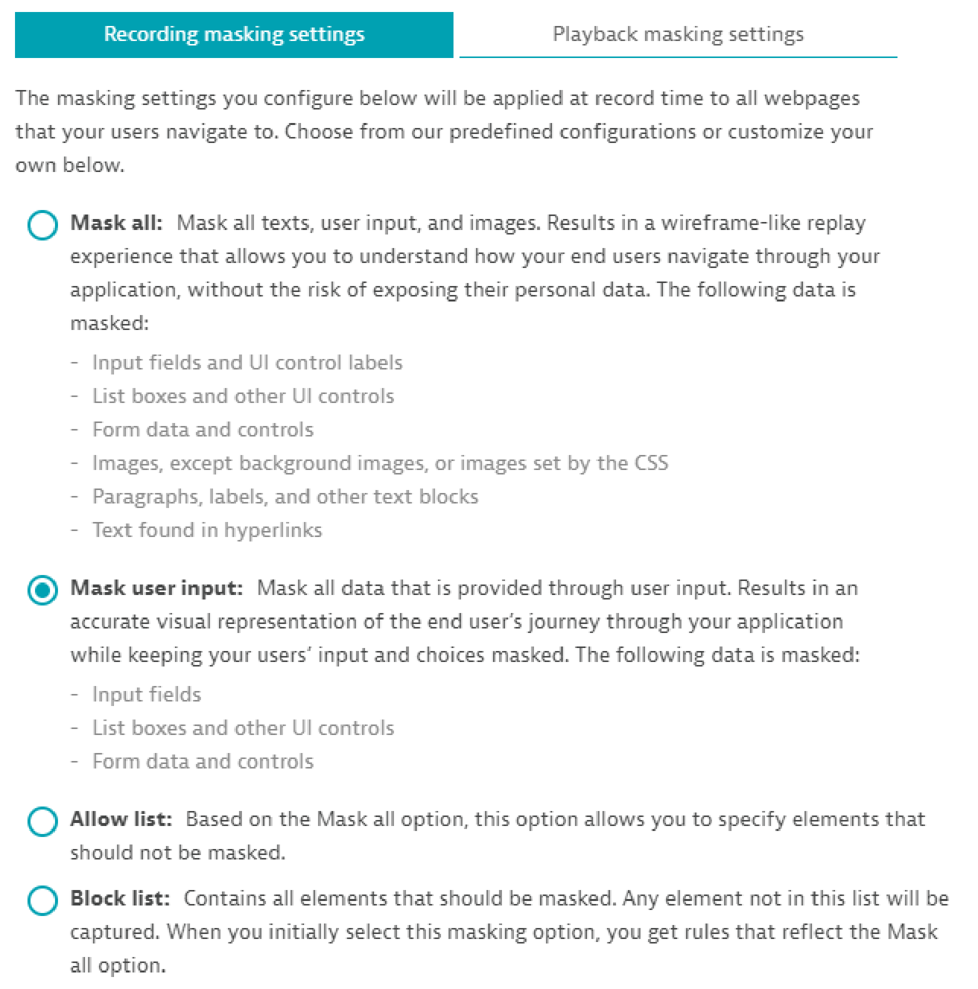
Speed 1x

▨ Load action ● User action or event ● Errors and annoyances

Keyboard shortcuts

Environment Permissions

- Replay session data without masking
  - Allows replaying recorded user sessions without playback masking rules applied.
    - Note: Any data masked at time of *recording* is never captured, therefore, always masked during play.
  - Recording and Playback masking rules are set within each application



The masking settings you configure below will be applied at record time to all webpages that your users navigate to. Choose from our predefined configurations or customize your own below.

○ **Mask all:** Mask all texts, user input, and images. Results in a wireframe-like replay experience that allows you to understand how your end users navigate through your application, without the risk of exposing their personal data. The following data is masked:

- Input fields and UI control labels
- List boxes and other UI controls
- Form data and controls
- Images, except background images, or images set by the CSS
- Paragraphs, labels, and other text blocks
- Text found in hyperlinks

● **Mask user input:** Mask all data that is provided through user input. Results in an accurate visual representation of the end user's journey through your application while keeping your users' input and choices masked. The following data is masked:

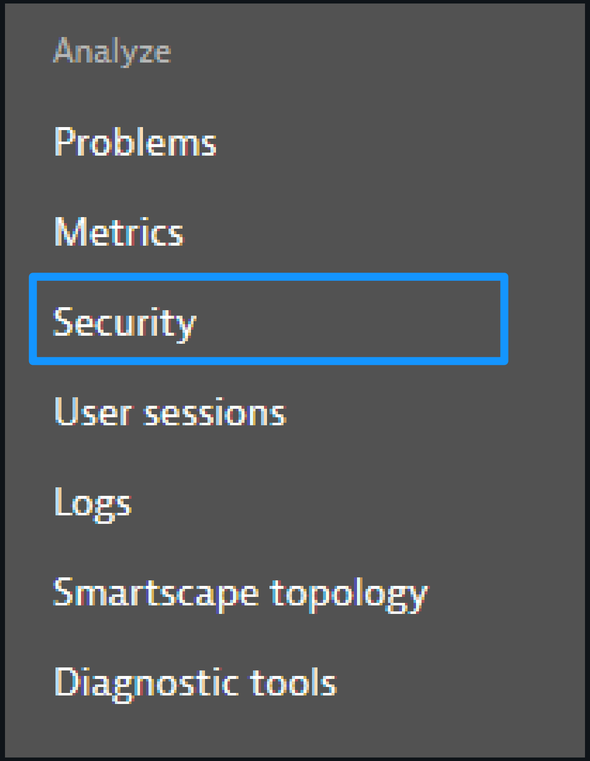
- Input fields
- List boxes and other UI controls
- Form data and controls

○ **Allow list:** Based on the Mask all option, this option allows you to specify elements that should not be masked.

○ **Block list:** Contains all elements that should be masked. Any element not in this list will be captured. When you initially select this masking option, you get rules that reflect the Mask all option.

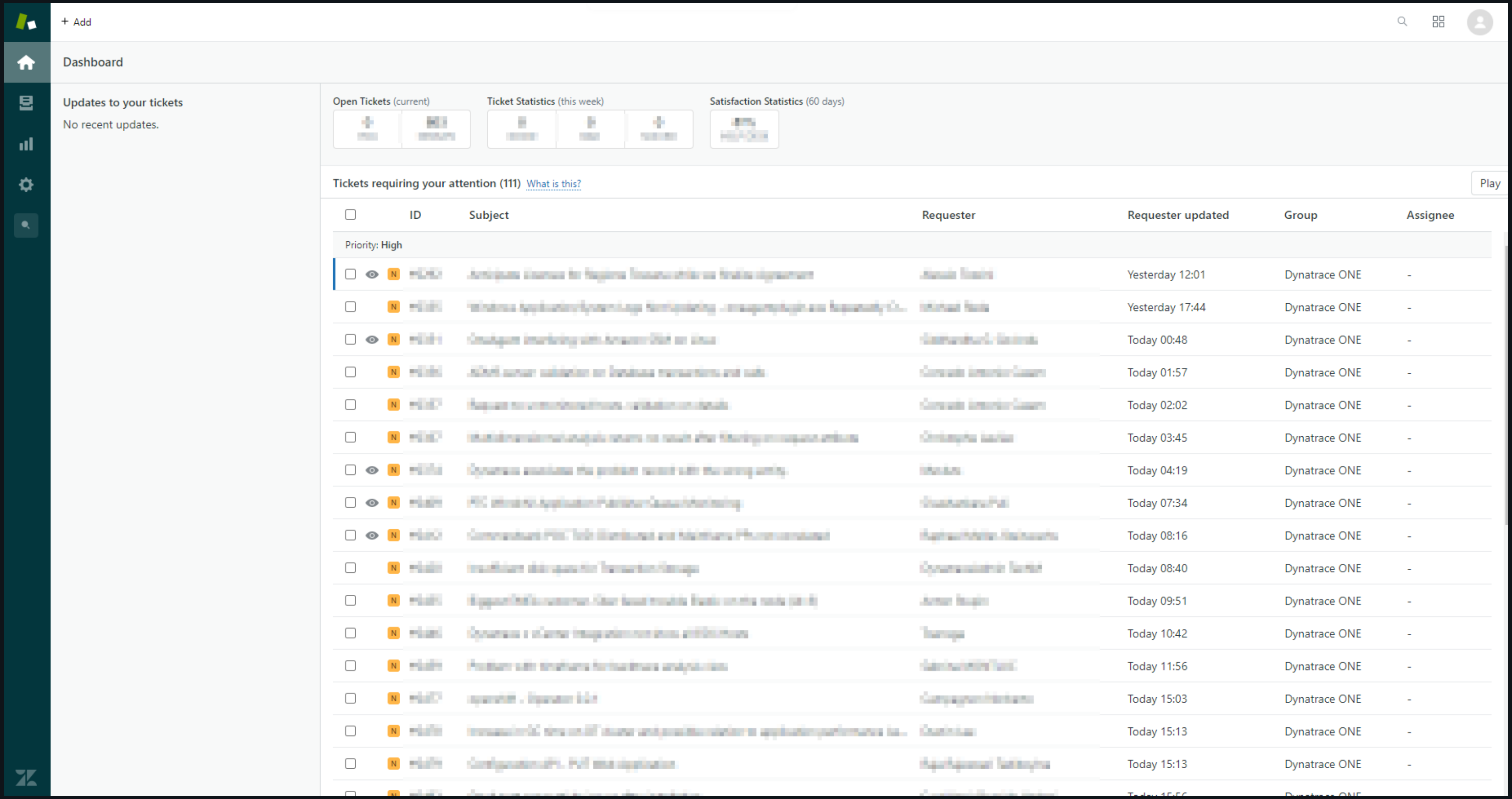
Environment Permissions

- Manage security problems
  - Allows management of problems reported by Dynatrace Application Security



Environment Permissions

- Manage Support Tickets
  - Allows access to all support tickets that have been created for this environment.



+ Add

Dashboard

Updates to your tickets

No recent updates.

Open Tickets (current) [redacted]

Ticket Statistics (this week) [redacted]

Satisfaction Statistics (60 days) [redacted]

Tickets requiring your attention (111) What is this?

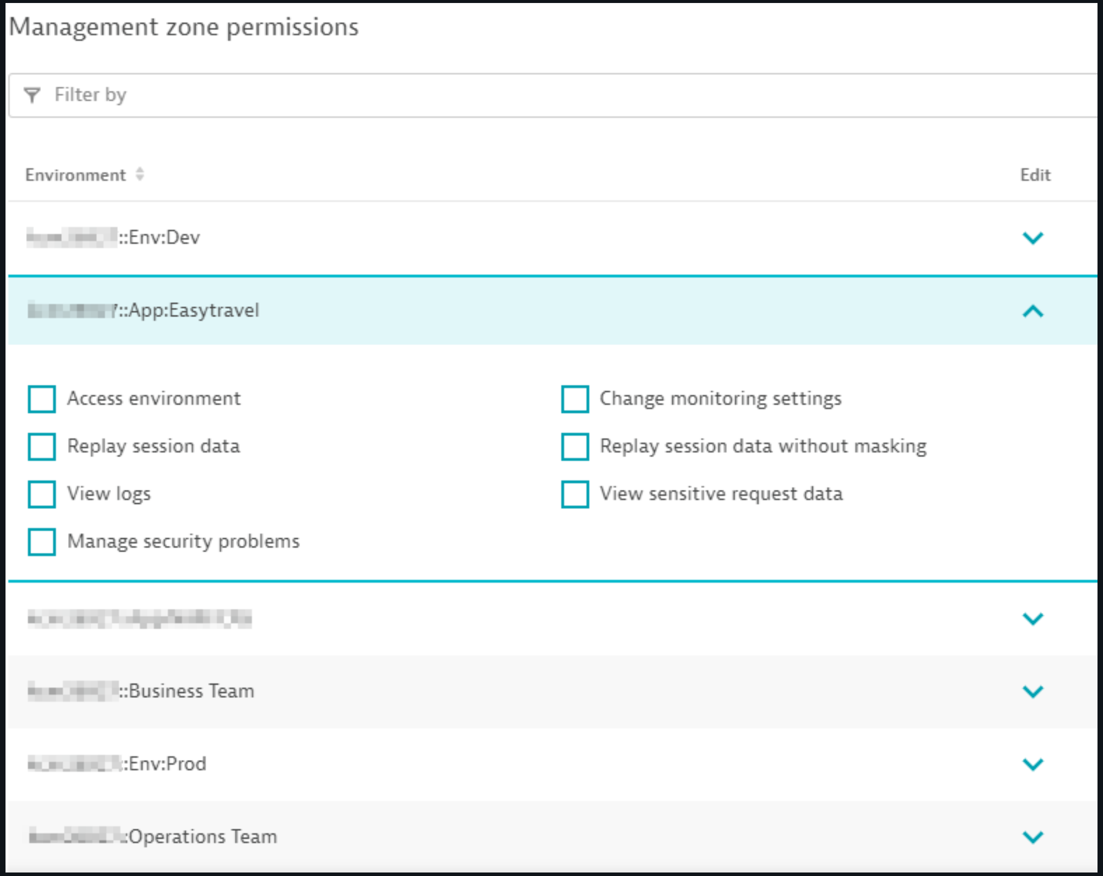
Play

☐			ID	Subject	Requester	Requester updated	Group	Assignee
Priority: High								
☐	👁	N	[redacted]	[redacted]	[redacted]	Yesterday 12:01	Dynatrace ONE	-
☐		N	[redacted]	[redacted]	[redacted]	Yesterday 17:44	Dynatrace ONE	-
☐	👁	N	[redacted]	[redacted]	[redacted]	Today 00:48	Dynatrace ONE	-
☐		N	[redacted]	[redacted]	[redacted]	Today 01:57	Dynatrace ONE	-
☐		N	[redacted]	[redacted]	[redacted]	Today 02:02	Dynatrace ONE	-
☐		N	[redacted]	[redacted]	[redacted]	Today 03:45	Dynatrace ONE	-
☐	👁	N	[redacted]	[redacted]	[redacted]	Today 04:19	Dynatrace ONE	-
☐	👁	N	[redacted]	[redacted]	[redacted]	Today 07:34	Dynatrace ONE	-
☐	👁	N	[redacted]	[redacted]	[redacted]	Today 08:16	Dynatrace ONE	-
☐		N	[redacted]	[redacted]	[redacted]	Today 08:40	Dynatrace ONE	-
☐		N	[redacted]	[redacted]	[redacted]	Today 09:51	Dynatrace ONE	-
☐		N	[redacted]	[redacted]	[redacted]	Today 10:42	Dynatrace ONE	-
☐		N	[redacted]	[redacted]	[redacted]	Today 11:56	Dynatrace ONE	-
☐		N	[redacted]	[redacted]	[redacted]	Today 15:03	Dynatrace ONE	-
☐		N	[redacted]	[redacted]	[redacted]	Today 15:13	Dynatrace ONE	-
☐		N	[redacted]	[redacted]	[redacted]	Today 15:13	Dynatrace ONE	-

Management Zone Permissions

Management Zone Permissions

- Managed and SaaS Management Zone Permissions
  - https://www.dynatrace.com/support/help/shortlink/user-groups-setup#management-zone-permissions-



Management zone permissions

Filter by

Environment — Edit

[redacted]::Env:Dev

[redacted]::App:Easytravel

□ Access environment
□ Replay session data
□ View logs
□ Manage security problems
□ Change monitoring settings
□ Replay session data without masking
□ View sensitive request data

[redacted]

[redacted]::Business Team

[redacted]:Env:Prod

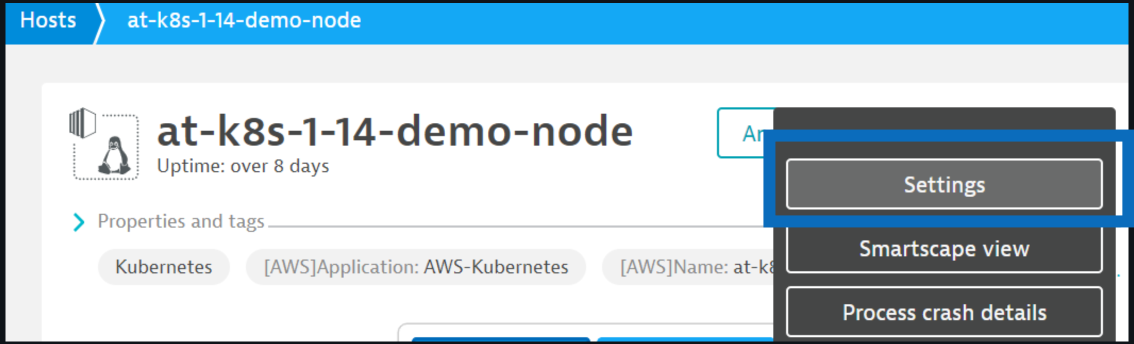
[redacted]:Operations Team

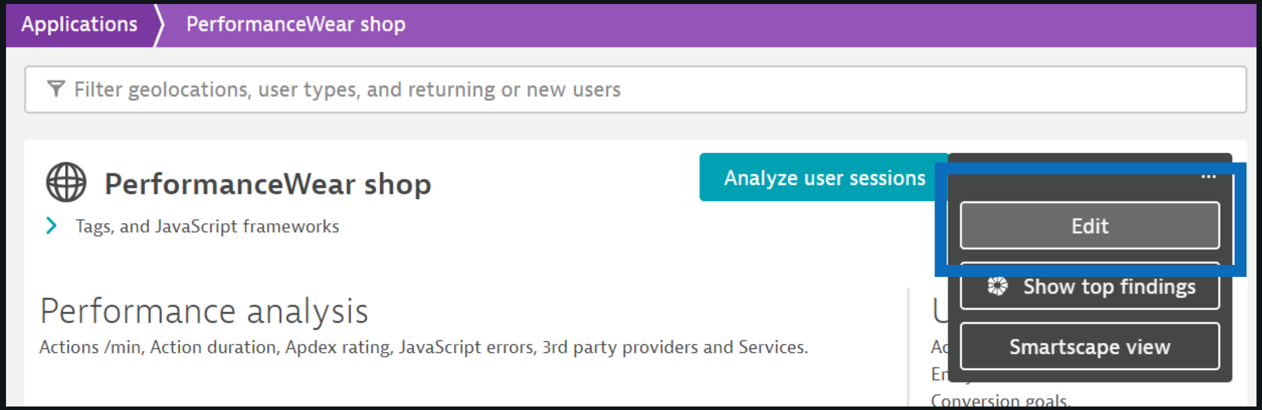
Management Zone Permissions

- Access Environment
  - Allows read-only access to the entities within the Management Zone. Can’t change settings. Can’t install OneAgent.
  - The Access Environment Permission on the Management Zone allow the users to do the following:
    - View the monitored data
    - View Dynatrace reports
    - Build, clone, & share dashboards
    - Create custom charts
    - Add/Remove key requests
  - “Access Environment” is automatically selected for the management zone when you select any other management zone permission.

Management Zone Permissions

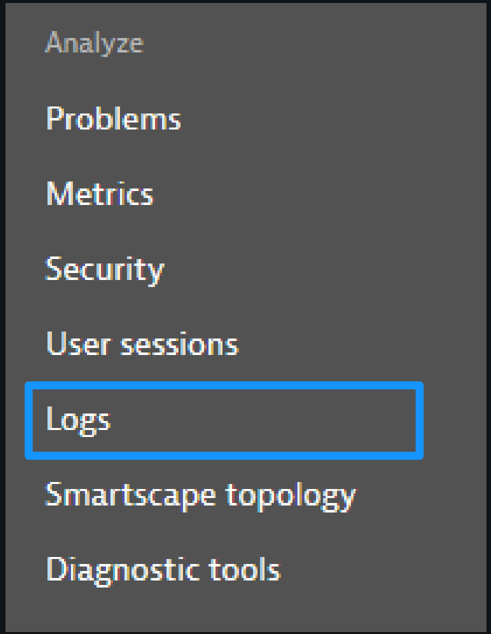
- Change monitoring settings
  - Can change entity monitoring settings for the entities within the Management Zone.
  - Create Synthetic Monitors in the Management Zone.
  - No Access to Environment Settings

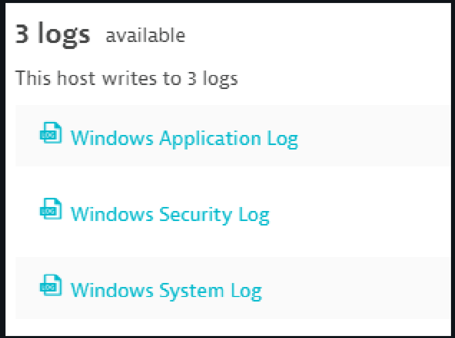



Applications
PerformanceWear shop
Filter geolocations, user types, and returning or new users
PerformanceWear shop
Tags, and JavaScript frameworks
Analyze user sessions
...
Edit
Show top findings
Smartscape view
Performance analysis
Actions /min, Action duration, Apdex rating, JavaScript errors, 3rd party providers and Services.
U
Ac
Er
Conversion goals

Management Zone Permissions

- View logs
  - Allows access to log file content for entities within the Management Zone, which may contain sensitive information
- Log file data can be masked by the OneAgent prior to being seen in the UI or stored on the Dynatrace Server
  - https://www.dynatrace.com/support/help/shortlink/log-analytics-mask-info#mask-personal-data

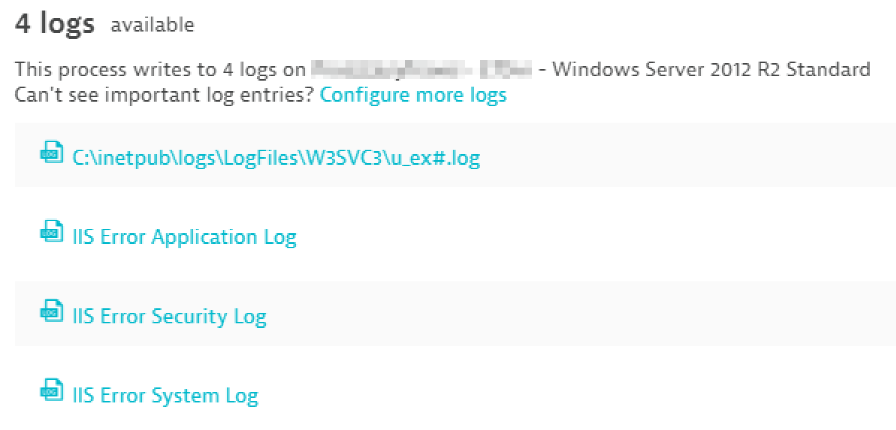




3 logs available

This host writes to 3 logs

- Windows Application Log
- Windows Security Log
- Windows System Log



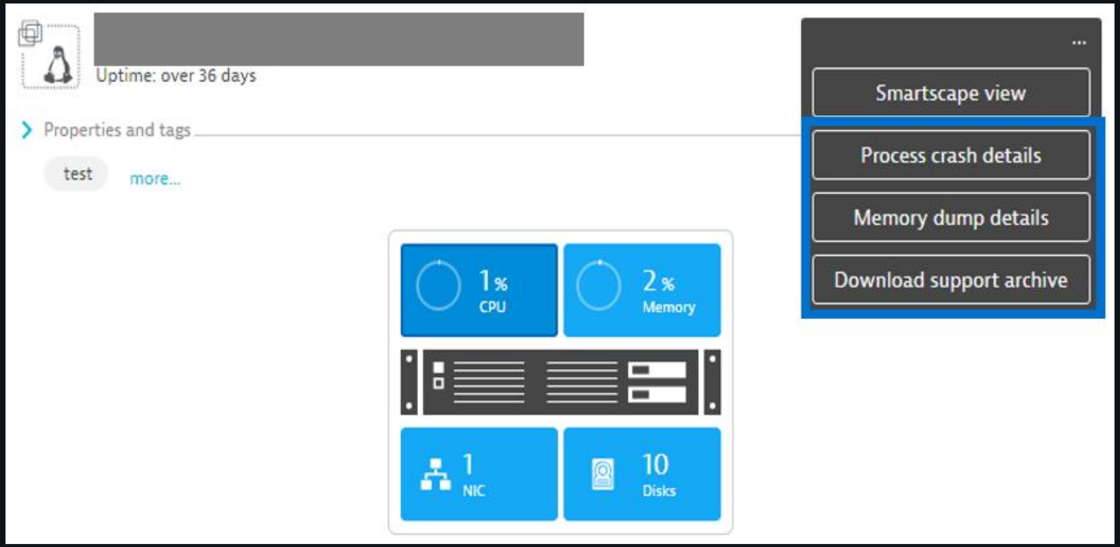
4 logs available

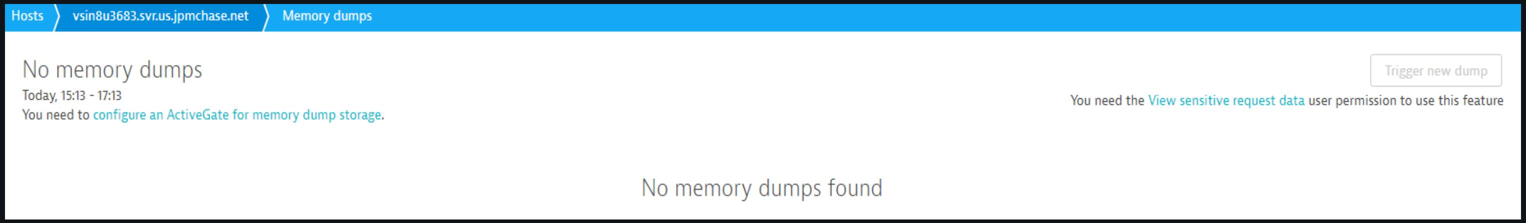
This process writes to 4 logs on [redacted] - Windows Server 2012 R2 Standard
Can't see important log entries? Configure more logs

- C:\inetpub\logs\LogFiles\W3SVC3\u_ex#.log
- IIS Error Application Log
- IIS Error Security Log
- IIS Error System Log

Management Zone Permissions

- View sensitive request data
  - Allows viewing of potentially sensitive data
  - Users who do not have this permission see that the data point exists, but the personal data is masked by asterisks (*****)
  - See details of what is considered sensitive on next slide





No memory dumps

Today, 15:13 - 17:13

You need to configure an ActiveGate for memory dump storage.

You need the View sensitive request data user permission to use this feature

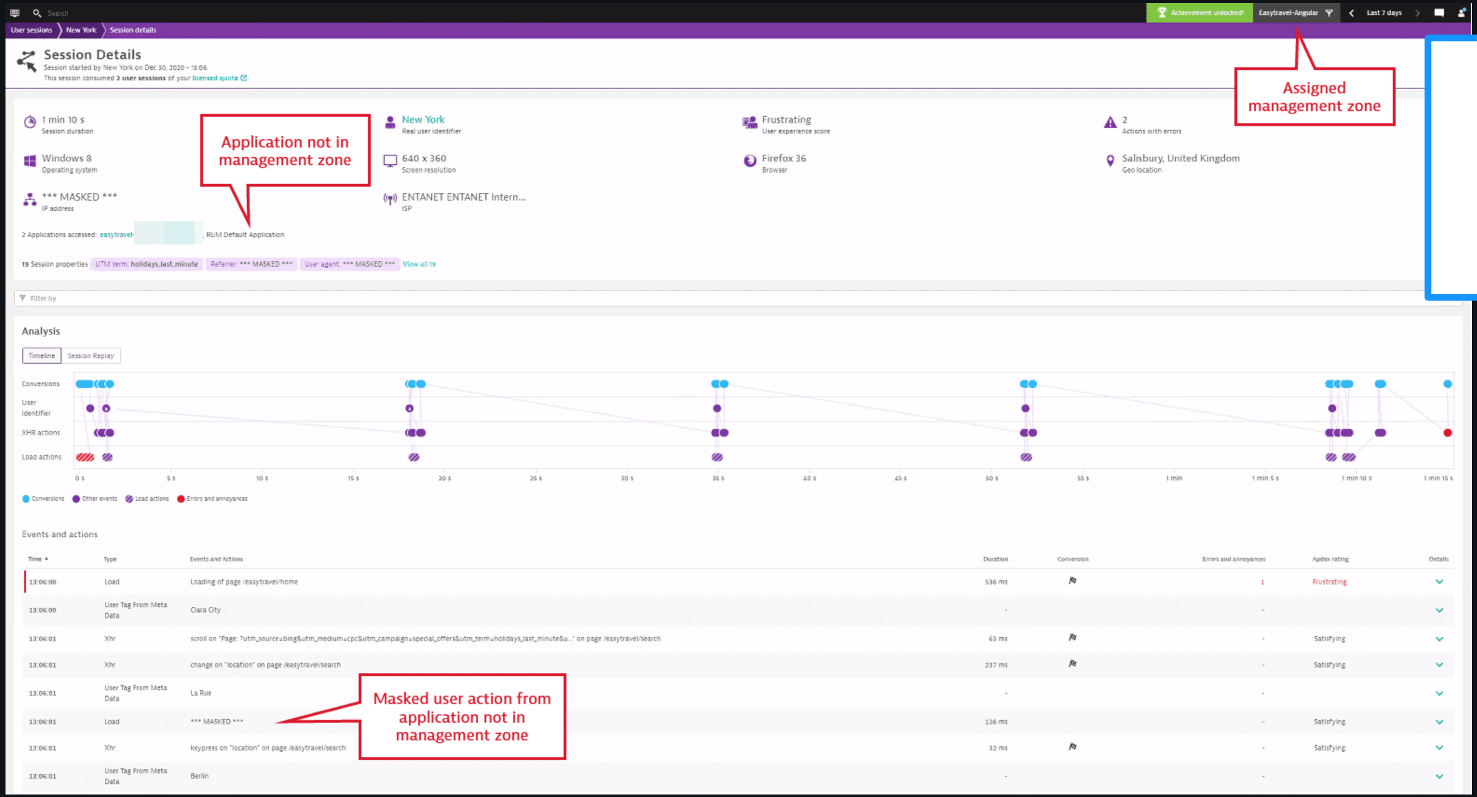
No memory dumps found

Sensitive Data

- Dynatrace will automatically classify certain data items as sensitive
- This includes things like client IP addresses, Exception messages, URL query parameters, HTTP Headers/post paramters and extends to certain patterns in exception messages like GUIDs
- Users are able to configure the capture of additional data, which will require the user to have the permission to do so (Configure capture of sensitive data)
  - The User will be able to explicitly designate these newly captured data points as sensitive or non sensitive
- OneAgent diagnostics and memory dumps are also considered sensitive data
- https://www.dynatrace.com/support/help/shortlink/sensitive-data
- https://www.dynatrace.com/support/help/shortlink/section-data-privacy-and-security

Management Zone Permissions

- Replay session data
  - Allows replaying recorded user sessions with playback masking rules applied at the time of *playback*.
    - Note: Any data masked at time of *recording* is never captured, therefore, always masked during play.
  - Applications outside of the user’s assigned management zone will have user actions masked.



Session Details

Session started by New York on Dec 30, 2020 - 13:06.

This session consumed **2 user sessions** of your licensed quota.

1 min 10 s — Session duration

Windows 8 — Operating system

*** MASKED *** — IP address

New York — Real user identifier

640 x 360 — Screen resolution

ENTANET ENTANET Intern... — ISP

Frustrating — User experience score

Firefox 36 — Browser

2 — Actions with errors

Salisbury, United Kingdom — Geo location

2 Applications accessed: easytravel-, RUM Default Application

19 Session properties: UTM term: holidays_last_minute | Referrer: *** MASKED *** | User agent: *** MASKED *** | View all 19

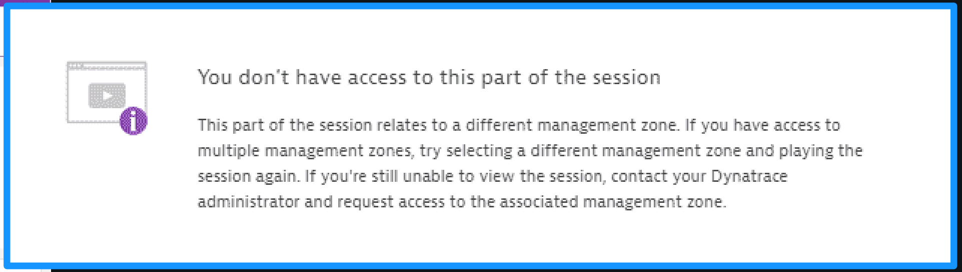
Events and actions

Time ▲	Type	Events and Actions	Duration	Conversion	Errors and annoyances	Apdex rating	Details
13:06:00	Load	Loading of page /easytravel/home	536 ms	⚑	1	Frustrating	⌄
13:06:00	User Tag From Meta Data	Clara City	-		-		⌄
13:06:01	Xhr	scroll on "Page: ?utm_source=bing&utm_medium=cpc&utm_campaign=special_offers&utm_term=holidays_last_minute&u..." on page /easytravel/search	63 ms	⚑	-	Satisfying	⌄
13:06:01	Xhr	change on "location" on page /easytravel/search	237 ms	⚑	-	Satisfying	⌄
13:06:01	User Tag From Meta Data	La Rue	-		-		⌄
13:06:01	Load	*** MASKED ***	126 ms		-	Satisfying	⌄
13:06:01	Xhr	keypress on "location" on page /easytravel/search	32 ms	⚑	-	Satisfying	⌄
13:06:01	User Tag From Meta Data	Berlin	-		-		⌄

Application not in management zone

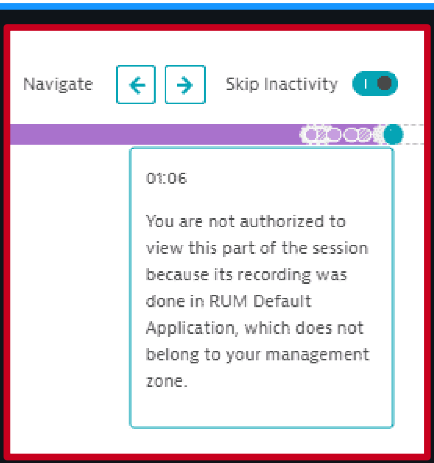
Assigned management zone

Masked user action from application not in management zone



You don’t have access to this part of the session

This part of the session relates to a different management zone. If you have access to multiple management zones, try selecting a different management zone and playing the session again. If you're still unable to view the session, contact your Dynatrace administrator and request access to the associated management zone.

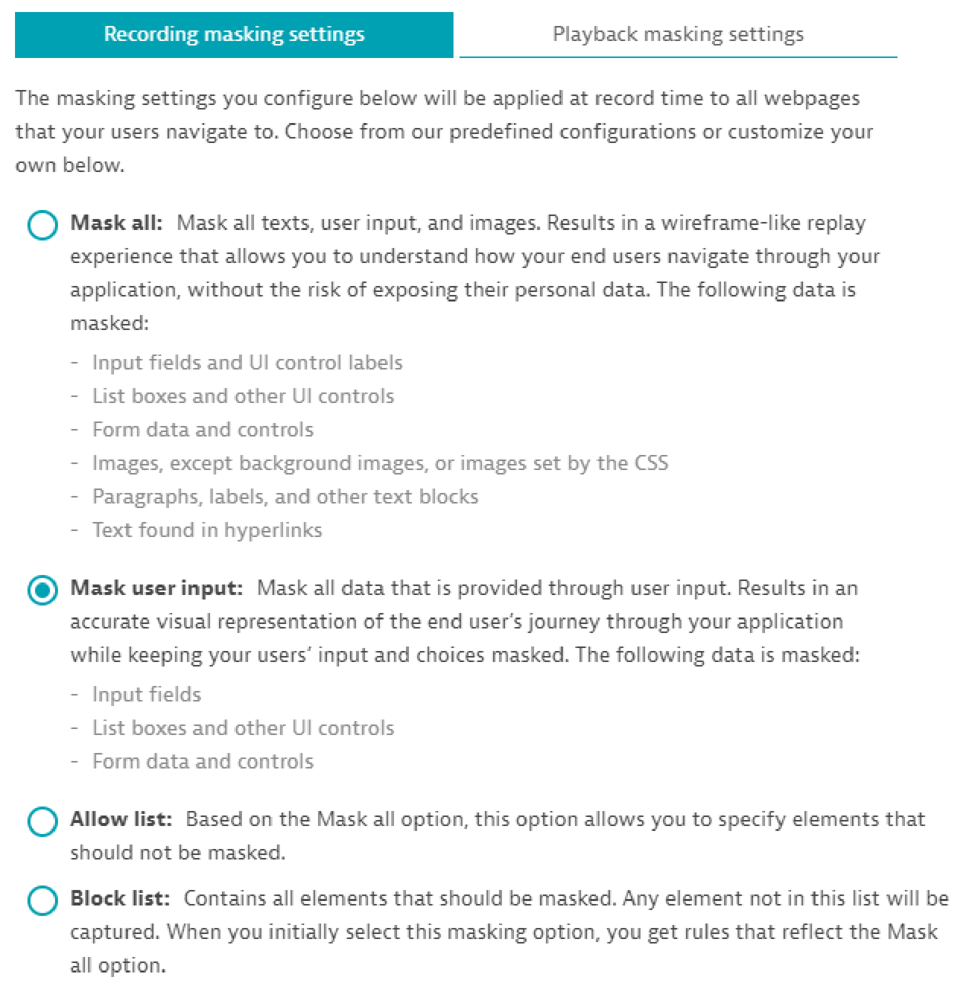


01:06

You are not authorized to view this part of the session because its recording was done in RUM Default Application, which does not belong to your management zone.

Management Zone Permissions

- Replay session data without masking
  - Allows replaying recorded user sessions without playback masking rules applied.
    - Note: Any data masked at time of *recording* is never captured, therefore, always masked during play.
  - Applications outside of the user's assigned management zone will have user actions masked.
  - Recording and Playback masking rules are set within each application



The masking settings you configure below will be applied at record time to all webpages that your users navigate to. Choose from our predefined configurations or customize your own below.

○ **Mask all:** Mask all texts, user input, and images. Results in a wireframe-like replay experience that allows you to understand how your end users navigate through your application, without the risk of exposing their personal data. The following data is masked:

- Input fields and UI control labels
- List boxes and other UI controls
- Form data and controls
- Images, except background images, or images set by the CSS
- Paragraphs, labels, and other text blocks
- Text found in hyperlinks

● **Mask user input:** Mask all data that is provided through user input. Results in an accurate visual representation of the end user's journey through your application while keeping your users' input and choices masked. The following data is masked:

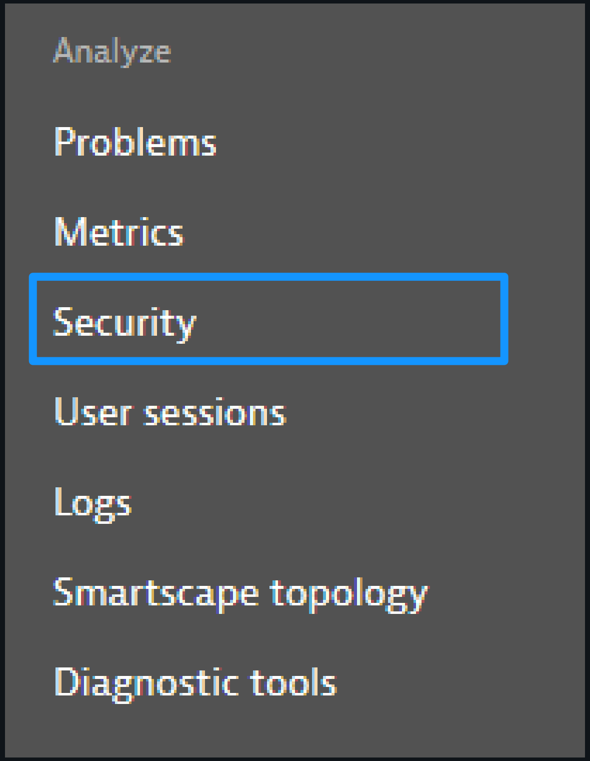
- Input fields
- List boxes and other UI controls
- Form data and controls

○ **Allow list:** Based on the Mask all option, this option allows you to specify elements that should not be masked.

○ **Block list:** Contains all elements that should be masked. Any element not in this list will be captured. When you initially select this masking option, you get rules that reflect the Mask all option.

Management Zone Permissions

- Manage security problems
  - Allows management of problems reported by Dynatrace Application Security



Manage Groups and Users

Manage Groups and Users

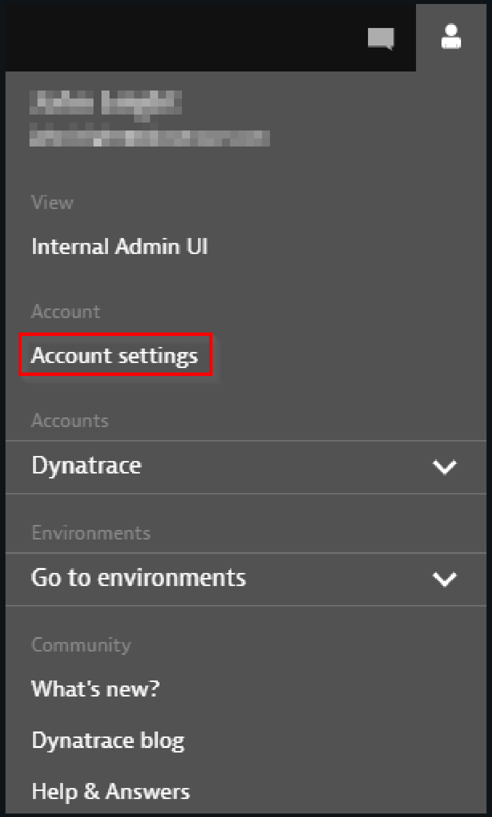
- You can perform the following tasks:
  - Users
    - View a list of users
    - Export a list of users
    - Add or Invite a user to your account
    - Edit a user’s group assignments
    - Delete a user

    Note: User management options are slightly different between SaaS and Managed
  - Groups
    - View a list of groups
    - Create a new group
    - Edit a group
    - Delete/Remove a group

SaaS Identity Management

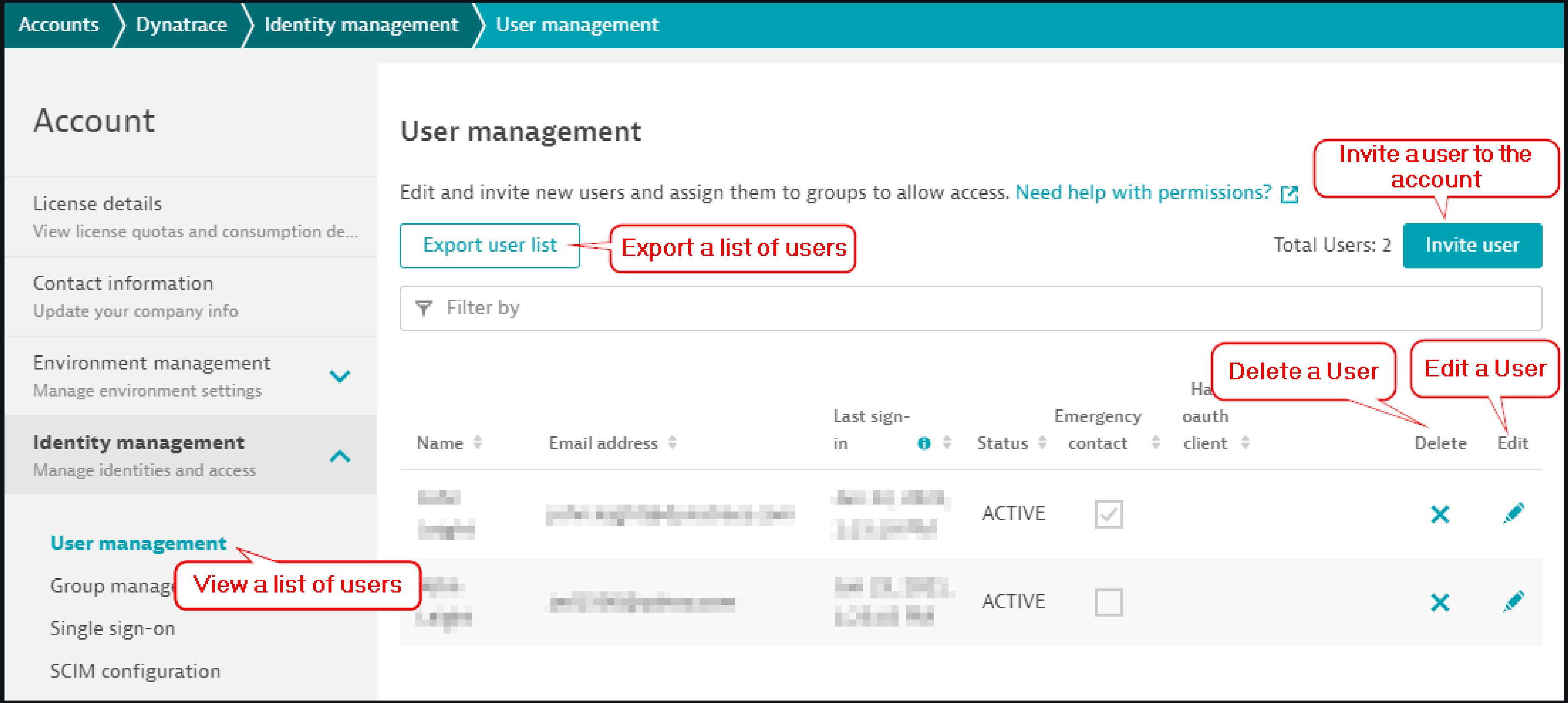
SaaS

- Configure SaaS Identity Management from the Account Settings



SaaS

- Manage Users



Accounts 〉 Dynatrace 〉 Identity management 〉 User management

Account

License details
View license quotas and consumption de...

Contact information
Update your company info

Environment management
Manage environment settings

Identity management
Manage identities and access

User management
Group manage
Single sign-on
SCIM configuration

View a list of users

User management

Edit and invite new users and assign them to groups to allow access. Need help with permissions?

Invite a user to the account

Export user list

Export a list of users

Total Users: 2

Invite user

Filter by

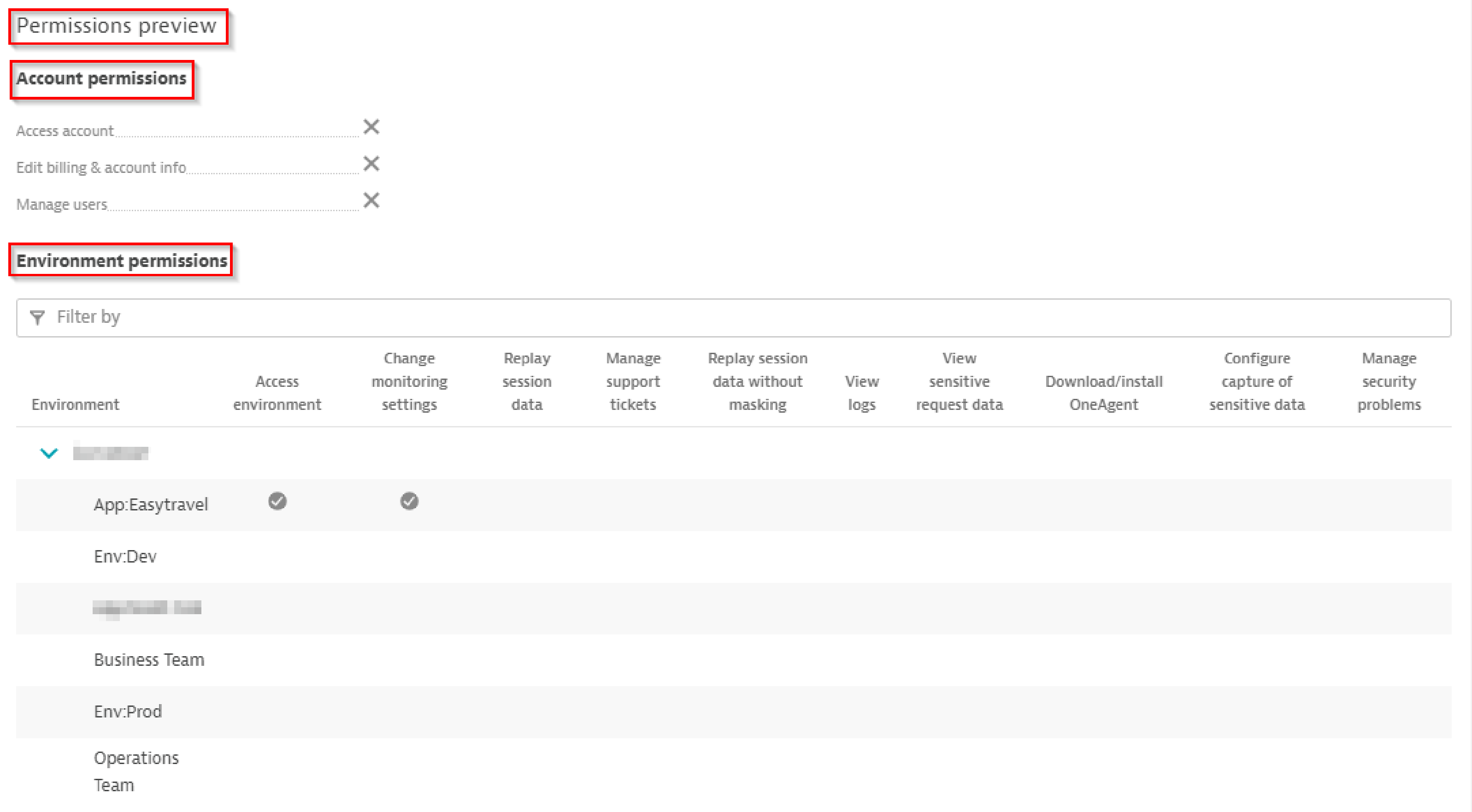
Delete a User

Edit a User

Name	Email address	Last sign-in	Status	Emergency contact	Ha oauth client	Delete	Edit
[redacted]	[redacted]	[redacted]	ACTIVE	☑		✕	✎
[redacted]	[redacted]	[redacted]	ACTIVE	☐		✕	✎

SaaS

- Edit a user to preview their Account, Environment and Management Zone permissions
- Permissions are based on Group Membership



Permissions preview

Account permissions

Access account	✕
Edit billing & account info	✕
Manage users	✕

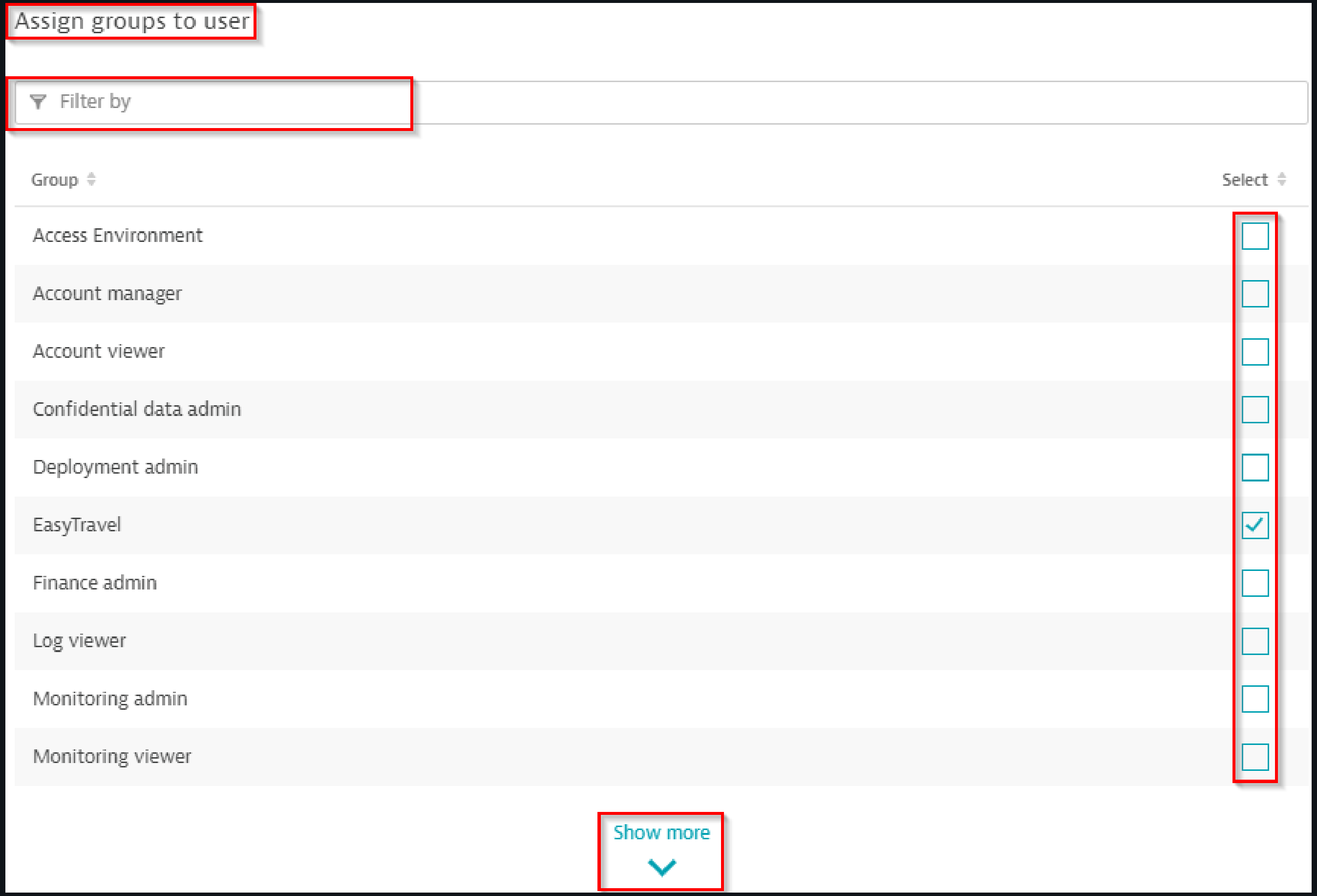
Environment permissions

Filter by

Environment	Access environment	Change monitoring settings	Replay session data	Manage support tickets	Replay session data without masking	View logs	View sensitive request data	Download/install OneAgent	Configure capture of sensitive data	Manage security problems
[redacted]										
App:Easytravel	✓	✓								
Env:Dev										
[redacted]										
Business Team										
Env:Prod										
Operations Team										

SaaS

- Edit a user to assign group membership
- Filter groups by name in the filter bar
- Use “Show More” to extend the list of Groups

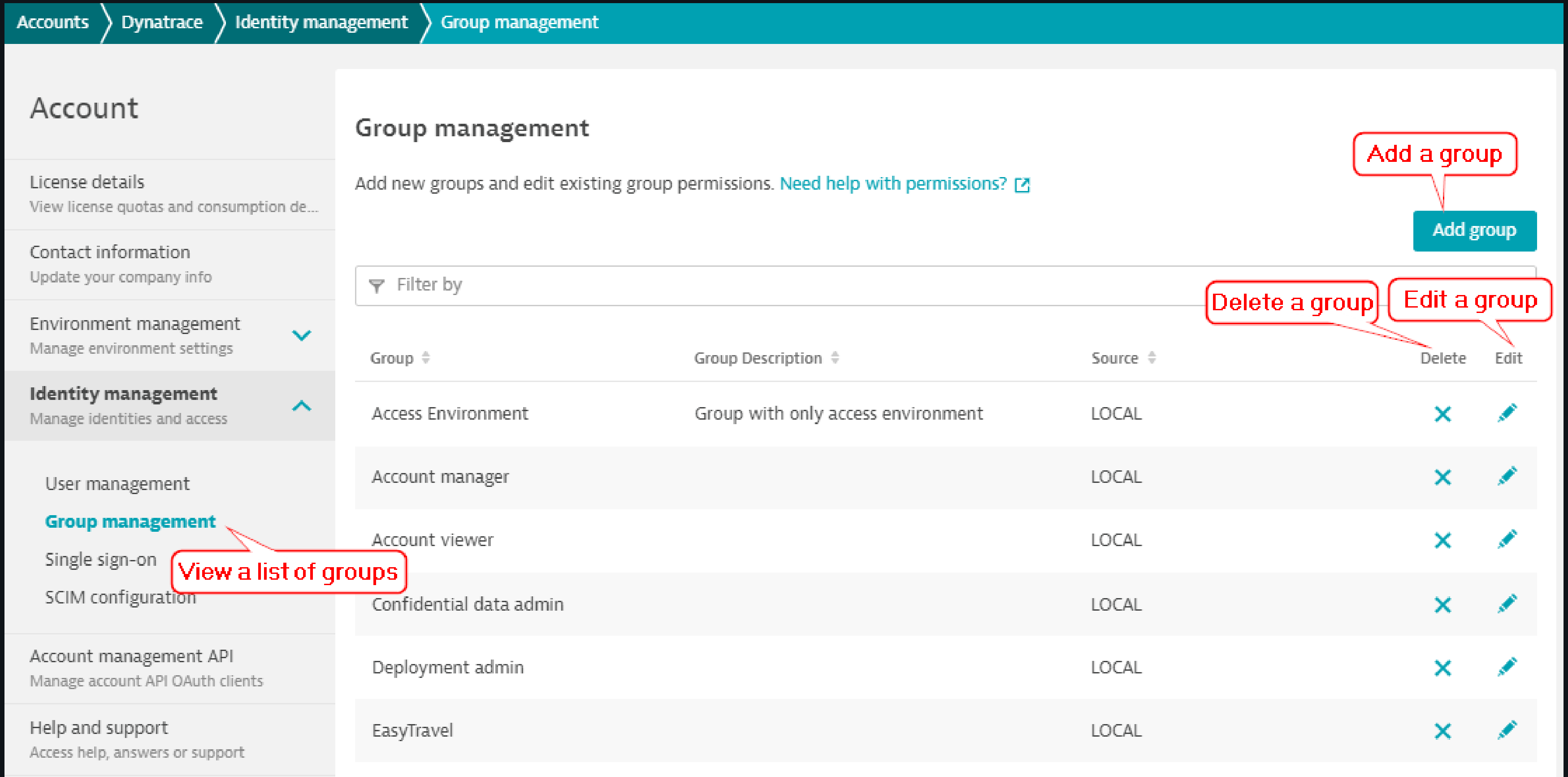


Assign groups to user

Group	Select
Access Environment	□
Account manager	□
Account viewer	□
Confidential data admin	□
Deployment admin	□
EasyTravel	☑
Finance admin	□
Log viewer	□
Monitoring admin	□
Monitoring viewer	□

SaaS

- Use Groups to manage permissions



Accounts 〉 Dynatrace 〉 Identity management 〉 Group management

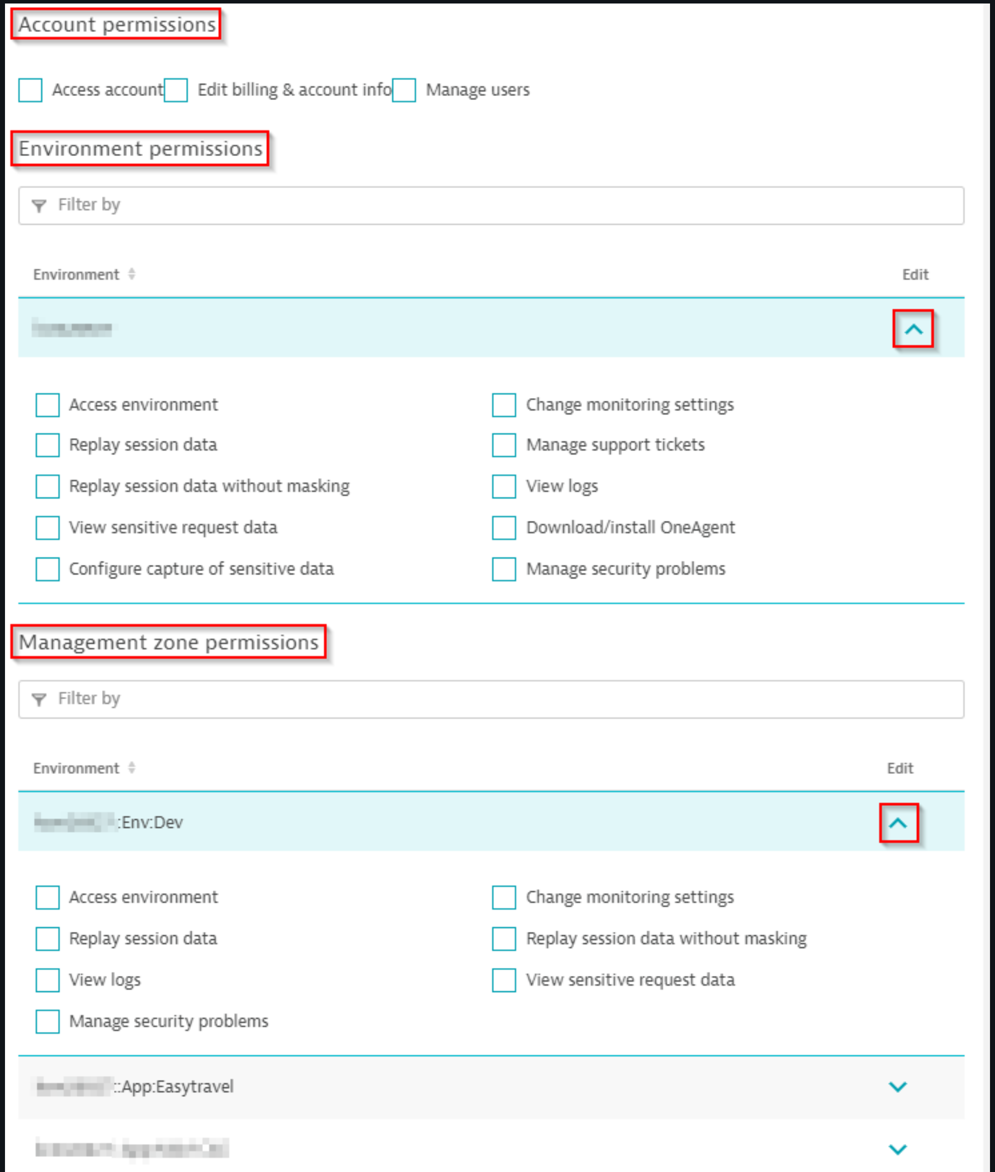
Group management

Add new groups and edit existing group permissions. Need help with permissions?

Group	Group Description	Source	Delete	Edit
Access Environment	Group with only access environment	LOCAL	✕	✎
Account manager		LOCAL	✕	✎
Account viewer		LOCAL	✕	✎
Confidential data admin		LOCAL	✕	✎
Deployment admin		LOCAL	✕	✎
EasyTravel		LOCAL	✕	✎

SaaS

- Create or edit a group to set Account, Environment or Management Zone permissions



Account permissions

□ Access account □ Edit billing & account info □ Manage users

Environment permissions

Filter by

Environment Edit

[redacted]

□ Access environment
□ Replay session data
□ Replay session data without masking
□ View sensitive request data
□ Configure capture of sensitive data
□ Change monitoring settings
□ Manage support tickets
□ View logs
□ Download/install OneAgent
□ Manage security problems

Management zone permissions

Filter by

Environment Edit

[redacted]:Env:Dev

□ Access environment
□ Replay session data
□ View logs
□ Manage security problems
□ Change monitoring settings
□ Replay session data without masking
□ View sensitive request data

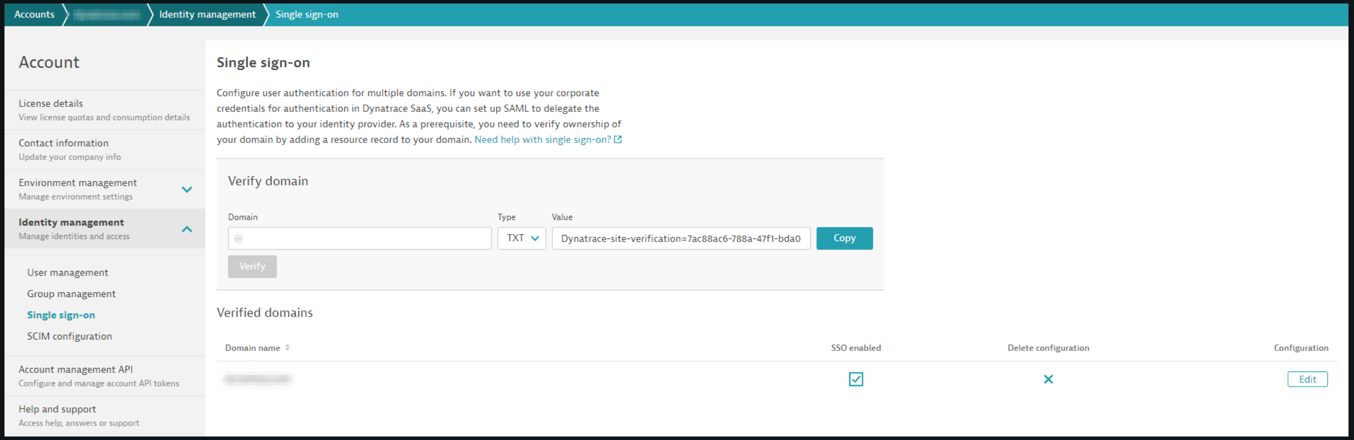
[redacted]::App:Easytravel

[redacted]

SaaS – SSO

- SAML Authentication
  - SAML 2.0 is used
  - Can also be used to manage permissions
  - Examples are:
    - Active Directory FS SAML
    - Azure SAML
    - Gsuite SAML
    - Okta SAML
  - Ensure you have a fallback account specified to avoid being locked out by an incorrect configuration!

https://www.dynatrace.com/support/help/shortlink/manage-users-groups-with-saml



Single sign-on

Configure user authentication for multiple domains. If you want to use your corporate credentials for authentication in Dynatrace SaaS, you can set up SAML to delegate the authentication to your identity provider. As a prerequisite, you need to verify ownership of your domain by adding a resource record to your domain. Need help with single sign-on?

Verify domain

Domain: @

Type: TXT

Value: Dynatrace-site-verification=7ac88ac6-788a-47f1-bda0

Copy

Verify

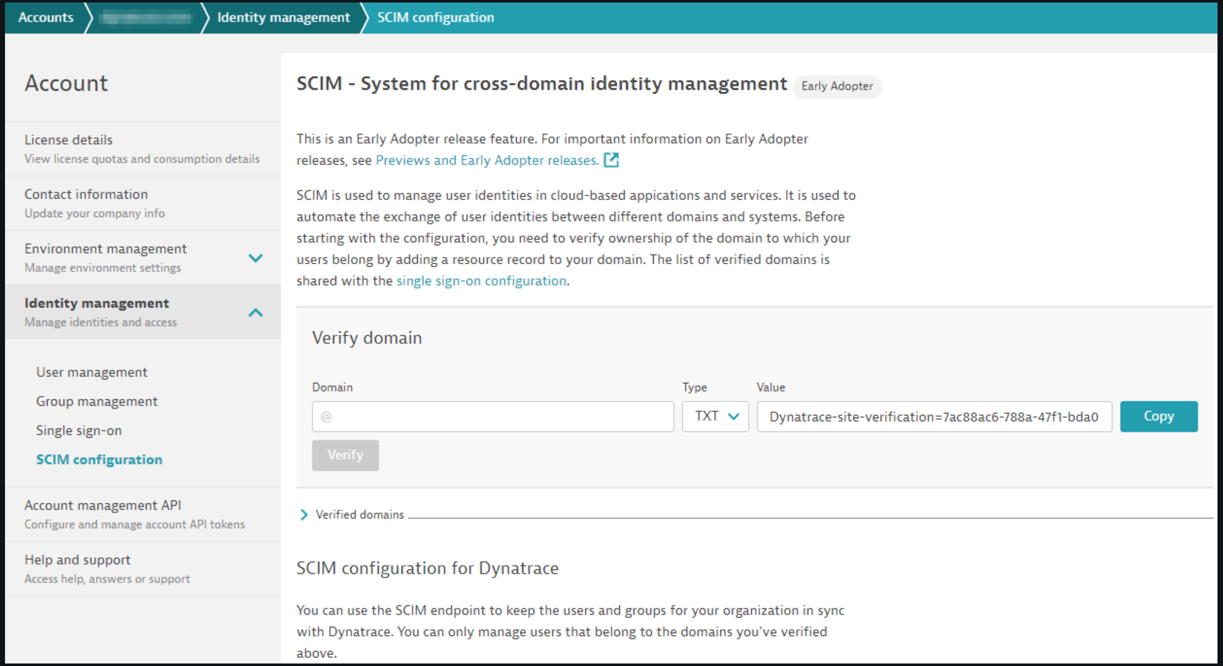
Verified domains

Domain name	SSO enabled	Delete configuration	Configuration
[redacted]	☑	✕	Edit

SaaS – SCIM

- SCIM Authentication
  - SCIM 2.0 is supported
  - Only users whose email domains have been verified for ownership can be synchronized with Dynatrace via SCIM.
  - Should take over SAML as it streamlines not only user but group management
  - Examples are:
    - Azure SCIM
    - Okta SCIM
  - Ensure you have a non-federated user created (different email domain) with admin permissions to avoid being locked out by an incorrect configuration!

https://www.dynatrace.com/support/help/shortlink/manage-users-groups-with-scim



SCIM - System for cross-domain identity management Early Adopter

This is an Early Adopter release feature. For important information on Early Adopter releases, see Previews and Early Adopter releases.

SCIM is used to manage user identities in cloud-based appications and services. It is used to automate the exchange of user identities between different domains and systems. Before starting with the configuration, you need to verify ownership of the domain to which your users belong by adding a resource record to your domain. The list of verified domains is shared with the single sign-on configuration.

Verify domain

Domain: @

Type: TXT

Value: Dynatrace-site-verification=7ac88ac6-788a-47f1-bda0

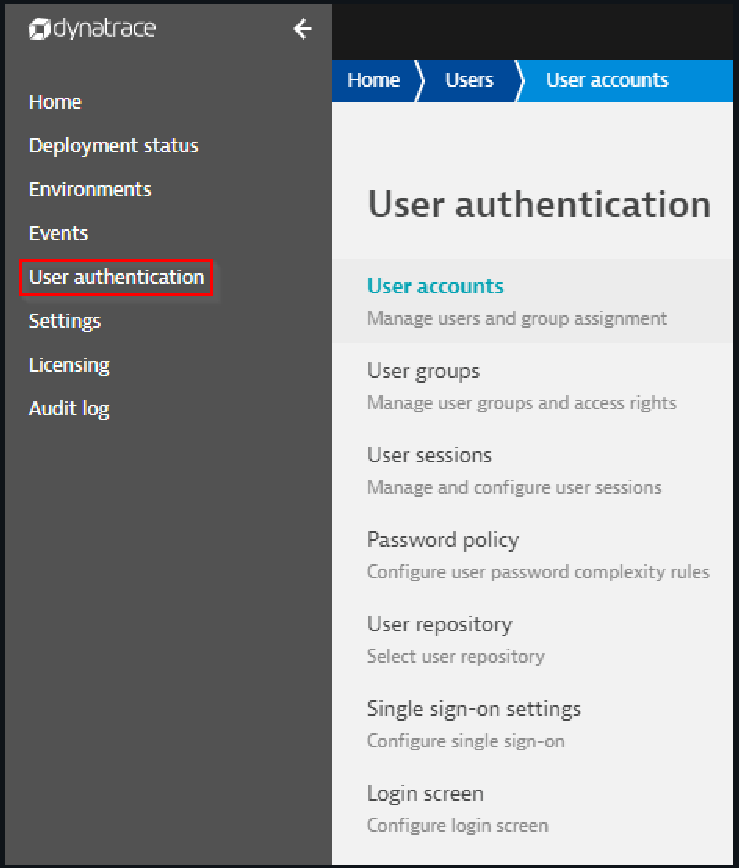
SCIM configuration for Dynatrace

You can use the SCIM endpoint to keep the users and groups for your organization in sync with Dynatrace. You can only manage users that belong to the domains you've verified above.

Managed User Authentication

Managed

- Configure User Authentication in Dynatrace Managed from the CMC (Cluster Management Console)



User authentication

User accounts
Manage users and group assignment

User groups
Manage user groups and access rights

User sessions
Manage and configure user sessions

Password policy
Configure user password complexity rules

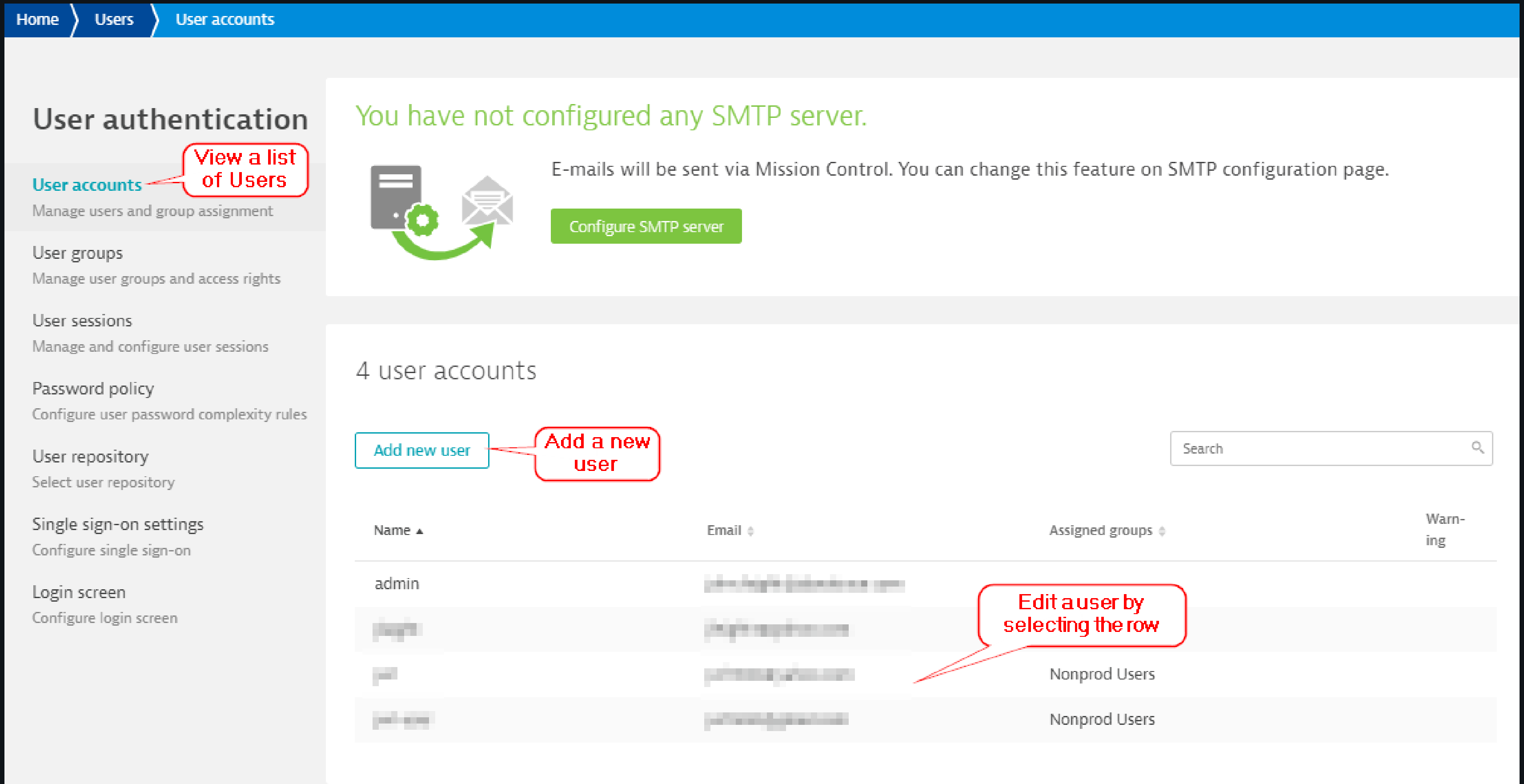
User repository
Select user repository

Single sign-on settings
Configure single sign-on

Login screen
Configure login screen

Managed

- Manage Users



User authentication

User accounts
Manage users and group assignment

View a list of Users

User groups
Manage user groups and access rights

User sessions
Manage and configure user sessions

Password policy
Configure user password complexity rules

User repository
Select user repository

Single sign-on settings
Configure single sign-on

Login screen
Configure login screen

You have not configured any SMTP server.

E-mails will be sent via Mission Control. You can change this feature on SMTP configuration page.

4 user accounts

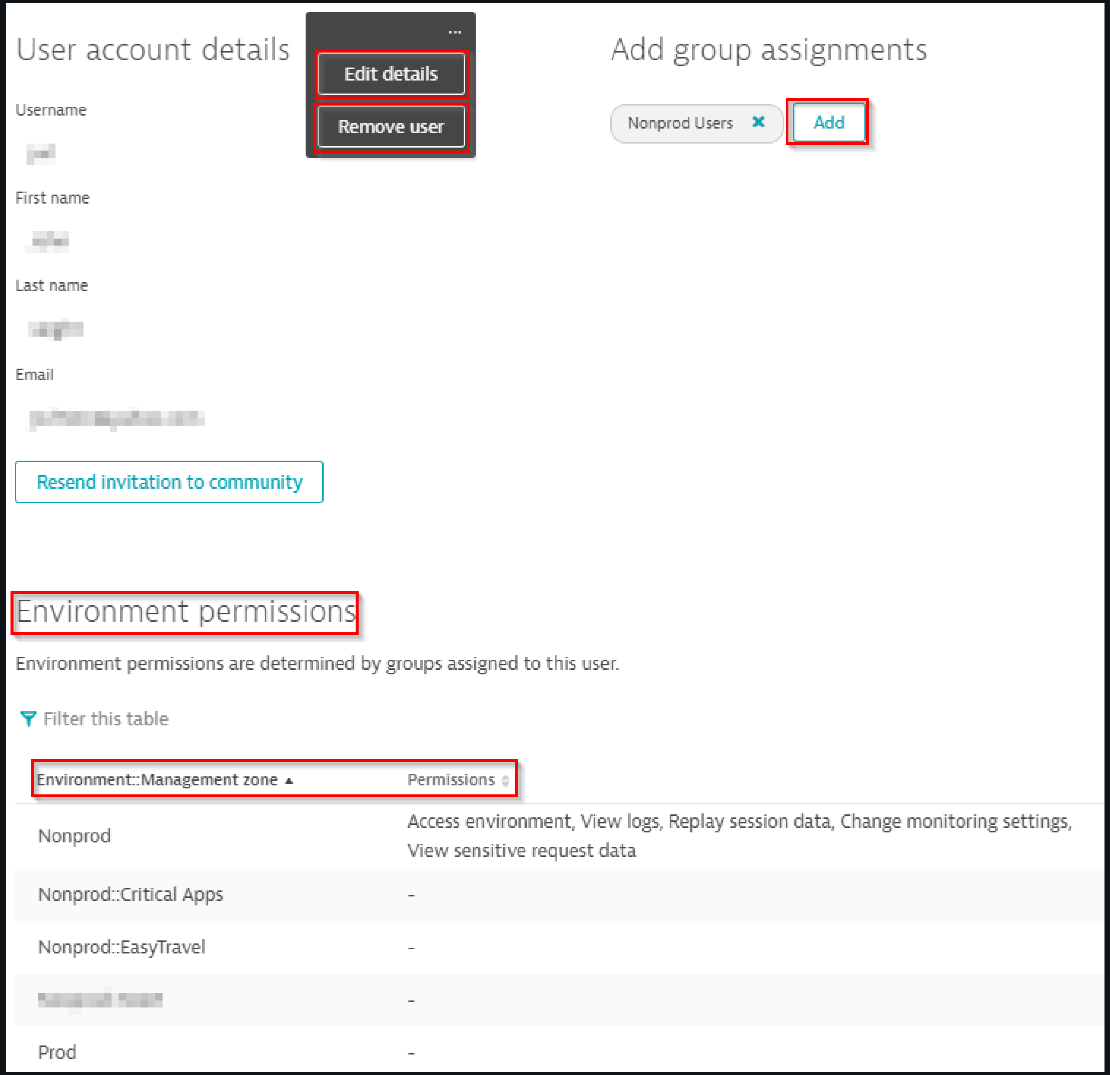
Add a new user

Name ▲	Email ⇕	Assigned groups ⇕	Warning
admin	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]	Nonprod Users	
[redacted]	[redacted]	Nonprod Users	

Edit a user by selecting the row

Managed

- Edit a user to
  - Edit their details
  - Remove the user
  - Assign groups
  - Preview their Environment and Management Zone permissions
- Permissions are based on Group Membership



User account details

Username

[redacted]

First name

[redacted]

Last name

[redacted]

Email

[redacted]

Add group assignments

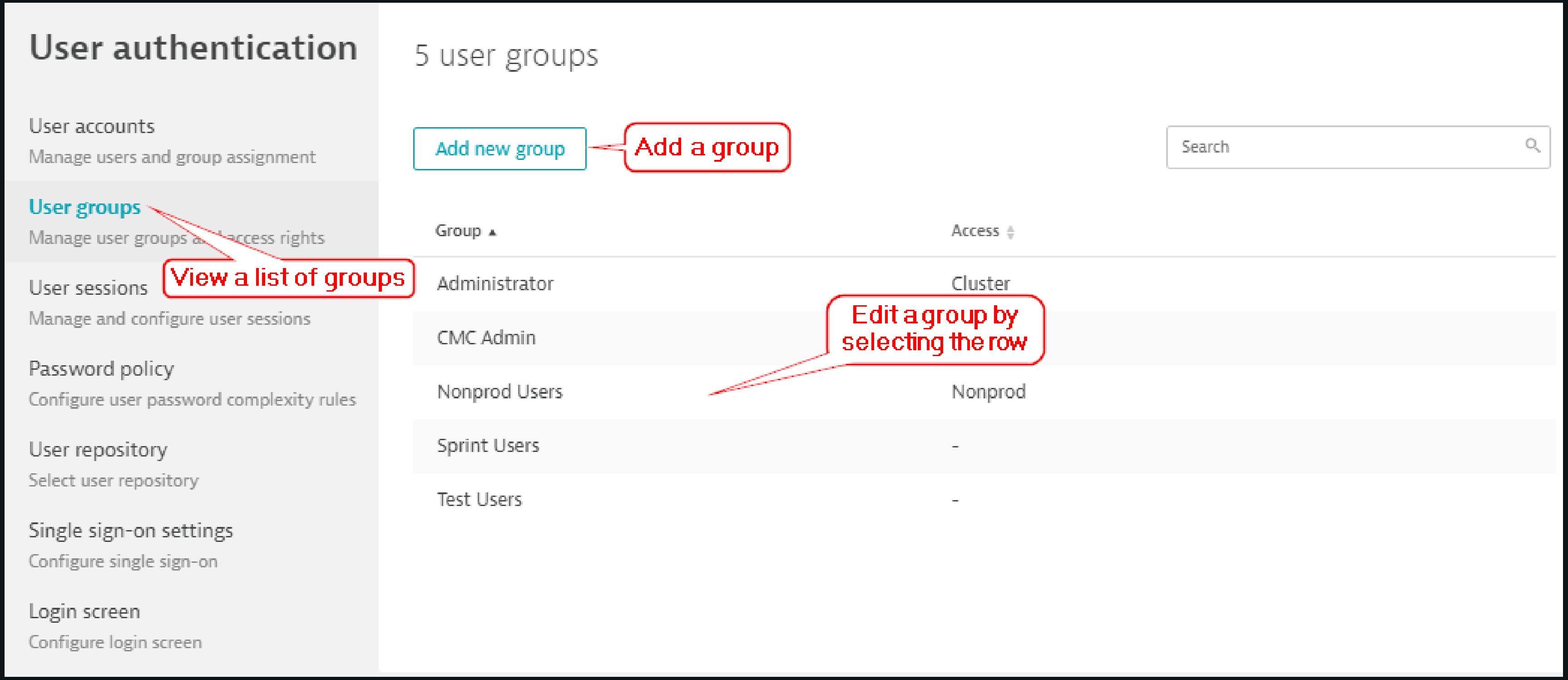
Environment permissions

Environment permissions are determined by groups assigned to this user.

Environment::Management zone ▲	Permissions
Nonprod	Access environment, View logs, Replay session data, Change monitoring settings, View sensitive request data
Nonprod::Critical Apps	-
Nonprod::EasyTravel	-
[redacted]	-
Prod	-

Managed

- Use groups to manage permissions for each Environment



User authentication

User accounts
Manage users and group assignment

User groups
Manage user groups and access rights

User sessions
Manage and configure user sessions

Password policy
Configure user password complexity rules

User repository
Select user repository

Single sign-on settings
Configure single sign-on

Login screen
Configure login screen

5 user groups

Group ▲	Access
Administrator	Cluster
CMC Admin	
Nonprod Users	Nonprod
Sprint Users	-
Test Users	-

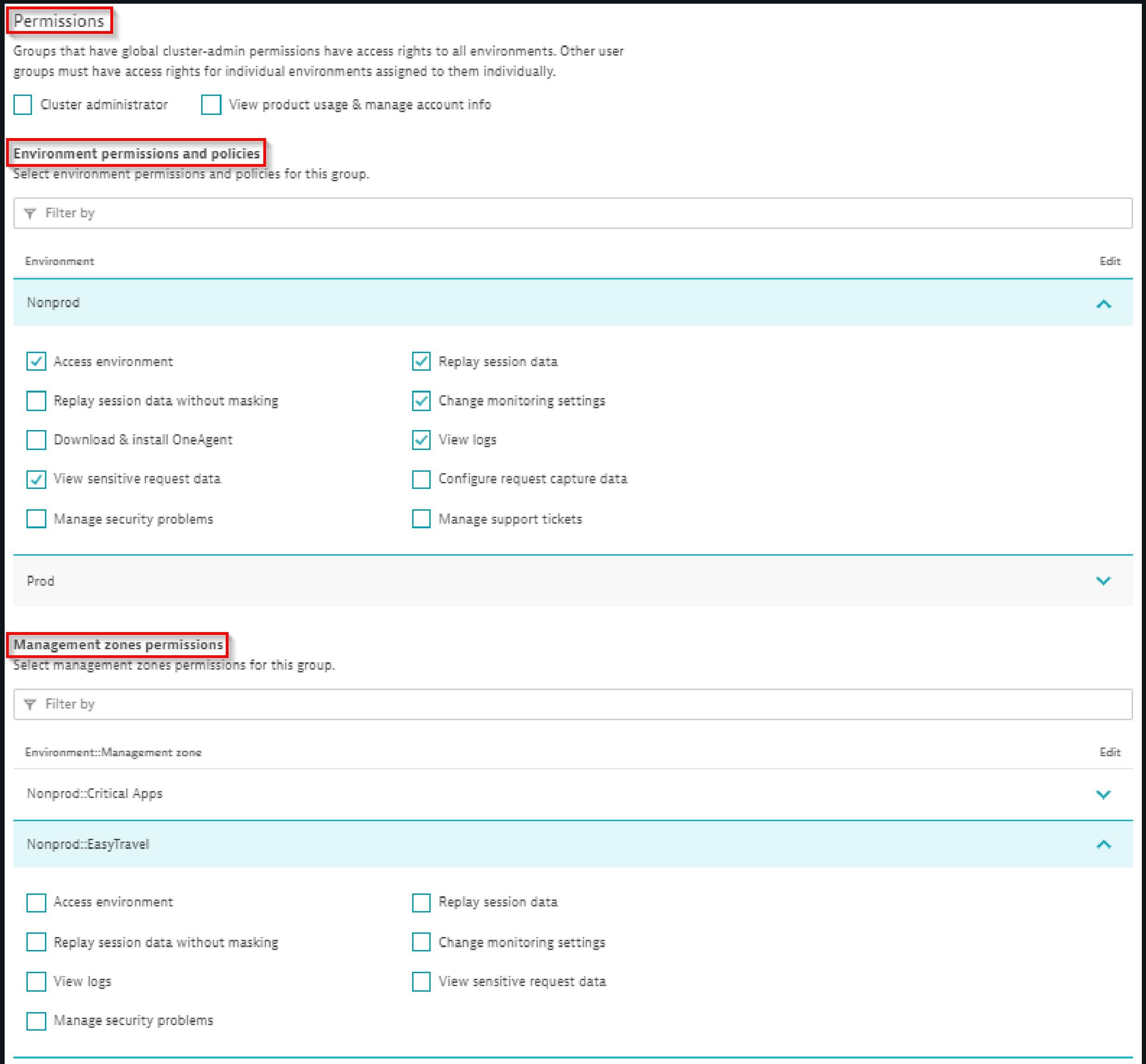
Add a group

View a list of groups

Edit a group by selecting the row

Managed

- Create or edit a group to set Cluster, Environment or Management Zone permissions



Permissions

Groups that have global cluster-admin permissions have access rights to all environments. Other user groups must have access rights for individual environments assigned to them individually.

□ Cluster administrator □ View product usage & manage account info

Environment permissions and policies

Select environment permissions and policies for this group.

Filter by

Environment Edit

Nonprod

☑ Access environment ☑ Replay session data

□ Replay session data without masking ☑ Change monitoring settings

□ Download & install OneAgent ☑ View logs

☑ View sensitive request data □ Configure request capture data

□ Manage security problems □ Manage support tickets

Prod

Management zones permissions

Select management zones permissions for this group.

Filter by

Environment::Management zone Edit

Nonprod::Critical Apps

Nonprod::EasyTravel

□ Access environment □ Replay session data

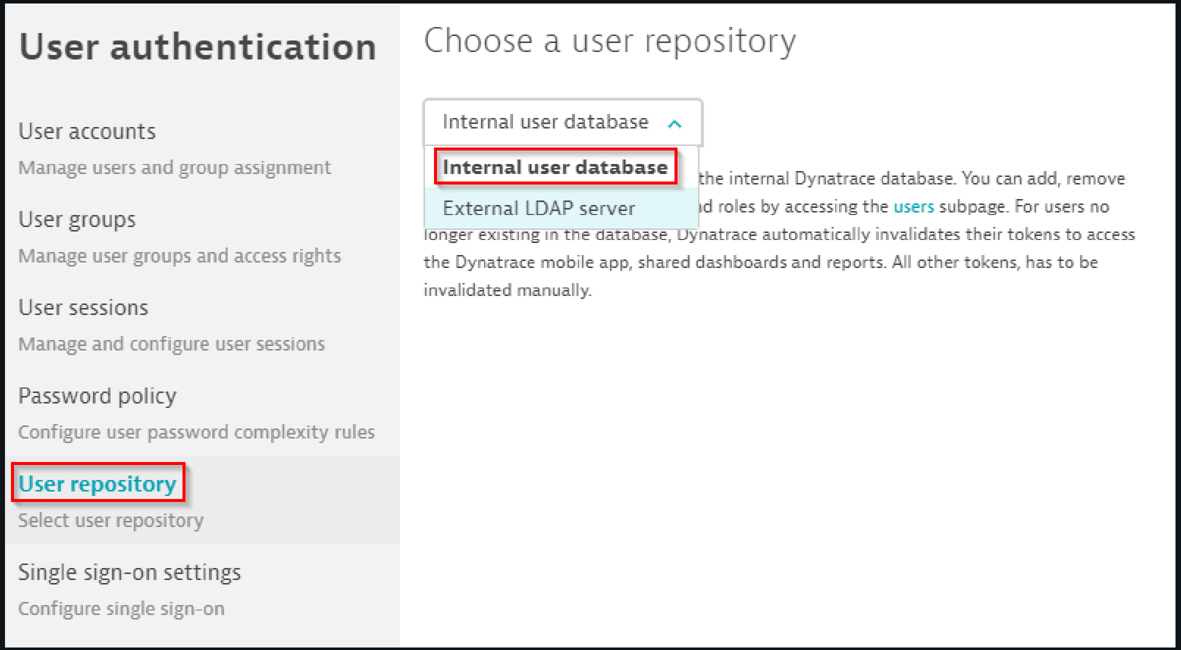
□ Replay session data without masking □ Change monitoring settings

□ View logs □ View sensitive request data

□ Manage security problems

Managed

- User Repository – Internal User Database
  - All the user data is being stored in the internal Dynatrace database
  - The default administrator account created during Dynatrace Managed installation exists regardless of the authentication type you select (internal or LDAP).
  - The default administrator account has cluster permissions.



User authentication

User accounts
Manage users and group assignment

User groups
Manage user groups and access rights

User sessions
Manage and configure user sessions

Password policy
Configure user password complexity rules

User repository
Select user repository

Single sign-on settings
Configure single sign-on

Choose a user repository

Internal user database

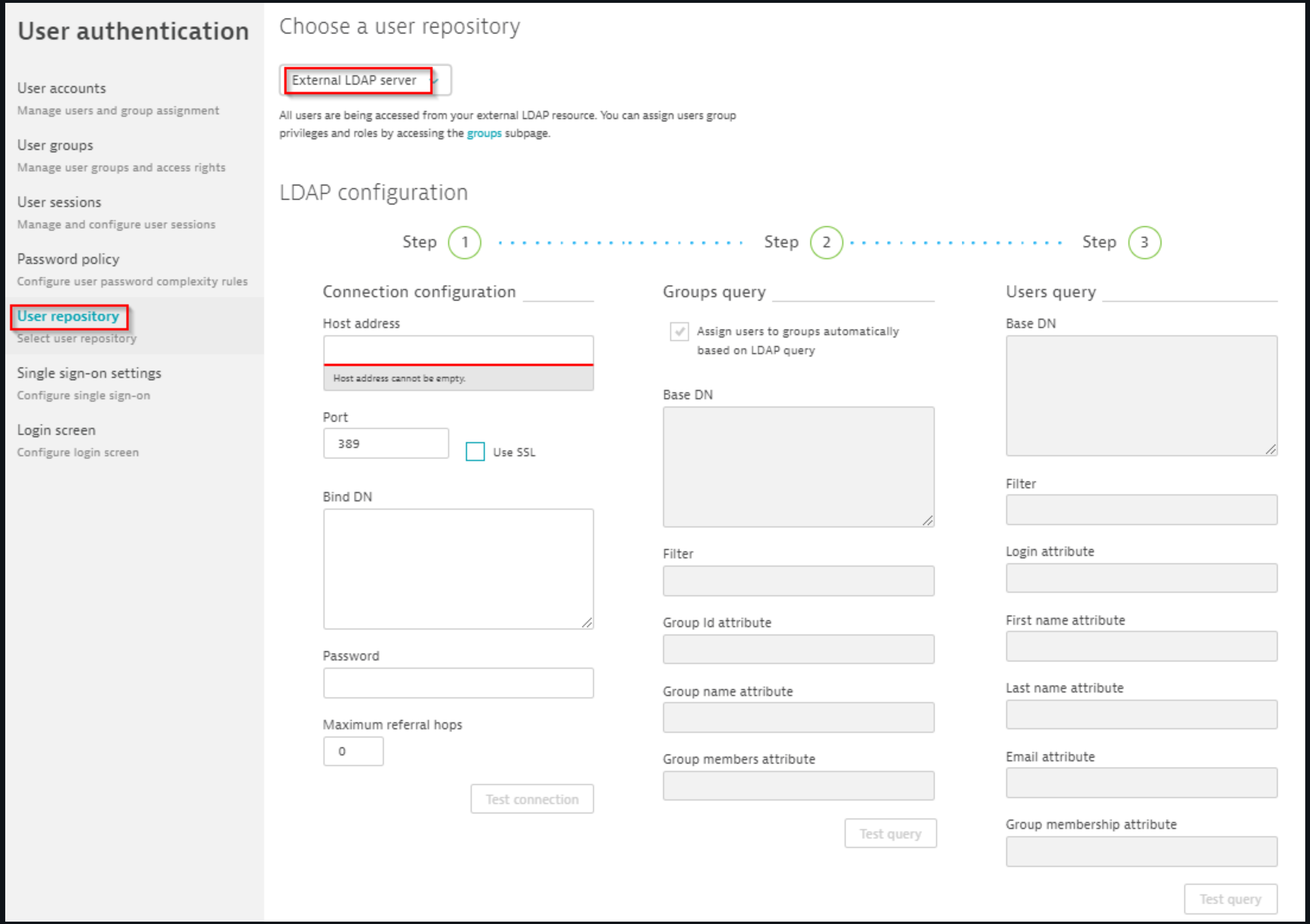
Internal user database
External LDAP server

the internal Dynatrace database. You can add, remove
d roles by accessing the users subpage. For users no
longer existing in the database, Dynatrace automatically invalidates their tokens to access the Dynatrace mobile app, shared dashboards and reports. All other tokens, has to be invalidated manually.

Managed

- User Repository – External LDAP Server
  - Connect to LDAP for authentication, user and group management.
  - You can then assign users to groups in Dynatrace, or groups can be assigned to users based on LDAP information
  - After you switch to LDAP authentication Local accounts (other than the administrator account) will stop working

  https://www.dynatrace.com/support/help/shortlink/managed-ldap



Choose a user repository: External LDAP server

All users are being accessed from your external LDAP resource. You can assign users group privileges and roles by accessing the groups subpage.

Host address cannot be empty.

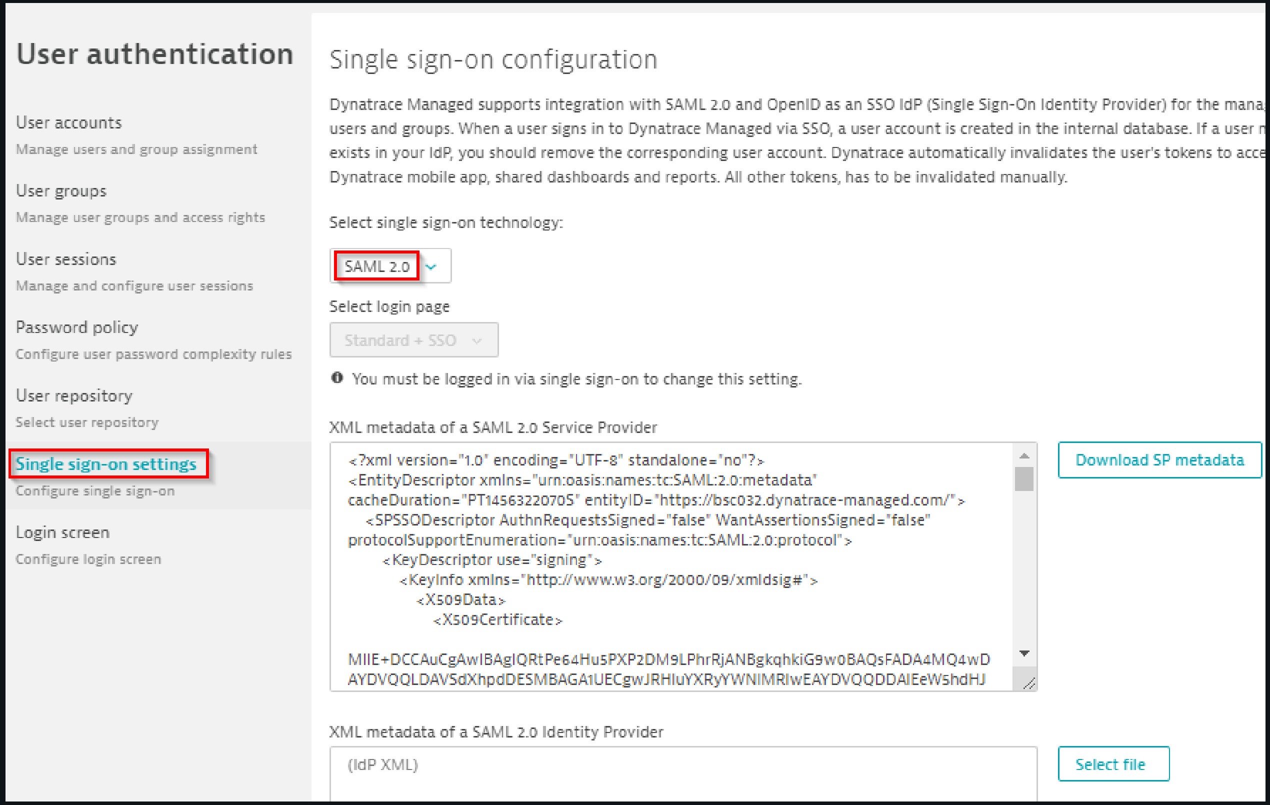
Port: 389

Maximum referral hops: 0

Managed – SSO SAML

- SAML Authentication
  - SAML 2.0 is used
  - Can also be used to manage users, groups and permissions
  - When a user signs in to Dynatrace Managed via SSO, a user account is created in the internal database

  https://www.dynatrace.com/support/help/shortlink/managed-saml



Single sign-on configuration

Dynatrace Managed supports integration with SAML 2.0 and OpenID as an SSO IdP (Single Sign-On Identity Provider) for the mana
users and groups. When a user signs in to Dynatrace Managed via SSO, a user account is created in the internal database. If a user n
exists in your IdP, you should remove the corresponding user account. Dynatrace automatically invalidates the user's tokens to acce
Dynatrace mobile app, shared dashboards and reports. All other tokens, has to be invalidated manually.

Select single sign-on technology:

SAML 2.0

Select login page

Standard + SSO

You must be logged in via single sign-on to change this setting.

XML metadata of a SAML 2.0 Service Provider

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
cacheDuration="PT1456322070S" entityID="https://bsc032.dynatrace-managed.com/">
  <SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <X509Data>
          <X509Certificate>

MIIE+DCCAuCgAwIBAgIQRtPe64Hu5PXP2DM9LPhrRjANBgkqhkiG9w0BAQsFADA4MQ4wD
AYDVQQLDAV5dXhpdDESMBAGA1UECgwJRHluYXRyYWNlMRIwEAYDVQQDDAlEeW5hdHJ
```

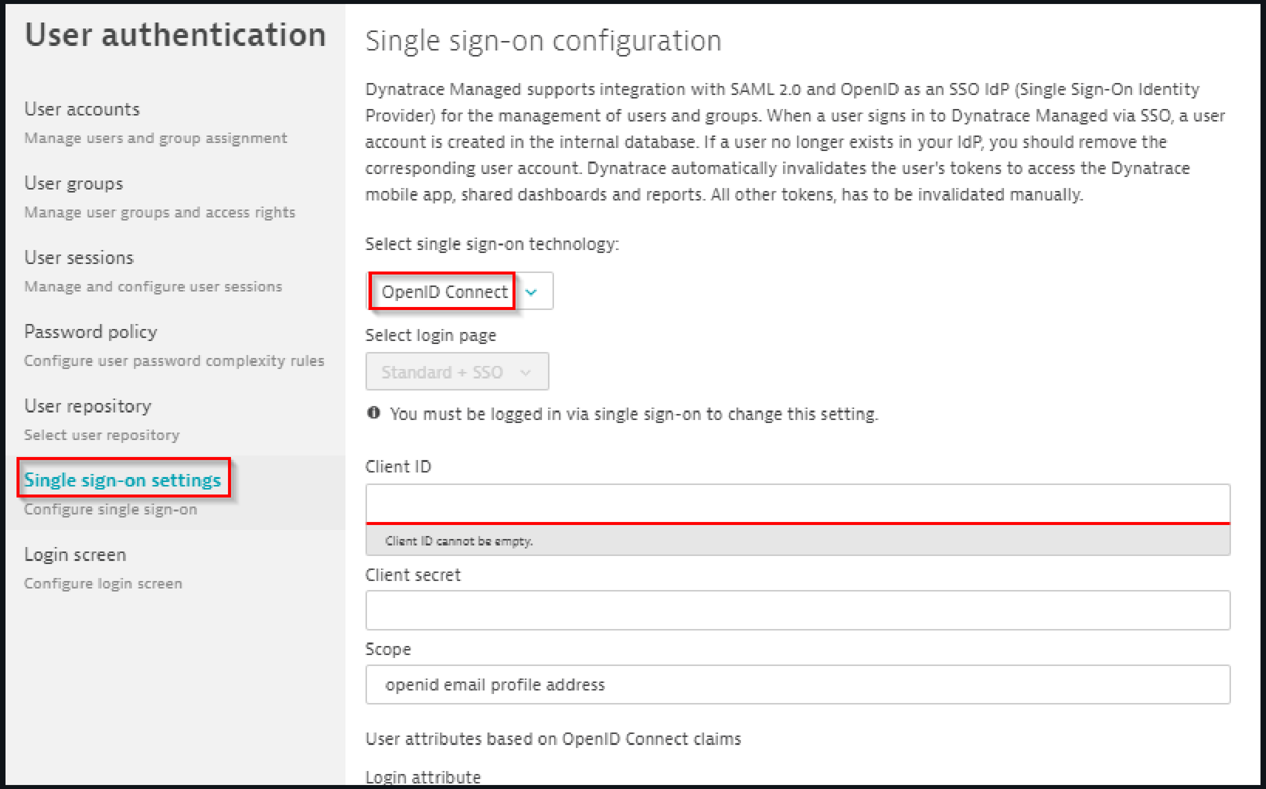
XML metadata of a SAML 2.0 Identity Provider

(IdP XML)

Managed – SSO OpenID

- OpenID Authentication
  - OpenID Core 1.0 specification is used
  - Can also be used to manage users, groups and permissions
  - When a user signs in to Dynatrace Managed via SSO, a user account is created in the internal database

  https://www.dynatrace.com/support/help/shortlink/managed-openid



User authentication

User accounts
Manage users and group assignment

User groups
Manage user groups and access rights

User sessions
Manage and configure user sessions

Password policy
Configure user password complexity rules

User repository
Select user repository

Single sign-on settings
Configure single sign-on

Login screen
Configure login screen

Single sign-on configuration

Dynatrace Managed supports integration with SAML 2.0 and OpenID as an SSO IdP (Single Sign-On Identity Provider) for the management of users and groups. When a user signs in to Dynatrace Managed via SSO, a user account is created in the internal database. If a user no longer exists in your IdP, you should remove the corresponding user account. Dynatrace automatically invalidates the user's tokens to access the Dynatrace mobile app, shared dashboards and reports. All other tokens, has to be invalidated manually.

Select single sign-on technology: OpenID Connect

Select login page: Standard + SSO

You must be logged in via single sign-on to change this setting.

Client ID:

Client ID cannot be empty.

Client secret:

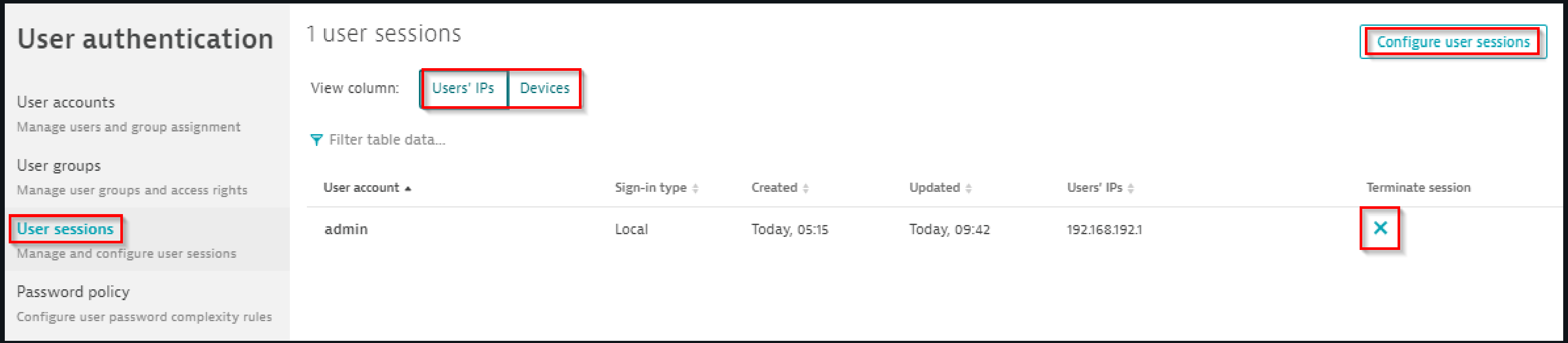
Scope: openid email profile address

User attributes based on OpenID Connect claims

Login attribute

Managed

- View, terminate and set limits to concurrent user sessions



User authentication

User accounts
Manage users and group assignment

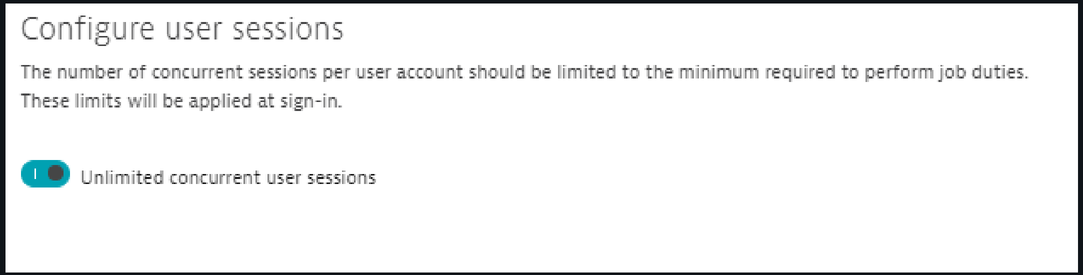
User groups
Manage user groups and access rights

User sessions
Manage and configure user sessions

Password policy
Configure user password complexity rules

1 user sessions

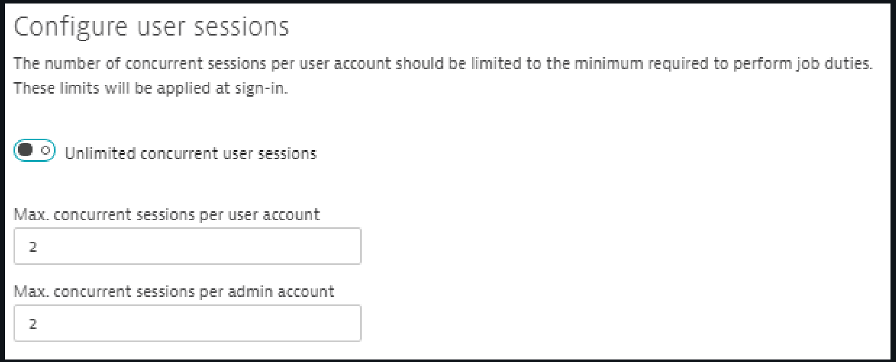
User account ▲	Sign-in type	Created	Updated	Users' IPs	Terminate session
admin	Local	Today, 05:15	Today, 09:42	192.168.192.1	✕



Configure user sessions

The number of concurrent sessions per user account should be limited to the minimum required to perform job duties. These limits will be applied at sign-in.

● Unlimited concurrent user sessions



Configure user sessions

The number of concurrent sessions per user account should be limited to the minimum required to perform job duties. These limits will be applied at sign-in.

○ Unlimited concurrent user sessions

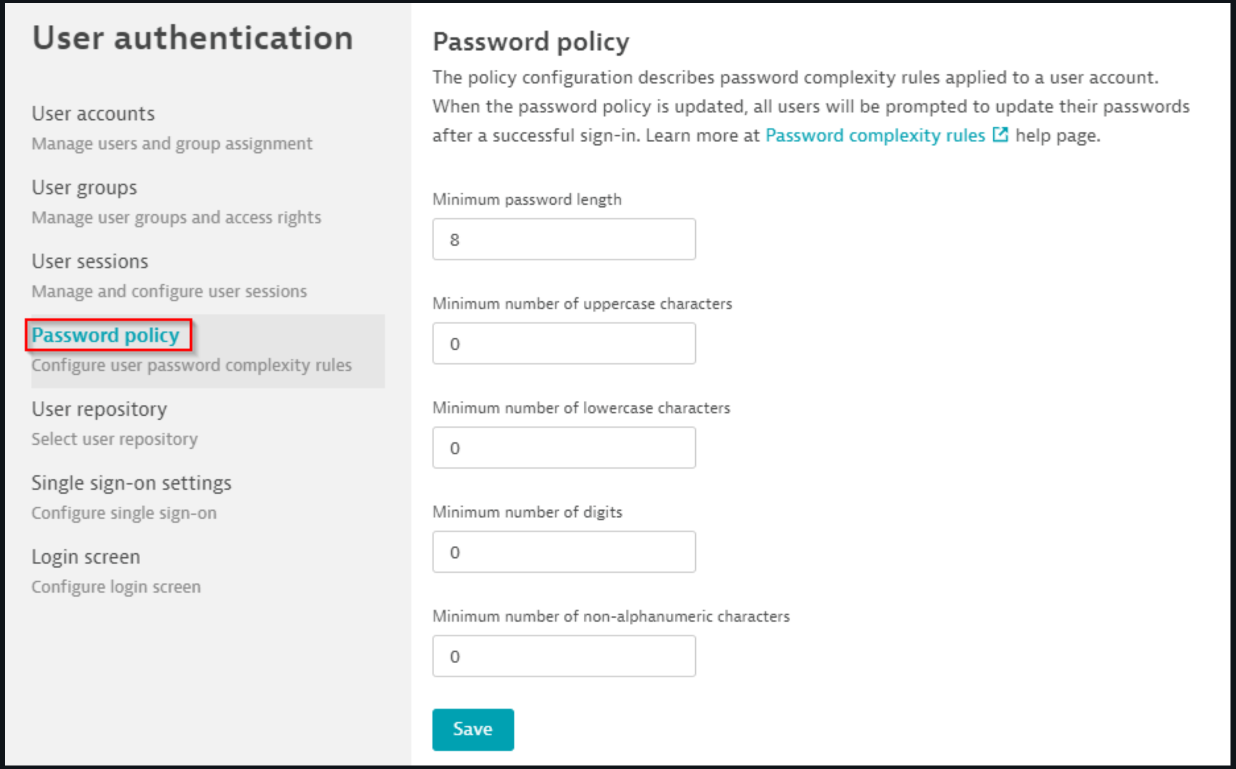
Max. concurrent sessions per user account
2

Max. concurrent sessions per admin account
2

Managed

- Manage the password policy for the embedded administrator account and internal user accounts

https://www.dynatrace.com/support/help/shortlink/managed-password-complexity-rules



Password policy

The policy configuration describes password complexity rules applied to a user account. When the password policy is updated, all users will be prompted to update their passwords after a successful sign-in. Learn more at Password complexity rules help page.

Minimum password length: 8

Minimum number of uppercase characters: 0

Minimum number of lowercase characters: 0

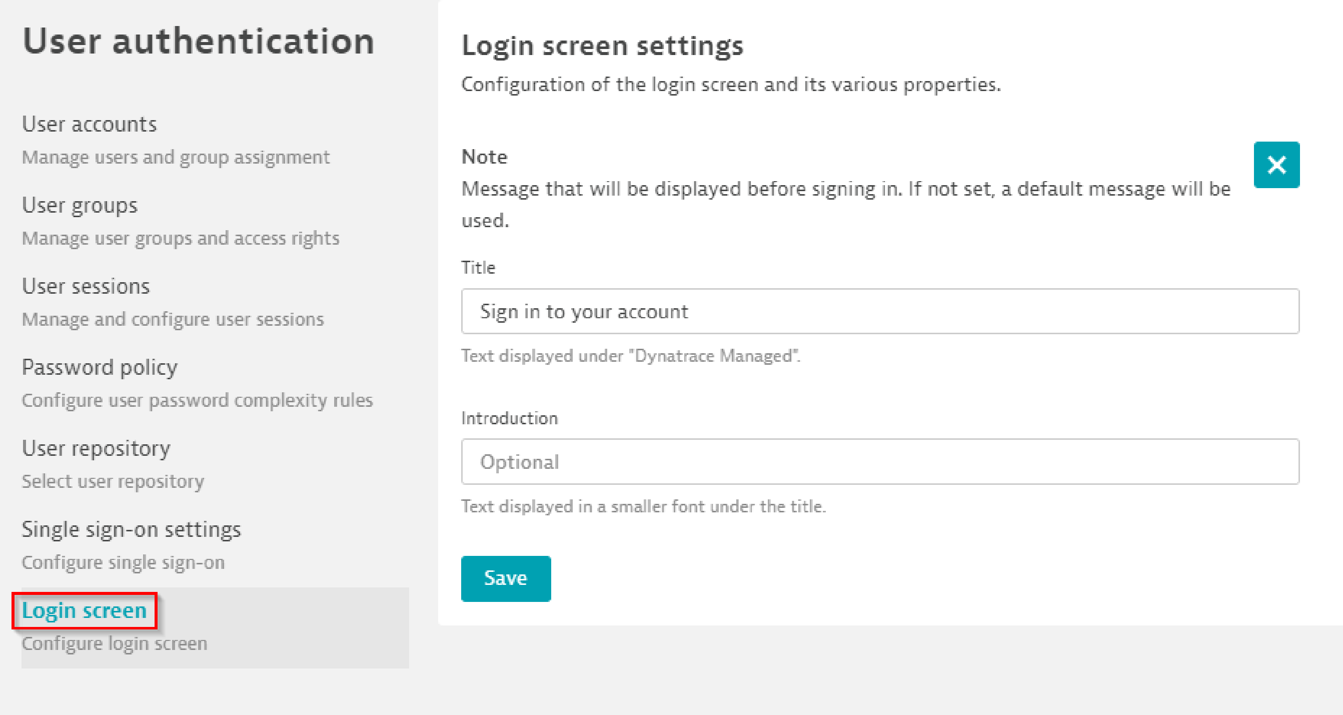
Minimum number of digits: 0

Minimum number of non-alphanumeric characters: 0

Managed

- Customize the login screen to pass information to cluster users before signing in
- Display system information, authentication details, legal notes, or an administrator contact

https://www.dynatrace.com/support/help/shortlink/managed-sign-in-customization



Login screen settings

Configuration of the login screen and its various properties.

Note

Message that will be displayed before signing in. If not set, a default message will be used.

Title

Sign in to your account

Text displayed under "Dynatrace Managed".

Introduction

Optional

Text displayed in a smaller font under the title.

Questions?

dynatrace

Simply smarter clouds